

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		
Grado	Ciberseguridad		
DENOMINACIÓN ESPECÍFICA			
Graduado o Graduada en Ciberseguridad por la Universidad Internacional de La Rioja			
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		
Tipo Documento	Número Documento		
NIF	24236227T		
RESPONSABLE DEL TÍTULO			
NOMBRE Y APELLIDOS	CARGO		
Pablo Moreno Ger	Director de la Escuela Superior de Ingeniería y Tecnología		
Tipo Documento	Número Documento		
NIF	47027774L		
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 26 de mayo de 2021

Firma: Representante legal de la Universidad



1. DESCRIPCIÓN DEL TÍTULO

1.1. DATOS BÁSICOS

NIVEL	DENOMINACIÓN ESPECIFICA	CONJUNTO	CONVENIO	CONV. ADJUNTO
Grado	Graduado o Graduada en Ciberseguridad por la Universidad Internacional de La Rioja	No		Ver Apartado 1: Anexo 1.
LISTADO DE MENCIONES				
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 FORMACIÓN BÁSICA	CRÉDITOS EN PRÁCTICAS EXTERNAS
240	60	0
CRÉDITOS OPTATIVOS	CRÉDITOS OBLIGATORIOS	CRÉDITOS TRABAJO FIN GRADO/MÁSTER
12	156	12
LISTADO DE MENCIONES		
MENCIÓN		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	SEMIPRESENCIAL	A DISTANCIA
No	No	Sí
PLAZAS DE NUEVO INGRESO OFERTADAS		
PRIMER AÑO IMPLANTACIÓN	SEGUNDO AÑO IMPLANTACIÓN	TERCER AÑO IMPLANTACIÓN
150	150	150
CUARTO AÑO IMPLANTACIÓN	TIEMPO COMPLETO	
150	ECTS MATRÍCULA MÍNIMA	ECTS MATRÍCULA MÁXIMA



PRIMER AÑO	60.0	90.0
RESTO DE AÑOS	49.0	90.0
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
CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio
CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio
CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía
GENERALES
CG1 - Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías en el campo de la ciberseguridad, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.
CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad.
CG3 - Capacidad para saber comunicar y transmitir ideas conocimientos, habilidades y destrezas de la profesión en Ciberseguridad a un público tanto especializado como no.
CG4 - Capacidad para identificar, analizar, peritar y auditar las deficiencias, incidentes, requisitos y riesgos de seguridad de los sistemas de información, a nivel físico, arquitectura, sistema operativo, aplicación y comunicación.
CG5 - Capacidad para identificar e implementar los mecanismos más adecuados para la protección de la información y comunicaciones mediante la comprensión de los riesgos de seguridad de los distintos componentes de un sistema de tecnología de la información.
CG6 - Capacidad para concebir, diseñar, redactar, organizar, planificar y gestionar proyectos de ciberseguridad de acuerdo a los requisitos del sistema informático y de la información tratada por el mismo según el marco legislativo vigente.
CG7 - Capacidad para implementar las políticas y planes de gobernanza de la seguridad necesarios para proteger información, sistemas o arquitecturas informáticas tanto a nivel hardware, como software y redes.
CG8 - Capacidad para configurar y mantener sistemas, servicios y aplicaciones informáticas de protección de la información y las comunicaciones, o concebir y desarrollar las soluciones informáticas necesarias para dicha protección empleando los métodos de la ingeniería del software como instrumento que garantice su calidad.
CG9 - Capacidad para conocer, comprender y aplicar la legislación relativa a ciberseguridad y manejar las especificaciones, reglamentos y normas de obligado cumplimiento de dicho ámbito.
CG10 - Conocimiento básico de gestión y estructura empresarial e industrial, para identificar, auditar y proteger aquellos procesos o información sensibles desde el punto de vista de la ciberseguridad.
3.2 COMPETENCIAS TRANSVERSALES
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje.
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos.
3.3 COMPETENCIAS ESPECÍFICAS
CE1 - Capacidad para la resolución de los problemas matemáticos que puedan plantearse en la profesión de ciberseguridad. Aptitud para aplicar los conocimientos sobre: álgebra lineal; cálculo diferencial e integral; métodos numéricos; algorítmicos numéricos; estadísticos y optimización.



CE2 - Comprensión y dominio de los conceptos básicos de campos y ondas y electromagnetismo, teoría de circuitos eléctricos, circuitos electrónicos, principio físico de los semiconductores y familias lógicas, dispositivos electrónicos y fotónicos, y su aplicación para la resolución de problemas propios del campo informático.
CE3 - Capacidad para comprender y dominar los conceptos básicos de matemática discreta, lógica, algorítmica y complejidad computacional, y su aplicación para la resolución de problemas propios en el campo de la ciberseguridad.
CE4 - Conocimientos básicos sobre el uso, configuración y programación de los ordenadores, sistemas operativos, bases de datos y programas informáticos con aplicación en el campo de la ciberseguridad.
CE5 - Conocimiento y aplicación de los principios y técnicas fundamentales de paradigmas y lenguajes de programación avanzados utilizados en la administración de sistemas informáticos.
CE6 - Conocimiento y capacidad de gestión de las arquitecturas y protocolos de red que permiten la comunicación de sistemas informáticos tanto a nivel local como de Internet, así como diseñar e implementar aplicaciones basadas en ellas.
CE7 - Comprender los fundamentos de la estructura, arquitectura y componentes básicos de los computadores para conocer los vectores de ataque derivados del hardware y el firmware.
CE8 - Conocimiento y aplicación de los procedimientos algorítmicos y estructuras de datos básicos de las tecnologías informáticas para diseñar soluciones a problemas, analizando la idoneidad y complejidad de los algoritmos propuestos.
CE9 - Capacidad para analizar, diseñar, construir y mantener aplicaciones de seguridad informática de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados.
CE10 - Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos conforme a los riesgos de seguridad y las características de la plataforma o entorno de implantación.
CE11 - Conocer la legislación, normativas y regulaciones aplicables en el área de ciberseguridad, teniendo la capacidad de elaborar el pliego de condiciones técnicas de seguridad de un sistema o infraestructura informático respecto a dicho marco legislativo.
CE12 - Conocer y aplicar los protocolos y sistemas criptográficos de autenticación, identificación y certificación digital, así como capacidad para analizar su idoneidad y aplicabilidad según los requisitos de seguridad de un sistema informático.
CE13 - Conocer las características de los sistemas de cadenas de bloques (Blockchain) y tratamiento masivo de datos para identificar vulnerabilidades e implementar las medidas necesarias para la protección de la información.
CE14 - Capacidad de administración de los componentes y servicios relacionados con la seguridad de un sistema operativo y su conectividad por red, resolviendo las incidencias que se produzcan y las vulnerabilidades que se detecten.
CE15 - Entender las particularidades de las comunicaciones inalámbricas respecto a la seguridad, así como tener la capacidad para configurar e implementar las medidas necesarias para la protección de la información transmitida.
CE16 - Comprender y gestionar las principales técnicas de ataques de seguridad a nivel de aplicaciones informáticas y comunicaciones para poder diseñar, implementar y desplegar las contramedidas oportunas.
CE17 - Conocer los distintos tipos de malware y tener la capacidad de analizar sus características en función de su vector de infección, mecanismos de propagación y consecuencias para así diseñar, implementar y desplegar las soluciones de protección necesarias.
CE18 - Conocer e identificar los procedimientos de ataque informático orquestados por grupos organizados para ser capaz de diseñar e implantar las planes y contramedidas de protección adecuadas.
CE19 - Comprender las características de las infraestructuras críticas, identificar los riesgos potenciales y capacidad para aplicar las medidas necesarias para su protección según las normativas y legislación vigentes.
CE20 - Conocer, utilizar y aplicar sistemas de gestión, análisis de riesgo e implantación de planes de contingencia relacionados con la seguridad de la información.
CE21 - Conocimiento adecuado del concepto de empresa, marco institucional y jurídico de la empresa. Organización y gestión de empresas.
CE22 - Entender, diseñar y desarrollar planes directores de seguridad informática que tengan en cuenta los marcos de referencia normativos, ciclos de vida de las políticas y la planificación de recursos necesarios.
CE23 - Escoger el tipo de auditoría más adecuado para cada contexto, identificando las herramientas más adecuadas para llevarla a cabo y teniendo la capacidad para realizar un análisis crítico y concluyente de los resultados.
CE24 - Comprender y desarrollar las técnicas de generación, recopilación y análisis de evidencias digitales en el ámbito del hardware, aplicaciones informáticas, servicios basados en ellas y telecomunicaciones para extraer conclusiones post-incidente y realizar análisis forenses.
CE25 - Capacidad para elaborar un trabajo original y estructurado, consistente en un proyecto en el ámbito de Ciberseguridad en el que se sintetizan e integran las competencias adquiridas en enseñanzas del título.

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 Requisitos de acceso y 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 compuesta por, al menos:

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

La admisión al título se ajustará al Real Decreto 412/2014 que regula los requisitos de admisión a las enseñanzas de Grado.

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

- Nota media del expediente que dé acceso a los estudios de grado (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.

Acceso para mayores de 40 años por su experiencia profesional o laboral

A efectos de lo dispuesto en el RD 412/2014 por el que se establece la normativa básica de los procedimientos de admisión a las enseñanzas universitarias oficiales de Grado, en el acceso a la Universidad para mayores de 40 años por su experiencia profesional o laboral, podrán acceder a los estudios del presente Grado en Ciberseguridad las personas con experiencia laboral o profesional en relación con el ámbito de la Ingeniería y Arquitectura, 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 acceso a los estudios del Grado requerirá la realización de una prueba de acceso, que constará de dos partes:

1. Valoración del currículum del solicitante para acreditar la adecuación entre la actividad profesional del candidato y el Grado al que se desea acceder.
2. Entrevista personal. El candidato realizará una entrevista personal que valorará los siguientes aspectos:
 - Formación académica. Realización de cursos (formación continua, universitarios, etc.) relacionado con algunas de las asignaturas del Grado.
 - Experiencia laboral. Experiencia en algún campo directamente relacionado con alguna de las asignaturas de la titulación.
 - Competencias. Inquietud cultural, habilidades lectoras, uso de las Tecnologías de la Información y la Comunicación tanto para vida profesional como laboral, organización del tiempo, motivación para el estudio, etc.

Esta prueba de acceso será válida únicamente para cursar el Grado en Ciberseguridad en la Universidad Internacional de La Rioja.

Ambas fases tienen una ponderación del 50 %, siendo necesaria la obtención de, al menos, 5 sobre 10 puntos en cada uno de los apartados. Se considera que el candidato ha superado el acceso a la Universidad por esta vía cuando obtenga una calificación igual o superior a 5 puntos (calificada de 0 a 10 puntos, y expresada con dos cifras decimales), como media aritmética simple de ambas fases.

4.2.1 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 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 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 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

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 Procedimiento de acogida: 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 estudiante 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 pretenden lograr los siguientes objetivos:

- Favorecer la educación integral de los estudiantes.
- Potenciar una educación lo más personalizada posible y que tenga en cuenta las necesidades de cada estudiante 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 estudiantes 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 estudiantes 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	30

Reconocimiento de Créditos Cursados en Títulos Propios

MÍNIMO	MÁXIMO
0	36

Adjuntar Título Propio

Ver Apartado 4: Anexo 2.

Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional

MÍNIMO	MÁXIMO
0	36

Reconocimiento de Créditos Cursados por Estudios Superiores Oficiales no Universitarios

En cuanto al reconocimiento de créditos de enseñanzas superiores oficiales no universitarias, se aplicará lo que regula el Real Decreto 1618/2011, de 14 de noviembre, sobre reconocimiento de estudios en el ámbito de la Educación Superior.

En cualquier caso, se podrán reconocer, tras un estudio previo de los contenidos y las competencias, créditos de los Ciclos Formativos de Grado Superior correspondientes a los títulos de:

Técnico Superior en Desarrollo de Aplicaciones Multiplataforma (Real Decreto 450/2010)



Ha de entenderse, no obstante, que esta lista debe de quedar abierta ya que están apareciendo otros nuevos que podrán ser objeto de reconocimiento de créditos.

A continuación, se adjuntan las tablas de reconocimientos entre cada uno de los módulos de los C.F.G.S. mencionados y las asignaturas del grado:

MÓDULOS PROFESIONALES DE FP: T.S. EN Desarrollo de Aplicaciones Multiplataforma / Horas lectivas	ASIGNATURAS DEL GRADO EN CIBERSEGURIDAD / N° ECTS
Empresa e Iniciativa Emprendedora / 60 horas	Fundamentos de la Empresa / 6 ECTS
Programación / 230 horas	Fundamentos de Programación / 6 ECTS
	Algoritmia y Complejidad / 6 ECTS
Sistemas Informáticos / 170 horas	Sistemas Operativos / 6 ECTS
Bases de datos / 170 horas	Bases de Datos / 6 ECTS
	ECTS reconocidos: 30

A efectos de esta tabla, se ha tenido en cuenta el currículo del Ciclo Formativo publicado en el Real Decreto 450/2010, del 16 de abril, por el que se establece el Título de Técnico Superior en Desarrollo de Aplicaciones Multiplataforma y se fijan sus enseñanzas mínimas, disponible en el siguiente enlace: <https://www.boe.es/buscar/doc.php?id=BOE-A-2010-8067>

Además, se han tenido como referencias normativas las siguientes:

- **Ley Orgánica 4/2011**, de 11 de marzo, complementaria de la Ley de Economía Sostenible, por la que se modifican las Leyes Orgánicas 5/2002, de 19 de junio, de las Cualificaciones y de la Formación Profesional, 2/2006, de 3 de mayo, de Educación, y 6/1985, de 1 de julio, del Poder Judicial. La disposición adicional primera, apartado 3 de la Ley Orgánica 4/2011, de 11 de marzo, complementaria de la Ley de Economía Sostenible, establece que las Universidades deberán convalidar al menos 30 créditos ECTS a quienes posean el título de Técnico Superior de Formación Profesional, o equivalente a efectos académicos, y estén cursando enseñanzas universitarias de Grado relacionadas con dicho título.
- El artículo 10 del **Real Decreto 412/2014** (BOE 07/06/2014) regula los procedimientos generales de admisión en las enseñanzas universitarias oficiales de grado, señalando: "Además, en los títulos oficiales de Técnico Superior en Formación Profesional, de Técnico Superior en Artes Plásticas y Diseño y de Técnico Deportivo Superior se tendrá en cuenta su adscripción a las ramas del conocimiento establecidas en el Real Decreto 1618/2011, de 14 de noviembre, sobre reconocimiento de estudios en el ámbito de la Educación Superior, así como las relaciones directas que se establezcan entre los estudios anteriormente citados y los Grados universitarios."
- **Real Decreto 1618/2011**, de 14 de noviembre, sobre reconocimiento de estudios en el ámbito de la Educación Superior. (BOE 16/12/2011).

Reconocimiento de Créditos Cursados en Títulos Propios

De acuerdo con lo establecido en el art. 6.2 del Real Decreto 1393/2007, podrán ser objeto de reconocimiento los créditos cursados en enseñanzas universitarias conducentes a la obtención de títulos propios expedidos conforme al artículo 34.1 *in fine* de la Ley 6/2001, de 21 de diciembre, de Universidades. No obstante, se fijan, de acuerdo con la Normativa de UNIR de reconocimiento y transferencia de créditos, los siguientes límites y criterios para poder proceder a este reconocimiento:

- El máximo de créditos que podrá ser objeto de reconocimiento (tanto por experiencia profesional o laboral previa, como por haber superado estas enseñanzas universitarias no oficiales, no podrá ser superior, en su conjunto, a 36 créditos, correspondientes, según el artículo 6.3 del RD 1393/2007, al 15 por ciento del total de créditos que constituyen el plan de estudios.



- El reconocimiento no incorporará calificación ni computará a efectos de baremación de expediente.

- Solo se admitirán aquellos estudios propios en los que se garantice una adecuada evaluación del proceso formativo. A tal fin, en ningún caso, la simple asistencia podrá ser medio suficiente para acreditar la adquisición de competencia alguna. Tampoco serán aceptadas las acreditaciones o certificaciones expedidas por Departamentos o unidades universitarias que no tengan claras competencias en materia de títulos propios. - De no estar específicamente delimitado el perfil competencial del estudio propio de origen, solo será posible el reconocimiento en caso de que exista una inequívoca equivalencia entre los conocimientos y competencias adquiridas con alguna o algunas materias concretas del título de destino, o bien que, de acuerdo con el artículo 13.c del R.D 1393/2007, tengan un claro carácter transversal.

Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional

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

El Real Decreto 861/2010 modifica el artículo 6 del Real Decreto 1393/2007, fijando el límite máximo de reconocimiento a partir de experiencia profesional o laboral en el 15 % del total de créditos que constituyen el plan de estudios. En el caso de un Grado de 240 ECTS, esto equivale a 36 ECTS.

Según lo anterior y teniendo en cuenta que la experiencia laboral y profesional aportada por el estudiante debe proporcionar las mismas competencias que se adquieren con las asignaturas reconocidas, podrán ser objeto de reconocimiento por experiencia profesional y laboral las siguientes:

- Fundamentos de la Empresa (6 ECTS).
- Ingeniería del *Software* (6 ECTS).
- Redes de Ordenadores (6 ECTS).
- Sistemas Operativos (6 ECTS).
- Fundamentos de Programación (6 ECTS).
- Programación para la Administración de Sistemas (6 ECTS).
- Fundamentos de Seguridad (6 ECTS).

El Departamento de Reconocimiento y Transferencia de Créditos revisará la documentación aportada en cada caso, para verificar que se cumplen los requisitos descritos en el apartado anterior. Asimismo, teniendo en cuenta la diversidad de experiencias profesionales que los estudiantes pueden aportar, se podrán realizar otros reconocimientos siempre que, siguiendo las directrices del Real Decreto 1393/2007, dichos reconocimientos estén justificado en términos de competencias.

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

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

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

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

Materia	Asignatura (ECTS)	Competencias Específicas	Justificación
Gestión de la Seguridad	Fundamentos de la Empresa (6 ECTS)	CE21	Tipo de entidad: empresa pública o privada <u>Duración</u> : periodo mínimo de 300 horas. <u>Tareas desempeñadas</u> : Planificación y programación de la producción; diseño de nuevos productos y servicios; selección y diseño de procesos; gestión de la cadena de suministro; gestión de inventarios; planificación de la capacidad y localización; gestión de la calidad; gestión del mantenimiento, entre otros.



Seguridad en el <i>Software</i>	Ingeniería del <i>Software</i> (6 ECTS)	CE9	<u>Tipo de entidad:</u> empresa pública o privada <u>Duración:</u> periodo mínimo de 300 horas. <u>Tareas desempeñadas:</u> experiencia como ingeniero de <i>software</i> en diseño, ejecución, implementación y/o validación de proyectos informáticos.
Seguridad en Sistemas y Comunicaciones	Redes de Ordenadores (6 ECTS)	CE6	<u>Tipo de entidad:</u> empresa pública o privada <u>Duración:</u> periodo mínimo de 300 horas. <u>Tareas desempeñadas:</u> experiencia como responsable-administrador de redes en gran empresa u organismo público.
Seguridad en Sistemas y Comunicaciones	Sistemas Operativos (6 ECTS)	CE4	<u>Tipo de entidad:</u> empresa pública o privada <u>Duración:</u> periodo mínimo de 600 horas. <u>Tareas desempeñadas:</u> experiencia como responsable-administrador de sistemas en gran empresa u organismo público.
Programación y Algoritmia	Fundamentos de Programación (6 ECTS)	CE4	<u>Tipo de entidad:</u> empresa pública o privada <u>Duración:</u> periodo mínimo de 300 horas. <u>Tareas desempeñadas:</u> experiencia como analista-programador en proyectos informáticos de implantación en cliente final.
Programación y Algoritmia	Programación para la Administración de Sistemas (6 ECTS)	CE5, CE9	<u>Tipo de entidad:</u> empresa pública o privada <u>Duración:</u> periodo mínimo de 600 horas. <u>Tareas desempeñadas:</u> experiencia como analista-programador en proyectos informáticos de implantación en cliente final.
Fundamentos de Seguridad	Fundamentos de Seguridad (6 ECTS)	CE10, CE11	<u>Tipo de entidad:</u> empresa pública o privada <u>Duración:</u> periodo mínimo de 300 horas. <u>Tareas desempeñadas:</u> experiencia como responsable de sistemas y/o seguridad informática en gran empresa u organismo público.

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 aquella 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 alegaciones 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 legítima 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 advierte 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.



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
Trabajos y casos prácticos
Test de evaluación
Laboratorios virtuales
Tutorías
Estancia en Centro
Redacción de la memoria de prácticas
Lectura de documentación del centro de prácticas
Tutorías (Prácticas)
Sesión inicial de presentación de Trabajo Fin de Grado
Lectura de material en el aula virtual (TFG)
Tutorías (TFG)
Sesiones grupales de Trabajo Fin de Grado
Elaboración del Trabajo Fin de Grado
5.3 METODOLOGÍAS DOCENTES
Métodos de enseñanza magistral con mediación tecnológica: aquí se incluirían las clases presenciales virtuales, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.
Métodos activos: son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje-servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.
Métodos fundamentados en el aprendizaje individual: estudio personal, aprendizaje acompañado a través de lecturas de material complementario y realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.
5.4 SISTEMAS DE EVALUACIÓN
Participación del estudiante
Trabajos, laboratorios y/o casos
Test de evaluación
Examen final
Evaluación según el informe del tutor externo
Memoria de prácticas
Evaluación de la estructura del Trabajo Fin de Grado
Evaluación de la exposición del Trabajo Fin de Grado
Evaluación del contenido individual del Trabajo Fin de Grado
5.5 SIN NIVEL 1
NIVEL 2: Fundamentos Matemáticos de la Informática



5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	RAMA	MATERIA
Básica	Ingeniería y Arquitectura	Matemáticas
ECTS NIVEL2	24	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
6	18	
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
ECTS Cuatrimestral 10	ECTS Cuatrimestral 11	ECTS Cuatrimestral 12
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: Álgebra y Matemática Discreta		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Básica	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: Lógica Computacional		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Básica	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: Cálculo y Métodos Numéricos		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Básica	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: Estadística		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Básica	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

Álgebra y Matemática Discreta

- Resolver problemas matemáticos que puedan plantearse en el campo de la computación.
- Comprender y dominar los conceptos básicos de matemática discreta, lógica, algorítmica y complejidad computacional, y su aplicación para la resolución de problemas propios de la Informática.
- Aplicar los conocimientos de álgebra lineal a problemas propios de la Informática.
- Comprender, manejar y analizar algoritmos clásicos y computacionalmente eficientes en aritmética entera.

Lógica Computacional

- Resolver problemas matemáticos que puedan plantearse en el campo de la computación.
- Aplicar los métodos formales de la lógica proposicional.
- Describir cómo las herramientas de la lógica son usadas para modelar algoritmos y situaciones de la vida real. Describir la importancia y las limitaciones del cálculo de predicados.
- Saber aplicar métodos formales de lógica proposicional y lógica de predicados.
- Describir cómo herramientas formales de lógica simbólica se utilizan para modelar situaciones reales, incluyendo aquellas que surgen en contextos informáticos como corrección de programas o consultas en bases de datos.
- Describir la importancia y limitaciones de la lógica de predicados.
- Comprender y saber resolver problemas relacionados con autómatas y lenguajes formales básicos.

Cálculo y Métodos Numéricos

- Resolver problemas matemáticos que puedan plantearse en el campo de la computación.
- Comprender y manejar conceptos básicos de la teoría de números elemental. Aplicar la aritmética modular al estudio de la primalidad y la factorización de números enteros.
- Comprender y usar las nociones básicas asociadas a problemas de optimización lineal.
- Describir los algoritmos básicos en programación lineal.
- Entender el concepto de derivada de una función en una variable, su relevancia en el estudio cuantitativo de las funciones y su uso en aplicaciones en problemas prácticos, especialmente problemas de optimización.
- Comprender qué es la integración y su relación con problemas de tipo geométrico.
- Comprender las limitaciones inherentes al cálculo de integrales y deducir la necesidad del uso de técnicas de aproximación para el cálculo de integrales definidas.
- Comprender la necesidad del uso de funciones en varias variables. Comprender la forma de extender los conceptos asociados al cálculo en una variable a varias variables.
- Aplicar la integración en varias variables a la resolución de problemas prácticos.
- Comprender, manejar y analizar algoritmos clásicos y computacionalmente eficientes en aritmética entera.

Estadística

- Resolver problemas matemáticos que puedan plantearse en el campo de la computación.
- Diferenciar entre probabilidad y estadística. Diferenciar entre probabilidad discreta y continua. Comprender la importancia de la estimación y los conceptos de correlación y regresión.
- Calcular probabilidades y esperanzas de variables aleatorias. Diferenciar entre sucesos dependientes e independientes. Reconocer situaciones en las cuales es apropiado considerar la relevancia de las distribuciones normal y/o exponencial.
- Conocer el papel de los test de hipótesis.
- Conocer las propiedades y características más relevantes de las distribuciones de probabilidad y su aplicación a casos prácticos.

5.5.1.3 CONTENIDOS

Álgebra y Matemática Discreta

- Elementos básicos de álgebra lineal.
- Técnicas de prueba.
- Funciones, relaciones y conjuntos.
- El concepto matemático de la recursión.
- Grafos y árboles como estructuras matemáticas.

Lógica Computacional

- Lógica proposicional.
- Tablas de verdad.



- Validación
- Formas normales
- Lógica de predicados
- Cuantificación universal y existencial.
- Modus pollens y modus tollens.

Cálculo y Métodos Numéricos

- Cálculo diferencial
- Cálculo integral.
- Análisis numérico.
- Principios básicos de conteo.

Estadística

- Estadística descriptiva.
- Probabilidad discreta y distribuciones de probabilidad.
- Inferencia estadística.
- Técnicas de regresión.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías en el campo de la ciberseguridad, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.

CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio

CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio

CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética

CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado

CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

5.5.1.5.2 TRANSVERSALES

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

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

5.5.1.5.3 ESPECÍFICAS

CE1 - Capacidad para la resolución de los problemas matemáticos que puedan plantearse en la profesión de ciberseguridad. Aptitud para aplicar los conocimientos sobre: álgebra lineal; cálculo diferencial e integral; métodos numéricos; algorítmicos numéricos; estadísticos y optimización.

CE3 - Capacidad para comprender y dominar los conceptos básicos de matemática discreta, lógica, algorítmica y complejidad computacional, y su aplicación para la resolución de problemas propios en el campo de la ciberseguridad.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	60	100
Recursos didácticos audiovisuales	24	0
Estudio del material básico	208	0
Lectura del material complementario	100	0
Trabajos y casos prácticos	80	0
Test de evaluación	16	0



Laboratorios virtuales	48	16.7
Tutorías	64	30
5.5.1.7 METODOLOGÍAS DOCENTES		
Métodos de enseñanza magistral con mediación tecnológica: aquí se incluirían las clases presenciales virtuales, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.		
Métodos activos: son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje-servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.		
Métodos fundamentados en el aprendizaje individual: estudio personal, aprendizaje acompañado a través de lecturas de material complementario y realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Participación del estudiante	0.0	20.0
Trabajos, laboratorios y/o casos	20.0	40.0
Test de evaluación	0.0	20.0
Examen final	60.0	60.0
NIVEL 2: Fundamentos Físicos de la Informática		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	RAMA	MATERIA
Básica	Ingeniería y Arquitectura	Física
ECTS NIVEL2	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: Fundamentos Físicos de la Informática		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Básica	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		
Fundamentos Físicos de la Informática • Comprender la evolución y las tendencias en los sustentos físicos de la tecnología de los computadores. • Aplicar los conceptos físicos al estudio de los procesos físicos y tecnológicos implicados en el funcionamiento de los dispositivos informáticos. • Conocer las tecnologías de diseño de computadores y sus fundamentos físicos. • Comprender los conceptos básicos de los circuitos eléctricos y electrónicos. • Conocer los principales dispositivos electrónicos, fotónicos y magnéticos de aplicación en el campo de la informática.		
5.5.1.3 CONTENIDOS		
Fundamentos Físicos de la Informática • Corriente eléctrica. Dispositivos semiconductores. • Campos magnéticos en el vacío y en medios materiales. • Tecnologías base para la construcción de computadores: circuitos eléctricos y electrónicos. • Dispositivos electrónicos, fotónicos y magnéticos de aplicación a la informática.		
5.5.1.4 OBSERVACIONES		
5.5.1.5 COMPETENCIAS		
5.5.1.5.1 BÁSICAS Y GENERALES		
CG1 - Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías en el campo de la ciberseguridad, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.		
CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio		
CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio		
CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía		
5.5.1.5.2 TRANSVERSALES		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje.		



CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos.		
5.5.1.5.3 ESPECÍFICAS		
CE2 - Comprensión y dominio de los conceptos básicos de campos y ondas y electromagnetismo, teoría de circuitos eléctricos, circuitos electrónicos, principio físico de los semiconductores y familias lógicas, dispositivos electrónicos y fotónicos, y su aplicación para la resolución de problemas propios del campo informático.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	15	100
Recursos didácticos audiovisuales	6	0
Estudio del material básico	52	0
Lectura del material complementario	25	0
Trabajos y casos prácticos	20	0
Test de evaluación	4	0
Laboratorios virtuales	12	16.7
Tutorías	16	30
5.5.1.7 METODOLOGÍAS DOCENTES		
Métodos de enseñanza magistral con mediación tecnológica: aquí se incluirían las clases presenciales virtuales, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.		
Métodos activos: son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje-servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.		
Métodos fundamentados en el aprendizaje individual: estudio personal, aprendizaje acompañado a través de lecturas de material complementario y realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Participación del estudiante	0.0	20.0
Trabajos, laboratorios y/o casos	20.0	40.0
Test de evaluación	0.0	20.0
Examen final	60.0	60.0
NIVEL 2: Fundamentos de Seguridad		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
6		
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
ECTS Cuatrimestral 10	ECTS Cuatrimestral 11	ECTS Cuatrimestral 12
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: Fundamentos de Seguridad		
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		
Fundamentos de Seguridad • Conocer los conceptos fundamentales de la ciberseguridad, elementos y actores implicados. • Comprender el marco legislativo y normativo del ámbito de la seguridad de la información. • Entender las distintas técnicas y tecnologías involucradas en la ciberseguridad. • Conocer los distintos tipos de ataques y contramedidas utilizados en la seguridad informática.		
5.5.1.3 CONTENIDOS		
Fundamentos de Seguridad • Conceptos fundamentales de la ciberseguridad. • Impacto y alcance socioeconómico de la ciberseguridad. • Tipologías de ataques y amenazas a sistemas informáticos. • Introducción al marco normativo y procedimientos de gestión de la ciberseguridad.		
5.5.1.4 OBSERVACIONES		
5.5.1.5 COMPETENCIAS		
5.5.1.5.1 BÁSICAS Y GENERALES		
CG3 - Capacidad para saber comunicar y transmitir ideas conocimientos, habilidades y destrezas de la profesión en Ciberseguridad a un público tanto especializado como no.		
CG4 - Capacidad para identificar, analizar, peritar y auditar las deficiencias, incidentes, requisitos y riesgos de seguridad de los sistemas de información, a nivel físico, arquitectura, sistema operativo, aplicación y comunicación.		



CG9 - Capacidad para conocer, comprender y aplicar la legislación relativa a ciberseguridad y manejar las especificaciones, reglamentos y normas de obligado cumplimiento de dicho ámbito.		
CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio		
CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio		
CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía		
5.5.1.5.2 TRANSVERSALES		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje.		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos.		
5.5.1.5.3 ESPECÍFICAS		
CE10 - Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos conforme a los riesgos de seguridad y las características de la plataforma o entorno de implantación.		
CE11 - Conocer la legislación, normativas y regulaciones aplicables en el área de ciberseguridad, teniendo la capacidad de elaborar el pliego de condiciones técnicas de seguridad de un sistema o infraestructura informático respecto a dicho marco legislativo.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	15	100
Recursos didácticos audiovisuales	6	0
Estudio del material básico	52	0
Lectura del material complementario	25	0
Trabajos y casos prácticos	32	0
Test de evaluación	4	0
Tutorías	16	30
5.5.1.7 METODOLOGÍAS DOCENTES		
Métodos de enseñanza magistral con mediación tecnológica: aquí se incluirían las clases presenciales virtuales, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.		
Métodos activos: son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje-servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.		
Métodos fundamentados en el aprendizaje individual: estudio personal, aprendizaje acompañado a través de lecturas de material complementario y realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Participación del estudiante	0.0	20.0
Trabajos, laboratorios y/o casos	20.0	40.0



Test de evaluación	0.0	20.0
Examen final	60.0	60.0
NIVEL 2: Estructura de la Información		
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
		6
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
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: Estructura de Datos		
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: Bases de Datos		
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
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		
Estructura de Datos - Definir tipos abstractos de datos. - Saber implementar las distintas estructuras de datos y sus operaciones. - Saber escoger la estructura de datos más adecuada para resolver un problema, de acuerdo con criterios de eficiencia temporal y espacial. Bases de Datos - Conocer los distintos modelos de bases de datos. - Saber diseñar y construir bases de datos relacionales. - Saber manejar bases de datos a través de lenguajes de consulta.		
5.5.1.3 CONTENIDOS		
Estructura de Datos - Tipos Abstractos de Datos. - Estructuras de datos lineales. - Tablas de dispersión. - Árboles y grafos. Bases de Datos - Modelos y sistemas de información. - Sistemas de bases de datos. - Modelado conceptual de datos. - Diseño de bases de datos. - Lenguajes de consulta.		
5.5.1.4 OBSERVACIONES		
5.5.1.5 COMPETENCIAS		
5.5.1.5.1 BÁSICAS Y GENERALES		
CG1 - Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías en el campo de la ciberseguridad, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.		
CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad.		



CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio		
CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio		
CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía		
5.5.1.5.2 TRANSVERSALES		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje.		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos.		
5.5.1.5.3 ESPECÍFICAS		
CE4 - Conocimientos básicos sobre el uso, configuración y programación de los ordenadores, sistemas operativos, bases de datos y programas informáticos con aplicación en el campo de la ciberseguridad.		
CE8 - Conocimiento y aplicación de los procedimientos algorítmicos y estructuras de datos básicos de las tecnologías informáticas para diseñar soluciones a problemas, analizando la idoneidad y complejidad de los algoritmos propuestos.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	30	100
Recursos didácticos audiovisuales	12	0
Estudio del material básico	104	0
Lectura del material complementario	50	0
Trabajos y casos prácticos	40	0
Test de evaluación	8	0
Laboratorios virtuales	24	16.7
Tutorías	32	30
5.5.1.7 METODOLOGÍAS DOCENTES		
Métodos de enseñanza magistral con mediación tecnológica: aquí se incluirían las clases presenciales virtuales, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.		
Métodos activos: son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje-servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.		
Métodos fundamentados en el aprendizaje individual: estudio personal, aprendizaje acompañado a través de lecturas de material complementario y realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Participación del estudiante	0.0	20.0
Trabajos, laboratorios y/o casos	20.0	40.0
Test de evaluación	0.0	20.0



Examen final	60.0	60.0
NIVEL 2: Ingeniería de Computadores		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	RAMA	MATERIA
Mixta	Ingeniería y Arquitectura	Informática
ECTS NIVEL2		
ECTS OPTATIVAS	ECTS OBLIGATORIAS	ECTS BÁSICAS
0	6	6
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
6		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: Tecnología de Computadores		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Básica	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 Arquitecturas de Computadores		



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		
Tecnología de Computadores • Diseñar circuitos básicos utilizando los bloques fundamentales de construcción de arquitecturas. • Comprender y saber utilizar las distintas representaciones de datos a nivel máquina. • Comprender los bloques básicos de construcción las arquitecturas de computadores y su papel en las mismas. • Conocer la arquitectura básica de von Neumann. • Conocer la arquitectura básica de un micro-procesador y la ruta de datos de control. • Conocer el concepto básico y funcionamiento de interrupción y operación de entrada/salida. • Conocer los distintos tipos de memoria y la jerarquía de memoria. • Comprender los principios de almacenamiento en memoria. • Escribir programas básicos en ensamblador. Seguridad en Arquitecturas de Computadores • Conocer los principales vectores de ataque de un computador a nivel de arquitectura <i>hardware</i> y <i>firmware</i>. • Conocer los fundamentos de los principales ataques de canal lateral; y sus tipologías y contramedidas aplicables. • Conocer los fundamentos de los principales ataques de inyección de fallos; y sus tipologías y contramedidas aplicables. • Conocer las principales vulnerabilidades a nivel de <i>firmware</i>. • Conocer las amenazas y mecanismos de seguridad de los ataques de arranque (BIOS, UEFI) • Identificar las amenazas derivadas de conectar periféricos a un dispositivo. • Utilizar los lenguajes máquina y ensamblador de un computador digital para codificar ataques de seguridad elementales.		
5.5.1.3 CONTENIDOS		
Tecnología de Computadores • Lógica digital, sistemas digitales y representación de datos. • Organización del procesador • Ruta de datos del control. • Organización y jerarquía de memoria. • Buses, entrada/salida y almacenamiento. • Programación básica en ensamblador. Seguridad en Arquitecturas de Computadores • Tipología y fundamentos de vulnerabilidades a nivel de hardware y firmware. • Ataques de canal lateral y de inyección de fallos. Contramedidas: • Ataques al firmware. • Ataques de arranque		



Contramedidas: A ataques mediante dispositivos externos. Desarrollo de ataques básicos a nivel de ensamblador.		
5.5.1.4 OBSERVACIONES		
5.5.1.5 COMPETENCIAS		
5.5.1.5.1 BÁSICAS Y GENERALES		
CG1 - Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías en el campo de la ciberseguridad, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.		
CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio		
CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio		
CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía		
5.5.1.5.2 TRANSVERSALES		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje.		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos.		
5.5.1.5.3 ESPECÍFICAS		
CE7 - Comprender los fundamentos de la estructura, arquitectura y componentes básicos de los computadores para conocer los vectores de ataque derivados del hardware y el firmware.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	30	100
Recursos didácticos audiovisuales	12	0
Estudio del material básico	104	0
Lectura del material complementario	50	0
Trabajos y casos prácticos	40	0
Test de evaluación	8	0
Laboratorios virtuales	24	16.7
Tutorías	32	30
5.5.1.7 METODOLOGÍAS DOCENTES		
Métodos de enseñanza magistral con mediación tecnológica: aquí se incluirían las clases presenciales virtuales, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.		
Métodos activos: son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje-servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.		



Métodos fundamentados en el aprendizaje individual: estudio personal, aprendizaje acompañado a través de lecturas de material complementario y realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Participación del estudiante	0.0	20.0
Trabajos, laboratorios y/o casos	20.0	40.0
Test de evaluación	0.0	20.0
Examen final	60.0	60.0

NIVEL 2: Programación y Algoritmia

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	RAMA	MATERIA
Mixta	Ingeniería y Arquitectura	Informática
ECTS NIVEL2		
ECTS OPTATIVAS	ECTS OBLIGATORIAS	ECTS BÁSICAS
0	6	12

DESPLIEGUE TEMPORAL: Cuatrimestral

ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
6	6	
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
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: Fundamentos de Programación

5.5.1.1.1 Datos Básicos del Nivel 3

CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Básica	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: Algoritmia y Complejidad		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Básica	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: Programación para la Administración de Sistemas		
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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
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	
Fundamentos de Programación • Manejar las estructuras básicas que conforman un programa. • Realizar diseños modulares de programas. • Saber verificar el buen funcionamiento de un programa. Algoritmia y Complejidad • Adoptar y diseñar el mejor algoritmo para solucionar un problema. • Saber estudiar la computabilidad de un problema. • Saber medir la complejidad de un algoritmo. • Codificar programas de forma efectiva y eficiente. Programación para la Administración de Sistemas • Saber desarrollar programas utilizando técnicas de programación orientada a eventos y a objetos. • Saber desarrollar programas en lenguajes de script de sistema operativo como Bash o PowerShell. • Saber utilizar lenguajes interpretados de ámbito científico como Python. • Saber documentar programas utilizando las técnicas más habituales. • Ser capaz de implementar <i>interfaces</i> de usuario.	
5.5.1.3 CONTENIDOS	
Fundamentos de Programación • Construcciones básicas para el desarrollo de programas. • Abstracción y modularidad. • Estructuras básicas para la representación de datos. • Recursividad. Algoritmia y Complejidad • Algoritmos y resolución de problemas. • Análisis de algoritmos. • Estrategias básicas de algoritmia. • Algoritmos clásicos para diferentes tipos de problemas. Programación para la Administración de Sistemas • Programación orientada a objetos y eventos. • Programación en Shell Scripts: Bash y PowerShell. • Programación en Python. • <i>Interfaces</i> de usuario.	
5.5.1.4 OBSERVACIONES	
5.5.1.5 COMPETENCIAS	
5.5.1.5.1 BÁSICAS Y GENERALES	
CG1 - Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías en el campo de la ciberseguridad, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.	
CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad.	
CG8 - Capacidad para configurar y mantener sistemas, servicios y aplicaciones informáticas de protección de la información y las comunicaciones, o concebir y desarrollar las soluciones informáticas necesarias para dicha protección empleando los métodos de la ingeniería del software como instrumento que garantice su calidad.	
CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio	
CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio	
CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética	



CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado

CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

5.5.1.5.2 TRANSVERSALES

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

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

5.5.1.5.3 ESPECÍFICAS

CE4 - Conocimientos básicos sobre el uso, configuración y programación de los ordenadores, sistemas operativos, bases de datos y programas informáticos con aplicación en el campo de la ciberseguridad.

CE5 - Conocimiento y aplicación de los principios y técnicas fundamentales de paradigmas y lenguajes de programación avanzados utilizados en la administración de sistemas informáticos.

CE8 - Conocimiento y aplicación de los procedimientos algorítmicos y estructuras de datos básicos de las tecnologías informáticas para diseñar soluciones a problemas, analizando la idoneidad y complejidad de los algoritmos propuestos.

CE9 - Capacidad para analizar, diseñar, construir y mantener aplicaciones de seguridad informática de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	45	100
Recursos didácticos audiovisuales	18	0
Estudio del material básico	156	0
Lectura del material complementario	75	0
Trabajos y casos prácticos	60	0
Test de evaluación	12	0
Laboratorios virtuales	36	16.7
Tutorías	48	30

5.5.1.7 METODOLOGÍAS DOCENTES

Métodos de enseñanza magistral con mediación tecnológica: aquí se incluirían las clases presenciales virtuales, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.

Métodos activos: son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje-servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.

Métodos fundamentados en el aprendizaje individual: estudio personal, aprendizaje acompañado a través de lecturas de material complementario y realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Participación del estudiante	0.0	20.0
Trabajos, laboratorios y/o casos	20.0	40.0
Test de evaluación	0.0	20.0
Examen final	60.0	60.0

NIVEL 2: Seguridad de la Información

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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
	6	
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
6		
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: Fundamentos de Criptografía		
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: Autenticación e Infraestructuras de Clave Pública		
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



ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
	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 Bases de Datos, Blockchain y 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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
6		
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		
Fundamentos de Criptografía • Conocer la evolución histórica y fundamentos matemáticos de la criptografía • Comprender y aplicar sistemas de criptografía simétrica para la protección de la información y comunicaciones. • Entender el funcionamiento y utilidad de funciones Hash • Comprender y aplicar sistemas de criptografía asimétrica para la protección de la información y comunicaciones. • Conocer las limitaciones y vulnerabilidades de los distintos algoritmos criptográficos utilizados para la protección de la información y las comunicaciones. • Saber elegir el sistema de cifrado, autenticación o de protección de la información más adecuado dadas las características y requisitos de un sistema informático. Autenticación e Infraestructuras de Clave Pública • Conocer las distintas técnicas de autenticación y saber utilizar y configurar aplicaciones y sistemas operativos para que la utilicen. • Conocer, configurar y aplicar técnicas de autenticación biométrica. • Entender los fundamentos de la certificación digital. Autoridades de Certificación. Cadenas de certificados. • Ser capaz de instalar y configurar sistemas de autenticación basados en certificación digital. • Entender el funcionamiento y ser capaz de instalar y configurar una Infraestructura de Clave Pública.		



Seguridad en Bases de Datos, Blockchain y Big Data

- Conocer los requisitos, mecanismos y sistemas de seguridad de los sistemas de gestión de bases de datos.
- Entender los fundamentos, características y funcionamiento de los sistemas de cadenas de bloques (*Blockchain*).
- Conocer los requisitos, mecanismos y sistemas de seguridad de los sistemas de cadenas de bloques (*Blockchain*).
- Entender los fundamentos, características y funcionamiento de los sistemas de tratamiento masivo de datos (*Big Data*).
- Conocer los requisitos, mecanismos y sistemas de seguridad de los sistemas de tratamiento masivo de datos (*Big Data*).

5.5.1.3 CONTENIDOS

Fundamentos de Criptografía

- Historia y fundamentos de la criptografía
- Criptografía simétrica en flujo y en bloque
- Funciones Hash
- Criptografía asimétrica

Autenticación e Infraestructuras de Clave Pública

- Usos de Hashes en autenticación
- Técnicas de autenticación. Autenticación biométrica.
- Autoridades de certificación y certificados digitales X.509
- Implementación de una Infraestructura de Clave Pública (PKI) y gestión de certificados digitales X.509

Seguridad en Bases de Datos, Blockchain y Big Data

- Características y vulnerabilidades de los sistemas de almacenamiento y procesamiento de información.
- Seguridad en bases de datos.
- Seguridad en *Blockchain*.
- Seguridad en entornos *Big Data*.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías en el campo de la ciberseguridad, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.

CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad.

CG4 - Capacidad para identificar, analizar, peritar y auditar las deficiencias, incidentes, requisitos y riesgos de seguridad de los sistemas de información, a nivel físico, arquitectura, sistema operativo, aplicación y comunicación.

CG6 - Capacidad para concebir, diseñar, redactar, organizar, planificar y gestionar proyectos de ciberseguridad de acuerdo a los requisitos del sistema informático y de la información tratada por el mismo según el marco legislativo vigente.

CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio

CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio

CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética

CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado

CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

5.5.1.5.2 TRANSVERSALES

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

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

5.5.1.5.3 ESPECÍFICAS



CE3 - Capacidad para comprender y dominar los conceptos básicos de matemática discreta, lógica, algorítmica y complejidad computacional, y su aplicación para la resolución de problemas propios en el campo de la ciberseguridad.		
CE12 - Conocer y aplicar los protocolos y sistemas criptográficos de autenticación, identificación y certificación digital, así como capacidad para analizar su idoneidad y aplicabilidad según los requisitos de seguridad de un sistema informático.		
CE13 - Conocer las características de los sistemas de cadenas de bloques (Blockchain) y tratamiento masivo de datos para identificar vulnerabilidades e implementar las medidas necesarias para la protección de la información.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	45	100
Recursos didácticos audiovisuales	18	0
Estudio del material básico	156	0
Lectura del material complementario	75	0
Trabajos y casos prácticos	60	0
Test de evaluación	12	0
Laboratorios virtuales	36	16.7
Tutorías	48	30
5.5.1.7 METODOLOGÍAS DOCENTES		
Métodos de enseñanza magistral con mediación tecnológica: aquí se incluirían las clases presenciales virtuales, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.		
Métodos activos: son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje-servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.		
Métodos fundamentados en el aprendizaje individual: estudio personal, aprendizaje acompañado a través de lecturas de material complementario y realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Participación del estudiante	0.0	20.0
Trabajos, laboratorios y/o casos	20.0	40.0
Test de evaluación	0.0	20.0
Examen final	60.0	60.0
NIVEL 2: Seguridad en Sistemas y Comunicaciones		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	RAMA	MATERIA
Mixta	Ingeniería y Arquitectura	Informática
ECTS NIVEL2		
ECTS OPTATIVAS	ECTS OBLIGATORIAS	ECTS BÁSICAS
0	24	6
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
		6
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
6	6	
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9



12		
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: Sistemas Operativos		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Básica	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: Redes de Ordenadores		
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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
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 Operativos y Redes		
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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
	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: Arquitecturas Seguras		
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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
6		
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 Comunicaciones Inalámbricas		
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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
6		
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		
Sistemas Operativos - Razonar la necesidad de los sistemas operativos en los entornos de computación actuales. - Explicar el papel del sistema operativo como interfaz entre el hardware y los programas de usuario. - Diferenciar las técnicas de planificación de tareas más relevantes, tanto para sistemas batch, interactivos y de tiempo real. - Comprender la necesidad de gestión de la memoria física y virtual. - Comprender las técnicas generales de gestión de E/S y su relación con el sistema de archivos. - Conocer las características y estructura, organización, interface, componentes y servicios de un sistema. - Comprender la necesidad de gestión del almacenamiento secundario. Redes de Ordenadores - Reconocer la necesidad y utilidad de las redes de comunicaciones. - Distinguir las distintas topologías y escenarios de aplicación de una red de comunicaciones. - Identificar los distintos elementos que conforman una red y describir su función básica. - Reconocer la importancia del proceso de estandarización y regulación y conocer los principales organismos activos en él. - Conocer el concepto de protocolo de comunicaciones y su aplicación en modelos de pilas de protocolos. - Distinguir las funciones específicas de los niveles clásicos de una pila de protocolos de red y diferenciar los modelos más importantes de pilas de protocolos utilizados en redes. - Conocer, administrar y utilizar las aplicaciones y servicios de red más comunes. - Explicar los elementos, sus funciones y relaciones de un modelo cliente/servidor. - Comprender y analizar los mecanismos, técnicas y algoritmos que implementan los protocolos de comunicaciones. - Comprender las tecnologías de banda ancha. - Instalar y configurar redes. Seguridad en Sistemas Operativos y Redes - Conocer los principios y mecanismos de seguridad de los distintos sistemas operativos, incluyendo los de dispositivos móviles. - Configurar y administrar los componentes y servicios relacionados con la seguridad de los distintos sistemas operativos, incluyendo los de dispositivos móviles. - Conocer las implicaciones y restricciones de los sistemas operativos respecto al desarrollo de aplicaciones seguras. - Administrar los sistemas de gestión de cuentas y credenciales de usuario de los sistemas operativos. - Entender, configurar y administrar los permisos de acceso y ejecución de los distintos sistemas de gestión de ficheros. - Entender las vulnerabilidades más frecuentes y críticas de los sistemas operativos. - Conocer y ser capaz de administrar los mecanismos de seguridad de red. - Utilizar los mecanismos de actualización y resolución de vulnerabilidades de los componentes de un sistema operativo. - Administrar sistemas de cortafuegos de red. - Instalar, configurar y administrar sistemas de túneles y Redes Privadas Virtuales (VPNs). Arquitecturas Seguras		



- Conocer las distintas arquitecturas informáticas respecto su tolerancia a ataques externos e internos.
- Conocer las implicaciones de seguridad de las distintas topologías de red.
- Conocer, instalar y administrar los distintos modelos de control de acceso a una instalación informática.
- Gestionar políticas de acceso multinivel dependiendo de los tipos de usuario y recursos del sistema.
- Diseñar mecanismos de seguridad multilateral, identificando componentes independientes y minimizando su interdependencia.
- Utilizar y configurar mecanismos y dispositivos de seguridad física.

Seguridad en Comunicaciones Inalámbricas

- Entender las distintas topologías de red inalámbrica y sus características de cara a la seguridad de las arquitecturas informáticas.
- Conocer, gestionar y configurar los distintos elementos de seguridad en redes *Wireless LAN*.
- Conocer, gestionar y configurar los distintos elementos de seguridad en protocolos *Bluetooth*, *NFC* y *RFID*.
- Entender las características de seguridad en las comunicaciones en redes de telefonía móvil y sus implicaciones en la seguridad de arquitecturas informáticas seguras.

5.5.1.3 CONTENIDOS

Sistemas Operativos

- Revisión e historia de los sistemas operativos.
- Principios y bloques fundamentales de los sistemas operativos.
- Concurrencia y multiproceso. Planificación.
- Gestión de memoria. Almacenamiento secundario.
- Entrada y salida.

Redes de Ordenadores

- Introducción a la computación centrada en red.
- Redes y comunicaciones. Topologías.
- Principales protocolos de red.
- Internet como ejemplo de computación cliente- servidor.

Seguridad en Sistemas Operativos y Redes

- Seguridad en sistemas operativos Windows, Linux y MAC.
- Sistemas de autenticación.
- Seguridad en sistemas operativos de dispositivos móviles: Android e iOS.
- Filtros, cortafuegos, topologías, túneles y Redes Privadas Virtuales (VPN).

Arquitecturas Seguras

- Tolerancia frente a ataques.
- Control de accesos.
- Seguridad multinivel y multilateral.
- Seguridad física.

Seguridad en Comunicaciones Inalámbricas

- Topologías de redes inalámbricas.
- Seguridad de *Wireless LAN*.
- Seguridad en *Bluetooth*, *NFC* y *RFID*.
- Seguridad de comunicaciones en redes de telefonía móvil.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías en el campo de la ciberseguridad, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.

CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad.

CG4 - Capacidad para identificar, analizar, peritar y auditar las deficiencias, incidentes, requisitos y riesgos de seguridad de los sistemas de información, a nivel físico, arquitectura, sistema operativo, aplicación y comunicación.

CG5 - Capacidad para identificar e implementar los mecanismos más adecuados para la protección de la información y comunicaciones mediante la comprensión de los riesgos de seguridad de los distintos componentes de un sistema de tecnología de la información.

CG7 - Capacidad para implementar las políticas y planes de gobernanza de la seguridad necesarios para proteger información, sistemas o arquitecturas informáticas tanto a nivel hardware, como software y redes.



CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio		
CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio		
CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía		
5.5.1.5.2 TRANSVERSALES		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje.		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos.		
5.5.1.5.3 ESPECÍFICAS		
CE4 - Conocimientos básicos sobre el uso, configuración y programación de los ordenadores, sistemas operativos, bases de datos y programas informáticos con aplicación en el campo de la ciberseguridad.		
CE6 - Conocimiento y capacidad de gestión de las arquitecturas y protocolos de red que permiten la comunicación de sistemas informáticos tanto a nivel local como de Internet, así como diseñar e implementar aplicaciones basadas en ellas.		
CE10 - Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos conforme a los riesgos de seguridad y las características de la plataforma o entorno de implantación.		
CE12 - Conocer y aplicar los protocolos y sistemas criptográficos de autenticación, identificación y certificación digital, así como capacidad para analizar su idoneidad y aplicabilidad según los requisitos de seguridad de un sistema informático.		
CE14 - Capacidad de administración de los componentes y servicios relacionados con la seguridad de un sistema operativo y su conectividad por red, resolviendo las incidencias que se produzcan y las vulnerabilidades que se detecten.		
CE15 - Entender las particularidades de las comunicaciones inalámbricas respecto a la seguridad, así como tener la capacidad para configurar e implementar las medidas necesarias para la protección de la información transmitida.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	75	100
Recursos didácticos audiovisuales	30	0
Estudio del material básico	260	0
Lectura del material complementario	125	0
Trabajos y casos prácticos	100	0
Test de evaluación	20	0
Laboratorios virtuales	60	16.7
Tutorías	80	30
5.5.1.7 METODOLOGÍAS DOCENTES		
Métodos de enseñanza magistral con mediación tecnológica: aquí se incluirían las clases presenciales virtuales, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.		
Métodos activos: son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje-servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.		



Métodos fundamentados en el aprendizaje individual: estudio personal, aprendizaje acompañado a través de lecturas de material complementario y realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Participación del estudiante	0.0	20.0
Trabajos, laboratorios y/o casos	20.0	40.0
Test de evaluación	0.0	20.0
Examen final	60.0	60.0

NIVEL 2: Detección y Protección frente Ciberataques

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	30

DESPLIEGUE TEMPORAL: Cuatrimestral

ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
	6	12
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
6	6	
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: Amenazas en el Ciberespacio

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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
	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: Técnicas de Hacking y Auditoría de Sistemas		
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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
		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: Ingeniería Inversa 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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
		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: Amenazas Persistentes Avanzadas		



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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
6		
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: Protección de Infraestructuras Críticas		
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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
	6	
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		
Amenazas en el Ciberespacio - Entender y diferenciar las distintas amenazas presentes en el ciberespacio. - Reconocer los tipos de ciberataques y fenómenos dentro del ciberactivismo. - Distinguir los medios empleados por el ciberterrorismo, su alcance, riesgo e implicaciones, además de conocer los agentes involucrados en el mismo. - Identificar incidentes reales de ciberterrorismo y plantear las contramedidas de seguridad necesarias. - Categorizar las aplicaciones y sistemas informáticos objetivo de las distintas amenazas de seguridad, entendiendo la naturaleza de las vulnerabilidades potenciales.		



- Conocer las diferentes acciones llevadas a cabo por los estados u organizaciones para penetrar en los ordenadores y redes de otros países: espionaje, sabotaje, propaganda, perturbación económica y ataque cibernético director.
- Analizar distintos casos de uso en ciber guerra, comprendiendo sus implicaciones tecnológicas y alcance.

Técnicas de Hacking y Auditoría de Sistemas

- Conocer e identificar las técnicas de *Hacking*, sus principios técnicos y dominar las herramientas utilizadas.
- Aplicar técnicas de *Hacking* ético para identificar vulnerabilidades de seguridad en un sistema informático.
- Conocer, instalar y configurar las contramedidas y soluciones necesarias para evitar o solucionar ataques informáticos.
- Conocer y aplicar técnicas de recopilación de información y huella digital sobre un sistema informático, organización o individuo. Desarrollar las contramedidas oportunas.
- Conocer, entender y dominar las herramientas de identificación de vulnerabilidades de Metasploit.
- Desarrollo, personalización y ejecución de *exploits* contra máquinas remotas.
- Implementación de las contramedidas de seguridad contra *exploits*.
- Entender y desarrollar ataques de credenciales de usuario y aplicar las contramedidas oportunas.
- Entender los fundamentos y desarrollo de los test de penetración, identificando fallos, vulnerabilidades y demás errores de seguridad para implementar las contramedidas oportunas.

Ingeniería Inversa y Análisis de Malware

- Conocer las características de los tipos de *malware* y vulnerabilidades asociadas.
- Entender y aplicar técnicas de análisis de *malware*.
- Dominio de las principales herramientas utilizadas para el análisis de *malware*.
- Conocer los distintos comportamientos del *software* malicioso para implementar las contramedidas oportunas.

Amenazas Persistentes Avanzadas

- Conocer e identificar los distintos tipos de amenazas persistentes avanzadas, sus características e implicaciones de seguridad.
- Entender los mecanismos de comando y control frente a las ciberamenazas.
- Conocer los mecanismos de sigilo y evasión utilizados durante los incidentes de amenazas persistentes avanzadas.

Protección de Infraestructuras Críticas

- Comprender las características y requisitos de seguridad de las infraestructuras críticas.
- Entender el concepto de seguridad nacional y los agentes y mecanismos implicados.
- Conocer los requisitos de seguridad en instalaciones industriales.
- Examinar planes de gestión de riesgos y contingencia para infraestructuras críticas.
- Realizar y presentar un análisis crítico de incidentes y respuestas de seguridad en infraestructuras críticas.

5.5.1.3 CONTENIDOS

Amenazas en el Ciberespacio

- Definiciones y alcances del ciberespacio
- Ciberataques y ciberactivismo
- Ciberterrorismo
- Ciber guerra

Técnicas de Hacking y Auditoría de Sistemas

- Footprinting y fingerprinting
- Metasploit
- Ataques a credenciales
- *Pentesting*

Ingeniería Inversa y Análisis de Malware

- Tipologías de *Malware* y vulnerabilidades.
- Comportamientos de *Malware*.
- Técnicas básicas de análisis.
- Técnicas avanzadas de análisis.

Amenazas Persistentes Avanzadas

- Persistencia en sistemas comprometidos.
- Técnicas de comando y control.
- Mecanismos de sigilo y evasión.
- Contramedidas y políticas específicas de protección.

Protección de Infraestructuras Críticas

- Infraestructuras críticas y seguridad nacional.
- Ciberseguridad industrial.
- Gestión de riesgos y planes de contingencia para infraestructuras críticas
- Análisis de incidentes y respuestas a incidentes de ciberseguridad.

5.5.1.4 OBSERVACIONES

Las horas asociadas a la actividad formativa "Laboratorios virtuales", se desarrollan en las asignaturas "Técnicas de Hacking y Auditoría de Sistemas", "Ingeniería Inversa y Análisis de Malware", "Amenazas Persistentes Avanzadas" y "Protección de Infraestructuras Críticas".



5.5.1.5 COMPETENCIAS		
5.5.1.5.1 BÁSICAS Y GENERALES		
CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad.		
CG3 - Capacidad para saber comunicar y transmitir ideas conocimientos, habilidades y destrezas de la profesión en Ciberseguridad a un público tanto especializado como no.		
CG4 - Capacidad para identificar, analizar, peritar y auditar las deficiencias, incidentes, requisitos y riesgos de seguridad de los sistemas de información, a nivel físico, arquitectura, sistema operativo, aplicación y comunicación.		
CG5 - Capacidad para identificar e implementar los mecanismos más adecuados para la protección de la información y comunicaciones mediante la comprensión de los riesgos de seguridad de los distintos componentes de un sistema de tecnología de la información.		
CG6 - Capacidad para concebir, diseñar, redactar, organizar, planificar y gestionar proyectos de ciberseguridad de acuerdo a los requisitos del sistema informático y de la información tratada por el mismo según el marco legislativo vigente.		
CG7 - Capacidad para implementar las políticas y planes de gobernanza de la seguridad necesarios para proteger información, sistemas o arquitecturas informáticas tanto a nivel hardware, como software y redes.		
CG10 - Conocimiento básico de gestión y estructura empresarial e industrial, para identificar, auditar y proteger aquellos procesos o información sensibles desde el punto de vista de la ciberseguridad.		
CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio		
CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio		
CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía		
5.5.1.5.2 TRANSVERSALES		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje.		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos.		
5.5.1.5.3 ESPECÍFICAS		
CE10 - Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos conforme a los riesgos de seguridad y las características de la plataforma o entorno de implantación.		
CE16 - Comprender y gestionar las principales técnicas de ataques de seguridad a nivel de aplicaciones informáticas y comunicaciones para poder diseñar, implementar y desplegar las contramedidas oportunas.		
CE17 - Conocer los distintos tipos de malware y tener la capacidad de analizar sus características en función de su vector de infección, mecanismos de propagación y consecuencias para así diseñar, implementar y desplegar las soluciones de protección necesarias.		
CE18 - Conocer e identificar los procedimientos de ataque informático orquestados por grupos organizados para ser capaz de diseñar e implantar las planes y contramedidas de protección adecuadas.		
CE19 - Comprender las características de las infraestructuras críticas, identificar los riesgos potenciales y capacidad para aplicar las medidas necesarias para su protección según las normativas y legislación vigentes.		
CE23 - Escoger el tipo de auditoría más adecuado para cada contexto, identificando las herramientas más adecuadas para llevarla a cabo y teniendo la capacidad para realizar un análisis crítico y concluyente de los resultados.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	75	100



Recursos didácticos audiovisuales	30	0
Estudio del material básico	260	0
Lectura del material complementario	125	0
Trabajos y casos prácticos	112	0
Test de evaluación	20	0
Laboratorios virtuales	48	16.7
Tutorías	80	30

5.5.1.7 METODOLOGÍAS DOCENTES

Métodos de enseñanza magistral con mediación tecnológica: aquí se incluirían las clases presenciales virtuales, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.

Métodos activos: son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje-servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.

Métodos fundamentados en el aprendizaje individual: estudio personal, aprendizaje acompañado a través de lecturas de material complementario y realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Participación del estudiante	0.0	20.0
Trabajos, laboratorios y/o casos	20.0	40.0
Test de evaluación	0.0	20.0
Examen final	60.0	60.0

NIVEL 2: Seguridad en el Software

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	24

DESPLIEGUE TEMPORAL: Cuatrimestral

ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
		6
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
	6	6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
6		
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: Ingeniería del Software		
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 de Software Seguro		
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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
	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 Web		
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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
		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 Aplicaciones Móviles		
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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
6		
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		
Ingeniería del Software • Integrar las habilidades necesarias para realizar el análisis, modelado, definición y resolución de problemas. • Saber recoger y estructurar información para la confección de requisitos y especificaciones. • Conocer como analizar los sistemas organizativos, realizar un diseño lógico para mejorarlos y desarrollar y analizar alternativas que impliquen la implementación de paquetes, su personalización, la construcción de <i>software</i> o el uso de herramientas CASE. • Identificar y saber aplicar mecanismos para el desarrollo rápido de sistemas de información, tales como prototipos. • Presentar y usar métricas de complejidad y calidad para estimar y valorar el <i>software</i> a desarrollar y mantener. • Saber realizar, evaluar y presentar un plan de proyecto y ser capaz de diseñar tanto su desarrollo como su plan de implementación. • Adquirir y practicar habilidades esenciales de gestión de proyectos, como la gestión de los datos y la información y la identificación de elementos críticos, entre otros. • Saber elegir y utilizar herramientas y métodos de gestión de proyectos <i>software</i>. • Iniciar, diseñar, implementar y discutir la terminación de un proyecto. Desarrollo de Software Seguro		



- Conocer las metodologías de desarrollo de *software* seguro.
- Identificar la metodología de desarrollo de *software* seguro más adecuada según los requisitos de un proyecto de ingeniería del *software*.
- Comprender y presentar los requisitos de seguridad durante el ciclo de vida de un desarrollo *software*.
- Aplicar buenas prácticas desarrollo de *software* seguro.
- Conocer, identificar y solucionar los errores de programación más comunes respecto a la seguridad de una solución informática.
- Aplicar los mecanismos de prueba y validación de *software*, tanto desde el punto de vista funcional como el de la seguridad de la aplicación.

Seguridad en Web

- Conocer las arquitecturas de aplicaciones *web* y entender sus características desde el punto de vista de la seguridad.
- Entender las características concretas del desarrollo de aplicaciones *web* desde el punto de vista de la ingeniería del *software*.
- Identificar las vulnerabilidades de seguridad de las aplicaciones *web* y de los protocolos y lenguajes utilizados.
- Conocer y entender los fundamentos y alcance de los distintos tipos de ataques sufridos por los entornos *web*.
- Utilizar las herramientas de análisis y manipulación orientadas a la identificación de vulnerabilidades *web*.
- Administrar y configurar los servidores *web* de cara a su seguridad, así como cualquier otro tipo de *software* o entorno utilizado por las aplicaciones *web*.
- Integrar los requisitos de seguridad en el proceso de desarrollo de las aplicaciones *web*.

Seguridad en Aplicaciones Móviles

- Conocer los lenguajes y tecnologías utilizadas para el desarrollo de aplicaciones móviles.
- Entender las características concretas del desarrollo de aplicaciones móviles desde el punto de vista de la ingeniería del *software*.
- Identificar los riesgos y vulnerabilidades de seguridad de las aplicaciones *web* dependiendo de su tipología y plataforma de desarrollo.
- Integrar los requisitos de seguridad en el proceso de desarrollo de las aplicaciones móviles.
- Conocer y administrar las restricciones de seguridad y acceso a la información de las distintas plataformas móviles.
- Utilizar los mecanismos para el almacenamiento seguro de datos de las distintas plataformas móviles.
- Conocer el proceso de desarrollo, despliegue y distribución segura de aplicaciones móviles.

5.5.1.3 CONTENIDOS

Ingeniería del *Software*

- Requisitos y especificaciones *software*
- Diseño de *software*
- Herramientas y entornos de diseño de *software*
- Verificación y prueba del *software*
- Mantenimiento y evolución del *software*
- Gestión de la configuración del *software*

Desarrollo de *Software* Seguro

- Metodologías de desarrollo de *software* seguro
- Seguridad en el ciclo de vida del *software*
- Buenas prácticas en el desarrollo de *software* seguro
- Errores de programación

Seguridad en Web

- Vulnerabilidades y protocolos *web*
- Herramientas de análisis y manipulación *web*
- Ataques en entornos *web*
- Instalación de Servidores Web Seguros

Seguridad en Aplicaciones Móviles

- Tipología y características de las aplicaciones móviles
- Restricciones de acceso a la información
- Almacenamiento seguro de datos
- Firmado y empaquetado de aplicaciones

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad.

CG8 - Capacidad para configurar y mantener sistemas, servicios y aplicaciones informáticas de protección de la información y las comunicaciones, o concebir y desarrollar las soluciones informáticas necesarias para dicha protección empleando los métodos de la ingeniería del software como instrumento que garantice su calidad.

CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio



CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio

CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética

CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado

CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

5.5.1.5.2 TRANSVERSALES

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

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

5.5.1.5.3 ESPECÍFICAS

CE9 - Capacidad para analizar, diseñar, construir y mantener aplicaciones de seguridad informática de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados.

CE10 - Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos conforme a los riesgos de seguridad y las características de la plataforma o entorno de implantación.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	60	100
Recursos didácticos audiovisuales	24	0
Estudio del material básico	208	0
Lectura del material complementario	100	0
Trabajos y casos prácticos	80	0
Test de evaluación	16	0
Laboratorios virtuales	48	16.7
Tutorías	64	30

5.5.1.7 METODOLOGÍAS DOCENTES

Métodos de enseñanza magistral con mediación tecnológica: aquí se incluirían las clases presenciales virtuales, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.

Métodos activos: son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje-servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.

Métodos fundamentados en el aprendizaje individual: estudio personal, aprendizaje acompañado a través de lecturas de material complementario y realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Participación del estudiante	0.0	20.0
Trabajos, laboratorios y/o casos	20.0	40.0
Test de evaluación	0.0	20.0
Examen final	60.0	60.0

NIVEL 2: Legislación y Auditoría de la Seguridad



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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
6	6	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: Legislación, Regulación y Cumplimiento		
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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
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: Auditoría Informática		
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



ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
	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: Técnicas Forenses en Sistemas Informáticos		
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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
		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	
5.5.1.1.2 RESULTADOS DE APRENDIZAJE		
Legislación, Regulación y Cumplimiento - Conocer la legislación y marco normativo en el ámbito de la Protección de Datos. - Conocer los derechos de las personas respecto a la protección de datos. - Conocer las disposiciones aplicables a tratamientos concretos. - Identificar las responsabilidades respecto al tratamiento de la información. - Conocer y ser capaz de aplicar códigos de conducta y certificación. - Identificar las principales autoridades de protección de datos. - Aplicar en casos prácticos de la Ley General de Protección de Datos. - Conocer de manera básica de las normativas internacionales. - Interpretar documentación técnica relacionada con la materia. Auditoría Informática - Comprender la necesidad de controles y auditorías de seguridad. - Entender las funciones de un auditor y su metodología de trabajo. - Identificar los distintos procedimientos y herramientas de auditoría y su aplicabilidad a cada caso práctico. - Conocer v aplicar los estándares de auditoría y certificación existentes.		



- Capacidad para redactar y presentar informes de auditoría tanto a una audiencia especializada como no.
- Capacidad para interpretar y comprender documentación sobre los procesos normativos, auditoría y certificación.

Técnicas Forenses en Sistemas Informáticos

- Entender los conceptos básicos de la computación forense. Objetivos y alcance.
- Comprender los procedimientos y actores implicados en el análisis forense.
- Conocer y aplicar las técnicas de análisis forense.
- Conocer y utilizar las herramientas de análisis forense.
- Conocer e identificar las técnicas antiforenses más comunes.
- Capacidad para elaborar y presentar informes con el desarrollo y conclusiones de los análisis forenses tanto a una audiencia especializada como no.

5.5.1.3 CONTENIDOS

Legislación, Regulación y Cumplimiento

- Legislación en protección de datos
- Legislación en sistemas de información y seguridad
- Delincuencia y cibercriminos
- Regulación y cumplimiento

Auditoría Informática

- Fundamentos de la auditoría de los sistemas de información
- Metodología de la auditoría de los sistemas de información
- Procedimientos de una auditoría
- Casos prácticos de auditoría informática.

Técnicas Forenses en Sistemas Informáticos

- Computación forense.
- Normativa, análisis y procedimientos forenses en sistemas informáticos.
- Herramientas de análisis forense en sistemas informáticos.
- Técnicas anti-forense en sistemas informáticos

5.5.1.4 OBSERVACIONES

Las horas asociadas a la actividad formativa "Laboratorios virtuales", se desarrollan en las asignaturas "Auditoría Informática" y "Técnicas Forenses en Sistemas Informáticos".

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG3 - Capacidad para saber comunicar y transmitir ideas conocimientos, habilidades y destrezas de la profesión en Ciberseguridad a un público tanto especializado como no.

CG5 - Capacidad para identificar e implementar los mecanismos más adecuados para la protección de la información y comunicaciones mediante la comprensión de los riesgos de seguridad de los distintos componentes de un sistema de tecnología de la información.

CG6 - Capacidad para concebir, diseñar, redactar, organizar, planificar y gestionar proyectos de ciberseguridad de acuerdo a los requisitos del sistema informático y de la información tratada por el mismo según el marco legislativo vigente.

CG9 - Capacidad para conocer, comprender y aplicar la legislación relativa a ciberseguridad y manejar las especificaciones, reglamentos y normas de obligado cumplimiento de dicho ámbito.

CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio

CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio

CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética

CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado

CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

5.5.1.5.2 TRANSVERSALES

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



CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos.		
5.5.1.5.3 ESPECÍFICAS		
CE11 - Conocer la legislación, normativas y regulaciones aplicables en el área de ciberseguridad, teniendo la capacidad de elaborar el pliego de condiciones técnicas de seguridad de un sistema o infraestructura informático respecto a dicho marco legislativo.		
CE23 - Escoger el tipo de auditoría más adecuado para cada contexto, identificando las herramientas más adecuadas para llevarla a cabo y teniendo la capacidad para realizar un análisis crítico y concluyente de los resultados.		
CE24 - Comprender y desarrollar las técnicas de generación, recopilación y análisis de evidencias digitales en el ámbito del hardware, aplicaciones informáticas, servicios basados en ellas y telecomunicaciones para extraer conclusiones post-incidente y realizar análisis forenses.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	45	100
Recursos didácticos audiovisuales	18	0
Estudio del material básico	156	0
Lectura del material complementario	75	0
Trabajos y casos prácticos	72	0
Test de evaluación	12	0
Laboratorios virtuales	24	16.7
Tutorías	48	30
5.5.1.7 METODOLOGÍAS DOCENTES		
Métodos de enseñanza magistral con mediación tecnológica: aquí se incluirían las clases presenciales virtuales, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.		
Métodos activos: son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje-servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.		
Métodos fundamentados en el aprendizaje individual: estudio personal, aprendizaje acompañado a través de lecturas de material complementario y realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Participación del estudiante	0.0	20.0
Trabajos, laboratorios y/o casos	20.0	40.0
Test de evaluación	0.0	20.0
Examen final	60.0	60.0
NIVEL 2: Gestión de la Seguridad		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	RAMA	MATERIA
Mixta	Ingeniería y Arquitectura	Empresa
ECTS NIVEL2		
ECTS OPTATIVAS	ECTS OBLIGATORIAS	ECTS BÁSICAS
0	12	6
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3



	6	
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
6		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: Fundamentos de la Empresa		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Básica	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: Sistemas de Gestión de Seguridad de la Información		
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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
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: Ciberinteligencia y Gobierno 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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
		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		
Fundamentos de la Empresa - Conocer el papel de la empresa en la economía y las relaciones con su entorno. - Conocer las áreas funcionales de la empresa y su interrelación. - Conocer los fundamentos de la gestión de recursos humanos. - Conocer los trámites para la creación de empresas y las subvenciones posibles, así como el proceso de creación de una empresa desde la idea hasta la puesta en marcha. - Conocer las técnicas de planificación y control organizativo de la empresa. - Diseñar, implantar y efectuar la evaluación de los sistemas de control organizativo. - Análisis de los procedimientos, métodos y soporte documental de las diferentes áreas de la empresa. - Conocer y seleccionar las técnicas matemáticas más adecuadas para la valoración de inversiones y de la financiación. Sistemas de Gestión de Seguridad de la Información - Conocer la familia de normativa ISO en seguridad. - Entender los procesos y actores implicados en los sistemas de análisis de riesgos. - Conocer y aplicar los procedimientos de gestión de riesgo más adecuados según los requisitos de seguridad de un sistema informático. - Conocer los procedimientos de implantación de los sistemas de gestión de la seguridad. - Redactar y presentar proyectos de implantación de sistemas de gestión de seguridad según los requisitos y normativa aplicable tanto a un público especializado como no. - Redactar el pliego de condiciones técnicas de seguridad de un sistema o infraestructura informática. - Diseñar planes de contingencia y contramedidas de protección según los requisitos de seguridad de un sistema informático respecto a los potenciales ataques de los que puede ser objeto por parte tanto de individuos como de grupos organizados. - Redactar y presentar planes de contingencia y continuidad de negocio según los requisitos de seguridad de un sistema informático tanto a un público especializado como no.		



- Ser capaz de concebir, desarrollar e implantar los procedimientos necesarios para implantar sistemas de gestión de la seguridad en empresas, organismos e instituciones.

Ciberinteligencia y Gobierno de la Ciberseguridad

- Entender los conceptos y objetivos de la Ciberinteligencia y el Gobierno de la Seguridad.
- Conocer los mecanismos generales de gobernanza de la Seguridad Informática.
- Conocer las prácticas de Gobierno del Dato, entendiendo su ciclo de vida y actores involucrados.
- Entender las distintas estrategias de Ciberinteligencia dependiendo de la naturaleza de las amenazas de seguridad.
- Estimar los recursos necesarios para la implantación de las estrategias de Ciberinteligencia y Gobierno de la Seguridad.
- Ser capaz de concebir, desarrollar e implantar las políticas necesarias para implantar planes de contingencia y de continuidad de negocio en empresas, organismos e instituciones.
- Ser capaz de redactar y presentar las políticas de gobernanza de la seguridad de una empresa, organismo o institución tanto a un público especializado como no.
- Conocer los procesos de análisis utilizados en la Ciberinteligencia.
- Comprender las distintas fases del ciclo de Ciberinteligencia.
- Conocer los procesos de Inteligencia de Fuentes Abiertas (OSINT) y utilizar las herramientas asociadas.
- Conocer los procesos de Inteligencia Basada en Redes Sociales (SOCMINT) y utilizar las herramientas asociadas.

5.5.1.3 CONTENIDOS

Fundamentos de la Empresa

- Concepto y tipos de empresa.
- Papel de la empresa en el sistema económico.
- Fundamentos básicos de dirección y planificación en las empresas.
- Procedimientos organizativos de empresas.
- Mecanismos y técnicas de financiación de la empresa.

Sistemas de Gestión de Seguridad de la Información

- Familia de normas ISO en seguridad informática.
- Gestión de proyectos de ciberseguridad. Elaboración de pliegos de condiciones técnicas. Procesos y procedimientos.
- Implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) y controles.
- Planes de contingencia y de continuidad de negocio.

Ciberinteligencia y Gobierno de la Ciberseguridad

- Mecanismos de gobernanza de la seguridad informática.
- Gobierno del dato. Ciclo de vida. Trazabilidad y calidad.
- Políticas, objetivos y estrategias de ciberinteligencia. Unidades de ciberinteligencia en la empresa y marco jurídico.
- Herramientas, procesos de análisis, y fases del ciclo de ciberinteligencia OSINT/SOCMINT.

5.5.1.4 OBSERVACIONES

Las horas asociadas a la actividad formativa "Laboratorios virtuales", se desarrollan en las asignaturas "Sistemas de Gestión de Seguridad de la Información" y "Ciberinteligencia y Gobierno de la Ciberseguridad".

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG3 - Capacidad para saber comunicar y transmitir ideas conocimientos, habilidades y destrezas de la profesión en Ciberseguridad a un público tanto especializado como no.

CG6 - Capacidad para concebir, diseñar, redactar, organizar, planificar y gestionar proyectos de ciberseguridad de acuerdo a los requisitos del sistema informático y de la información tratada por el mismo según el marco legislativo vigente.

CG7 - Capacidad para implementar las políticas y planes de gobernanza de la seguridad necesarios para proteger información, sistemas o arquitecturas informáticas tanto a nivel hardware, como software y redes.

CG9 - Capacidad para conocer, comprender y aplicar la legislación relativa a ciberseguridad y manejar las especificaciones, reglamentos y normas de obligado cumplimiento de dicho ámbito.

CG10 - Conocimiento básico de gestión y estructura empresarial e industrial, para identificar, auditar y proteger aquellos procesos o información sensibles desde el punto de vista de la ciberseguridad.

CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio

CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio

CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética



CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado

CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

5.5.1.5.2 TRANSVERSALES

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

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

5.5.1.5.3 ESPECÍFICAS

CE11 - Conocer la legislación, normativas y regulaciones aplicables en el área de ciberseguridad, teniendo la capacidad de elaborar el pliego de condiciones técnicas de seguridad de un sistema o infraestructura informático respecto a dicho marco legislativo.

CE18 - Conocer e identificar los procedimientos de ataque informático orquestados por grupos organizados para ser capaz de diseñar e implantar las planes y contramedidas de protección adecuadas.

CE20 - Conocer, utilizar y aplicar sistemas de gestión, análisis de riesgo e implantación de planes de contingencia relacionados con la seguridad de la información.

CE21 - Conocimiento adecuado del concepto de empresa, marco institucional y jurídico de la empresa. Organización y gestión de empresas.

CE22 - Entender, diseñar y desarrollar planes directores de seguridad informática que tengan en cuenta los marcos de referencia normativos, ciclos de vida de las políticas y la planificación de recursos necesarios.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	45	100
Recursos didácticos audiovisuales	18	0
Estudio del material básico	156	0
Lectura del material complementario	75	0
Trabajos y casos prácticos	72	0
Test de evaluación	12	0
Laboratorios virtuales	24	16.7
Tutorías	48	30

5.5.1.7 METODOLOGÍAS DOCENTES

Métodos de enseñanza magistral con mediación tecnológica: aquí se incluirían las clases presenciales virtuales, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.

Métodos activos: son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje-servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.

Métodos fundamentados en el aprendizaje individual: estudio personal, aprendizaje acompañado a través de lecturas de material complementario y realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Participación del estudiante	0.0	20.0
Trabajos, laboratorios y/o casos	20.0	40.0
Test de evaluación	0.0	20.0
Examen final	60.0	60.0



NIVEL 2: Optativas		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
ECTS NIVEL 2	24	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
	24	
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 MENCIONES		
No existen datos		
NIVEL 3: Criptografía Avanzada		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Optativa	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
	6	
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 MENCIONES		
No existen datos		
NIVEL 3: Inteligencia Artificial Aplicada a la Ciberseguridad		



5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Optativa	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
	6	
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 MENCIONES		
No existen datos		
NIVEL 3: Análisis de Redes Sociales		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Optativa	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
	6	
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 MENCIONES		
No existen datos		
NIVEL 3: Comunicación y Liderazgo		
5.5.1.1.1 Datos Básicos del Nivel 3		



CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Optativa	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
	6	
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 MENCIONES		
No existen datos		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
Criptografía Avanzada - Conocer los principales protocolos de criptografía avanzada. - Entender las técnicas de criptografía basada en identidad y biométrica. - Conocer las técnicas de cifrado homomórfico. - Conocer las técnicas de criptografía poscuántica. - Entender las técnicas de criptografía ligera y computación multiparte segura. - Valorar la aplicabilidad de las técnicas de criptografía avanzada para la seguridad de sistemas informáticos. Inteligencia Artificial Aplicada a la Ciberseguridad - Entender los distintos tipos de inteligencia artificial, posibilidades y alcance. - Conocer las principales técnicas de aprendizaje automático. - Aplicar técnicas de aprendizaje no supervisado sobre conjuntos de datos y registros de los sistemas de seguridad informática. - Crear modelos de predicción y clasificación supervisados sobre conjuntos de datos y registros de sistemas de seguridad informática. - Conocer los mecanismos de validación cruzada. - Conocer las principales métricas de evaluación de los sistemas de aprendizaje automático y tener la capacidad de interpretar los resultados. Análisis de Redes Sociales - Conocer las características y propiedades del análisis de redes sociales. - Obtener las principales métricas de análisis de redes sociales. - Aplicar algoritmos de visualización y poda sobre redes sociales. - Entender y aplicar algoritmos de detección de comunidades en redes sociales. - Comprender las dinámicas de evolución de comportamientos y eventos en redes sociales. Comunicación y Liderazgo - Conocer las herramientas necesarias para mejorar sus habilidades de comunicación y liderazgo. - Conocer y entender el manejo adecuado de las técnicas y herramientas para una comunicación efectiva y asertiva. - Conocer y entender las relaciones interpersonales y el manejo adecuado de conflictos.		
5.5.1.3 CONTENIDOS		
Criptografía Avanzada - Protocolos criptográficos. - Criptografía basada en identidad y biometría. - Cifrado homomórfico y criptografía poscuántica. - Criptografía ligera y computación multiparte Segura (SMPC).		



Inteligencia Artificial Aplicada a la Ciberseguridad

- Introducción a la inteligencia artificial y aprendizaje automático.
- Técnicas de aprendizaje no supervisado.
- Técnicas de aprendizaje supervisado.
- Evaluación y análisis de resultados.

Análisis de Redes Sociales

- Introducción y propiedades.
- Algoritmos de visualización y poda.
- Detección de comunidades.
- Dinámica de las redes.

Comunicación y Liderazgo

- Fundamentos y elementos principales de la comunicación, la seriedad y el liderazgo.
- Enfoques sobre liderazgo y administración.
- Credibilidad y liderazgo.
- Comunicación, conflicto y liderazgo.
- Herramientas y técnicas de soporte.

5.5.1.4 OBSERVACIONES

Los estudiantes obtendrán las siguientes competencias adicionales descritas, según cursen cada una de las asignaturas optativas.

Criptografía Avanzada

CE26: Conocer y ser capaz de aplicar de sistemas criptográficos avanzados para la protección de la información y la autenticación de usuarios.

Inteligencia Artificial Aplicada a la Ciberseguridad

CE27: Conocer las técnicas de Aprendizaje Automático, tanto supervisadas como no supervisadas, para la realización y evaluación de sistemas de predicción y clasificación de amenazas de seguridad.

Análisis de Redes Sociales

CE28: Capacidad de analizar la estructura y comportamiento dentro de distintos tipos de redes sociales, identificando los principales riesgos o amenazas potenciales.

Comunicación y Liderazgo

CE29: Capacidad para comprender la importancia de la negociación, los hábitos de trabajo efectivos, el liderazgo y las habilidades de comunicación en los entornos de uso de datos masivos.

Las horas dedicadas a la actividad formativa "Laboratorios virtuales" están asignadas a las asignaturas "Criptografía Avanzada", "Inteligencia Artificial Aplicada a la Ciberseguridad" y "Análisis de Redes Sociales".

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG3 - Capacidad para saber comunicar y transmitir ideas conocimientos, habilidades y destrezas de la profesión en Ciberseguridad a un público tanto especializado como no.

CG4 - Capacidad para identificar, analizar, peritar y auditar las deficiencias, incidentes, requisitos y riesgos de seguridad de los sistemas de información, a nivel físico, arquitectura, sistema operativo, aplicación y comunicación.

CG5 - Capacidad para identificar e implementar los mecanismos más adecuados para la protección de la información y comunicaciones mediante la comprensión de los riesgos de seguridad de los distintos componentes de un sistema de tecnología de la información.

CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio

CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio

CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética

CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado



CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía		
5.5.1.5.2 TRANSVERSALES		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje.		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos.		
5.5.1.5.3 ESPECÍFICAS		
No existen datos		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	60	100
Recursos didácticos audiovisuales	24	0
Estudio del material básico	208	0
Lectura del material complementario	100	0
Trabajos y casos prácticos	92	0
Test de evaluación	16	0
Laboratorios virtuales	36	16.7
Tutorías	64	30
5.5.1.7 METODOLOGÍAS DOCENTES		
Métodos de enseñanza magistral con mediación tecnológica: aquí se incluirían las clases presenciales virtuales, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.		
Métodos activos: son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje-servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.		
Métodos fundamentados en el aprendizaje individual: estudio personal, aprendizaje acompañado a través de lecturas de material complementario y realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Participación del estudiante	0.0	20.0
Trabajos, laboratorios y/o casos	20.0	40.0
Test de evaluación	0.0	20.0
Examen final	60.0	60.0
NIVEL 2: Prácticas en Empresa		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
	6	



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 MENCIONES		
No existen datos		
NIVEL 3: Prácticas en Empresa		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Optativa	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
	6	
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 MENCIONES		
No existen datos		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
Al finalizar las Prácticas en Empresa, el estudiante será capaz de: • Aplicar programas especializados en entornos reales. • Utilizar de forma crítica sus conocimientos en ciberseguridad para su aplicación en casos reales y para el desarrollo de recursos digitales.		
5.5.1.3 CONTENIDOS		
Realización de labores básicas relacionadas con los contenidos del Grado, 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 estudiante. Los detalles de las tareas a desarrollar por el estudiante durante el periodo de prácticas en la empresa serán acordes a lo indicado en el proyecto formativo que la universidad facilitará al centro de prácticas. Dentro de este marco, los detalles de las tareas concretas a realizar por el estudiante, serán fijadas por el Tutor de Prácticas Externas y se adaptarán a las peculiaridades propias de cada centro.		
5.5.1.4 OBSERVACIONES		



Competencias

La materia no tiene competencias específicas asignadas. No obstante, los estudiantes que opten por esta asignatura también adquirirán las siguientes competencias específicas:

CPE-01 - Capacidad para aplicar las competencias y conocimientos adquiridos en el Grado en una situación concreta dentro de un ámbito laboral.

CPE-02 - Capacidad para integrarse en un entorno laboral y hacerse responsable de tareas relacionadas con las competencias y conocimientos propios de la Ciberseguridad.

Desarrollo de las prácticas

Dado que cada vez es más común en las grandes empresas la actividad laboral mediante teletrabajo, se contemplará la realización de prácticas en esta modalidad en determinadas circunstancias que evaluará la dirección del grado.

En relación a la actividad formativa "Estancia en Centro", su presencialidad depende de la opción elegida por el estudiante pudiendo realizar estas prácticas de manera virtual o físicamente en el centro. En el caso de que el estudiante elija la opción virtual o de teletrabajo, existirá una presencia síncrona entre estudiante y tutor de prácticas en el centro, que dependerá de las tareas o proyectos realizados por el estudiante en el centro de prácticas, no pudiendo ser cuantificada *a priori*.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías en el campo de la ciberseguridad, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.

CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad.

CG3 - Capacidad para saber comunicar y transmitir ideas conocimientos, habilidades y destrezas de la profesión en Ciberseguridad a un público tanto especializado como no.

CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio

5.5.1.5.2 TRANSVERSALES

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

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

5.5.1.5.3 ESPECÍFICAS

No existen datos

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	3	100
Estancia en Centro	96	100
Redacción de la memoria de prácticas	27	0
Lectura de documentación del centro de prácticas	9	0
Tutorías (Prácticas)	15	100

5.5.1.7 METODOLOGÍAS DOCENTES

Métodos activos: son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje-servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.

Métodos fundamentados en el aprendizaje individual: estudio personal, aprendizaje acompañado a través de lecturas de material complementario y realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
-----------------------	--------------------	--------------------



Evaluación según el informe del tutor externo	40.0	40.0
Memoria de prácticas	60.0	60.0
NIVEL 2: Trabajo Fin de Grado		
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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
	12	
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 MENCIONES		
No existen datos		
NIVEL 3: Trabajo Fin de Grado		
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
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
	12	
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

Trabajo Fin de Grado

- Analizar un problema y relacionarlo con los conocimientos adquiridos.
- Descomponer un problema complejo en unidades de menor complejidad que permitan abordarlo de forma apropiada.
- Planificar y organizar temporalmente de las tareas de un problema complejo.
- Buscar información que ayude a resolver partes del problema de los que no se conoce la solución.
- Analizar, seleccionar y utilizar diferentes tecnologías de la información, herramientas y metodologías de desarrollo necesarias para resolver el problema.
- Saber buscar y adquirir nuevos conocimientos y habilidades necesarios para resolver parte del problema.
- Evaluar de forma rigurosa los resultados de la resolución del problema.
- Redactar una memoria científico-técnica del trabajo realizado, de acuerdo a estándares profesionales.
- Comunicar los resultados de la resolución del problema, los conocimientos adquiridos y argumentar la solución propuesta, contrastándola con otras posibles.

5.5.1.3 CONTENIDOS

Trabajo Fin de Grado

Esta materia no tiene contenidos específicos, pero en todos los casos el trabajo realizado tendrá un carácter aplicado y deberá implicar la realización de actividades técnicas y de gestión de proceso, la redacción de una memoria y la defensa ante una comisión evaluadora y se deberán ejercitar competencias adquiridas en el resto de las asignaturas del grado.

El trabajo fin de grado permitirá aplicar, en función de su temática, diferentes competencias específicas del grado, y deberá tener en cuenta los criterios de elaboración profesional recogidos en las competencias generales del grado.

Las características del trabajo, los tipos de trabajo, estructura y demás características estarán publicadas en la plataforma de aprendizaje.

5.5.1.4 OBSERVACIONES

El estudiante reforzará, dentro de las competencias asignadas a esta materia, las correspondientes al tema del Trabajo Fin de Grado realizado en cada caso.

El trabajo fin de grado se realiza individualmente o de manera grupal, con el seguimiento continuo por parte de un profesor-director de TFG, durante la elaboración de este.

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

Elaboración

En el caso de que el trabajo fin de grado 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 TFG asegurará un correcto **seguimiento individual** de cada uno de los integrantes del grupo a través de **tutorías individuales (3 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 (3 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 TFG 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 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 TFG 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 TFG 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 TFG 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 la comisión evaluadora podrá dirigir las cuestiones que 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 grado la ponderación de los sistemas de evaluación, es la siguiente:

SISTEMA DE EVALUACIÓN	PONDERACIÓN
Evaluación de la estructura del Trabajo Fin de Grado	20 %
Evaluación de la exposición del Trabajo Fin de Grado	30 %



Evaluación del contenido individual del Trabajo Fin de Grado		50 %
La evaluación final, por tanto, tiene dos componentes: uno individual y otro grupal. Individual: "Evaluación de la exposición del Trabajo Fin de Grado". 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 Grado". 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 Grado". Representa el 20 % de la calificación final y, dado que, la estructura del TFG 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		
CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad.		
CG3 - Capacidad para saber comunicar y transmitir ideas conocimientos, habilidades y destrezas de la profesión en Ciberseguridad a un público tanto especializado como no.		
CG9 - Capacidad para conocer, comprender y aplicar la legislación relativa a ciberseguridad y manejar las especificaciones, reglamentos y normas de obligado cumplimiento de dicho ámbito.		
CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio		
CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio		
CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía		
5.5.1.5.2 TRANSVERSALES		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje.		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos.		
5.5.1.5.3 ESPECÍFICAS		
CE25 - Capacidad para elaborar un trabajo original y estructurado, consistente en un proyecto en el ámbito de Ciberseguridad en el que se sintetizan e integran las competencias adquiridas en enseñanzas del título.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesión inicial de presentación de Trabajo Fin de Grado	2	100
Lectura de material en el aula virtual (TFG)	5	0
Tutorías (TFG)	6	100
Sesiones grupales de Trabajo Fin de Grado	3	100
Elaboración del Trabajo Fin de Grado	284	0



5.5.1.7 METODOLOGÍAS DOCENTES

Métodos activos: son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje-servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.

Métodos fundamentados en el aprendizaje individual: estudio personal, aprendizaje acompañado a través de lecturas de material complementario y realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación de la estructura del Trabajo Fin de Grado	20.0	20.0
Evaluación de la exposición del Trabajo Fin de Grado	30.0	30.0
Evaluación del contenido individual del Trabajo Fin de Grado	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	30	100	30
Universidad Internacional de La Rioja	Profesor Asociado (incluye profesor asociado de C.C.: de Salud)	20	100	20
Universidad Internacional de La Rioja	Ayudante	50	0	50
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 %
65	30	85
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		
8.2 Procedimiento general para valorar el progreso y los resultados de aprendizaje La política de calidad de 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 Interno 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 <i>Manual de calidad</i> y sus procedimientos. La estructura definida en el <i>Manual de calidad</i> 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). Para garantizar el adecuado funcionamiento del SAIC se han establecido diferentes instrumentos de seguimiento que aparecen recogidos en el procedimiento PA-5-1.2 donde se describe cómo se realiza la medición, el análisis de los resultados y la mejora continua: - 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 (DA-5-1.2-1 Informe Anual de la Unidad de Calidad de titulación y DA-5-1.2-3 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. En particular, y adaptado a esta titulación y a estos resultados el procedimiento es el siguiente: Tras cada periodo de evaluación, a través de la aplicación informática de informes de calidad, la 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, estudiantes y la propia coordinación) 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 (PA-5-3 Procedimiento para la aprobación/modificación de procedimientos y control de la documentación). 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 (DA-5-1.2-1 Informe Anual de la Unidad de Calidad de titulación y DA-5-1.2-3 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.6.2 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 la 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	2021
Ver Apartado 10: Anexo 1.	
10.2 PROCEDIMIENTO DE ADAPTACIÓN	
No aplicable.	
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
47027774L	Pablo	Moreno	Ger
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 de la Escuela Superior de Ingeniería y Tecnología
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
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_Justificación+alegaciones.pdf

HASH SHA1 :4C3CA7054764FBB44D4558318EB05847C0D129C7

Código CSV :439572943962522391401910

Ver Fichero: 2_Justificación+alegaciones.pdf



Apartado 4: Anexo 1

Nombre :4.1_Sistemas de información previo.pdf

HASH SHA1 :A5D119DA3E8397F66164B6518DADD78E42EBFE4B

Código CSV :426428253123374255920784

Ver Fichero: 4.1_Sistemas de información previo.pdf



Apartado 5: Anexo 1

Nombre :5.1_Planificación de las enseñanzas.pdf

HASH SHA1 :97F9D98CAE734C28C98CBFE49171EEF1054C8C96

Código CSV :439573131030810089218387

Ver Fichero: 5.1_Planificación de las enseñanzas.pdf



Apartado 6: Anexo 1

Nombre :6.1_Profesorado.pdf

HASH SHA1 :CCF80B7E404E0515A5165029DB9EAAF9F2EED7EE

Código CSV :439819569189488353864089

Ver Fichero: 6.1_Profesorado.pdf



Apartado 6: Anexo 2

Nombre :6.2_Otros recursos humanos.pdf

HASH SHA1 :E98973586639E7E0CFF85D5303581D096FC15D42

Código CSV :439575586201144766680467

Ver Fichero: 6.2_Otros recursos humanos.pdf



Apartado 7: Anexo 1

Nombre :7_Recursos materiales y servicios.pdf

HASH SHA1 :237A4DED68096622D9E1CAB4E4F091A3A96EA197

Código CSV :439360645776905779197778

Ver Fichero: 7_Recursos materiales y servicios.pdf



Apartado 8: Anexo 1

Nombre :8.1_Estimación de valores cuantitativos.pdf

HASH SHA1 :83128EFFCA3CC57636215BACB4B929A7B8F0D295

Código CSV :426272135909799019524691

Ver Fichero: 8.1_Estimación de valores cuantitativos.pdf



Apartado 10: Anexo 1

Nombre :10_Calendario de implantación.pdf

HASH SHA1 :9F2C1B636540557A383C4BAD271375F35B00AFFF

Código CSV :426272184074669133440485

Ver Fichero: 10_Calendario de implantación.pdf



Apartado 11: Anexo 1

Nombre :Delegacion_Representante_Legal_PABLO_GUZMAN_18052016.pdf

HASH SHA1 :696FC98FF975A5B37661B7B0E2045AAC3B731F8C

Código CSV :426365651506682229810209

Ver Fichero: Delegacion_Representante_Legal_PABLO_GUZMAN_18052016.pdf



