

## IMPRESO SOLICITUD PARA VERIFICACIÓN DE TÍTULOS OFICIALES

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

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

UNIVERSIDAD SOLICITANTE		CENTRO	CÓDIGO CENTRO
Universidad Internacional de La Rioja		Escuela Superior de Ingeniería y Tecnología	26004007
NIVEL		DENOMINACIÓN CORTA	
Grado		Ciberseguridad	
DENOMINACIÓN ESPECÍFICA			
Graduado o Graduada en Ciberseguridad por la Universidad Internacional de La Rioja			
NIVEL MECES			
2			
RAMA DE CONOCIMIENTO		ÁMBITO DE CONOCIMIENTO	CONJUNTO
Ingeniería y Arquitectura		Ingeniería informática y de sistemas	No
SOLICITANTE			
NOMBRE Y APELLIDOS		CARGO	
Virginia Montiel Martín		Responsable de programas ANECA	
REPRESENTANTE LEGAL			
NOMBRE Y APELLIDOS		CARGO	
Juan Pablo Guzmán Palomino		Secretario General	
RESPONSABLE DEL TÍTULO			
NOMBRE Y APELLIDOS		CARGO	
Oscar Sanjuan Martínez		Director de la Escuela Superior de Ingeniería y Tecnología	
2. DIRECCIÓN A EFECTOS DE NOTIFICACIÓN			
A los efectos de la práctica de la NOTIFICACIÓN de todos los procedimientos relativos a la presente solicitud, las comunicaciones se dirigirán a la dirección que figure en el presente apartado.			
DOMICILIO		CÓDIGO POSTAL	MUNICIPIO
Avenida de la Paz, 137		26006	Logroño
E-MAIL		PROVINCIA	TELÉFONO
virginia.montiel@unir.net		La Rioja	676614276
E-MAIL		PROVINCIA	FAX
virginia.montiel@unir.net		La Rioja	902877037
3. PROTECCIÓN DE DATOS PERSONALES			
De acuerdo con lo previsto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se informa que los datos solicitados en este impreso son necesarios para la tramitación de la solicitud y podrán ser objeto de tratamiento automatizado. La responsabilidad del fichero automatizado corresponde al Consejo de Universidades. Los solicitantes, como cedentes de los datos podrán ejercer ante el Consejo de Universidades los derechos de información, acceso, rectificación y cancelación a los que se refiere el Título III de la citada Ley Orgánica 3/2018, de 5 de diciembre.			
El solicitante declara conocer los términos de la convocatoria y se compromete a cumplir los requisitos de la misma, consintiendo expresamente la notificación por medios telemáticos a los efectos de lo dispuesto en el artículo 43 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.			
		En: La Rioja, AM 14 de noviembre de 2024	
		Firma: Representante legal de la Universidad	



# 1. DESCRIPCIÓN, OBJETIVOS FORMATIVOS Y JUSTIFICACIÓN DEL TÍTULO

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

NIVEL	DENOMINACIÓN ESPECÍFICA	CONJUNTO	CONVENIO	CONV. ADJUNTO
Grado	Graduado o Graduada en Ciberseguridad por la Universidad Internacional de La Rioja	No		Ver Apartado 1: Anexo 1.
<b>RAMA</b>				
Ingeniería y Arquitectura				
<b>ÁMBITO</b>				
Ingeniería informática y de sistemas				
<b>AGENCIA EVALUADORA</b>				
Agencia Nacional de Evaluación de la Calidad y Acreditación				
<b>LISTADO DE MENCIONES</b>				
No existen datos				
<b>MENCIÓN DUAL</b>				
No				

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

<b>UNIVERSIDAD SOLICITANTE</b>		
Universidad Internacional de La Rioja		
<b>LISTADO DE UNIVERSIDADES</b>		
CÓDIGO	UNIVERSIDAD	
077	Universidad Internacional de La Rioja	
<b>LISTADO DE UNIVERSIDADES EXTRANJERAS</b>		
CÓDIGO	UNIVERSIDAD	
No existen datos		
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

### 1.4-1.9 Universidad Internacional de La Rioja

#### 1.4-1.9.1 CENTROS EN LOS QUE SE IMPARTE

<b>LISTADO DE CENTROS</b>			
CÓDIGO	CENTRO	CENTRO RESPONSABLE	CENTRO ACREDITADO INSTITUCIONALMENTE
26004007	Escuela Superior de Ingeniería y Tecnología	Si	Si

#### 1.4-1.9.2 Escuela Superior de Ingeniería y Tecnología

##### 1.4-1.9.2.1 Datos asociados al centro

<b>MODALIDADES DE ENSEÑANZA EN LAS QUE SE IMPARTE EL TÍTULO</b>		
PRESENCIAL	SEMIPRESENCIAL/HÍBRIDA	A DISTANCIA/VIRTUAL
No	No	Si
<b>PLAZAS POR MODALIDAD</b>		
		600
NÚMERO TOTAL DE PLAZAS	NÚMERO DE PLAZAS DE NUEVO INGRESO PARA PRIMER CURSO	
2400	600	
<b>IDIOMAS EN LOS QUE SE IMPARTE</b>		



CASTELLANO	CATALÁN	EUSKERA
Sí	No	No
GALLEGO	VALENCIANO	INGLÉS
No	No	No
FRANCÉS	ALEMÁN	PORTUGUÉS
No	No	No
ITALIANO	OTRAS	
No	No	

## 1.10 JUSTIFICACIÓN

### JUSTIFICACIÓN DEL INTERÉS DEL TÍTULO Y CONTEXTUALIZACIÓN

Ver Apartado 1: Anexo 6.

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

### OBJETIVOS FORMATIVOS

El objetivo principal del Grado en Ciberseguridad es formar profesionales que puedan ejercer en el amplio abanico de salidas laborales existentes en el área de seguridad de las tecnologías de la información, siendo capaces de identificar, proteger, detectar, gestionar, peritar y auditar la gran variedad de incidentes y amenazas a las que se enfrentan las redes y sistemas de información utilizados por individuos, empresas e instituciones.

### ESTRUCTURAS CURRICULARES ESPECÍFICAS Y ESTRATEGIAS METODOLÓGICAS DE INNOVACIÓN DOCENTE

## 1.14 PERFILES FUNDAMENTALES DE EGRESO Y PROFESIONES REGULADAS

### PERFILES DE EGRESO

<https://static.unir.net/ingenieria/grado-ciberseguridad/1.14.pdf>

### HABILITA PARA EL EJERCICIO DE PROFESIONES REGULADAS

No

### NO ES CONDICIÓN DE ACCESO PARA TÍTULO PROFESIONAL

## 2. RESULTADOS DEL PROCESO DE FORMACIÓN Y DE APRENDIZAJE

### RESULTADOS DEL PROCESO DE FORMACIÓN Y DE APRENDIZAJE

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. TIPO: Conocimientos o contenidos

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. TIPO: Competencias

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. TIPO: Habilidades o destrezas

CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Habilidades o destrezas

CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. TIPO: Habilidades o destrezas

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. TIPO: Habilidades o destrezas

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. TIPO: Competencias

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. TIPO: Conocimientos o contenidos

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. TIPO: Competencias



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. TIPO: Conocimientos o contenidos
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. TIPO: Competencias
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. TIPO: Competencias
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. TIPO: Competencias
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. TIPO: Conocimientos o contenidos
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. TIPO: Competencias
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. TIPO: Conocimientos o contenidos
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. TIPO: Conocimientos o contenidos
CE20 - Conocer, utilizar y aplicar sistemas de gestión, análisis de riesgo e implantación de planes de contingencia relacionados con la seguridad de la información. TIPO: Competencias
CE21 - Conocimiento adecuado del concepto de empresa, marco institucional y jurídico de la empresa. Organización y gestión de empresas. TIPO: Conocimientos o contenidos
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. TIPO: Competencias
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. TIPO: Competencias
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. TIPO: Competencias
CE25 - Capacidad para elaborar un trabajo original y estructurado, consistente en un proyecto en el ámbito de Ciberseguridad en el que se sinteticen e integren los conocimientos, habilidades y capacidades adquiridos en enseñanzas del título. TIPO: Competencias
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. TIPO: Conocimientos o contenidos
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. TIPO: Conocimientos o contenidos
CE5 - Conocimiento y aplicación de los principios y técnicas fundamentales de paradigmas y lenguajes de programación avanzados utilizados en la administración de sistemas informáticos. TIPO: Conocimientos o contenidos
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 TIPO: Conocimientos o contenidos
CE7 - Conocer, comprender y evaluar la estructura y arquitectura de los computadores, así como los componentes básicos que los conforman para conocer los vectores de ataque derivados del hardware y el firmware. TIPO: Conocimientos o contenidos
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. TIPO: Conocimientos o contenidos
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. TIPO: Competencias
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. TIPO: Conocimientos o contenidos



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. TIPO: Conocimientos o contenidos
CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad. TIPO: Habilidades o destrezas
CG3 - Capacidad para saber comunicar y transmitir ideas conocimientos, habilidades y destrezas de la profesión en Ciberseguridad a un público tanto especializado como no. TIPO: Habilidades o destrezas
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. TIPO: Competencias
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. TIPO: Competencias
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. TIPO: Competencias
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. TIPO: Competencias
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. TIPO: Competencias
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. TIPO: Conocimientos o contenidos
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas

### 3. ADMISIÓN, RECONOCIMIENTO Y MOVILIDAD

#### 3.1 REQUISITOS DE ACCESO Y PROCEDIMIENTOS DE ADMISIÓN

##### 3.1 Requisitos de acceso y procedimientos de admisión de estudiantes.

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

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

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

La admisión al título se ajustará al Real Decreto 412/2014 534/2024 que regula tanto los requisitos de admisión a las enseñanzas universitarias oficiales de Grado como la prueba de acceso a la Universidad y la normativa básica de los procedimientos de admisión

Según la disposición transitoria única de este Real Decreto, en los procedimientos de admisión a las enseñanzas universitarias oficiales de Grado para el curso 2024-2025 seguirá siendo de aplicación lo dispuesto 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.

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 534/2024 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.

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

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

[https://static.unir.net/documentos/reglamento\\_acceso\\_admision\\_e\\_o\\_unir.pdf](https://static.unir.net/documentos/reglamento_acceso_admision_e_o_unir.pdf)

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

### 3.2 CRITERIOS PARA EL RECONOCIMIENTO Y TRANSFERENCIAS DE CRÉDITOS

#### Reconocimiento de Créditos Cursados en Enseñanzas Superiores Oficiales no Universitarias

MÍNIMO	MÁXIMO
0	30

#### Adjuntar Convenio

#### Reconocimiento de Créditos Cursados en Títulos Propios

MÍNIMO	MÁXIMO
0	36

#### Adjuntar Título Propio

Ver Apartado 3: Anexo 2.

#### Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional

MÍNIMO	MÁXIMO
0	36

#### DESCRIPCIÓN

### 3.2. Criterios para el reconocimiento y transferencia de créditos

#### 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.

Se incluye enlace de descarga al Convenio de Colaboración para el Reconocimiento de Créditos firmado con la Consejería de Educación, Cultura, Deporte y Juventud del Gobierno de La Rioja (31 de mayo de 2023), para el reconocimiento de créditos entre los títulos de Técnico Superior, impartidos en la Comunidad Autónoma de La Rioja, y los títulos de Grado, impartidos en la Universidad Internacional de La Rioja: <https://bit.ly/409Z281>

El resumen de dicho convenio fue publicado el 01 de agosto de 2023 en el Boletín Oficial de La Rioja: <https://bit.ly/3StDPV1>

En dicho Convenio se indica:

#se garantizará el reconocimiento mínimo de acuerdo con lo previsto en el Anexo I del Real Decreto 1618/2011#

(  
)

#Cuando entre dos estudios se haya determinado la existencia de relación directa, procederá el reconocimiento mínimo que prevé el Anexo I del Real Decreto 1618/2011.#



Se listan en el Anexo I del citado convenio los títulos de Técnico Superior, impartidos en la Comunidad Autónoma de La Rioja, con relación directa con el Grado para los que se contempla el reconocimiento mínimo de 30 ECTS indicado en el Real Decreto 1618/2011.

Así, por ejemplo, en dicho listado se contempla el reconocimiento del siguiente Ciclo Formativo:

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

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 / Nº 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
	<b>ECTS reconocidos: 30</b>

A efectos de esta tabla, se ha tenido en cuenta el currículum 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:

- **Lej 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 o de formación permanente**

De acuerdo con lo establecido en el art. 10.4, del Real Decreto 822/2021, de 28 de septiembre podrán ser objeto de reconocimiento los créditos cursados en enseñanzas universitarias conducentes a la obtención de títulos propios. 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 10.5 del Real Decreto 822/2021, 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.

**Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional**



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

El Real Decreto 822/2021 fija el límite máximo de reconocimiento a partir de experiencia profesional o laboral en el 15 % del total de créditos que constituyen el plan de estudios. En el caso de un 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 los mismos resultados del proceso de formación y aprendizaje que se adquieren con las asignaturas reconocidas, podrán ser objeto de reconocimiento por experiencia profesional y laboral 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 RD 822/2021, dicha experiencia se muestre estrechamente relacionada con los conocimientos, competencias y habilidades propias de título universitario oficial.

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

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

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

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

Materia	Asignatura (ECTS)	Resultados de Aprendizaje Específicos	Justificación
Gestión de la Seguridad	Fundamentos de la Empresa (6 ECTS)	CE21	<u>Tipo de entidad:</u> 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 aplicable:**

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

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

<http://static.unir.net/documentos/normativa-RTC.pdf>

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

**3.3 MOVILIDAD DE LOS ESTUDIANTES PROPIOS Y DE ACOGIDA**

Información indicada en el Anexo I de la memoria.

**4. PLANIFICACIÓN DE LAS ENSEÑANZAS**

**4.1 ESTRUCTURA BÁSICA DE LAS ENSEÑANZAS**

**DESCRIPCIÓN DEL PLAN DE ESTUDIOS**

Ver Apartado 4: Anexo 1.

**4.1 SIN NIVEL 1**

**NIVEL 2: Fundamentos Matemáticos de la Informática**

**4.1.1.1 Datos Básicos del Nivel 2**

CARÁCTER	ÁMBITO	
Básica	26 Matemáticas y estadística	
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
<b>NIVEL 3: Álgebra y Matemática Discreta</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Básica	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>NIVEL 3: Lógica Computacional</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Básica	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>NIVEL 3: Cálculo y Métodos Numéricos</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Básica	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>NIVEL 3: Estadística</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Básica	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
	6	
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
ECTS Cuatrimestral 10	ECTS Cuatrimestral 11	ECTS Cuatrimestral 12



4.1.1.2 RESULTADOS DE APRENDIZAJE		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		
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. TIPO: Habilidades o destrezas		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Habilidades o destrezas		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. TIPO: Habilidades o destrezas		
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. TIPO: Habilidades o destrezas		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Conocimientos o contenidos		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas		
NIVEL 2: Fundamentos Físicos de la Informática		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	ÁMBITO	
Básica	24 Ingeniería informática y de sistemas	
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
NIVEL 3: Fundamentos Físicos de la Informática		
4.1.1.1.1 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
<b>4.1.1.2 RESULTADOS DE APRENDIZAJE</b>		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		
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. TIPO: Habilidades o destrezas		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Habilidades o destrezas		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. TIPO: Habilidades o destrezas		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Conocimientos o contenidos		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas		
<b>NIVEL 2: Fundamentos de Seguridad</b>		
<b>4.1.1.1 Datos Básicos del Nivel 2</b>		
<b>CARÁCTER</b>	Obligatoria	
<b>ECTS NIVEL 2</b>	6	
<b>DESPLIEGUE TEMPORAL: Cuatrimestral</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
6		
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>NIVEL 3: Fundamentos de Seguridad</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
6		
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>4.1.1.2 RESULTADOS DE APRENDIZAJE</b>		



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. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		
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. TIPO: Habilidades o destrezas		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Habilidades o destrezas		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. TIPO: Habilidades o destrezas		
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. TIPO: Competencias		
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. TIPO: Conocimientos o contenidos		
CG3 - Capacidad para saber comunicar y transmitir ideas conocimientos, habilidades y destrezas de la profesión en Ciberseguridad a un público tanto especializado como no. TIPO: Habilidades o destrezas		
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. TIPO: Competencias		
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. TIPO: Conocimientos o contenidos		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas		
<b>NIVEL 2: Estructura de la Información</b>		
<b>4.1.1.1 Datos Básicos del Nivel 2</b>		
<b>CARÁCTER</b>	Obligatoria	
<b>ECTS NIVEL 2</b>	12	
<b>DESPLIEGUE TEMPORAL: Cuatrimestral</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
		6
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
6		
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>NIVEL 3: Estructura de Datos</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
		6
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>



ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
ECTS Cuatrimestral 10	ECTS Cuatrimestral 11	ECTS Cuatrimestral 12
<b>NIVEL 3: Bases de Datos</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>4.1.1.2 RESULTADOS DE APRENDIZAJE</b>		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		
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. TIPO: Habilidades o destrezas		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Habilidades o destrezas		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. TIPO: Habilidades o destrezas		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Conocimientos o contenidos		
CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad. TIPO: Habilidades o destrezas		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas		
<b>NIVEL 2: Ingeniería de Computadores</b>		
<b>4.1.1.1 Datos Básicos del Nivel 2</b>		
CARÁCTER	ÁMBITO	
Mixta	24 Ingeniería informática y de sistemas	
ECTS NIVEL2		
ECTS OPTATIVAS	ECTS OBLIGATORIAS	ECTS BÁSICAS



0	6	6
<b>DESPLIEGUE TEMPORAL: Cuatrimestral</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
6		6
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>NIVEL 3: Tecnología de Computadores</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Básica	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
6		
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>NIVEL 3: Seguridad en Arquitecturas de Computadores</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
		6
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>4.1.1.2 RESULTADOS DE APRENDIZAJE</b>		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		
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. TIPO: Habilidades o destrezas		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Habilidades o destrezas		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. TIPO: Habilidades o destrezas		
CE7 - Conocer, comprender y evaluar la estructura y arquitectura de los computadores, así como los componentes básicos que los conforman para conocer los vectores de ataque derivados del hardware y el firmware. TIPO: Conocimientos o contenidos		



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. TIPO: Conocimientos o contenidos		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas		
<b>NIVEL 2: Programación y Algoritmia</b>		
<b>4.1.1.1 Datos Básicos del Nivel 2</b>		
<b>CARÁCTER</b>	<b>ÁMBITO</b>	
Mixta	24 Ingeniería informática y de sistemas	
<b>ECTS NIVEL2</b>		
<b>ECTS OPTATIVAS</b>	<b>ECTS OBLIGATORIAS</b>	<b>ECTS BÁSICAS</b>
0	6	12
<b>DESPLIEGUE TEMPORAL: Cuatrimestral</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
6	6	
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
6		
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>NIVEL 3: Fundamentos de Programación</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Básica	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
6		
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>NIVEL 3: Algoritmia y Complejidad</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Básica	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
	6	
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>NIVEL 3: Programación para la Administración de Sistemas</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>



Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
6		
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>4.1.1.2 RESULTADOS DE APRENDIZAJE</b>		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		
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. TIPO: Habilidades o destrezas		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Habilidades o destrezas		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. TIPO: Habilidades o destrezas		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Conocimientos o contenidos		
CE5 - Conocimiento y aplicación de los principios y técnicas fundamentales de paradigmas y lenguajes de programación avanzados utilizados en la administración de sistemas informáticos. TIPO: Conocimientos o contenidos		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		
CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad. TIPO: Habilidades o destrezas		
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. TIPO: Competencias		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas		
<b>NIVEL 2: Seguridad de la Información</b>		
<b>4.1.1.1 Datos Básicos del Nivel 2</b>		
<b>CARÁCTER</b>	Obligatoria	
<b>ECTS NIVEL 2</b>	18	
<b>DESPLIEGUE TEMPORAL: Cuatrimestral</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>



		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
<b>NIVEL 3: Fundamentos de Criptografía</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>NIVEL 3: Autenticación e Infraestructuras de Clave Pública</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>NIVEL 3: Seguridad en Bases de Datos, Blockchain y Big Data</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
6		
ECTS Cuatrimestral 10	ECTS Cuatrimestral 11	ECTS Cuatrimestral 12
<b>4.1.1.2 RESULTADOS DE APRENDIZAJE</b>		
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. TIPO: Conocimientos o contenidos		



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. TIPO: Competencias		
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. TIPO: Habilidades o destrezas		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Habilidades o destrezas		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. TIPO: Habilidades o destrezas		
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. TIPO: Competencias		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Conocimientos o contenidos		
CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad. TIPO: Habilidades o destrezas		
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. TIPO: Competencias		
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. TIPO: Competencias		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas		
<b>NIVEL 2: Seguridad en Sistemas y Comunicaciones</b>		
<b>4.1.1.1 Datos Básicos del Nivel 2</b>		
<b>CARÁCTER</b>	<b>ÁMBITO</b>	
Mixta	24 Ingeniería informática y de sistemas	
<b>ECTS NIVEL2</b>		
<b>ECTS OPTATIVAS</b>	<b>ECTS OBLIGATORIAS</b>	<b>ECTS BÁSICAS</b>
0	24	6
<b>DESPLIEGUE TEMPORAL: Cuatrimestral</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
		6
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
6	6	
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
12		
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>NIVEL 3: Sistemas Operativos</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>



Básica	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>NIVEL 3: Redes de Ordenadores</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>NIVEL 3: Seguridad en Sistemas Operativos y Redes</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>NIVEL 3: Arquitecturas Seguras</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>NIVEL 3: Seguridad en Comunicaciones Inalámbricas</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		



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
<b>4.1.1.2 RESULTADOS DE APRENDIZAJE</b>		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		
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. TIPO: Habilidades o destrezas		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Habilidades o destrezas		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. TIPO: Habilidades o destrezas		
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. TIPO: Competencias		
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. TIPO: Competencias		
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. TIPO: Competencias		
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. TIPO: Competencias		
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. TIPO: Conocimientos o contenidos		
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 TIPO: Conocimientos o contenidos		
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. TIPO: Conocimientos o contenidos		
CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad. TIPO: Habilidades o destrezas		
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. TIPO: Competencias		
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. TIPO: Competencias		
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. TIPO: Competencias		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas		
<b>NIVEL 2: Detección y Protección frente Ciberataques</b>		



4.1.1.1 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
NIVEL 3: Amenazas en el Ciberespacio		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Obligatoria	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
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
NIVEL 3: Técnicas de Hacking y Auditoría de Sistemas		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Obligatoria	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
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
NIVEL 3: Ingeniería Inversa y Análisis de Malware		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Obligatoria	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
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
NIVEL 3: Amenazas Persistentes Avanzadas		
4.1.1.1.1 Datos Básicos del Nivel 3		



CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>NIVEL 3: Protección de Infraestructuras Críticas</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>4.1.1.2 RESULTADOS DE APRENDIZAJE</b>		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		
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. TIPO: Habilidades o destrezas		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Habilidades o destrezas		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. TIPO: Habilidades o destrezas		
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. TIPO: Competencias		
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. TIPO: Competencias		
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. TIPO: Conocimientos o contenidos		
CE18 - Conocer e identificar los procedimientos de ataque informático orquestados por grupos organizados para ser capaz de diseñar e implantar los planes y contramedidas de protección adecuadas. TIPO: Competencias		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		
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. TIPO: Conocimientos o contenidos		



CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad. TIPO: Habilidades o destrezas		
CG3 - Capacidad para saber comunicar y transmitir ideas conocimientos, habilidades y destrezas de la profesión en Ciberseguridad a un público tanto especializado como no. TIPO: Habilidades o destrezas		
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. TIPO: Competencias		
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. TIPO: Competencias		
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. TIPO: Competencias		
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. TIPO: Competencias		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas		
<b>NIVEL 2: Seguridad en el Software</b>		
<b>4.1.1.1 Datos Básicos del Nivel 2</b>		
<b>CARÁCTER</b>	Obligatoria	
<b>ECTS NIVEL 2</b>	24	
<b>DESPLIEGUE TEMPORAL: Cuatrimestral</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
		6
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
	6	6
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
6		
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>NIVEL 3: Ingeniería del Software</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
		6
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>NIVEL 3: Desarrollo de Software Seguro</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>



	6	
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
ECTS Cuatrimestral 10	ECTS Cuatrimestral 11	ECTS Cuatrimestral 12
<b>NIVEL 3: Seguridad en Web</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>NIVEL 3: Seguridad en Aplicaciones Móviles</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>4.1.1.2 RESULTADOS DE APRENDIZAJE</b>		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		
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. TIPO: Habilidades o destrezas		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Habilidades o destrezas		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. TIPO: Habilidades o destrezas		
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. TIPO: Competencias		
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. TIPO: Competencias		
CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad. TIPO: Habilidades o destrezas		



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. TIPO: Competencias		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas		
<b>NIVEL 2: Legislación y Auditoría de la Seguridad</b>		
<b>4.1.1.1 Datos Básicos del Nivel 2</b>		
<b>CARÁCTER</b>	Obligatoria	
<b>ECTS NIVEL 2</b>	18	
<b>DESPLIEGUE TEMPORAL: Cuatrimestral</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
6	6	6
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>NIVEL 3: Legislación, Regulación y Cumplimiento</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
6		
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>NIVEL 3: Auditoría Informática</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
	6	
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>NIVEL 3: Técnicas Forenses en Sistemas Informáticos</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>



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
4.1.1.2 RESULTADOS DE APRENDIZAJE		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		
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. TIPO: Habilidades o destrezas		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Habilidades o destrezas		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. TIPO: Habilidades o destrezas		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		
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. TIPO: Competencias		
CG3 - Capacidad para saber comunicar y transmitir ideas conocimientos, habilidades y destrezas de la profesión en Ciberseguridad a un público tanto especializado como no. TIPO: Habilidades o destrezas		
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. TIPO: Competencias		
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. TIPO: Competencias		
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. TIPO: Conocimientos o contenidos		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas		
NIVEL 2: Gestión de la Seguridad		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	ÁMBITO	
Mixta	7 Ciencias económicas, administración y dirección de empresas, márketing, comercio, contabilidad y turismo	
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
<b>NIVEL 3: Fundamentos de la Empresa</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Básica	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>NIVEL 3: Sistemas de Gestión de Seguridad de la Información</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>NIVEL 3: Ciberinteligencia y Gobierno de la Ciberseguridad</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Obligatoria	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>4.1.1.2 RESULTADOS DE APRENDIZAJE</b>		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		



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. TIPO: Habilidades o destrezas		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Habilidades o destrezas		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. TIPO: Habilidades o destrezas		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		
CE20 - Conocer, utilizar y aplicar sistemas de gestión, análisis de riesgo e implantación de planes de contingencia relacionados con la seguridad de la información. TIPO: Competencias		
CE21 - Conocimiento adecuado del concepto de empresa, marco institucional y jurídico de la empresa. Organización y gestión de empresas. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		
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. TIPO: Conocimientos o contenidos		
CG3 - Capacidad para saber comunicar y transmitir ideas conocimientos, habilidades y destrezas de la profesión en Ciberseguridad a un público tanto especializado como no. TIPO: Habilidades o destrezas		
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. TIPO: Competencias		
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. TIPO: Competencias		
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. TIPO: Conocimientos o contenidos		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas		
<b>NIVEL 2: Optativas</b>		
<b>4.1.1.1 Datos Básicos del Nivel 2</b>		
<b>CARÁCTER</b>	Optativa	
<b>ECTS NIVEL 2</b>	24	
<b>DESPLIEGUE TEMPORAL: Cuatrimestral</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
	24	
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>NIVEL 3: Criptografía Avanzada</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Optativa	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>



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
<b>NIVEL 3: Inteligencia Artificial Aplicada a la Ciberseguridad</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Optativa	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>NIVEL 3: Análisis de Redes Sociales</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Optativa	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>NIVEL 3: Comunicación y Liderazgo</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Optativa	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
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
<b>4.1.1.2 RESULTADOS DE APRENDIZAJE</b>		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		



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. TIPO: Habilidades o destrezas		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Habilidades o destrezas		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. TIPO: Habilidades o destrezas		
CG3 - Capacidad para saber comunicar y transmitir ideas conocimientos, habilidades y destrezas de la profesión en Ciberseguridad a un público tanto especializado como no. TIPO: Habilidades o destrezas		
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. TIPO: Competencias		
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. TIPO: Competencias		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas		
<b>NIVEL 2: Prácticas en Empresa</b>		
<b>4.1.1.1 Datos Básicos del Nivel 2</b>		
<b>CARÁCTER</b>	Optativa	
<b>ECTS NIVEL 2</b>	6	
<b>DESPLIEGUE TEMPORAL: Cuatrimestral</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
	6	
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>NIVEL 3: Prácticas en Empresa</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Optativa	6	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
	6	
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>4.1.1.2 RESULTADOS DE APRENDIZAJE</b>		
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. TIPO: Competencias		
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. TIPO: Conocimientos o contenidos		
CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad. TIPO: Habilidades o destrezas		



CG3 - Capacidad para saber comunicar y transmitir ideas conocimientos, habilidades y destrezas de la profesión en Ciberseguridad a un público tanto especializado como no. TIPO: Habilidades o destrezas		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas		
<b>NIVEL 2: Trabajo Fin de Grado</b>		
<b>4.1.1.1 Datos Básicos del Nivel 2</b>		
<b>CARÁCTER</b>	Trabajo Fin de Grado / Máster	
<b>ECTS NIVEL 2</b>	12	
<b>DESPLIEGUE TEMPORAL: Cuatrimestral</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
	12	
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>NIVEL 3: Trabajo Fin de Grado</b>		
<b>4.1.1.1.1 Datos Básicos del Nivel 3</b>		
<b>CARÁCTER</b>	<b>ECTS ASIGNATURA</b>	<b>DESPLIEGUE TEMPORAL</b>
Trabajo Fin de Grado / Máster	12	Cuatrimestral
<b>DESPLIEGUE TEMPORAL</b>		
<b>ECTS Cuatrimestral 1</b>	<b>ECTS Cuatrimestral 2</b>	<b>ECTS Cuatrimestral 3</b>
<b>ECTS Cuatrimestral 4</b>	<b>ECTS Cuatrimestral 5</b>	<b>ECTS Cuatrimestral 6</b>
<b>ECTS Cuatrimestral 7</b>	<b>ECTS Cuatrimestral 8</b>	<b>ECTS Cuatrimestral 9</b>
	12	
<b>ECTS Cuatrimestral 10</b>	<b>ECTS Cuatrimestral 11</b>	<b>ECTS Cuatrimestral 12</b>
<b>4.1.1.2 RESULTADOS DE APRENDIZAJE</b>		
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. TIPO: Conocimientos o contenidos		
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. TIPO: Competencias		
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. TIPO: Habilidades o destrezas		
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Habilidades o destrezas		
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. TIPO: Habilidades o destrezas		
CE25 - Capacidad para elaborar un trabajo original y estructurado, consistente en un proyecto en el ámbito de Ciberseguridad en el que se sinteticen e integren los conocimientos, habilidades y capacidades adquiridos en enseñanzas del título. TIPO: Competencias		
CG2 - Capacidad para resolver problemas del ámbito de la seguridad de las tecnologías de la información con iniciativa, toma de decisiones, autonomía y creatividad. TIPO: Habilidades o destrezas		
CG3 - Capacidad para saber comunicar y transmitir ideas conocimientos, habilidades y destrezas de la profesión en Ciberseguridad a un público tanto especializado como no. TIPO: Habilidades o destrezas		



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. TIPO: Conocimientos o contenidos							
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas							
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas							
NO CONSTAN ELEMENTOS DE NIVEL 2							
<b>4.2 ACTIVIDADES Y METODOLOGÍAS DOCENTES</b>							
<b>ACTIVIDADES FORMATIVAS</b>							
<p><b>Denominación de las actividades formativas según las definiciones y datos aportados en el apartado 4.1.</b></p> <p>Sesiones presenciales virtuales</p> <p>Recursos didácticos audiovisuales</p> <p>Estudio del material básico</p> <p>Lectura del material complementario</p> <p>Trabajos y casos prácticos</p> <p>Test de evaluación</p> <p>Laboratorios virtuales</p> <p>Tutorías</p> <p>Estancia en Centro</p> <p>Redacción de la memoria de prácticas</p> <p>Lectura de documentación del centro de prácticas</p> <p>Tutorías (Prácticas)</p> <p>Sesión inicial de presentación de Trabajo Fin de Grado</p> <p>Lectura de material en el aula virtual (TFG)</p> <p>Tutorías (TFG)</p> <p>Sesiones grupales de Trabajo Fin de Grado</p> <p>Elaboración del Trabajo Fin de Grado</p> <p>Adicionalmente, en el PDF del apartado 4.1. se indican las definiciones de las actividades formativas, así como su asignación en horas y porcentaje de presencialidad física / interacción virtual síncrona en las diferentes materias del título.</p>							
<b>METODOLOGÍAS DOCENTES</b>							
<p><b>Metodologías docentes</b></p> <table border="1"> <tr> <td>MD1</td> <td><b>Métodos de enseñanza magistral con mediación tecnológica:</b> 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.</td> </tr> <tr> <td>MD2</td> <td><b>Métodos activos:</b> 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.</td> </tr> <tr> <td>MD3</td> <td><b>Métodos fundamentados en el aprendizaje individual:</b> estudio personal, aprendizaje acompañado a través de lecturas de material complementario, realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.</td> </tr> </table> <p>Adicionalmente, en el PDF del apartado 4.1. se indica la asignación de las metodologías docentes a las diferentes materias del título.</p>		MD1	<b>Métodos de enseñanza magistral con mediación tecnológica:</b> aquí se incluirían las clases presenciales virtuales, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.	MD2	<b>Métodos activos:</b> son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje - servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.	MD3	<b>Métodos fundamentados en el aprendizaje individual:</b> estudio personal, aprendizaje acompañado a través de lecturas de material complementario, realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.
MD1	<b>Métodos de enseñanza magistral con mediación tecnológica:</b> aquí se incluirían las clases presenciales virtuales, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.						
MD2	<b>Métodos activos:</b> son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje - servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.						
MD3	<b>Métodos fundamentados en el aprendizaje individual:</b> estudio personal, aprendizaje acompañado a través de lecturas de material complementario, realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.						
<b>4.3 SISTEMAS DE EVALUACIÓN</b>							
<p><b>Denominación de los sistemas de evaluación según las definiciones y datos aportados en el apartado 4.1.</b></p> <p>Participación del estudiante</p> <p>Trabajos, laboratorios y/o casos</p> <p>Test de evaluación</p> <p>Examen final</p> <p>Evaluación según el informe del tutor externo</p> <p>Memoria de prácticas</p> <p>Evaluación de la estructura del Trabajo Fin de Grado</p>							



Evaluación de la exposición del Trabajo Fin de Grado  
Evaluación del contenido individual del Trabajo Fin de Grado

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

**4.4 ESTRUCTURAS CURRICULARES ESPECÍFICAS**



## 5. PERSONAL ACADÉMICO Y DE APOYO A LA DOCENCIA

<b>PERSONAL ACADÉMICO</b>
Ver Apartado 5: Anexo 1.
<b>OTROS RECURSOS HUMANOS</b>
Ver Apartado 5: Anexo 2.

## 6. RECURSOS MATERIALES E INFRAESTRUCTURALES, PRÁCTICAS Y SERVICIOS

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

## 7. CALENDARIO DE IMPLANTACIÓN

<b>7.1 CRONOGRAMA DE IMPLANTACIÓN</b>	
<b>CURSO DE INICIO</b>	2021
Ver Apartado 7: Anexo 1.	
<b>7.2 PROCEDIMIENTO DE ADAPTACIÓN</b>	
No aplicable.	
<b>7.3 ENSEÑANZAS QUE SE EXTINGUEN</b>	
<b>CÓDIGO</b>	ESTUDIO - CENTRO

## 8. SISTEMA INTERNO DE GARANTÍA DE LA CALIDAD Y ANEXOS

<b>8.1 SISTEMA INTERNO DE GARANTÍA DE LA CALIDAD</b>	
<b>ENLACE</b>	<a href="http://www.unir.net/universidad-online/manual-calidad-procedimientos/">http://www.unir.net/universidad-online/manual-calidad-procedimientos/</a>
<b>8.2 INFORMACIÓN PÚBLICA</b>	
<p><b>8.2. Medios de información pública relevante</b></p> <p><b>8.2.1 Canales de difusión de la información y su gestión.</b></p> <p>Para informar tanto al estudiantado, previamente a su matriculación y durante el proceso de formación y aprendizaje, como al profesorado, a los empleadores y a la sociedad en su conjunto se dispone de la <b>página web oficial de la Universidad Internacional de La Rioja</b> donde se aporta la información sobre las características del título (resultados de aprendizaje, temporalización del plan de estudios que incluye asignaturas, actividades formativas y sistemas de evaluación), sistemas de acceso y admisión, idioma de impartición, etc.</p> <p>La Universidad dispone de sistemas para el <b>control periódico de la información</b> disponible en la página web. Por ello, se verifica periódicamente que la información disponible en la página web del título es suficientemente completa, adecuada y relevante para el estudiantado. El coordinador académico del título hace constar en el informe anual de la Unidad de Calidad de Titulación (UCT) esta revisión periódica.</p> <p><b>Información pública relevante del plan de estudios</b></p> <p>UNIR pone a disposición del estudiantado, el profesorado, los empleadores y la sociedad en su conjunto toda la información actualizada del plan de estudios a través de las guías docentes disponibles en la página web de la Universidad. Así, a través de la guía docente de cada una de las asignaturas que forman el plan de estudios, se puede acceder a la siguiente información:</p> <ul style="list-style-type: none"> <li>• <b>Presentación:</b> describe el objetivo de la asignatura y cómo su contenido es relevante para el desarrollo del plan de estudios.</li> <li>• <b>Competencias:</b> se enumeran y describen las competencias y/o resultados de aprendizaje desarrollados en el título.</li> <li>• <b>Contenidos:</b> se detalla por temas el contenido desarrollado en la asignatura.</li> <li>• <b>Metodología:</b> se describen las actividades formativas de la asignatura especificando las horas de dedicación indicadas en la memoria para cada actividad formativa, así como su presencialidad.</li> </ul> <p>Además, se incluye la distribución temporal prevista para la asignatura.</p> <ul style="list-style-type: none"> <li>• <b>Bibliografía:</b> se detalla la bibliografía básica, considerada imprescindible para el estudio de la asignatura, así como, en su caso, la bibliografía complementaria, para ayudar a profundizar más en los temas de mayor interés.</li> <li>• <b>Evaluación y calificación:</b> se detallan los sistemas de evaluación y sus porcentajes de evaluación, así como los requisitos específicos, en su caso, para aprobar la asignatura.</li> <li>• <b>Profesorado:</b> se presentan los datos básicos del profesor encargado de impartir la asignatura.</li> <li>• <b>Orientaciones para el estudio:</b> se dan orientaciones al estudiante de cómo organizar el estudio de la asignatura, así como diferentes consejos para un adecuado seguimiento de la asignatura.</li> </ul> <p><b>8.2.2 Sistemas de información previa: información transparente y accesible</b></p> <p>Con carácter general, por parte de UNIR se pondrá a disposición de los potenciales estudiantes toda la información necesaria para que puedan realizar la elección de su titulación con los mayores elementos de juicio posibles. <b>Se garantiza una información transparente y accesible sobre los requisitos de acceso específicos para el título y los procedimientos de admisión, descritos en la presente memoria</b>, estando disponibles a través de la página web de la Universidad para todos los grupos de interés del título</p> <p>En las condiciones de matrícula, disponibles en el apartado normativa de la página web de la universidad, se alude a los requisitos tecnológicos e informáticos precisos para seguir el curso adecuadamente, dichas condiciones son conocidas y firmadas por el estudiante al matricularse de sus estudios.</p>	



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

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

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

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

#### Recomendaciones de *hardware* y *software* mínimos

Debido al carácter técnico del Grado, los estudiantes deberán disponer de un ordenador personal para realizar las diferentes actividades docentes propuestas. Sin embargo, no es necesario que dicho equipamiento sea de altas prestaciones ya que UNIR dispone de escritorios virtuales en la nube que pueden ser utilizados para ejecutar aquellas aplicaciones informáticas con requisitos adicionales. Teniendo en cuenta que la rápida evolución en dichos requisitos puede variar rápidamente, una configuración mínima recomendada podría ser:

- 8 GB de RAM.
- Conexión a Internet superior a 6 Mbit/s (>1Mbit/s de subida).
- 256 GB. de disco duro.
- Tarjeta de sonido o altavoces o auriculares para poder utilizar el material multimedia.
- Webcam y micrófono si se desea participar en conversaciones face-to-face con el profesor u otros estudiantes.
- Sistema operativo Windows, Mac OS o Linux.
- Acceso de administrador al sistema.
- Navegador web actualizado.

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

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

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

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

#### 8.2.4 Perfil de ingreso recomendado

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

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

El **perfil recomendado de ingreso** corresponde al de un estudiante que, cumpliendo los requisitos de acceso establecidos en el apartado 3.1, posea unas aptitudes que le permitan integrar y relacionar sus conocimientos previos con los que desarrollará en el título:

- Capacidad de abstracción, análisis, y síntesis.
- Aptitud para el razonamiento numérico y lógico.
- Facilidad para comprender y razonar sobre modelos abstractos que generalicen los aspectos particulares de casos prácticos.
- Capacidad de percepción y atención.
- Disponer de sentido práctico de la organización.

### 8.3 ANEXOS

Ver Apartado 8: Anexo 1.

## PERSONAS ASOCIADAS A LA SOLICITUD

RESPONSABLE DEL TÍTULO			
CARGO	NOMBRE	PRIMER APELLIDO	SEGUNDO APELLIDO
Director de la Escuela Superior de Ingeniería y Tecnología	Oscar	Sanjuan	Martínez
DOMICILIO	CÓDIGO POSTAL	PROVINCIA	MUNICIPIO
Avenida de la Paz, 137	26006	La Rioja	Logroño



EMAIL	FAX		
virginia.montiel@unir.net	902877037		
REPRESENTANTE LEGAL			
CARGO	NOMBRE	PRIMER APELLIDO	SEGUNDO APELLIDO
Secretario General	Juan Pablo	Guzmán	Palomino
DOMICILIO	CÓDIGO POSTAL	PROVINCIA	MUNICIPIO
Avenida de la Paz, 137	26006	La Rioja	Logroño
EMAIL	FAX		
virginia.montiel@unir.net	902877037		
El Rector de la Universidad no es el Representante Legal			
Ver Personas asociadas a la solicitud: Anexo 1.			
SOLICITANTE			
El responsable del título no es el solicitante			
CARGO	NOMBRE	PRIMER APELLIDO	SEGUNDO APELLIDO
Responsable de programas ANECA	Virginia	Montiel	Martín
DOMICILIO	CÓDIGO POSTAL	PROVINCIA	MUNICIPIO
Avenida de la Paz, 137	26006	La Rioja	Logroño
EMAIL	FAX		
virginia.montiel@unir.net	902877037		

### INFORME DEL SIGC

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



## **Apartado 1: Anexo 6**

**Nombre** :1.10\_G\_Ciberseguridad\_completo.pdf

**HASH SHA1** :C8ED8707A20170B00CBD6B049CA30A303E4EE895

**Código CSV** :812895055265209328686606

**Ver Fichero**: 1.10\_G\_Ciberseguridad\_completo.pdf



### Apartado 3: Anexo 1

Nombre :Convenio\_FP\_Aplicacion\_3.2.pdf

HASH SHA1 :F09A2B7EE0F62C5E94373EFFE10D4362CE6F8237

Código CSV :684294832294450422833608

Ver Fichero: Convenio\_FP\_Aplicacion\_3.2.pdf



#### **Apartado 4: Anexo 1**

**Nombre :**4.1\_G\_Ciberseguridad.pdf

**HASH SHA1 :**C86D84A5FBDFFF62CD6AAE89857778C4817A3458

**Código CSV :**812888795179798445447960

**Ver Fichero:** 4.1\_G\_Ciberseguridad.pdf



## Apartado 5: Anexo 1

Nombre :5.1\_G\_Ciberseguridad.pdf

HASH SHA1 :6704EF936FD190A7B491C4EFC40FD2904D181B00

Código CSV :812883846082499061000861

Ver Fichero: 5.1\_G\_Ciberseguridad.pdf



## Apartado 5: Anexo 2

Nombre :5.2\_GCIB.pdf

HASH SHA1 :04359A67482CBBA015142AF8AC6A46DB9BED9EEB

Código CSV :693141962638317217800074

Ver Fichero: 5.2\_GCIB.pdf



## Apartado 6: Anexo 1

Nombre :6.pdf

HASH SHA1 :89E73CD200833E15F3FBDBD8767F7EB1E236B3E8

Código CSV :799839279282899890861407

Ver Fichero: 6.pdf



## Apartado 7: Anexo 1

Nombre :7.pdf

HASH SHA1 :CD0802595EA9F182986D6705DC79E59E3ED12FA9

Código CSV :812875713441169054611059

Ver Fichero: 7.pdf



## Apartado 8: Anexo 1

Nombre :8.3.pdf

HASH SHA1 :EC281308E48D6F0B30B47682A6889F155AB2EE9B

Código CSV :812875661240390065674640

Ver Fichero: 8.3.pdf



## **Apartado Personas asociadas a la solicitud: 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



## Apartado Informe del SIGC: Anexo 1

Nombre :Informe\_SGIC\_20240726\_G\_ Ciberseguridad\_aplicacion.pdf

HASH SHA1 :5E633C756A2274946A95CCEF045E1273634934CD

Código CSV :803914344248302651371918

Ver Fichero: Informe\_SGIC\_20240726\_G\_ Ciberseguridad\_aplicacion.pdf



