

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 1393/2007, por el que se establece la ordenación de las Enseñanzas Universitarias Oficiales

UNIVERSIDAD SOLICITANTE	CENTRO	CÓDIGO CENTRO	
Universidad Internacional de La Rioja	Escuela Superior de Ingeniería y Tecnología	26004007	
NIVEL	DENOMINACIÓN CORTA		
Máster	Ciberseguridad		
DENOMINACIÓN ESPECÍFICA			
Máster Universitario en Ciberseguridad por la Universidad Internacional de La Rioja			
NIVEL MECES			
3 3			
RAMA DE CONOCIMIENTO	CONJUNTO		
Ingeniería y Arquitectura	No		
HABILITA PARA EL EJERCICIO DE PROFESIONES REGULADAS	NORMA HABILITACIÓN		
No			
SOLICITANTE			
NOMBRE Y APELLIDOS	CARGO		
Virginia Montiel Martín	Responsable de programas ANECA		
Tipo Documento	Número Documento		
NIF	16609588T		
REPRESENTANTE LEGAL			
NOMBRE Y APELLIDOS	CARGO		
Juan Pablo Guzmán Palomino	Secretario General de la Universidad		
Tipo Documento	Número Documento		
NIF	24236227T		
RESPONSABLE DEL TÍTULO			
NOMBRE Y APELLIDOS	CARGO		
Manuel Sánchez Rubio	Director del Máster		
Tipo Documento	Número Documento		
NIF	08978689H		
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 5/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, 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 5-1999, 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 59 de la 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en su versión dada por la Ley 4/1999 de 13 de enero.

	En: La Rioja, AM 18 de octubre de 2021
	Firma: Representante legal de la Universidad



1. DESCRIPCIÓN DEL TÍTULO

1.1. DATOS BÁSICOS

NIVEL	DENOMINACIÓN ESPECÍFICA	CONJUNTO	CONVENIO	CONV. ADJUNTO
Máster	Máster Universitario en Ciberseguridad por la Universidad Internacional de La Rioja	No		Ver Apartado 1: Anexo 1.
LISTADO DE ESPECIALIDADES				
No existen datos				
RAMA		ISCED 1	ISCED 2	
Ingeniería y Arquitectura		Ciencias de la computación		
NO HABILITA O ESTÁ VINCULADO CON PROFESIÓN REGULADA ALGUNA				
AGENCIA EVALUADORA				
Agencia Nacional de Evaluación de la Calidad y Acreditación				
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				
LISTADO DE INSTITUCIONES PARTICIPANTES				
No existen datos				

1.2. DISTRIBUCIÓN DE CRÉDITOS EN EL TÍTULO

CRÉDITOS TOTALES	CRÉDITOS DE COMPLEMENTOS FORMATIVOS	CRÉDITOS EN PRÁCTICAS EXTERNAS
60		6
CRÉDITOS OPTATIVOS	CRÉDITOS OBLIGATORIOS	CRÉDITOS TRABAJO FIN GRADO/ MÁSTER
0	42	12
LISTADO DE ESPECIALIDADES		
ESPECIALIDAD	CRÉDITOS OPTATIVOS	
No existen datos		

1.3. Universidad Internacional de La Rioja

1.3.1. CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS	
CÓDIGO	CENTRO
26004007	Escuela Superior de Ingeniería y Tecnología

1.3.2. Escuela Superior de Ingeniería y Tecnología

1.3.2.1. Datos asociados al centro

TIPOS DE ENSEÑANZA QUE SE IMPARTEN EN EL CENTRO		
PRESENCIAL	SEMPRESENCIAL	VIRTUAL
No	No	Sí
PLAZAS DE NUEVO INGRESO OFERTADAS		
PRIMER AÑO IMPLANTACIÓN	SEGUNDO AÑO IMPLANTACIÓN	
450	450	
	TIEMPO COMPLETO	



	ECTS MATRÍCULA MÍNIMA	ECTS MATRÍCULA MÁXIMA
PRIMER AÑO	60.0	60.0
RESTO DE AÑOS	49.0	60.0
TIEMPO PARCIAL		
	ECTS MATRÍCULA MÍNIMA	ECTS MATRÍCULA MÁXIMA
PRIMER AÑO	22.0	48.0
RESTO DE AÑOS	22.0	48.0
NORMAS DE PERMANENCIA		
http://static.unir.net/documentos/normativa_permanencia_estudiante.pdf		
LENGUAS EN LAS 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	



2. JUSTIFICACIÓN, ADECUACIÓN DE LA PROPUESTA Y PROCEDIMIENTOS

Ver Apartado 2: Anexo 1.

3. COMPETENCIAS

3.1 COMPETENCIAS BÁSICAS Y GENERALES
BÁSICAS
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
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
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
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
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.
GENERALES
CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarrollarlos mediante los métodos y procesos adecuados.
CG1 - Aplicar los conocimientos adquiridos y ser capaces de resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con el área de la seguridad informática.
CG2 - Integrar conocimientos para formular juicios a partir de determinada información. A la vez, incluir reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios en materia de asesoramiento en seguridad informática.
CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación continua en su futuro desempeño profesional como experto en seguridad informática.
CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de la entidades de TI.
CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática.
CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes.
CG8 - Tener la capacidad analítica y de resolución para atender a los problemas reales de acuerdo con los valores éticos y sociales y con el máximo respeto a la legalidad vigente.
CG9 - Manejar adecuadamente información relativa al sector de la seguridad informática. Atendiendo a la legislación vigente, notas técnicas, revistas especializadas, Internet, documentos internos de la empresa, etc.
3.2 COMPETENCIAS TRANSVERSALES
CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line.
CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc.
CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento.
CT4 - Capacidad para realizar una enseñanza personalizada adaptada al espacio (aula virtual multicultural y multirracial) a los recursos y a las situaciones y necesidades personales de los alumnos.
CT5 - Capacidad de investigar y comunicar los resultados de la investigación.
3.3 COMPETENCIAS ESPECÍFICAS
CE18 - Optimizar las políticas de seguridad de la infraestructura de la red de la entidad.
CE19 - Proteger la integridad de las bases de datos para asegurar la confidencialidad de la información sensible contenida.
CE20 - Asesorar sobre las distintas medidas de seguridad aplicables a los sistemas informáticos para disminuir el impacto de sus posibles fallos.



CE21 - Analizar la infraestructura de red para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas, tanto en entorno local como en la nube.
CE22 - Diseñar las políticas de recuperación de datos más adecuadas par disminuir el impacto ante incidentes.
CE23 - Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones.
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención.
CE25 - Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, infraestructuras críticas y principales conceptos de auditoría de sistemas.
CE26 - Implantar procesos de análisis forense de cualquier sistema informático.
CE27 - Diseñar, implantar e institucionalizar un proceso de análisis y gestión de riesgos de los sistemas de información en cualquier organización.
CE1 - Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles.
CE2 - Adquirir una visión general e integrada del asesoramiento en seguridad que permita la colaboración con otros departamentos de la entidad.
CE3 - Identificar, analizar y definir los riesgos de los servicios de las empresas para poder gestionarlos con criterio y de manera efectiva, en función de sus perfiles de seguridad.
CE4 - Asesorar sobre el cumplimiento de la legislación reguladora de la protección de datos en materia de seguridad, en especial sobre la adopción de las medidas de índole técnica y organizativas necesarias considerando la problemática de los datos almacenados en la nube.
CE5 - Discernir sobre los distintos entornos de seguridad existentes, tanto en local como en la nube, para poder seleccionar el óptimo siguiendo un razonamiento profesional y completo.
CE6 - Analizar el funcionamiento de herramientas de seguridad y su uso conjugado.
CE7 - Identificar y proceder contra aquellas conductas tipificadas como delito informático en el marco jurídico actual.
CE8 - Tomar decisiones proactivas y reactivas frente los posibles fallos de seguridad, investigando las causas que las originan.
CE9 - Comprender el funcionamiento, características y nivel de riesgo de los servicios de las empresas y establecer mecanismos de protección.
CE10 - Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos.
CE11 - Conocer todos los activos del negocio de la empresa y las variables necesarias para poder implementar un SGSI.
CE12 - Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa.
CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada implantación en su infraestructura.
CE14 - Diseñar las correctas políticas para analizar y reproducir los hechos ante un incidente de seguridad informática.
CE15 - Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad.
CE16 - Conocer y comprender la legislación europea en materia de seguridad, para poder emitir juicios sobre su aplicabilidad y relevancia en cada ámbito.
CE17 - Discernir los distintos mecanismos criptográficos para seleccionar el óptimo en cada ámbito de aplicación.

4. ACCESO Y ADMISIÓN DE ESTUDIANTES

4.1 SISTEMAS DE INFORMACIÓN PREVIO

Ver Apartado 4: Anexo 1.

4.2 REQUISITOS DE ACCESO Y CRITERIOS DE ADMISIÓN

4.2.1. Requisitos de acceso con carácter general

Las enseñanzas de los diversos Másteres de la UNIR se ofrecen a cualquier persona que reuniendo las condiciones de acceso que expresa la ley 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.

4.2.2. Requisitos de acceso con carácter específico:



Ingenieros o ingenieros técnicos en Informática, Telecomunicaciones o Telemática fundamentalmente, así como en cualquier otra ingeniería relacionada con las TICs. También profesionales con grado de diplomados, ingenieros técnicos, licenciados o ingenieros con amplia y constatable experiencia laboral en TICs.

4.2.3. Criterios de admisión

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 formada por tres miembros:

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

Para poder acceder al Máster Universitario de Seguridad Informática en Ciberseguridad

, es necesario contar con Titulación Universitaria. Este requisito se corresponde con los criterios de acceso establecidos en el artículo 16 del Real Decreto

1393/2007

de 29 de octubre, sobre Organización de las Enseñanzas Universitarias Oficiales, modificado por el Real Decreto 861/2010, de 2 de julio

:

- Estar en posesión de un título universitario oficial español u otro expedido por una institución de educación superior

perteneciente a otro estado integrante del Espacio Europeo de Educación Superior que faculte en el mismo para el acceso a enseñanzas de máster.

Para los titulados conforme a sistemas educativos ajenos al Espacio Europeo de Educación Superior sin necesidad de homologar sus Títulos, previa comprobación por la Universidad de que aquellos acreditan un nivel de formación equivalente a los correspondientes Títulos universitarios oficiales españoles y que facultan en el país expedidor del Título para el acceso a enseñanzas de postgrado. El acceso por esta vía no implicará en ningún caso, la homologación del Título previo de que esté en posesión el interesado, ni su reconocimiento a otros efectos que el cursar las enseñanzas del Máster.

Satisfechos los requisitos de admisión 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.

4.2.4. Atención a estudiantes con necesidades especiales

Existe en UNIR el Servicio de Atención a las Necesidades Especiales que presta apoyo a los estudiantes en situación de diversidad funcional, temporal o permanente, aportando las soluciones más adecuadas a cada caso. Su objetivo prioritario es conseguir la plena integración en la vida universitaria de todos los estudiantes buscando los medios y recursos necesarios para hacer una universidad para todos.

La detección de dichas necesidades se realiza a través de diversos mecanismos:

- Estudiantes con certificado de discapacidad: siguiendo la idea central de proactividad se llama a todos los estudiantes.
- Desde tutorías: los tutores remiten al Servicio los casos de estudiantes sin certificado de discapacidad.
- Admisiones: los asesores remiten las dudas de los posibles futuros estudiantes con discapacidad, el Servicio se pone en contacto directamente con ellos.
- Otros departamentos: SOA (Servicio de Orientación Académica), Defensor Universitario, Solicitudes, etc.

En el contacto con el estudiante se definen los ámbitos de actuación: diagnóstico de necesidades, identificación de barreras, asesoramiento personalizado, etc.

Entre los servicios que presta se encuentran adaptaciones de materiales, curriculares, en los exámenes, asesoramiento pedagógico, etc., involucrando en cada caso a los departamentos implicados (Departamento de Exámenes, Dirección Académica, Profesorado, etc.).

ANEXO: NORMATIVA APLICABLE

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

Preámbulo

El estudio, en la Universidad Internacional de La Rioja, se rige por los criterios y procedimientos de acceso y admisión que, con carácter general, son definidos para todas las Universidades por la normativa estatal y autonómica de aplicación y, en particular, lo establecido en la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, modificada por la Ley Orgánica 4/2007, de 12 de abril y por la Ley Orgánica 8/2013, de 9 de diciembre, para la Mejora de la Calidad Educativa (LOMCE), el Real Decreto 412/2014, de 6 de junio, por el que se establece la normativa básica de los



procedimientos de admisión a las enseñanzas universitarias oficiales de Grado, el Real Decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales, el Real Decreto 99/2011, de 28 de enero, por el que se regulan las enseñanzas oficiales de doctorado, y demás órdenes ministeriales de desarrollo de la normativa anterior, así como la Orden 3/2015, de 25 de marzo, de la Consejería de Educación, Cultura y Turismo, por la que se regulan las pruebas de acceso a los estudios universitarios de Grado en la Comunidad Autónoma de La Rioja de las personas mayores de veinticinco y cuarenta y cinco años.

El presente reglamento general concreta y desarrolla aquellos elementos que la normativa estatal y autonómica define dentro del marco de autonomía universitaria, todo ello con absoluto respeto a los principios de normalización, accesibilidad universal y diseño para todos establecidos en la Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.

Por todo ello, el Consejo Directivo de la Universidad Internacional de La Rioja, aprobó el presente reglamento en sesión celebrada, en su Comisión Permanente, el 14 de julio de 2016 de Acceso a estudios oficiales de la Universidad Internacional de La Rioja:

Capítulo I. Disposiciones Generales

Artículo 1. Ámbito de Aplicación.

La presente normativa es de aplicación en los procedimientos de acceso y admisión de cualesquiera de los estudios oficiales de grado, master y doctor impartidos por la Universidad internacional de La Rioja.

Artículo 2. Definiciones.

1. Requisitos de acceso: Conjunto de requisitos necesarios para cursar unas determinadas enseñanzas universitarias oficiales de Grado, Máster o Doctorado en la Universidad Internacional de La Rioja. Los requisitos de acceso serán los determinados con carácter general en la normativa estatal y autonómica de aplicación y los que adicionalmente puedan haberse determinado en las respectivas memorias de verificación de cada estudio.

2. Admisión: Supone la adjudicación de las plazas ofrecidas por la Universidad Internacional de La Rioja para iniciar alguno de sus estudios oficiales. La admisión requiere la previa comprobación del cumplimiento de los requisitos de acceso.

3. Criterios de Admisión: Conjunto de criterios de valoración de méritos de los distintos candidatos a fin de establecer la prelación entre ellos. Son criterios de admisión aquellos que hayan sido fijados en esta normativa o en la correspondiente memoria de verificación del estudio. En ningún caso tales criterios podrán ser discriminatorios y habrán de tener un carácter objetivo y comprobable.

4. Admisión Directa: En aquellas titulaciones en las que la demanda de plazas no supera a la oferta, el Departamento de Admisiones podrá proceder a la admisión directa, previa solicitud de la plaza y a la verificación del cumplimiento de los requisitos de acceso.

5. Procedimiento de Admisión: Es el proceso por el que, una vez verificado que los candidatos ostentan todos los requisitos de acceso, se procede a la asignación de las correspondientes plazas, de acuerdo con los criterios de admisión aprobados. El procedimiento de admisión, que podrá consistir en pruebas o evaluaciones, valoración de la documentación que acredite la formación previa, entrevistas, u otros mecanismos, se llevará a cabo conforme al procedimiento previsto en esta normativa, así como en la correspondiente memoria de verificación del estudio.

Los sistemas y procedimientos de admisión prestarán especial atención a los estudiantes con necesidades educativas especiales derivadas de la discapacidad. A tal fin, el Servicio de Atención a las Necesidades Especiales (SANNEE) evaluará la necesidad de posibles adaptaciones curriculares, itinerarios o estudios alternativos a estos estudiantes.

Capítulo II. Estudios de Grado

Artículo 3. Acceso a los estudios de grado.

El acceso a los estudios de grado requerirá el cumplimiento por los candidatos de los requisitos de acceso previstos en el artículo 3 del Real Decreto 412/2014, de 6 de junio, que se acreditará en el momento de la matriculación con la documentación indicada en el anexo IV.

Asimismo, el acceso a cada estudio concreto requerirá el cumplimiento de los requisitos adicionales que pudieran haberse determinado en la correspondiente memoria de verificación del estudio.

Se definen las siguientes vías de acceso a los estudios de grado:

1. Superación de la Evaluación de Bachillerato para el Acceso a la Universidad (EBAU) y pruebas de acceso a la universidad anteriores.
2. Título de Bachiller, sin necesidad de superar la evaluación de bachillerato para el acceso a la universidad, para quienes durante el curso 2016-2017 hubiesen cursado materias de Bachillerato del currículo anterior al definido por la Ley Orgánica 8/2013, de 9 de diciembre, y quienes habiendo obtenido el título de Bachiller en el curso 2015-2016 no hubieran accedido a la universidad al finalizar dicho curso, de conformidad con lo previsto en la Disposición Transitoria Única de la Orden ECD/1941/2016, de 22 de diciembre.
3. Títulos de Técnico Superior de Formación Profesional, de Técnico Superior de Artes Plásticas y Diseño o de Técnico Deportivo Superior del Sistema Educativo Español, equivalentes u homologados.
4. Superación de prueba de Acceso de Mayores de 25 años.
5. Superación de prueba de Acceso de Mayores de 40 años.
6. Superación de prueba de Acceso de Mayores de 45 años.
7. Titulado Universitario.
8. Acceso por reconocimiento de estudios universitarios parciales españoles (mínimo 30 créditos ECTS).
9. Acceso por reconocimiento de estudios parciales en otros sistemas universitarios diversos del español (mínimo 30 créditos ECTS).
10. Otras vías permitidas por las ordenaciones anteriores a la Ley Orgánica 8/2013, de 9 de diciembre, para la mejora de la calidad educativa.



El Acceso a los estudios de Grado por parte de Estudiantes procedentes de sistemas educativos extranjeros se regirá por lo dispuesto en el procedimiento que se adjunta como Anexo III de esta Normativa.

Artículo 4. Acceso con carácter condicional.

Conforme a lo establecido en el artículo 4 del Real Decreto 412/2014, de 6 de junio, la Universidad Internacional de La Rioja facilitará el acceso con carácter condicional a aquellos estudiantes que soliciten el acceso mediante la presentación de un título que requiera la previa homologación, siempre que acrediten haber presentado la correspondiente solicitud de homologación.

El acceso y admisión condicional se regirá por lo dispuesto en el procedimiento que se adjunta como Anexo III de esta Normativa.

Artículo 5. Admisión a los estudios de grado.

5.1. Admisión directa.

Con carácter general, salvo en los supuestos en los que la demanda supere la oferta de plazas disponibles en un año académico, se utilizará la vía de admisión directa, a no ser que la memoria de verificación del estudio disponga lo contrario.

5.2. Admisión a través de un procedimiento específico definido en la memoria del título

Cuando el número de plazas disponibles sea inferior a la demanda, al término del plazo de solicitudes, se llevará a cabo de acuerdo con el procedimiento y criterios de admisión que hayan sido definidos en la memoria de verificación del estudio.

Artículo 6. Acceso y Admisión de personas mayores de 25 años.

Las personas mayores de 25 años que no posean ninguna titulación académica que de acceso a la Universidad por otras vías, podrán acceder mediante la superación de la prueba de acceso de mayores de 25 años.

El procedimiento de acceso y admisión se regirá por lo establecido en el procedimiento específico de acceso y admisión definido en el Capítulo IV del Real Decreto 412/2014, de 6 de junio, y la Orden 3/2015, de 25 de marzo, de la Consejería de Educación, Cultura y Turismo, por la que se regulan las pruebas de acceso a los estudios universitarios de Grado en la Comunidad Autónoma de La Rioja de las personas mayores de veinticinco y cuarenta y cinco años.

Artículo 7. Acceso y Admisión de personas mayores de 40 años.

Podrán acceder a la universidad por esta vía los candidatos con experiencia laboral o profesional en relación con la materia propia de un determinado grado, que no posean ninguna titulación académica habilitante para acceder a la universidad por otras vías y cumplan o hayan cumplido los 40 años de edad en el año natural de comienzo del curso académico.

El procedimiento de acceso y admisión se regirá por lo dispuesto en la Sección Segunda del Capítulo IV del Real Decreto 412/2014, de 6 de junio, así como por el procedimiento que se incluye en el Anexo I de esta normativa.

Artículo 8. Acceso y Admisión de personas mayores de 45 años.

Las personas mayores de 45 años que no posean ninguna titulación académica que de acceso a la Universidad por otras vías, podrán acceder mediante la superación de la prueba de acceso de mayores de 45 años.

El procedimiento de acceso y admisión se regirá por lo establecido en el procedimiento específico de acceso y admisión definido en el Capítulo IV del Real Decreto 412/2014, de 6 de junio y la Orden 3/2015, de 25 de marzo, de la Consejería de Educación, Cultura y Turismo, por la que se regulan las pruebas de acceso a los estudios universitarios de Grado en la Comunidad Autónoma de La Rioja de las personas mayores de veinticinco y cuarenta y cinco años.

Capítulo III. Estudios de Máster

Artículo 9. Acceso a estudios de Máster

El acceso a los estudios de Máster requerirá el cumplimiento por los candidatos de los requisitos de acceso previstos en el artículo 16 del Real Decreto 1393/2007, de 29 de octubre que se acreditará en el momento de la matriculación con la documentación indicada en el anexo IV.

Asimismo, el acceso a cada estudio concreto requerirá el cumplimiento de los requisitos adicionales que pudieran haberse determinado en la correspondiente memoria de verificación del estudio.

Artículo 10. Admisión a estudios de Máster

10.1. Admisión directa.

Con carácter general, salvo en los supuestos en los que la demanda supere la oferta de plazas disponibles, se utilizará la vía de admisión directa, a no ser que la memoria de verificación del estudio disponga lo contrario.

10.2. Admisión siguiendo un procedimiento específico previsto en la memoria del título

Cuando el número de plazas disponibles sea inferior a la demanda, al término del plazo de solicitudes, se llevará a cabo de acuerdo con el procedimiento y criterios de admisión que hayan sido definidos en la memoria de verificación del estudio.

Disposición Final. Entrada en vigor

Las modificaciones aprobadas en noviembre de 2020 entrarán en vigor el 18 de noviembre de 2020.



ANEXO I. PROCEDIMIENTO DE ACCESO A LAS ENSEÑANZAS OFICIALES DE GRADO DE LA UNIR DE MAYORES DE 40 AÑOS MEDIANTE ACREDITACIÓN DE EXPERIENCIA LABORAL Y PROFESIONAL

1. Requisitos.

De acuerdo con lo dispuesto en el artículo 16.1 del RD. 412/2014, podrán acceder por esta vía los candidatos que reúnan los siguientes requisitos:

1. Acreditar una determinada experiencia laboral y profesional en relación con la titulación o titulaciones universitarias oficiales de grado en las que se solicite ser admitido.
2. No estar en posesión de ninguna titulación académica que habilite para acceder a la universidad por otras vías.
3. Cumplir o haber cumplido los 40 años de edad en el año natural de comienzo del curso académico, entendiéndose por año natural el periodo comprendido entre el 1 de enero y el 31 de diciembre del año en cuestión.

2. Convocatoria

La Universidad Internacional de La Rioja realizará una convocatoria anual para el acceso por esta vía, en los plazos que permitan a los candidatos concurrir debidamente a los procedimientos de admisión. La convocatoria establecerá el modelo y los plazos de solicitud de cada llamamiento así como la documentación que se ha de entregar, que incluirá, en todo caso, un currículum vitae, en el que el candidato consignará de manera precisa, entre otros aspectos, su experiencia laboral y profesional y la documentación acreditativa correspondiente, y, de manera obligatoria, el certificado de vida laboral del candidato.

Los solicitantes que puedan acreditar experiencia laboral o profesional relacionada con más de una titulación universitaria oficial de grado podrán presentar más de una solicitud acompañadas de la documentación correspondiente en distintas titulaciones, y realizarán tantas entrevistas como solicitudes hayan presentado.

3. Comisión evaluadora.

El candidato deberá realizar, tal y como indica el artículo 16.3 del RD. 412/2014, de 6 de junio, una entrevista. A tal fin se constituirá una Comisión Evaluadora en cada una de las sedes de la UNIR, compuesta por dos profesores o expertos que serán designados por el Rector, a propuesta del Decano o Director, preferentemente de entre los coordinadores de los distintos grados.

La actuación de la Comisión tendrá como finalidad determinar si el candidato acredita o no experiencia laboral o profesional en relación con la titulación a la que solicita acceder y, en su caso, evaluar dicha documentación.

4. Procedimiento

Para establecer esta valoración, las Comisiones Evaluadoras deberán tener en cuenta los siguientes criterios:

- Experiencia laboral y profesional en relación con la titulación oficial de grado respecto de la que se solicita la admisión.
- Adecuación de los conocimientos y competencias del candidato a los objetivos y las competencias del título, recogidos en la correspondiente memoria de grado.

Con esta finalidad, las Comisiones Evaluadoras dividirán su actuación en dos fases. Con el fin de establecer el orden de las solicitudes, las Comisiones Evaluadoras calificarán cada fase con una puntuación de 0 y 10, expresada con tres cifras decimales.

Fase de Valoración. Consistirá en la valoración de la documentación presentada por el candidato. Para la evaluación del currículum se considerará la afinidad de la experiencia laboral y profesional en el ámbito y actividad asociados a los estudios solicitados, el tiempo dedicado y el nivel de competencias adquirido. Dichos extremos deberán ser acreditados mediante certificados, contratos de trabajo e informes de vida laboral de las empresas u organismos correspondientes, que incluyan la categoría profesional así como el detalle de las actividades realizadas. La valoración se realizará teniendo en cuenta la tabla relacional que se incluye como Anexo II, entre las Familias Profesionales del Real Decreto 1128/2008, de 5 de septiembre, por el que se regula el Catálogo Nacional de Cualificaciones Profesionales y las Ramas de Conocimiento establecidas en el Real Decreto 1393/2007, de 29 de octubre.

No se valorará ningún extremo incluido en el currículum que no quede suficientemente acreditado. Los candidatos que obtengan un mínimo de 5 puntos sobre 10 en la primera fase, accederán a la segunda fase.

Fase de Entrevista Personal. Consistirá en la realización y valoración de una entrevista personal ante la comisión evaluadora, cuya duración no superará los 20 minutos, con el fin de valorar la adecuación de los conocimientos y las competencias del candidato a los objetivos y competencias del título. La calificación de los candidatos en esta segunda fase deberá ser igual o superior a 5 sobre 10, para que pueda hacer media con la primera fase.

Superación de ambas fases. Se considerará que el candidato ha superado el acceso por esta vía cuando supere ambas fases. La calificación final obtenida será la media aritmética de ambas fases. La publicación de la resolución con los resultados se comunicará personalmente a los interesados.

5. Reclamación

Los aspirantes al acceso podrán presentar reclamación ante el Rector sobre la resolución relativa a las calificaciones de la prueba en el plazo de tres días hábiles contados a partir del día siguiente a partir del día siguiente al de la recepción de la notificación de la superación o no de la prueba. El Rector, oída la comisión evaluadora, podrá proveer con una resolución negativa, o que se proceda a valorar nuevamente el currículum, o que se repita la entrevista, o que se realicen ambas cosas. Contra una eventual nueva calificación negativa no se admitirá una ulterior reclamación.

6. Admisión

Los candidatos que hayan obtenido acceso deberán solicitar la matrícula en la UNIR, en la titulación correspondiente, en el mismo curso académico.

ANEXO II.



Adscripción de las familias profesionales del Real Decreto 1128/2003, de 5 de septiembre, por el que se regula el Catálogo Nacional de Cualificaciones Profesionales, a las ramas de conocimiento establecidas en el Real Decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales.

FAMILIA PROFESIONAL	RAMAS DE CONOCIMIENTO
Actividades Físicas y Deportivas	Ciencias de la Salud Ciencias Sociales y Jurídicas
Administración y Gestión	Artes y Humanidades Ciencias Sociales y Jurídicas
Agraria	Ciencias Ciencias de la Salud Ingeniería y Arquitectura
Artes Gráficas	Artes y Humanidades Ciencias Sociales y Jurídicas Ingeniería y Arquitectura
Artes y Artesanías	Artes y Humanidades Ingeniería y Arquitectura
Comercio y Marketing	Artes y Humanidades Ingeniería y Arquitectura
Edificación y Obra Civil	Ciencias / Ingeniería y Arquitectura
Electricidad y Electrónica	Ciencias / Ingeniería y Arquitectura
Energía y Agua	Ciencias / Ingeniería y Arquitectura
Fabricación Mecánica	Ciencias / Ingeniería y Arquitectura



Hostelería y Turismo	Artes y Humanidades Ciencias Sociales y Jurídicas
Imagen Personal	Ciencias de la Salud Ciencias Sociales y Jurídicas
Imagen y Sonido / Comunicación, Imagen y Sonido	Artes y Humanidades Ciencias
	Ciencias Sociales y Jurídicas Ingeniería y Arquitectura
Industrias Alimentarias	Ciencias Ciencias de la Salud Ingeniería y Arquitectura
Industrias Extractivas	Ciencias / Ingeniería y Arquitectura
Informática y Comunicaciones	Ciencias / Ingeniería y Arquitectura
Instalación y Mantenimiento	Ciencias / Ingeniería y Arquitectura
Madera, Mueble y Corcho	Ciencias / Ingeniería y Arquitectura
Marítimo#Pesquera	Ciencias / Ingeniería y Arquitectura
Química	Ciencias Ciencias de la Salud Ingeniería y Arquitectura



Sanidad	Ciencias Ciencias de la Salud
Seguridad y Medio Ambiente	Ciencias de la Salud Ciencias Sociales y Jurídicas
Servicios Socioculturales y a la Comunidad	Artes y Humanidades Ciencias de la Salud Ciencias Sociales y Jurídicas
Textil, Confección y Piel	Ciencias / Ingeniería y Arquitectura
Transporte y Mantenimiento de Vehículos	Ciencias / Ingeniería y Arquitectura
Vidrio y Cerámica	Ciencias / Ingeniería y Arquitectura

ANEXO III. PROCEDIMIENTO PARA EL ACCESO Y ADMISIÓN A LOS ESTUDIOS DE GRADO DE UNIR POR PARTE DE ESTUDIANTES PROCEDENTES DE SISTEMAS EDUCATIVOS EXTRANJEROS

La entrada en vigor de la Ley 8/2013, de 9 de diciembre, para la mejora de la calidad educativa modifica los requisitos de acceso y admisión a las enseñanzas oficiales de grado desde el título de Bachiller o equivalente establecido en el artículo 38 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación.

La introducción en la Ley Orgánica 2/2006, de 3 de mayo, de las nuevas disposiciones adicionales trigésima tercera y trigésima sexta abrieron la posibilidad del acceso y admisión a la Universidad española a los titulados en Bachillerato Europeo, en Bachillerato Internacional, y de alumnos y alumnas en posesión de un título, diploma o estudio obtenido o realizado en el extranjero equivalente al título de Bachiller o Técnico Superior.

Según el calendario de implantación fijado por la disposición final sexta de la Ley Orgánica 8/2013, de 9 de diciembre, para la mejora de la calidad educativa, y en el Real Decreto 412/2014, de 6 de junio, por el que se establece la normativa básica de los procedimientos de admisión a las enseñanzas universitarias oficiales de Grado, estos nuevos procedimientos de acceso y admisión a la Universidad española entrarán en vigor en el curso 2014/15.

Por todo ello, en ejecución de lo dispuesto en la mencionada ley Orgánica 8/2013, de 9 de diciembre, de acuerdo con lo previsto en el Real Decreto 412/2014, de 6 de junio, y teniendo en cuenta las instrucciones y notas informativas emanadas del Ministerio de Educación, Cultura y Deporte, se acuerda la aprobación del siguiente PROCEDIMIENTO PARA EL ACCESO Y ADMISIÓN A LOS ESTUDIOS DE GRADO DE LA UNIR POR PARTE DE ESTUDIANTES PROCEDENTES DE SISTEMAS EDUCATIVOS EXTRANJEROS.

1. Modalidades de Acceso.

Conforme al presente procedimiento, podrán acceder a la UNIR,

1. Estudiantes que hayan obtenido un título, diploma o estudios equivalentes al título de Bachillerato del Sistema Educativo Español,

1.1. Procedentes de sistemas educativo de **Estados miembros** de la Unión Europea o los de otros Estados con los que se hayan suscrito acuerdos internacionales aplicables a este respecto, en régimen de reciprocidad,

1.1.1. Cuando dichos estudiantes **cumplan los requisitos** académicos exigidos en sus sistemas educativos para acceder a sus Universidades.

1.1.2. Cuando dichos estudiantes **no cumplan los requisitos** académicos exigidos en sus sistemas educativos para acceder a sus Universidades.

1.2. Procedentes de sistemas educativos de **Estados que no sean miembros** de la Unión Europea con los que no se hayan suscrito acuerdos internacionales para el reconocimiento del título de Bachiller en régimen de reciprocidad.

2. Estudiantes que hayan obtenido el Título de Bachillerato Europeo (según el Convenio del Estatuto de las Escuelas Europeas, Luxemburgo, 1994).



3. Estudiantes que hayan obtenido el Diploma de Bachillerato Internacional, (expedido por la Organización del Bachillerato Internacional, Ginebra).
4. Estudiantes que hayan obtenido un título, diploma o estudios equivalentes al Título de Técnico Superior de Formación Profesional, de Técnico Superior de Artes Plásticas y Diseño, o de Técnico Deportivo Superior del Sistema Educativo Español.
5. Estudiantes en posesión de títulos, diplomas o estudios diferentes de los equivalentes a los títulos de Bachiller, Técnico Superior de Formación Profesional, Técnico Superior de Artes Plásticas y Diseño, o de Técnico Deportivo Superior del Sistema Educativo Español, obtenidos o realizados en un Estado miembro de la Unión Europea (o en otros Estados con los que se hayan suscrito acuerdos internacionales aplicables a este respecto, en régimen de reciprocidad), cuando los estudiantes cumplan los requisitos académicos exigidos en dicho Estado para acceder a sus Universidades.
6. Estudiantes que hayan cursado estudios universitarios parciales extranjeros o españoles, o que habiendo finalizado los estudios universitarios extranjeros no hayan obtenido su homologación en España.
7. Estudiantes en posesión de un título universitario oficial.

2. Requisitos de acceso.

Modalidad 1.1.1, 2 y 3. Estudiantes titulados en Bachillerato Europeo y en Bachillerato Internacional, así como los procedentes de sistemas educativos de Estados miembros de la Unión Europea o los de otros Estados con los que España haya suscrito Acuerdos internacionales aplicables a este respecto, en régimen de reciprocidad, que cumplan los requisitos académicos exigidos en sus sistemas educativos para acceder a sus universidades.

Para poder acceder a la UNIR, estos estudiantes deberán obtener previamente la CREDENCIAL DE ACCESO que, según los criterios de la Orden EDU/1161/2010, de 4 de mayo, será expedida por la Universidad Nacional de Educación a Distancia -UNED-.

Modalidad 1.1.2, 4, 5 y 7. Estudiantes en posesión de los títulos oficiales de Técnico Superior de Formación Profesional, de Técnico Superior de Artes Plásticas y Diseño, o de Técnico Deportivo Superior del Sistema Educativo Español, o en posesión de títulos, diplomas o estudios homologados o declarados equivalentes; Estudiantes en posesión de títulos, diplomas o estudios equivalentes al título de Bachiller del Sistema Educativo Español, procedentes de sistemas educativos de Estados miembros de la Unión Europea o los de otros Estados con los que se hayan suscrito acuerdos internacionales aplicables a este respecto, en régimen de reciprocidad, cuando dichos estudiantes no cumplan los requisitos académicos exigidos en sus sistemas educativos para acceder a sus Universidades; Estudiantes en posesión de títulos, diplomas o estudios, obtenidos o realizados en sistemas educativos de Estados que no sean miembros de la Unión Europea con los que no se hayan suscrito acuerdos internacionales para el reconocimiento del título de Bachiller en régimen de reciprocidad, homologados o declarados equivalentes al título de Bachiller del Sistema Educativo Español; así como estudiantes en posesión de un título universitario oficial.

Para poder acceder a la UNIR, estos estudiantes deberán obtener previamente la HOMOLOGACIÓN de sus estudios al correspondiente título español.

No obstante, la UNIR, podrá admitir a estos estudiantes, con carácter condicional, en tanto se resuelve el procedimiento de homologación, siempre que acrediten haber presentado la correspondiente solicitud de la homologación ante el Ministerio de Educación, Cultura y Deporte, y se acepten plenamente las condiciones y el procedimiento que se establece en el apartado 4 siguiente.

Modalidad 6. Estudiantes que hayan cursado estudios universitarios parciales extranjeros o españoles, o que habiendo finalizado los estudios universitarios extranjeros no hayan obtenido su homologación en España.

Para poder acceder a la UNIR, será requisito indispensable que hayan obtenido previamente el RECONOCIMIENTO de, al menos, 30 créditos.

3. Criterios de Admisión.

En aquellos supuestos en los que el número de solicitudes sea superior al de plazas ofertadas por la UNIR para una determinada titulación, el criterio de admisión será el siguiente:

Modalidades 1.1.1, 2 y 3. La calificación global del Bachillerato que conste en la credencial expedida por la UNED.

Modalidades 1.1.2, 4, 5 y 7. En caso de que no esté prevista la expedición de la credencial mencionada en el apartado anterior, se tendrá en cuenta la calificación global obtenida por el estudiante en sus estudios, previa transposición al sistema de calificaciones español en base 10, con aprobado en 5.0 puntos.

4. Admisión condicionada.

El acceso a la UNIR por estudiante que se encuentren en alguna de las modalidades a.1.1.2, 4, 5 y 7, previstas en el apartado 1, requerirá la previa homologación del título correspondiente.

No obstante, la UNIR, de conformidad con lo previsto en el artículo 4 del Real Decreto 412/2014, de 6 de junio, podrá admitir a estos estudiantes, con carácter condicional, en tanto se resuelve el procedimiento de homologación, para lo cual deberán seguirse las siguientes prescripciones:

- Los estudiantes deberán acreditar haber iniciado el procedimiento de Homologación ante el Ministerio de Educación, Cultura y Deporte, mediante la presentación del "Volante para la inscripción condicional en centros docentes o en exámenes oficiales", sellado por la Unidad de Registro donde se haya presentado la solicitud.
- La solicitud de admisión condicionada en la UNIR se realizará mediante la cumplimentación de un formulario específico en el que se informará al estudiante expresamente de los efectos jurídicos de la admisión condicionada:

"El solicitante declara conocer y acepta expresamente que, en el supuesto de que sobre el expediente de Homologación de su título recayera una resolución desfavorable, quedaría sin efectos la matrícula condicionalmente realizada, y se anularían todos los actos subsiguientes a la misma, y en especial los resultados de los exámenes que, eventualmente, pudieran haberse realizado.

La inscripción condicionada se realizará bajo la personal responsabilidad del solicitante y su no confirmación posterior, consecuencia de una resolución de homologación desfavorable, no dará lugar a la devolución del importe de matrícula ni otros gastos que eventualmente haya debido realizar para llevarla a cabo."

- La formalización de la solicitud de admisión condicionada supondrá la plena aceptación y sin reservas por el solicitante de las condiciones anteriormente mencionadas.



- La matrícula condicionada que describe este apartado tendrá efectos durante un curso académico. Excepcionalmente podrá admitirse matrícula condicionada en un curso posterior, sólo en el supuesto de que se verifique y/o acredite que el expediente de homologación está pendiente de resolución.

ANEXO IV

REQUISITOS DOCUMENTALES DE ACCESO Y ADMISIÓN

A los candidatos al acceso a estudios oficiales en Universidad Internacional de La Rioja ¿ UNIR, durante el proceso de admisión se le informará de la documentación requerida para poder matricularse. Y en el momento de matriculación se les solicitará la siguiente documentación:

a) Para acceso a grado deben presentar alguno de los siguientes documentos:

Certificado de superación de la Evaluación de Bachillerato para el Acceso a la Universidad (EBAU) o pruebas de acceso a la universidad de ordenaciones del Sistema Educativo Español anteriores.

Certificado de haber superado el bachillerato en el curso académico 2015/2016 o siendo repetidor total o parcialmente en el curso 2016/2017.

Credencial de homologación al título de bachillerato español.

Certificado de acceso a estudios universitarios de sistemas educativos de Estados miembros de la Unión Europea o los de otros Estados con los que se hayan suscrito acuerdos internacionales aplicables a este respecto, en régimen de reciprocidad.

Certificado de Título de Técnico Superior en Formación Profesional o equivalente.

Certificado de superación de la Prueba de Acceso a la Universidad para mayores de 25.

Certificado de superación de la Prueba de Acceso a la Universidad por Experiencia Profesional para mayores de 40.

Certificado de superación de la Prueba de Acceso a la Universidad para mayores de 45.

Certificado de estar en posesión de un título universitario oficial de Grado, Máster o título equivalente.

Certificado de notas de estudios universitarios españoles parciales, siempre que de los mismos esta institución le haya reconocido al menos 30 créditos ECTS.

Certificado de notas de estudios universitarios extranjeros, siempre que de los mismos esta institución le haya reconocido al menos 30 créditos ECTS.

Certificado de estar en posesión de un título una cceder a la universidad según ordenaciones del Sistema Educativo Español anteriores a la Ley Orgánica 8/2013, de 9 de diciembre.

Y, además, deberán presentar:

Documento de identidad válido.

Otros certificados que acrediten cumplir el perfil de admisión o de conocimientos de idiomas establecido en la memoria del grado, en caso de que esta lo solicite.

b) Para acceso a master deben presentar alguna de los siguientes documentos:

Certificado de estar en posesión de un título universitario oficial español.

Certificado de estar en posesión de un título expedido por una institución de educación superior perteneciente a otro Estado integrante del Espacio Europeo de Educación Superior que faculte en el mismo para el acceso a enseñanzas de Máster.

Certificado de estar en posesión de un título emitido conforme a sistemas educativos ajenos al Espacio Europeo de Educación Superior sin necesidad de la homologación de sus títulos, previa comprobación por la Universidad de que aquellos acreditan un nivel de formación equivalente a los correspondientes títulos universitarios oficiales españoles y que facultan en el país expedidor del título para el acceso a enseñanzas de postgrado.

Y, además deberá aportar:

Documento de identidad válido.

Otros certificados que acrediten cumplir el perfil de admisión o conocimientos de idiomas establecido en la memoria del máster, en caso de que esta lo solicite.

La universidad podrá exigir documentación adicional cuando sea necesario para verificar que la vía de acceso se ajusta a la legislación vigente en España.

En todo caso, deberá presentarse el documento original o una copia autenticada de los documentos de acceso y admisión. En el caso de documentos expedidos en Estados no miembros de la Unión Europea, los documentos deberán estar legalizados y, si están en un idioma distinto al español, inglés, portugués, francés o italiano, deberá aportarse, asimismo, la traducción jurada oficial de esos documentos.

4.3 APOYO A ESTUDIANTES



El Departamento de Educación en Internet es el encargado de garantizar el seguimiento y orientación de los estudiantes. Sus funciones se materializan en dos tipos de procedimientos referidos a:

1. Seguimiento y comprobación de la calidad de la orientación de los estudiantes a través del **Curso de introducción al campus virtual** que realizan la primera semana en cualquier titulación: incluye orientación relativa a la metodología docente de UNIR, papel de los tutores personales, modos de comunicación con el profesorado y con las autoridades académicas y, especialmente, el uso de las herramientas del aula virtual.
2. Seguimiento y comprobación de la calidad de la orientación de los estudiantes a través del **plan de acción tutorial personalizado**, que pretende garantizar la calidad de la orientación de los estudiantes a lo largo de todo el proceso formativo.

4.3.1. Primer contacto con el campus virtual

Cuando los estudiantes se enfrentan por primera vez a una herramienta como es una plataforma de formación en Internet pueden surgir muchas dudas de funcionamiento.

Este problema se soluciona en UNIR mediante un periodo de adaptación previo al comienzo del curso denominado "Curso de introducción al campus virtual", en el que el alumno dispone de un aula de información general que le permite familiarizarse con el campus virtual.

En esta aula se explica mediante vídeos y textos el concepto de UNIR como universidad en Internet. Incluye la metodología empleada, orientación para el estudio y la planificación del trabajo personal y sistemas de evaluación. El estudiante tiene un primer contacto con el uso de foros y envío de tareas a través del aula virtual.

Durante esta semana, el Departamento de Educación en Internet se encarga de:

1. **Revisión diaria de la actividad de los estudiantes en el campus virtual** a través de: correos electrónicos, llamadas de teléfono y del propio desarrollo de las actividades formativas. Los tutores personales realizan esta comprobación y si detectan alguna dificultad se ponen en contacto con el estudiante y le recomiendan que vuelva a los puntos que presentan mayor debilidad. Si persisten, el tutor personal resuelve de manera personal. Si aún persisten se pondrá en conocimiento de la dirección académica. Dicha incidencia será tomada en cuenta y tendrá un seguimiento especial durante los siguientes meses de formación.
2. **Test de autoaprendizaje al finalizar el curso de introducción al campus virtual.** Los tutores personales evalúan los resultados y en el caso de detectar alguna dificultad se ponen en contacto con el estudiante.

4.3.2. Seguimiento diario del alumnado

UNIR aplica un Plan de Acción Tutorial, que consiste en el acompañamiento y seguimiento del alumnado a lo largo del proceso educativo. Con ello se pretende lograr los siguientes objetivos:

- Favorecer la educación integral de los alumnos.
- Potenciar una educación lo más personalizada posible y que tenga en cuenta las necesidades de cada alumno y recurrir a los apoyos o actividades adecuadas.
- Promover el esfuerzo individual y el trabajo en equipo.

Para llevar a cabo el plan de acción tutorial, UNIR cuenta con un grupo de tutores personales. **Es personal no docente** que tiene como función la guía y asesoramiento del estudiante durante el curso. Todos ellos están en posesión de títulos superiores. Se trata de un sistema muy bien valorado por el alumnado, como se deduce de los resultados de las encuestas realizadas a los estudiantes.

A cada tutor personal se le asigna un grupo de alumnos para que realice su seguimiento. Para ello cuenta con la siguiente información:

- El acceso de cada usuario a los contenidos teóricos del curso además del tiempo de acceso.
- La utilización de las herramientas de comunicación del campus (foros, grupos de discusión, etc.).
- Los resultados de los test y actividades enviadas a través del campus.

Estos datos le permiten conocer el nivel de participación de cada estudiante para ofrecer la orientación adecuada.

4.3.3. Proceso para evitar abandonos

Dentro de las actuaciones del SOA (Servicio de Orientación Académica), las herramientas de organización y planificación, así como las metodologías de estudio que se les aporta a los estudiantes atendidos en este departamento, conducen a reducir posibles abandonos de los estudios. Por un lado, se mejora el aprendizaje y, por otro, se ayuda a los alumnos a valorar su disponibilidad de tiempo, de tal manera que la matriculación en el siguiente periodo se adapte verdaderamente a la carga lectiva que puedan afrontar.

4.4 SISTEMA DE TRANSFERENCIA Y RECONOCIMIENTO DE CRÉDITOS

Reconocimiento de Créditos Cursados en Enseñanzas Superiores Oficiales no Universitarias

MÍNIMO	MÁXIMO
0	9

Reconocimiento de Créditos Cursados en Títulos Propios

MÍNIMO	MÁXIMO
0	9

Adjuntar Título Propio

Ver Apartado 4: Anexo 2.

Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional

MÍNIMO	MÁXIMO
--------	--------



0

9

NORMATIVA DE RECONOCIMIENTO Y TRANSFERENCIA DE CRÉDITOS DE LA UNIVERSIDAD INTERNACIONAL DE LA RIOJA.

PREÁMBULO

El Real Decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales, modificado por el Real Decreto 861/2010, de 2 de julio, recoge ya en su preámbulo que "uno de los objetivos fundamentales de esta organización de las enseñanzas es fomentar la movilidad de los estudiantes, tanto dentro de Europa, como con otras partes del mundo, y sobre todo la movilidad entre las distintas universidades españolas y dentro de una misma universidad. En este contexto resulta imprescindible apostar por un sistema de reconocimiento y acumulación de créditos, en el que los créditos cursados en otra universidad serán reconocidos e incorporados al expediente del estudiante".

Con tal motivo, el RD en su artículo sexto "Reconocimiento y transferencia de créditos" establece que "las universidades elaborarán y harán pública su normativa sobre el sistema de reconocimiento y transferencia de créditos". Dicho artículo establece unas definiciones para el reconocimiento y para la transferencia que modifican sustancialmente los conceptos que hasta ahora se venían empleando para los casos en los que unos estudios parciales eran incorporados a los expedientes de los estudiantes que cambiaban de estudios, de plan de estudios o de universidad (mediante las figuras de la convalidación y la adaptación).

La Universidad Internacional de La Rioja comparte entre sus principios fundamentales la necesidad de intercambio y movilidad del estudiante como parte del enriquecimiento personal y la excelencia profesional en el entorno del Espacio Europeo de Educación Superior.

Las modificaciones incorporadas por el Real Decreto 861/2010 amplían y regulan con mayor detalle el marco en el que pueden realizarse los reconocimientos de créditos por experiencia profesional o laboral, Títulos Propios Universitarios y otras Enseñanzas Superiores no universitarias. Finalmente el Real Decreto 1618/2011, de 14 de noviembre fija las reglas que favorecen el reconocimiento entre los títulos universitarios de graduado, los títulos de graduado en enseñanzas artísticas, los títulos de técnico superior en artes plásticas y diseño, los títulos de técnico superior de formación profesional, y los títulos de técnico deportivo superior, tratando para ello de establecer, como indica en su exposición de motivos, "las «pasarelas» entre titulaciones directamente relacionadas".

Con fecha 29 de abril de 2021 el Consejo Directivo ha aprobado la modificación de estas normas.

CAPÍTULO I. OBJETO, ÁMBITO, RESPONSABLES Y PROCEDIMIENTO

Artículo 1. Objeto y ámbito de aplicación

La finalidad de esta normativa es regular los procedimientos de reconocimiento y transferencia de créditos que se han de aplicar en las titulaciones de Grado, Máster y Doctorado de la Universidad Internacional de La Rioja que formen parte de su oferta educativa dentro del Espacio Europeo de Educación Superior, desarrolladas al amparo del Real Decreto 1393/2007, de 29 de octubre.

Artículo 2. Definiciones

Se denominará titulación de origen aquélla en la que se han superado los créditos objeto de reconocimiento o transferencia. Se denominará titulación de destino aquella para la que se solicita el reconocimiento o la transferencia de los créditos.

Se entenderá por reconocimiento la aceptación por parte de la Universidad Internacional de La Rioja de los créditos que, habiendo sido obtenidos en unas enseñanzas oficiales, en la misma u otra universidad, son computados en otras enseñanzas distintas cursadas en nuestra universidad a efectos de la obtención de un título oficial. Así mismo, podrán ser objeto de reconocimiento los créditos cursados en otras enseñanzas superiores oficiales o en enseñanzas universitarias conducentes a la obtención de otros títulos, a los que se refiere el artículo 34.1 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.

La experiencia laboral y profesional acreditada podrá ser también reconocida en forma de créditos que computarán a efectos de la obtención de un título oficial, siempre que dicha experiencia esté relacionada con las competencias inherentes a dicho título.

Se entenderá por transferencia la consignación, en los documentos académicos oficiales acreditativos de las enseñanzas seguidas por cada estudiante, de todos los créditos obtenidos en enseñanzas oficiales cursadas con anterioridad, en la Universidad Internacional de La Rioja o en otras universidades del EEES, que no hayan conducido a la obtención de un título oficial.



Se denominará Resolución de Reconocimiento y Transferencia al documento en el cual la autoridad académica correspondiente refleja el acuerdo de reconocimiento y transferencia de los créditos objeto de solicitud. En ella, deberán constar: los créditos reconocidos y transferidos y, en su caso, las asignaturas o materias que deberán ser cursadas y las que no, por considerar adquiridas las competencias de esas asignaturas en los créditos reconocidos. Corresponderá a la Comisión de Reconocimiento y Transferencia de la Universidad Internacional de La Rioja, la aprobación del modelo de dicha resolución.

Artículo 3. Órganos y unidades responsables

1. Rector. Es el responsable de dictar resolución de reconocimiento y transferencia y resolver los recursos que pudieran plantearse. Dicha competencia podrá delegarla por escrito en los Decanos o Directores de Centros.

2. Comisión de Reconocimiento y Transferencia de la Universidad. Estará formada por los siguientes miembros:

- El Secretario General que actuará como presidente por Delegación del Rector.
- El Decano de cada Facultad que podrá delegar en el Vicedecano o Vicedecanos cuando así lo estime procedente.
- El Director del Departamento de Calidad, o persona en quien delegue.
- El Jefe de Área de Reconocimientos y Transferencia de Créditos que actuará como Secretario de la Comisión.

Serán funciones de la Comisión las siguientes:

- a) Autorizar las propuestas de reconocimiento y transferencia de créditos solicitadas por los alumnos e informadas por el Coordinador Académico de la titulación, de acuerdo con el procedimiento establecido en el artículo 4.
 - b) Mantener actualizado un catálogo de todas las materias y actividades cuyo reconocimiento haya sido informado o autorizado previamente. Para las materias y actividades incorporadas en dicho catálogo procederá, directamente, la resolución del Rector, sin que sea necesaria la emisión de nuevo informe del Coordinador Académico del título.
 - c) Informar las reclamaciones que se planteen ante el Rector contra Resoluciones de Reconocimiento y Transferencia.
 - d) Aclarar e interpretar las prescripciones establecidas en la presente normativa y dictar las resoluciones que procedan de homogeneización y estandarización de criterios.
3. Coordinador Académico de Titulación. Será el encargado de informar las peticiones de reconocimiento y transferencia de los alumnos de acuerdo con lo establecido en la presente normativa y las directrices que dicte la Comisión de Reconocimiento y Transferencia.
4. Unidad de Reconocimiento y Transferencia de Créditos de la Universidad. Es el equipo técnico administrativo encargado de dar soporte a la Comisión de Reconocimientos, al Coordinador del Título y al Rector en el proceso de Autorización del Reconocimiento.

Artículo 4. Procedimiento y Plazos

El reconocimiento de créditos previo a la matrícula podrá ser solicitado hasta 10 días antes de la formalización de la matrícula. Las solicitudes acompañarán la documentación necesaria para proceder al reconocimiento: Copia de

Certificación Académica y, en el caso de ser requeridos, los programas de las materias o asignaturas, así como cualquier documentación justificativa de la experiencia profesional acreditada, y títulos propios universitarios. El procedimiento podrá iniciarse por vía telemática, para lo que el estudiante aportará copia escaneada de los documentos indicados. Solo en el caso de que prosperase la solicitud de reconocimiento será necesario aportar los originales de dichos documentos o copia compulsada de los mismos.

Una vez recibidas las solicitudes, la Unidad de Reconocimientos remitirá al Coordinador Académico las propuestas de reconocimientos que no estén incluidas en el catálogo a que se refiere el artículo 3.1.b anterior. El coordinador académico dispondrá de un plazo de 3 días hábiles para emitir informe. Este informe no tendrá carácter vinculante.

De no emitirse el informe en el plazo señalado, se proseguirá con las actuaciones. El informe emitido fuera de plazo no habrá de ser tenido en cuenta al dictar resolución.

La Comisión de Reconocimiento y de Transferencia autorizará los reconocimientos que procedan elaborando la propuesta de Resolución. Con carácter previo a la Propuesta definitiva de resolución se pondrá en conocimiento del estudiante la propuesta de reconocimiento (Estudio Previo de Reconocimiento), a fin de que pueda formular las alega-



ciones que estime oportunas. En tal caso, el Coordinador y la Comisión de Reconocimientos las estudiarán y realizarán, en su caso, una nueva propuesta de resolución.

No podrá dictarse resolución por el Rector hasta tanto no conste en el expediente la documentación original o compulsada acreditativa de las competencias y conocimientos alegados previamente. La eficacia de la resolución del Rector quedará supeditada al abono por el alumno de la tasa de reconocimiento que corresponda.

El plazo máximo para resolver y notificar las resoluciones será de tres meses a partir del día siguiente al de entrada de la solicitud en la Universidad Internacional de La Rioja. El vencimiento del plazo máximo sin haberse notificado resolución expresa legitima al interesado o interesados que hubieran deducido la solicitud para entenderla desestimada por silencio administrativo.

CAPÍTULO II. RECONOCIMIENTO Y TRANSFERENCIA DE CRÉDITOS

Artículo 5.- Reconocimiento de Créditos. Disposiciones generales

Los créditos, en forma de unidad evaluada y certificable, pasarán a consignarse en el expediente del estudiante con expresión de la tipología de origen y destino de la materia y la calificación de origen, con indicación de la universidad en la que se superaron.

El formato y la información que se han de incluir en las certificaciones académicas oficiales y personales serán los que se determinen por la Comisión de Reconocimiento y Transferencia.

En todo caso no podrán ser objeto de reconocimiento los créditos correspondientes a los trabajos de fin de grado y máster.

De acuerdo con lo establecido en el artículo 3.1.b anterior, la Universidad podrá establecer, directamente o previa suscripción de convenios de colaboración, tablas de equivalencia, para posibilitar el reconocimiento parcial de estudios nacionales o extranjeros, a fin de facilitar la movilidad de estudiantes y la organización de programas interuniversitarios, todo ello de conformidad con lo establecido en el R.D. 1393/2007. Estas tablas deberán aprobarse con carácter previo por la Comisión de Reconocimiento y Transferencia de Créditos.

En la Resolución de Reconocimiento y Transferencia se deberá indicar el tipo de créditos reconocidos, así como las asignaturas que el estudiante no deberá cursar por considerar adquiridas las competencias correspondientes a los créditos reconocidos.

Salvo la garantía dispuesta en el artículo siguiente para el reconocimiento de créditos básicos, el reconocimiento se realizará teniendo en cuenta la adecuación entre las competencias y conocimientos adquiridos, bien en otras materias o enseñanzas superadas por el estudiante o bien asociados a una previa experiencia profesional y los previstos en el plan de estudios o que tengan carácter transversal. En todo caso, deberá garantizarse una adecuación entre competencias, contenidos y carga lectiva de un mínimo del 75% para que el reconocimiento pueda autorizarse.

Cuando el estudiante solicite reconocimiento aportando una certificación académica en donde consten asignaturas superadas por reconocimiento/convalidación/adaptación en otra universidad, y el estudiante solicite, además, reconocimiento por otras actividades susceptibles de reconocimiento (otros estudios universitarios, experiencia profesional, estudios superiores no universitarios, títulos propios, actividades de extensión universitaria), será necesario aportar el expediente académico de origen de las asignaturas inicialmente adaptadas, si estas han sido cursadas con anterioridad a la fecha en que se realice la adaptación.

Como excepción a lo previsto en el párrafo anterior, se podrá admitir un reconocimiento con una adecuación de la carga lectiva de un mínimo del 60% (la adecuación de competencias deberá ser, en todo caso, de un mínimo del 75%), cuando se de alguno de estos supuestos:

- a) Que se trate de una adaptación de un plan de estudios anterior de la misma titulación.
- b) Que el reconocimiento se realice en el marco de un convenio de doble titulación o de título conjunto.

En el caso de reconocimiento de créditos entre estudios correspondientes a enseñanzas diferentes, serán de aplicación específicamente los límites al reconocimiento que figuran en el artículo 6 del Real Decreto 1618/2011, de 14 de noviembre.

Artículo 6. Reconocimiento de créditos de formación básica

En consonancia con lo dispuesto en el Real Decreto 1393/2007, siempre que el título al que se pretende acceder pertenezca a la misma rama de conocimiento, serán objeto de reconocimiento al menos el 15 por ciento de los créditos correspondientes a materias de formación básica de dicha rama.



Artículo 7. Reconocimiento de créditos de materias obligatorias, optativas y prácticas externas de grado

En el caso de los créditos en materias obligatorias, optativas y de prácticas externas, se tendrá en cuenta la adecuación entre las competencias y conocimientos aportados por el estudiante y los previstos en el plan de estudios de destino.

Se aplicará a los créditos reconocidos la calificación de origen que corresponda. Cuando ello sea necesario, se especificará la calificación media ponderada de los créditos reconocidos, de acuerdo con la Normativa sobre Calificaciones y Media de Expediente de la Universidad Internacional de La Rioja.

Excepcionalmente, se podrán reconocer como créditos optativos en la titulación de destino, los superados por el estudiante en la titulación de origen, aun cuando no tengan equivalencia en materias concretas, cuando, atendiendo a su carácter transversal, su contenido se considere adecuado a los objetivos y competencias del título.

Si el alumno acredita, mediante certificación fehaciente expedida por la Escuela Oficial de Idiomas o por otro Centro Superior o Universidad de reconocido prestigio, el conocimiento de uno o más idiomas, dentro del Marco Europeo de Referencia para las Lenguas, de manera que resulte patente que posee las competencias y conocimiento asociados a una determinada materia de aprendizaje lingüístico, podrá ser autorizado a que, si lo solicita, le sean reconocidos los créditos correspondientes a dicha materia, con la calificación de Apto. En este supuesto, la asignatura reconocida no computará en el cálculo de la nota media del expediente.

Artículo 8. Transferencia de créditos

Los créditos superados por el estudiante en enseñanzas universitarias oficiales que no hayan conducido a la obtención de un título oficial y que no hayan sido objeto de reconocimiento, podrán consignarse en el expediente del estudiante. La solicitud de transferencia requerirá previamente el traslado de expediente y el abono de la tasa correspondiente.

En las certificaciones académicas, los créditos transferidos aparecerán claramente diferenciados de aquellos créditos que conducen a la obtención del título de grado o máster.

CAPÍTULO III. RECONOCIMIENTO DE CRÉDITOS. ESPECIFICIDADES

Artículo 9. Reconocimiento de experiencia laboral y profesional y de enseñanzas universitarias no oficiales

9. 1. Reconocimiento de experiencia laboral y profesional

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 las competencias inherentes a dicho título.

El expediente documental será conformado por el solicitante e 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 las competencias inherentes al título.

Cuando el expediente documental no se evidencie claramente que el solicitante haya adquirido las competencias alegadas, se procederá a la evaluación de competencias del candidato por parte del Coordinador Académico del Título. Podrá evaluarse mediante entrevista profesional, simulaciones, pruebas o informes estandarizados de competencia u otros métodos afines.

Cuando de la evaluación se desprenda que el solicitante tiene las competencias y conocimientos asociados a una determinada materia, podrá autorizarse el reconocimiento de los créditos correspondientes a ella.

Cuando la experiencia acreditada aporte competencias y conocimientos inherentes al título, pero que no coincidan con los de ninguna materia en particular, podrán reconocerse, atendiendo a su carácter transversal, en forma de créditos optativos.

El reconocimiento de estos créditos se calificará como APTO y no computarán a efectos de baremación del expediente.

9. 2. Reconocimiento de enseñanzas universitarias no oficiales



Podrán reconocerse créditos por enseñanzas universitarias no oficiales siempre que hayan sido impartidas por una Universidad legalmente reconocida y el diploma o título correspondiente advenga de la realización de la evaluación del aprendizaje.

El reconocimiento de estos créditos se calificará como APTO y no computarán a efectos de baremación del expediente.

El número de créditos que sean objeto de reconocimiento a partir de experiencia profesional o laboral y de enseñanzas universitarias no oficiales no podrá ser superior, en su conjunto, al 15 por ciento del total de créditos que constituyen el plan de estudios, salvo en el caso previsto en el artículo 6.4. del Real Decreto 1393/2007.

Artículo 10. Reconocimiento de estudios de enseñanzas superiores oficiales no universitarias

El reconocimiento de créditos por estudios superiores no universitarios se regulará por lo dispuesto en el R.D. 1618/2011, de 14 de noviembre, sobre reconocimiento de estudios en el ámbito de la Educación Superior, así como por los acuerdos que en su caso se suscriban con la Administración Educativa correspondiente y por lo dispuesto en la presente normativa.

Artículo 11. Reconocimiento de estudios completados de un plan de estudios desarrollado según regulaciones anteriores

En el caso de titulados de planes antiguos y siempre que ambas titulaciones pertenezcan a la misma rama de conocimiento, si la titulación de destino es un grado, se reconocerán un mínimo del 15% de los créditos de la titulación de destino, por considerar que el título obtenido le aporta las competencias básicas de la rama.

No obstante lo previsto en el apartado anterior, cuando la Comisión de Reconocimiento y Transferencia de Créditos considere que, por disparidad metodológica o material de las enseñanzas ya cursadas, no se han adquirido suficientemente los contenidos y competencias básicas del título de destino, podrá restringir el alcance del reconocimiento, a fin de garantizar que el estudiante pueda incorporarse adecuadamente a las enseñanzas del título de destino.

Respecto del resto de créditos se podrá realizar un reconocimiento asignatura por asignatura, de acuerdo con lo previsto en el artículo 7 anterior.

Artículo 12. Reconocimiento de estudios parciales de un plan de estudios desarrollado según regulaciones anteriores

Podrá realizarse el reconocimiento teniendo en cuenta la adecuación entre las competencias y conocimientos adquiridos de acuerdo con lo previsto en el artículo 7 anterior.

A efectos de lo dispuesto en el artículo 11 y en el párrafo anterior de este artículo, respecto del reconocimiento de créditos, se entenderá que la carga lectiva de un crédito de anteriores sistemas educativos equivale a un crédito ECTS.

Artículo 13. Reconocimiento de estudios parciales oficiales extranjeros

En el caso de estudios universitarios oficiales extranjeros, podrá realizarse el reconocimiento teniendo en cuenta la adecuación entre las competencias y conocimientos adquiridos de acuerdo con lo previsto en el artículo 7 anterior.

En el supuesto de Títulos Propios Universitarios extranjeros, se atenderá a lo dispuesto en el artículo 9.

En el supuesto de Títulos Extranjeros de Enseñanza Superior no Universitaria, podrán ser objeto de reconocimiento, de acuerdo con el artículo 10 anterior, condicionado a la obtención de la homologación del título al correspondiente título español de Enseñanza Superior no Universitaria.

Artículo 14. Reconocimiento de créditos por la participación en actividades culturales, deportivas, de representación estudiantil, solidarias y de cooperación

Conforme a lo que establece el artículo 46.2.i.) de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades y el artículo 12.8, del Real Decreto 1393/2007, "los estudiantes podrán obtener reconocimiento académico en créditos por la participación en actividades universitarias culturales, deportivas, de representación estudiantil, solidarias y de cooperación". Este reconocimiento se llevará a cabo de acuerdo con los siguientes criterios:



a) Será aplicable en los títulos de grado. El número máximo de créditos que podrá ser objeto de reconocimiento será el que establezca en la memoria del título. El Plan de Estudios habrá sido configurado de modo que, al menos, sean susceptibles de reconocimiento, 6 créditos sobre el total de dicho plan.

b) La actividad objeto de reconocimiento deberá haber sido desarrollada durante el período de estudios universitarios (período comprendido entre el acceso a la Universidad Internacional de La Rioja y la obtención del título), salvo que se trate habilidades lingüísticas acreditadas, en cuyo caso se podrán admitir certificados oficiales expedidos al estudiante antes de comenzar sus estudios en UNIR.

c) Las actividades específicas por las que puede ser solicitado el reconocimiento habrán de haber sido aprobadas por la Comisión de Reconocimiento y Transferencia.

d) Los créditos reconocidos serán incorporados al expediente del estudiante como "reconocimiento de créditos por participación en actividades universitarias" añadiendo, en su caso, el nombre de la actividad, con la calificación de Apto y no se tendrá en cuenta en la media del expediente académico, salvo que una norma estatal estableciera lo contrario, y eximirán de la realización de los créditos que correspondan.

Disposición Final. Entrada en vigor

Los cambios entrarán en vigor el 7 de mayo de 2021.

4.6 COMPLEMENTOS FORMATIVOS



5. PLANIFICACIÓN DE LAS ENSEÑANZAS

5.1 DESCRIPCIÓN DEL PLAN DE ESTUDIOS		
Ver Apartado 5: Anexo 1.		
5.2 ACTIVIDADES FORMATIVAS		
Sesiones presenciales virtuales		
Recursos didácticos audiovisuales		
Estudio del material básico		
Lectura del material complementario		
Proyectos y casos prácticos		
Prácticas informáticas		
Test de autoevaluación		
Tutorías		
Trabajo colaborativo		
Realización de prácticas en el centro		
Redacción de la memoria de prácticas		
Tutorías (Prácticas)		
Sesión Inicial de presentación de TFM		
Lectura de material en el aula virtual (TFM)		
Seminarios de TFM		
Tutorías (TFM)		
Sesiones grupales de TFM		
Elaboración del Trabajo Fin de Máster		
5.3 METODOLOGÍAS DOCENTES		
No existen datos		
5.4 SISTEMAS DE EVALUACIÓN		
Participación en foros y otros medios participativos		
Realización de proyectos y casos prácticos		
Prácticas informáticas		
Test de autoevaluación		
Prueba de evaluación final		
Evaluación con base en el informe del tutor externo		
Memoria de prácticas		
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		
5.5 SIN NIVEL 1		
NIVEL 2: GESTIÓN Y REGULACIÓN DE LA CIBERSEGURIDAD		
5.5.1.1 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
LENGUAS EN LAS 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	
NIVEL 3: Ciberdelitos y Regulación de la Ciberseguridad		
5.5.1.1.1 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
LENGUAS EN LAS 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	
NIVEL 3: Gobierno de la Ciberseguridad y Análisis de Riesgos		
5.5.1.1.1 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
LENGUAS EN LAS 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	
5.5.1.2 RESULTADOS DE APRENDIZAJE		
<p>Los resultados del aprendizaje esperados para esta materia pasan por la correcta comprensión de los aspectos relacionados con la legislación reguladora y su ámbito de aplicación, la protección de datos, la gestión de la seguridad, los delitos informáticos y los análisis de riesgos legales de los sistemas de información.</p>		
5.5.1.3 CONTENIDOS		
<p>Aspectos Legales y Regulatorios. Estudio genérico del marco legal vigente en materia de bienes y servicios informáticos, centrado en aspectos clave tales como propiedad industrial e intelectual, protección de datos o regulación de mercados.</p> <p>Análisis de Riesgos Legales. Metodología para una gestión proactiva de los riesgos legales inherentes al desarrollo, implantación y despliegue de actividad informática.</p> <p>Delitos Informáticos Ciberdelitos y Regulación de la Ciberseguridad . Estudio de la legislación penal en materia de infracciones cuyo medio de comisión u objeto de la misma sean bienes o servicios informáticos, de tal manera que se permita su identificación, su denuncia y correspondiente seguimiento procesal. La presente asignatura posee también un estudio genérico del marco legal vigente en materia de bienes y servicios informáticos, centrado en aspectos clave tales como propiedad industrial e intelectual, protección de datos o regulación de mercados.</p> <p>Gobierno de la Ciberseguridad y Análisis de Riesgos. Metodología para una gestión proactiva de los riesgos legales de los sistemas de información inherentes al desarrollo, implantación y despliegue de actividad informática, con especial atención a la industria del software, especialmente relevante en esta materia. Identificación de los problemas relacionados con la gestión de sistemas informáticos de seguridad, diseño de planes de auditoría, políticas de recuperación de datos, implantación de SGSI, grado de implantación de las normativas de seguridad, seguridad en la nube, infraestructuras críticas y diseño de planes de seguridad proactivos.</p> <p>Esta materia da una visión de conjunto sobre los aspectos legales y el marco jurídico institucional en relación a la seguridad informática. También se estudia cómo analizar y recomendar diversas estrategias en dicho ámbito.</p>		
5.5.1.4 OBSERVACIONES		
5.5.1.5 COMPETENCIAS		
5.5.1.5.1 BÁSICAS Y GENERALES		
CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarrollarlos mediante los métodos y procesos adecuados.		
CG1 - Aplicar los conocimientos adquiridos y ser capaces de resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con el área de la seguridad informática.		
CG2 - Integrar conocimientos para formular juicios a partir de determinada información. A la vez, incluir reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios en materia de asesoramiento en seguridad informática.		
CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación continua en su futuro desempeño profesional como experto en seguridad informática.		
CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de la entidades de TI.		
CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática.		



CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes.
CG8 - Tener la capacidad analítica y de resolución para atender a los problemas reales de acuerdo con los valores éticos y sociales y con el máximo respeto a la legalidad vigente.
CG9 - Manejar adecuadamente información relativa al sector de la seguridad informática. Atendiendo a la legislación vigente, notas técnicas, revistas especializadas, Internet, documentos internos de la empresa, etc.
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
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
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
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
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.
5.5.1.5.2 TRANSVERSALES
CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line.
CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc.
CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento.
CT4 - Capacidad para realizar una enseñanza personalizada adaptada al espacio (aula virtual multicultural y multirracial) a los recursos y a las situaciones y necesidades personales de los alumnos.
CT5 - Capacidad de investigar y comunicar los resultados de la investigación.
5.5.1.5.3 ESPECÍFICAS
CE21 - Analizar la infraestructura de red para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas, tanto en entorno local como en la nube.
CE22 - Diseñar las políticas de recuperación de datos más adecuadas par disminuir el impacto ante incidentes.
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención.
CE25 - Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, infraestructuras críticas y principales conceptos de auditoría de sistemas.
CE27 - Diseñar, implantar e institucionalizar un proceso de análisis y gestión de riesgos de los sistemas de información en cualquier organización.
CE1 - Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles.
CE2 - Adquirir una visión general e integrada del asesoramiento en seguridad que permita la colaboración con otros departamentos de la entidad.
CE3 - Identificar, analizar y definir los riesgos de los servicios de las empresas para poder gestionarlos con criterio y de manera efectiva, en función de sus perfiles de seguridad.
CE4 - Asesorar sobre el cumplimiento de la legislación reguladora de la protección de datos en materia de seguridad, en especial sobre la adopción de las medidas de índole técnica y organizativas necesarias considerando la problemática de los datos almacenados en la nube.
CE7 - Identificar y proceder contra aquellas conductas tipificadas como delito informático en el marco jurídico actual.
CE9 - Comprender el funcionamiento, características y nivel de riesgo de los servicios de las empresas y establecer mecanismos de protección.
CE10 - Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos.
CE11 - Conocer todos los activos del negocio de la empresa y las variables necesarias para poder implementar un SGSI.
CE12 - Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa.



CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada implantación en su infraestructura.		
CE15 - Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad.		
CE16 - Conocer y comprender la legislación europea en materia de seguridad, para poder emitir juicios sobre su aplicabilidad y relevancia en cada ámbito.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	30	100
Recursos didácticos audiovisuales	12	0
Estudio del material básico	120	0
Lectura del material complementario	90	0
Proyectos y casos prácticos	34	0
Prácticas informáticas	20	0
Test de autoevaluación	8	0
Tutorías	32	30
Trabajo colaborativo	14	0
5.5.1.7 METODOLOGÍAS DOCENTES		
No existen datos		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Participación en foros y otros medios participativos	0.0	10.0
Realización de proyectos y casos prácticos	10.0	20.0
Prácticas informáticas	20.0	30.0
Test de autoevaluación	0.0	10.0
Prueba de evaluación final	60.0	60.0
NIVEL 2: AUDITORÍA Y ANÁLISIS FORENSE		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	18	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
6	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
LENGUAS EN LAS 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	
NIVEL 3: Informática Forense y Respuesta ante Incidentes		
5.5.1.1.1 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
LENGUAS EN LAS 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	
NIVEL 3: Hacking Ético y Análisis de Malware		
5.5.1.1.1 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
LENGUAS EN LAS 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	
NIVEL 3: Desarrollo Seguro de Software y Auditoría de la Ciberseguridad		
5.5.1.1.1 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
LENGUAS EN LAS 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	
5.5.1.2 RESULTADOS DE APRENDIZAJE		
<p>Los resultados del aprendizaje esperados para esta materia pasan por la correcta comprensión de los aspectos relacionados con los análisis de riesgos vulnerabilidades en los sistemas, la securización del software, definir y desarrollar unos procesos correctos de auditoría de la seguridad, los mecanismos de protección, el diseño comprensión y ejecución de planes de una forma correcta de un análisis forense y la respuesta ante incidentes de seguridad, los SGSI, y la auditoría de sistemas en entornos sensibles.</p>		
5.5.1.3 CONTENIDOS		
<p>Gestión de la Seguridad. Identificación de los problemas relacionados con la gestión de sistemas informáticos de seguridad, diseño de planes de auditoría, implantación de SGSI, grado de implantación de las normativas de seguridad, diseño de planes de seguridad proactivos, desarrollo de políticas de seguridad, despliegue de políticas de seguridad, seguimiento de políticas de seguridad, autenticación, control de accesos, pruebas de conocimiento nulo.</p> <p>Informática Forense y Respuesta ante Incidentes. Diseño y desarrollo de un plan de respuesta ante incidentes para minimizar su impacto , contemplado en el diseño de los planes de seguridad y los planes de auditoría, durante el que se va a trabajar la recuperación de información, adquisición de datos, metodología de análisis forense, investigación de datos, documentación de procesos, herramientas de recuperación de información, medidas reactivas, protección ante desastres, redundancia de sistemas de ficheros, sistemas de ficheros avanzados.</p> <p>Hacking Ético y Análisis de Vulnerabilidades Malware . Estudio de los fallos de seguridad, tipos de vulnerabilidades, explotación de vulnerabilidades, gestión de memoria, mecanismos de protección de memoria, espacio de usuario y de sistema, exploits locales, exploits remotos, alteraciones básicas, explotaciones de memoria, shellcodes, escalada de privilegios, integer overflow, buffer overflow, heap overflow, inyección de código, puertas traseras, rootkits, protección de ejecutables. También se estudian las recomendaciones a tener en cuenta a la hora de desarrollar software y técnicas de análisis y reingeniería de malware aplicadas al análisis de malware para poder comprender el funcionamiento del código malicioso.</p> <p>Desarrollo Seguro de Software y Auditoría de la Cibers eguridad. Sistemas de memoria, fortificación de aplicaciones, prevención de desbordamientos de memoria, prevención de ataques basados en cadenas, condiciones de carrera, inducción de fallos, política de mínimos privilegios, autenticación, control de acceso. Planes de auditoría, auditoría técnica y de certificación, tipos de auditorías, auditorías de SGSI, aspectos documentales, metodologías de auditoría, ejecución de auditorías, herramientas de auditoría, ISO-27000, estudio comparativo de auditorías.</p> <p>Esta materia se centra en el estudio de los Sistemas de Gestión de la Seguridad que permitirán diseñar e implementar medidas y planes para mejorar la seguridad informática en una organización. Del mismo modo, se estudiarán las vulnerabilidades más utilizadas para desestabilizar sistemas informáticos permitiendo interrumpir su funcionamiento e incluso tomar control sobre ellos de forma no autorizada. El estudio de estos dos temas se complementará con la auditoría de seguridad, que servirá para comprender los procesos más avanzados utilizados en dicha disciplina.</p>		



5.5.1.4 OBSERVACIONES
5.5.1.5 COMPETENCIAS
5.5.1.5.1 BÁSICAS Y GENERALES
CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarrollarlos mediante los métodos y procesos adecuados.
CG1 - Aplicar los conocimientos adquiridos y ser capaces de resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con el área de la seguridad informática.
CG2 - Integrar conocimientos para formular juicios a partir de determinada información. A la vez, incluir reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios en materia de asesoramiento en seguridad informática.
CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación continua en su futuro desempeño profesional como experto en seguridad informática.
CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de la entidades de TI.
CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática.
CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes.
CG8 - Tener la capacidad analítica y de resolución para atender a los problemas reales de acuerdo con los valores éticos y sociales y con el máximo respeto a la legalidad vigente.
CG9 - Manejar adecuadamente información relativa al sector de la seguridad informática. Atendiendo a la legislación vigente, notas técnicas, revistas especializadas, Internet, documentos internos de la empresa, etc.
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
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
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
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
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.
5.5.1.5.2 TRANSVERSALES
CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line.
CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc.
CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento.
CT4 - Capacidad para realizar una enseñanza personalizada adaptada al espacio (aula virtual multicultural y multirracial) a los recursos y a las situaciones y necesidades personales de los alumnos.
CT5 - Capacidad de investigar y comunicar los resultados de la investigación.
5.5.1.5.3 ESPECÍFICAS
CE21 - Analizar la infraestructura de red para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas, tanto en entorno local como en la nube.
CE22 - Diseñar las políticas de recuperación de datos más adecuadas par disminuir el impacto ante incidentes.
CE23 - Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones.
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención.



CE25 - Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, infraestructuras críticas y principales conceptos de auditoría de sistemas.		
CE26 - Implantar procesos de análisis forense de cualquier sistema informático.		
CE1 - Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles.		
CE3 - Identificar, analizar y definir los riesgos de los servicios de las empresas para poder gestionarlos con criterio y de manera efectiva, en función de sus perfiles de seguridad.		
CE6 - Analizar el funcionamiento de herramientas de seguridad y su uso conjugado.		
CE8 - Tomar decisiones proactivas y reactivas frente los posibles fallos de seguridad, investigando las causas que las originan.		
CE9 - Comprender el funcionamiento, características y nivel de riesgo de los servicios de las empresas y establecer mecanismos de protección.		
CE12 - Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa.		
CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada implantación en su infraestructura.		
CE14 - Diseñar las correctas políticas para analizar y reproducir los hechos ante un incidente de seguridad informática.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	45	100
Recursos didácticos audiovisuales	18	0
Estudio del material básico	180	0
Lectura del material complementario	135	0
Proyectos y casos prácticos	51	0
Prácticas informáticas	30	0
Test de autoevaluación	12	0
Tutorías	48	30
Trabajo colaborativo	21	0
5.5.1.7 METODOLOGÍAS DOCENTES		
No existen datos		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Participación en foros y otros medios participativos	0.0	10.0
Realización de proyectos y casos prácticos	10.0	20.0
Prácticas informáticas	20.0	30.0
Test de autoevaluación	0.0	10.0
Prueba de evaluación final	60.0	60.0
NIVEL 2: TÉCNICAS AVANZADAS DE SEGURIDAD		
5.5.1.1 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
LENGUAS EN LAS 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	
NIVEL 3: Seguridad en Redes y Análisis Inteligente de Amenazas		
5.5.1.1.1 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
LENGUAS EN LAS 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	
NIVEL 3: Seguridad en Sistemas, Aplicaciones y el Big Data		
5.5.1.1.1 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
LENGUAS EN LAS 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	
5.5.1.2 RESULTADOS DE APRENDIZAJE		
<p>Los resultados del aprendizaje esperados para esta materia pasan por la correcta comprensión de proteger los aspectos relacionados con las distintas herramientas de principales sistemas operativos que hoy en día existen en el mundo de la informática, aplicar una seguridad; lo más óptima posible de una aplicación desplegada en online y de sus repositorios de datos asociados, como son los mecanismos de seguridad; Sistemas Gestores de Bases de Datos o los informes técnicos de seguridad; Servicios de Directorio Activo y describir las tecnologías de protección de los mecanismos criptográficos y los elementos involucrados en un entorno de seguridad sistemas de información distribuidos</p>		
5.5.1.3 CONTENIDOS		
<p>Seguridad en Redes y Análisis Inteligente de Amenazas</p> <ul style="list-style-type: none"> Aspectos avanzados sobre redes TCP/IP, seguridad en redes, ataques contra redes, denegaciones de servicio, analizadores de tráfico, zonas desmilitarizadas, características avanzadas de los sistemas de cortafuegos, redes privadas virtuales, sistemas remotos seguros, TLS/SSL, IPsec, algoritmos criptográficos usados en los protocolos de seguridad, sistemas de detección de intrusos, detección de ataques distribuidos, medidas de protección proactivas, escaneo de vulnerabilidades en redes, sistemas de gestión de identidades y control de acceso, búsqueda de patrones de ataque dinámicos, que van aprendiendo y evolucionando con el tiempo de forma autónoma <p>Seguridad en Sistemas operativos y el Big Data</p> <ul style="list-style-type: none"> Administración de servidores, estudio avanzado de servicios, estudio avanzado de sistemas de memoria, mecanismos de protección de memoria, sistemas de protección del espacio de núcleo, monitorización de procesos, sistemas de detección de intrusiones en sistemas de ficheros, cuotas de disco; monitorización de usuarios, gestión de permisos, políticas de sistemas operativos en organizaciones; administración de discos, denegaciones de servicio. Principales arquitecturas de bases de datos, inyección SQL, inyección SQL a ciegas, desbordamiento de memoria en bases de datos, Cross-site scripting, Cross-site request forgery, form tampering, clickjacking, remote file inclusión, escalada de directorios, escalada transversal de directorios, ataques a ciegas, acceso remoto a sistemas, protección de servidores web, medidas de seguridad en servidores tanto locales como en la nube ataques a sistemas desplegados sobre infraestructuras de red, autenticación, control de acceso. Análisis de información de los sistemas y aplicaciones mediante el uso de técnicas de Big Data para alertar de posibles ataques <p>Criptografía y mecanismos de seguridad. Fundamentos matemáticos avanzados sobre sistemas criptográficos, criptografía clásica, criptografía de clave secreta, criptografía de clave pública, sistemas criptográficos híbridos, funciones de resumen criptográfico hash, funciones de resumen criptográfico HMAC, autenticación de mensajes, firma digital, protocolos criptográficos seguros, transmisión segura de información, criptoanálisis, ataques de diccionario, ataques de fuerza bruta.</p> <p>Esta materia da una visión de conjunto sobre los aspectos más avanzados de la seguridad en redes, tratando temas que resultarán decisivos a la hora de proteger correctamente una red desde el punto de vista de la seguridad informática. Igualmente, se aprenderán las técnicas más avanzadas de seguridad en los distintos sistemas operativos y los sistemas criptográficos más modernos y seguros, que sustentan la arquitectura de seguridad de todos los sistemas críticos en Internet.</p>		
5.5.1.4 OBSERVACIONES		
5.5.1.5 COMPETENCIAS		
5.5.1.5.1 BÁSICAS Y GENERALES		
CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarrollarlos mediante los métodos y procesos adecuados.		
CG1 - Aplicar los conocimientos adquiridos y ser capaces de resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con el área de la seguridad informática.		



CG2 - Integrar conocimientos para formular juicios a partir de determinada información. A la vez, incluir reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios en materia de asesoramiento en seguridad informática.
CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación continua en su futuro desempeño profesional como experto en seguridad informática.
CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de la entidades de TI.
CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática.
CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes.
CG8 - Tener la capacidad analítica y de resolución para atender a los problemas reales de acuerdo con los valores éticos y sociales y con el máximo respeto a la legalidad vigente.
CG9 - Manejar adecuadamente información relativa al sector de la seguridad informática. Atendiendo a la legislación vigente, notas técnicas, revistas especializadas, Internet, documentos internos de la empresa, etc.
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
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
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
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
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.
5.5.1.5.2 TRANSVERSALES
CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line.
CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc.
CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento.
CT4 - Capacidad para realizar una enseñanza personalizada adaptada al espacio (aula virtual multicultural y multirracial) a los recursos y a las situaciones y necesidades personales de los alumnos.
CT5 - Capacidad de investigar y comunicar los resultados de la investigación.
5.5.1.5.3 ESPECÍFICAS
CE18 - Optimizar las políticas de seguridad de la infraestructura de la red de la entidad.
CE19 - Proteger la integridad de las bases de datos para asegurar la confidencialidad de la información sensible contenida.
CE20 - Asesorar sobre las distintas medidas de seguridad aplicables a los sistemas informáticos para disminuir el impacto de sus posibles fallos.
CE21 - Analizar la infraestructura de red para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas, tanto en entorno local como en la nube.
CE23 - Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones.
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención.
CE5 - Discernir sobre los distintos entornos de seguridad existentes, tanto en local como en la nube, para poder seleccionar el óptimo siguiendo un razonamiento profesional y completo.
CE6 - Analizar el funcionamiento de herramientas de seguridad y su uso conjugado.
CE9 - Comprender el funcionamiento, características y nivel de riesgo de los servicios de las empresas y establecer mecanismos de protección.



CE10 - Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos.		
CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada implantación en su infraestructura.		
CE15 - Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad.		
CE17 - Discernir los distintos mecanismos criptográficos para seleccionar el óptimo en cada ámbito de aplicación.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	30	100
Recursos didácticos audiovisuales	12	0
Estudio del material básico	120	0
Lectura del material complementario	90	0
Proyectos y casos prácticos	34	0
Prácticas informáticas	20	0
Test de autoevaluación	8	0
Tutorías	32	30
Trabajo colaborativo	14	0
5.5.1.7 METODOLOGÍAS DOCENTES		
No existen datos		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Participación en foros y otros medios participativos	0.0	10.0
Realización de proyectos y casos prácticos	10.0	20.0
Prácticas informáticas	20.0	30.0
Test de autoevaluación	0.0	10.0
Prueba de evaluación final	60.0	60.0
NIVEL 2: PRÁCTICAS EN EMPRESA		
5.5.1.1 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
LENGUAS EN LAS 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	
NIVEL 3: Prácticas en Empresa		
5.5.1.1.1 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
LENGUAS EN LAS 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	
5.5.1.2 RESULTADOS DE APRENDIZAJE		
<p>Los resultados del aprendizaje esperados para esta materia pasan por la correcta aplicación de los conocimientos adquiridos durante el estudio del resto de materias del plan de estudios.</p>		
5.5.1.3 CONTENIDOS		
<p>Prácticas en empresas Realización labores básicas de seguridad informática, tuteladas por un profesional que supervisa el correcto desarrollo de las tareas que se le asignen y mantiene las relaciones pertinentes con el tutor designado por la UNIR quienes, en régimen de colaboración, velan por la óptima formación del alumno.</p> <p>Los detalles de las tareas a desarrollar por el alumno durante la estaseia realización de las prácticas en la empresa serán fijadas por el Tutor de Prácticas Externas y se adaptarán a las peculiaridades propias de cada centro.</p>		
5.5.1.4 OBSERVACIONES		
<p>En relación a la actividad formativa "Realización de prácticas en el centro", se entiende por presencialidad, las tareas o proyectos realizados por el alumno en el centro de prácticas, ya sea de forma presencial o en la modalidad teletrabajo.</p>		
5.5.1.5 COMPETENCIAS		
5.5.1.5.1 BÁSICAS Y GENERALES		
CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarrollarlos mediante los métodos y procesos adecuados.		
CG1 - Aplicar los conocimientos adquiridos y ser capaces de resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con el área de la seguridad informática.		
CG2 - Integrar conocimientos para formular juicios a partir de determinada información. A la vez, incluir reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios en materia de asesoramiento en seguridad informática.		
CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación continua en su futuro desempeño profesional como experto en seguridad informática.		



CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de la entidades de TI.
CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática.
CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes.
CG8 - Tener la capacidad analítica y de resolución para atender a los problemas reales de acuerdo con los valores éticos y sociales y con el máximo respeto a la legalidad vigente.
CG9 - Manejar adecuadamente información relativa al sector de la seguridad informática. Atendiendo a la legislación vigente, notas técnicas, revistas especializadas, Internet, documentos internos de la empresa, etc.
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
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
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
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
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.
5.5.1.5.2 TRANSVERSALES
CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line.
CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc.
CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento.
CT4 - Capacidad para realizar una enseñanza personalizada adaptada al espacio (aula virtual multicultural y multirracial) a los recursos y a las situaciones y necesidades personales de los alumnos.
CT5 - Capacidad de investigar y comunicar los resultados de la investigación.
5.5.1.5.3 ESPECÍFICAS
CE18 - Optimizar las políticas de seguridad de la infraestructura de la red de la entidad.
CE19 - Proteger la integridad de las bases de datos para asegurar la confidencialidad de la información sensible contenida.
CE20 - Asesorar sobre las distintas medidas de seguridad aplicables a los sistemas informáticos para disminuir el impacto de sus posibles fallos.
CE21 - Analizar la infraestructura de red para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas, tanto en entorno local como en la nube.
CE22 - Diseñar las políticas de recuperación de datos más adecuadas par disminuir el impacto ante incidentes.
CE23 - Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones.
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención.
CE25 - Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, infraestructuras críticas y principales conceptos de auditoría de sistemas.
CE26 - Implantar procesos de análisis forense de cualquier sistema informático.
CE27 - Diseñar, implantar e institucionalizar un proceso de análisis y gestión de riesgos de los sistemas de información en cualquier organización.
CE1 - Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles.
CE2 - Adquirir una visión general e integrada del asesoramiento en seguridad que permita la colaboración con otros departamentos de la entidad.



CE3 - Identificar, analizar y definir los riesgos de los servicios de las empresas para poder gestionarlos con criterio y de manera efectiva, en función de sus perfiles de seguridad.
CE4 - Asesorar sobre el cumplimiento de la legislación reguladora de la protección de datos en materia de seguridad, en especial sobre la adopción de las medidas de índole técnica y organizativas necesarias considerando la problemática de los datos almacenados en la nube.
CE5 - Discernir sobre los distintos entornos de seguridad existentes, tanto en local como en la nube, para poder seleccionar el óptimo siguiendo un razonamiento profesional y completo.
CE6 - Analizar el funcionamiento de herramientas de seguridad y su uso conjugado.
CE7 - Identificar y proceder contra aquellas conductas tipificadas como delito informático en el marco jurídico actual.
CE8 - Tomar decisiones proactivas y reactivas frente los posibles fallos de seguridad, investigando las causas que las originan.
CE9 - Comprender el funcionamiento, características y nivel de riesgo de los servicios de las empresas y establecer mecanismos de protección.
CE10 - Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos.
CE11 - Conocer todos los activos del negocio de la empresa y las variables necesarias para poder implementar un SGSI.
CE12 - Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa.
CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada implantación en su infraestructura.
CE14 - Diseñar las correctas políticas para analizar y reproducir los hechos ante un incidente de seguridad informática.
CE15 - Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad.
CE16 - Conocer y comprender la legislación europea en materia de seguridad, para poder emitir juicios sobre su aplicabilidad y relevancia en cada ámbito.
CE17 - Discernir los distintos mecanismos criptográficos para seleccionar el óptimo en cada ámbito de aplicación.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	3	100
Realización de prácticas en el centro	126	100
Redacción de la memoria de prácticas	36	0
Tutorías (Prácticas)	15	0

5.5.1.7 METODOLOGÍAS DOCENTES

No existen datos

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación con base en el informe del tutor externo	40.0	40.0
Memoria de prácticas	60.0	60.0

NIVEL 2: TRABAJO FIN DE MÁSTER

5.5.1.1 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



LENGUAS EN LAS 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	
LISTADO DE ESPECIALIDADES		
No existen datos		
NIVEL 3: Trabajo Fin de Máster		
5.5.1.1.1 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
LENGUAS EN LAS 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	
5.5.1.2 RESULTADOS DE APRENDIZAJE		
<p>Los resultados del aprendizaje esperados para est a materia pasan por la correcta aplicación de los conocimientos adquiridos durante el estudio del resto de materias del plan de estudios</p>		
5.5.1.3 CONTENIDOS		
<p>Trabajo Fin de Máster</p> <p>Se realiza bajo el asesoramiento y orientación del Profesor, siguiendo las directrices marcadas por el Reglamento de Trabajos de Fin de Grado (TFG) y de Fin de Máster (TFM) en los programas de enseñanzas oficiales de la Universidad Internacional de La Rioja (UNIR).</p> <p>Elaboración, diseño y defensa pública de un caso teórico o práctico sobre seguridad informática, donde el estudiante deberá demostrar sus habilidades y conocimientos en relación a uno o varios de los siguientes aspectos:</p> <ul style="list-style-type: none"> Análisis exhaustivo de sistemas informáticos complejos, en los que la seguridad resulte un elemento crítico para su correcto funcionamiento. Identificación de las potenciales amenazas, debilidades y elementos inseguros, tanto externos como internos. Estos pueden pertenecer tanto al plano técnico, como administrativo, legal, o una combinación de los mismos. 		



- Realización de un análisis detallado de las amenazas, debilidades y elementos inseguros; para la posterior realización de un informe con posibles soluciones, así como con recomendaciones para mejorar el sistema desde el punto de vista de la seguridad informática.
- Presentación del plan de implantación para las soluciones anteriormente descritas.

5.5.1.4 OBSERVACIONES

De acuerdo con el Real Decreto 1393/2007, la defensa pública del Trabajo Fin de Máster tiene carácter obligatorio.

El trabajo fin de máster se realiza individualmente o de manera grupal, con el seguimiento continuo por parte de un profesor-director de TFM, durante la elaboración del mismo. En este máster se justifica la inclusión de la posibilidad de realizar el Trabajo Fin de Máster de manera grupal, debido a que en el mundo laboral dentro del sector de la ciberseguridad los trabajos se conciben en equipos multidisciplinares en los que deben trabajar en conjunto para poder afrontar los problemas/proyectos. Por ello, es necesario que los estudiantes de nuestra titulación desarrollen esta capacidad de trabajo en grupo, aprendiendo a justificar sus decisiones frente a sus compañeros, creando un entorno lo más similar posible a lo que será el ambiente laboral al que se van a tener que enfrentar al completar la titulación.

Elaboración, defensa y evaluación de trabajos grupales de fin de máster

Elaboración

En el caso de que el trabajo de fin de máster se realice en grupo, se deberá incluir un apartado específico sobre la organización del grupo dónde se especifiquen las partes en las que se ha dividido el trabajo, los objetivos y responsables de cada una de ellas y los mecanismos de coordinación entre los miembros del grupo.

El director del TFM asegurará un correcto **seguimiento individual** de cada uno de los integrantes del grupo a través de **tutorías individuales (4 horas)**. Prestará especial atención a verificar las tareas individualmente realizadas por cada uno de los miembros y su evolución para asegurar que cada uno de los miembros del grupo avanza adecuadamente. **Además**, se realizarán **tutorías grupales (4 horas)** con todos los componentes de modo que se pueda garantizar el avance adecuado (tanto individual como grupal) y ajustes del proceso. Estas tutorías servirán de mecanismo corrector para los obstáculos que se puedan observar pudiendo el director del TFM reasignar tareas si el trabajo final se pudiese ver comprometido.

El estudiante que no cumpla la planificación de trabajo comprometida, podrá ser objeto de apercibimiento de expulsión del grupo por parte de su director del trabajo. La persistente falta de colaboración e incumplimiento por parte de alguno de los integrantes del grupo, previamente constatada por el director de TFM y después del correspondiente apercibimiento, podrá tener como consecuencia la expulsión del equipo. El estudiante que resulte expulsado pasará a la realización de un trabajo realizado de manera individual.

En caso de que un estudiante por, cualquiera que sea la causa, hubiera de abandonar un TFM grupal y con el fin de no generar daños al resto del grupo, el Director/Coordinador del título o la Comisión Académica del título, será la encargada de gestionar la reorganización del grupo y de las tareas que queden pendientes de entrega. Así mismo, deberán garantizar la asignación de un nuevo director para el estudiante que hubo de abandonar el grupo, pudiendo encomendarse esta tarea a la propia Comisión Académica o Director/Coordinador del título.

Defensa y evaluación

El director de un TFM en grupo debe realizar el informe de autorización de forma individual para cada uno de los componentes del grupo, teniendo en cuenta para ello el seguimiento individual que haya realizado de cada uno de ellos. Por ello, cabe la posibilidad de que no todos los miembros del equipo obtengan autorización para defensa.

Durante la defensa cada miembro del grupo presentará una de las partes, aunque se podrá dirigir las cuestiones que se considere oportunas a cualquiera de sus componentes o solicitar a cualquier miembro que defienda y explique cualquier parte.

La calificación final se hará de manera individual a cada uno de los componentes del grupo, teniendo en cuenta sus aportaciones al trabajo final y la defensa individual de la parte que haya defendido y las contestaciones a las cuestiones planteadas.

Cabe recordar, según se indica en la ficha de la materia y en el apartado 5.1, que para el trabajo grupal de fin de máster la ponderación de los sistemas de evaluación, es la siguiente:

SISTEMA DE EVALUACIÓN	PONDERACIÓN
Evaluación de la estructura del Trabajo Fin de Máster	20 %
Evaluación de la exposición del Trabajo Fin de Máster	30 %
Evaluación del contenido individual del Trabajo Fin de Máster	50 %

La **evaluación final**, por tanto, tiene dos componentes: uno individual y otro grupal.

Individual:

"Evaluación de la exposición del Trabajo Fin de Máster". Representa el 30 % de la calificación final y refleja la exposición y defensa individual que el miembro del grupo realice.

"Evaluación del contenido individual del Trabajo Fin de Máster". Representa el 50 % de la calificación final y refleja la calificación que la Comisión evaluadora realiza de la parte del trabajo bajo responsabilidad del estudiante.

De este modo, la calificación individualizada supone el 80 % de la evaluación final.

Grupal:

"Evaluación de la estructura del Trabajo Fin de Máster". Representa el 20 % de la calificación final y, dado que, la estructura del TFM es única, será la misma calificación para todos los miembros del grupo.

De este modo, la calificación grupal supone el 20 % de la evaluación final.



5.5.1.5 COMPETENCIAS
5.5.1.5.1 BÁSICAS Y GENERALES
CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarrollarlos mediante los métodos y procesos adecuados.
CG1 - Aplicar los conocimientos adquiridos y ser capaces de resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con el área de la seguridad informática.
CG2 - Integrar conocimientos para formular juicios a partir de determinada información. A la vez, incluir reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios en materia de asesoramiento en seguridad informática.
CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación continua en su futuro desempeño profesional como experto en seguridad informática.
CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de la entidades de TI.
CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática.
CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes.
CG8 - Tener la capacidad analítica y de resolución para atender a los problemas reales de acuerdo con los valores éticos y sociales y con el máximo respeto a la legalidad vigente.
CG9 - Manejar adecuadamente información relativa al sector de la seguridad informática. Atendiendo a la legislación vigente, notas técnicas, revistas especializadas, Internet, documentos internos de la empresa, etc.
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
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
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
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
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.
5.5.1.5.2 TRANSVERSALES
CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line.
CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc.
CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento.
CT4 - Capacidad para realizar una enseñanza personalizada adaptada al espacio (aula virtual multicultural y multirracial) a los recursos y a las situaciones y necesidades personales de los alumnos.
CT5 - Capacidad de investigar y comunicar los resultados de la investigación.
5.5.1.5.3 ESPECÍFICAS
CE18 - Optimizar las políticas de seguridad de la infraestructura de la red de la entidad.
CE19 - Proteger la integridad de las bases de datos para asegurar la confidencialidad de la información sensible contenida.
CE20 - Asesorar sobre las distintas medidas de seguridad aplicables a los sistemas informáticos para disminuir el impacto de sus posibles fallos.
CE21 - Analizar la infraestructura de red para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas, tanto en entorno local como en la nube.
CE22 - Diseñar las políticas de recuperación de datos más adecuadas par disminuir el impacto ante incidentes.



CE23 - Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones.		
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención.		
CE25 - Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, infraestructuras críticas y principales conceptos de auditoría de sistemas.		
CE26 - Implantar procesos de análisis forense de cualquier sistema informático.		
CE27 - Diseñar, implantar e institucionalizar un proceso de análisis y gestión de riesgos de los sistemas de información en cualquier organización.		
CE1 - Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles.		
CE2 - Adquirir una visión general e integrada del asesoramiento en seguridad que permita la colaboración con otros departamentos de la entidad.		
CE3 - Identificar, analizar y definir los riesgos de los servicios de las empresas para poder gestionarlos con criterio y de manera efectiva, en función de sus perfiles de seguridad.		
CE4 - Asesorar sobre el cumplimiento de la legislación reguladora de la protección de datos en materia de seguridad, en especial sobre la adopción de las medidas de índole técnica y organizativas necesarias considerando la problemática de los datos almacenados en la nube.		
CE5 - Discernir sobre los distintos entornos de seguridad existentes, tanto en local como en la nube, para poder seleccionar el óptimo siguiendo un razonamiento profesional y completo.		
CE6 - Analizar el funcionamiento de herramientas de seguridad y su uso conjugado.		
CE7 - Identificar y proceder contra aquellas conductas tipificadas como delito informático en el marco jurídico actual.		
CE8 - Tomar decisiones proactivas y reactivas frente los posibles fallos de seguridad, investigando las causas que las originan.		
CE9 - Comprender el funcionamiento, características y nivel de riesgo de los servicios de las empresas y establecer mecanismos de protección.		
CE10 - Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos.		
CE11 - Conocer todos los activos del negocio de la empresa y las variables necesarias para poder implementar un SGSI.		
CE12 - Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa.		
CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada implantación en su infraestructura.		
CE14 - Diseñar las correctas políticas para analizar y reproducir los hechos ante un incidente de seguridad informática.		
CE15 - Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad.		
CE16 - Conocer y comprender la legislación europea en materia de seguridad, para poder emitir juicios sobre su aplicabilidad y relevancia en cada ámbito.		
CE17 - Discernir los distintos mecanismos criptográficos para seleccionar el óptimo en cada ámbito de aplicación.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesión Inicial de presentación de TFM	2	100
Lectura de material en el aula virtual (TFM)	5	0
Seminarios de TFM	2	100
Tutorías (TFM)	8	100
Sesiones grupales de TFM	3	100
Elaboración del Trabajo Fin de Máster	340	0
5.5.1.7 METODOLOGÍAS DOCENTES		
No existen datos		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA



Evaluación de la Estructura del Trabajo Fin de Máster	20.0	20.0
Evaluación de la Exposición del Trabajo Fin de Máster	30.0	30.0
Evaluación del Contenido individual del Trabajo Fin de Máster	50.0	50.0



6. PERSONAL ACADÉMICO

6.1 PROFESORADO Y OTROS RECURSOS HUMANOS				
Universidad	Categoría	Total %	Doctores %	Horas %
Universidad Internacional de La Rioja	Profesor Adjunto	19.5	100	19,5
Universidad Internacional de La Rioja	Profesor Asociado (incluye profesor asociado de C.C.: de Salud)	43.5	100	43,5
Universidad Internacional de La Rioja	Ayudante	37	0	37
PERSONAL ACADÉMICO				
Ver Apartado 6: Anexo 1.				
6.2 OTROS RECURSOS HUMANOS				
Ver Apartado 6: Anexo 2.				

7. RECURSOS MATERIALES Y SERVICIOS

Justificación de que los medios materiales disponibles son adecuados: Ver Apartado 7: Anexo 1.

8. RESULTADOS PREVISTOS

8.1 ESTIMACIÓN DE VALORES CUANTITATIVOS		
TASA DE GRADUACIÓN %	TASA DE ABANDONO %	TASA DE EFICIENCIA %
60	25	80
CODIGO	TASA	VALOR %
No existen datos		
Justificación de los Indicadores Propuestos:		
Ver Apartado 8: Anexo 1.		
8.2 PROCEDIMIENTO GENERAL PARA VALORAR EL PROCESO Y LOS RESULTADOS		
<p>8.2. Procedimiento general para valorar el progreso y los resultados de aprendizaje</p> <p>La Política de Calidad de la UNIR fue definida para promover y garantizar el logro de la misión de la organización. El despliegue de la Política de Calidad se evidencia en la implantación de un Sistema de Aseguramiento Intern de Calidad (SAIC) que es de aplicación en cada Centro y Departamento responsables de los Títulos de Grado, Máster, y Doctorado. Dicho sistema queda recogido en el criterio 9 de esta guía y aparece desarrollado en el Manual de Calidad y sus procedimientos. La estructura definida en el Manual de Calidad establece que la Unidad de Calidad, UNICA, será el órgano responsable del seguimiento y la toma de decisiones generales sobre el SAIC y de cada titulación, en este último caso recibe la asistencia y colaboración de las Unidades de Calidad de Titulación (en adelante UCT).</p> <p>Para garantizar el adecuado funcionamiento del SAIC se han establecido diferentes instrumentos de seguimiento que aparecen recogidos en el procedimiento PC-6-1.2 donde se describe cómo se realiza la medición, el análisis de los resultados y la mejora continua.</p> <ul style="list-style-type: none"> Las unidades de calidad que realizan el análisis del progreso, de los resultados de aprendizaje y del logro de los objetivos establecidos inicialmente, elaboran un informe anual de conclusiones indicando las posibles medidas correctivas, en su caso, y el correspondiente informe de propuestas de mejora (DC_6.1.2-1 Informe Anual de la Unidad de Calidad de titulación y DC_6.1.2-3 Informe de Propuestas de Mejora). La UNICA recibe y analiza la información de cada Titulación y de cada Departamento involucrado en la calidad del proceso de enseñanza-aprendizaje realizando, en su caso, las sugerencias que considere oportunas al Plan de Mejora. <p>En particular, y adaptado a esta titulación y a estos resultados el procedimiento es el siguiente:</p> <p>Tras cada periodo de evaluación, a través de la aplicación informática de informes de calidad, Dirección Académica del Título comprueba si los resultados obtenidos se adecúan a las expectativas, o si por el contrario, es necesario definir alguna medida (en la mayoría de los casos, estas medidas vendrán sugeridas por profesores, alumnos y la propia coordinación).</p> <p>La Coordinación Académica es la encargada de custodiar los datos y los registros necesarios. Para su custodia y comunicación dispone de un espacio compartido, el REPOSITORIO DOCUMENTAL, donde son controlados los documentos por parte del Departamento de Calidad, pero accesibles para su consulta por parte de todos los usuarios autorizados (PC-6-3 Procedimiento para la aprobación, modificación de procedimientos y control de la documentación</p>		



).

Con los datos obtenidos, la coordinación Académica realiza un análisis de los mismos y del logro de los objetivos establecidos inicialmente. Elabora un informe anual de conclusiones indicando las posibles medidas correctivas, en su caso, y el correspondiente informe de propuestas de mejora (DC_6.1.2-1 Informe Anual de la Unidad de Calidad de titulación y DC_6.1.2-3 Informe de Propuestas de Mejora).

UNICA recibe y analiza la información de cada Titulación realizando, en su caso, sugerencias al Plan de Mejora que se haya establecido en el informe.

UNICA traslada la información a la Comisión Permanente del Consejo Directivo para la aprobación de las medidas propuestas o su desestimación.

Toda información relevante se hace saber a los grupos implicados (ver Plan de comunicación y PA-5.2 de Comunicación Interna.)

De este modo la UNICA, tiene una visión conjunta de todas las titulaciones y propone en el Pleno de la UNICA, que se reúne al inicio y al final del curso, las acciones de mejora que son necesarias a nivel global de Universidad y ratifica las propuestas de cada UCT para su titulación.

9. SISTEMA DE GARANTÍA DE CALIDAD

ENLACE	http://www.unir.net/universidad-online/manual-calidad-procedimientos/
--------	---

10. CALENDARIO DE IMPLANTACIÓN

10.1 CRONOGRAMA DE IMPLANTACIÓN	
CURSO DE INICIO	2011
Ver Apartado 10: Anexo 1.	
10.2 PROCEDIMIENTO DE ADAPTACIÓN	
No procede	
10.3 ENSEÑANZAS QUE SE EXTINGUEN	
CÓDIGO	ESTUDIO - CENTRO

11. PERSONAS ASOCIADAS A LA SOLICITUD

11.1 RESPONSABLE DEL TÍTULO			
NIF	NOMBRE	PRIMER APELLIDO	SEGUNDO APELLIDO
08978689H	Manuel	Sánchez	Rubio
DOMICILIO	CÓDIGO POSTAL	PROVINCIA	MUNICIPIO
Avenida de la Paz, 137	26006	La Rioja	Logroño
EMAIL	MÓVIL	FAX	CARGO
virginia.montiel@unir.net	676614276	902877037	Director del Máster
11.2 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 de la Universidad
El Rector de la Universidad no es el Representante Legal			
Ver Apartado 11: Anexo 1.			
11.3 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
---------------------------	-----------	-----------	--------------------------------



Apartado 2: Anexo 1

Nombre : 2.Justificacion_COMPLETO.pdf

HASH SHA1 : CDECC1BEF7F9B438837FD59CFA3B8DA20CB78F47

Código CSV : 446687757542668398812804

Ver Fichero: 2.Justificacion_COMPLETO.pdf



Apartado 4: Anexo 1

Nombre : 4.1_Sistemas_de_información_previo.pdf

HASH SHA1 : 3C4A29E8874F0A7A0BC5C861FFD3468479A2A7A0

Código CSV : 446246065241502247153823

Ver Fichero: 4.1_Sistemas_de_información_previo.pdf



Apartado 5: Anexo 1

Nombre : 5.1_Descripción_del_plan_de_estudios.pdf

HASH SHA1 : 219C39DD7420F6B51BADAC5BD5C7341218A1A533

Código CSV : 446270564205228513974602

Ver Fichero: 5.1_Descripción_del_plan_de_estudios.pdf



Apartado 6: Anexo 1

Nombre : 6.1_Profesorado.pdf

HASH SHA1 : 1F023A4978307769BB955067AD212F6BC454B31E

Código CSV : 446255504585595898857300

Ver Fichero: 6.1_Profesorado.pdf



Apartado 6: Anexo 2

Nombre : 6.2_Otros_recursos_humanos.pdf

HASH SHA1 : A05CE0BA528CF12480196B3008EABC6B68F75E0E

Código CSV : 446263863020698028247718

Ver Fichero: 6.2_Otros_recursos_humanos.pdf



Apartado 7: Anexo 1

Nombre : 7_Recursos_materiales_y_servicios.pdf

HASH SHA1 : A39887745DA52663ED67B089911D0C29EFB84FDB

Código CSV : 446263785138471561745849

Ver Fichero: 7_Recursos_materiales_y_servicios.pdf



Apartado 8: Anexo 1

Nombre : 8.1_Estimacion_valores_cuantitativos.pdf

HASH SHA1 : 247FA6A127CCF89990ACCED571E462471F9DC030

Código CSV : 446687851065124944082745

Ver Fichero: 8.1_Estimacion_valores_cuantitativos.pdf



Apartado 10: Anexo 1

Nombre : 10_Calendario de implantacion.pdf

HASH SHA1 : 32693B58DD45079728266F15AD700174183D86F4

Código CSV : 446687887479666961596103

Ver Fichero: 10_Calendario de implantacion.pdf



Apartado 11: Anexo 1

Nombre : Delegacion_Representante_Legal_PABLO_GUZMAN_18052016.pdf

HASH SHA1 : 7D3DB15AB0D5DEAA1F83FB17B840A52C57F227EF

Código CSV : 243173502221459213834102

Ver Fichero: Delegacion_Representante_Legal_PABLO_GUZMAN_18052016.pdf



