GRADO EN CIBERSEGURIDAD

UNIVERSITAT AUTÒNOMA DE BARCELONA

> Memoria[1] para la verificación de titulaciones oficiales de Grado y Máster Universitario de acuerdo 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.

[1] Transitoriamente, y mientras no se disponga de una aplicación adaptada a los requerimientos del Anexo II del Real Decreto 822/2021, esta memoria se debe adjuntar transformada al formato PDF en los espacios de la actual aplicativo de verificación, preferentemente en el apartado 2 de Justificación de las enseñanzas.

Índice

1. DESCRIPCIÓN, OBJETIVOS FORMATIVOS Y JUSTIFICACIÓN DEL TÍTULO

TABLA 1. Descripción del título

1.1. Denominación del título	**Graduado o Graduada en Ciberseguridad por la Universidad Autónoma de Barcelona**
1.2. Ámbito de conocimiento	Ingeniería informática y de sistemas
1.2. Rama	Ingeniería y Arquitectura
Codi ISCED	**0619 Tecnologías de la información y las comunicaciones (otros estudios)**
1.3. Menciones y especialidades	*No hay Menciones*
1.4.a) Universidad responsable	Universitat Autònoma de Barcelona
1.4.b) Universidades participantes	-
1.4.c) Convenio títulos conjuntos	-
1.5.a) Centro de impartición responsable	Escuela de Ingeniería – 08071123
º1.5.b) Centros de impartición	*Escuela de Ingeniería* *Código RUCT* 08071123
1.6. Modalidad de enseñanza	Presencial
1.7. Número total de créditos	240
1.8. Idiomas de impartición	Catalán 90% Castellano 5% Inglés 5%
1.9.a) Oferta de plazas por modalidad	Presencial: 40
1.9.b) Número total de plazas ofertadas en el centro	160
1.9.c) Número de plazas de nuevo ingreso para primer curso	40

1.10. Justificación del interés del título

Dentro del marco de planificación estratégica en innovación docente de la Universitat Autònoma de Barcelona (UAB), se presenta este nuevo Grado en Ciberseguridad.

El *World Economic Forum*[2] indica que la falta de profesionales en el sector de la ciberseguridad es ya una amenaza real en el mundo. Citando un informe[3] del *International Information System Security Certification Consortium* (ISC2), se apunta que, a nivel global, el mundo dispone de 4,7 millones de profesionales dedicados a la ciberseguridad, pero hacen falta aun 3,4 millones más. Es decir, los profesionales actuales solamente cubren el 58% de la demanda. Esta situación, además, se acentúa cada vez más si añadimos que el crecimiento del uso de las tecnologías de la información en todos los ámbitos de la sociedad implicará que la necesidad de expertos en ciberseguridad aumente aún más. Concretamente, el ISC2 estima que el vacío entre los profesionales en seguridad y su demanda augmenta un 26,2% cada año, provocando que los profesionales del sector sean cada vez más escasos.

A diferencia de otros sectores, donde la falta de profesionales afecta al sector concreto de negocio y, por tanto, la no existencia de profesionales se limita al no crecimiento del propio sector, el ámbito de la seguridad es totalmente transversal. La nueva Directiva Europea *Security of Network and Information Systems*[4] (NIS 2) determina 15 ámbitos esenciales que engloban la práctica totalidad de los sectores productivos y de servicios que van desde la administración pública y las finanzas hasta la alimentación y el transporte, pasando por el sector de la energía o el farmacéutico. Por este motivo, el impacto económico que suponen los incidentes de ciberseguridad en todos los ámbitos es muy relevante. De hecho, los datos estiman que los ataques de ciberseguridad dejaron un impacto de 7.000 millones de euros durante 2022. Además, dada la afectación de ámbitos tan transversales, más allá de los efectos económicos, hay también una afectación de la seguridad física de las personas, en cuanto los ataques y sabotajes pueden afectar a infraestructuras críticas como hospitales, centrales de generación de energía o centros de tratamiento de agua potable.

Más concretamente, en el entorno de Cataluña, según el informe del 2022 de la *Agència de Ciberseguretat de Catalunya*[5], de la Generalitat de Catalunya, existen 495 empresas dedicadas a la ciberseguridad en Cataluña, un 15% más que el año anterior, que dan trabajo a más de 9.000 trabajadores. Pero, por otro lado, el mismo informe estima que hay una escasez de 10.000 profesionales en el sector de la ciberseguridad, más del doble de los existentes.

Si bien se puede ver que las necesidades de profesionales del sector son claramente relevantes, las titulaciones universitarias que forman a dichos profesionales son claramente insuficientes. La mayoría de las iniciativas se enmarcan en la formación de máster siendo la oferta de grado muy minoritaria. De hecho, en España, solamente siete universidades ofrecen grados de ciberseguridad (Universidad Rey Juan Carlos, Universidad Francisco de Vitoria, Universidad de la Rioja, Universidad Europea de Madrid, Universidad San Jorge, Universidad de Málaga , Escola de noves tecnologies interactives –UB)

[2] https://www.weforum.org/agenda/2023/05/the-cybersecurity-skills-gap-is-a-real-threat-heres-how-to-address-it

[3] https://www.isc2.org/News-and-Events/Press-Room/Posts/2022/10/20/ISC2-Research-Reveals-the-Cybersecurity-Profession-Must-Grow-by-3-4-Mil-to-Close-Workforce-Gap

[4] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

[5] https://www.accio.gencat.cat/ca/serveis/banc-coneixement/cercador/BancConeixement/la-ciberseguretat-a-catalunya

y algunos de ellos son grados mixtos de ciberseguridad y otras ramas de la informática, como la inteligencia artificial.

1.11. Objetivos formativos

1.11.a) Principales objetivos formativos del título

El grado en ciberseguridad que se propone es un grado emergente de 4 años dentro del ámbito de las ingenierías que tiene como objetivo principal la formación de profesionales que estén capacitados para dar respuesta a los múltiples retos que la ciberseguridad afronta en las distintas áreas de las tecnologías de la información.

El alumnado obtendrá una sólida formación en todas las disciplinas relacionadas con la ciberseguridad. El alumnado:

Obtendrá los fundamentos matemáticos, algorítmicos y computacionales sobre los que se asienta el conjunto de técnicas de ciberseguridad.

1. Obtendrá una formación específica en las técnicas y métodos propios de la ciberseguridad, haciendo hincapié en las bases criptográficas, los mecanismos de ataque/defensa y las herramientas de privacidad.
2. Estimular en el alumnado una cultura de la ciberseguridad con especial énfasis en el concepto de la mentalidad de adversario (*adversarial thinking*) en el que el análisis de seguridad se aplica a todos y cada uno de los procesos IT.
3. Formar profesionales que puedan afrontar los nuevos retos de seguridad que supone una sociedad cada vez más hiperconectada y automatizada.
4. Analizará las implicaciones éticas, legales y sociales del uso de técnicas de ciberseguridad en sus distintos entornos.

Con estos objetivos se persigue formar profesionales que puedan integrarse en equipos para dirigir, diseñar, desarrollar e implementar soluciones de ciberseguridad, en todos sus ámbitos de aplicación. Esto incluye tanto el análisis de sistemas existentes y la detección de sus vulnerabilidades como las tareas de despliegue de soluciones para la corrección de dichas vulnerabilidades, pasando por el análisis de la privacidad de las aplicaciones o los requisitos de las herramientas criptográficas aplicables en cada situación.

1.11.b) Objetivos formativos de las menciones o especialidades

No se han diseñado menciones para este grado.

1.12. Estructuras curriculares específicas y justificación de sus objetivos

No se prevén estructuras curriculares específicas en el grado que se propone.

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

No se utilizarán estrategias metodológicas de innovación docente específicas.

1.14. Perfiles fundamentales de egreso a los que se orientan las enseñanzas

Este grado forma profesionales especializados en la ciberseguridad, que son capaces de dar respuesta a los retos que la ciberseguridad afronta en las distintas áreas de las tecnologías de la información. Así, por ejemplo, los graduados en ciberseguridad pueden ocupar los siguientes roles profesionales:

- Auditoría de seguridad de sistemas de información.
- Especialistas en *pentesting* (de servidores de datos, de sistemas, de redes).
- Peritaje forense digital.
- Consultoría especializada en ciberseguridad (en comercio electrónico, banca digital, sistemas *blockchain*, administración electrónica, sistemas biométricos, inteligencia artificial, mecanismos de autenticación, despliegues criptográficos, privacidad y protección de datos).
- Dirección de proyectos de seguridad en el ámbito de las TIC.
- Delegado de protección de datos (DPO).
- Administración avanzada (de redes, sistemas o bases de datos).

1.14.bis) Actividad profesional regulada habilitada por el título

No habilita para profesión regulada.

No es condición de acceso para título profesional.

2. RESULTADOS DEL PROCESO DE FORMACIÓN Y DE APRENDIZAJE

2.1. Conocimientos o contenidos (Knowledge)

- KT01: Identificar los principales conceptos, tecnologías, entornos y herramientas en el ámbito de la ciberseguridad y privacidad de la información.
- KT02: Seleccionar las principales herramientas para el diseño, desarrollo, despliegue, administración de aplicaciones y servicios seguros que tengan en cuenta todos los elementos que actúan y el riesgo que comportan.
- KT03: Describir las bases matemáticas y mecanismos criptográficos, la estructura y funcionamiento de los sistemas operativos/distribuidos y la gestión y administración de redes desde el punto de vista de la seguridad de la información.
- KT04. Identificar los mecanismos, modelos y protocolos en la seguridad de los datos y protección de la privacidad de los usuarios, cumpliendo con las normativas nacionales/internacionales y los principios éticos que guían el análisis y los test de seguridad.
- KT05. Definir los mecanismos, lenguajes, dispositivos y herramientas de diseño, desarrollo, despliegue de software desde el punto de vista de la ciberseguridad
- KT06. Identificar las estructuras del software malicioso y los mecanismos utilizados durante su ciclo de vida, así como las vulnerabilidades de las aplicaciones, sistemas operativos, servicios y redes.
- KT07: Definir los métodos, herramientas, entornos y modelos de IA en la mejora de la seguridad de los sistemas de información para prevenir incidentes de seguridad, garantizando la privacidad con infraestructuras accesibles y seguras.
- KT08: Identificar los principios y metodologías para realizar una gestión de riesgos en ciberseguridad, como el análisis de impacto, la identificación y evaluación de amenazas y vulnerabilidades, la selección y aplicación de medidas de mitigación y la monitorización, la revisión continua del nivel de seguridad, el costo y el consumo energético.

2.2. Habilidades o destrezas (Skills)

- ST01: Analizar los métodos, procedimientos y protocolos orientados a incrementar la seguridad de los sistemas de información garantizando la privacidad de la misma.
- ST02: Determinar los componentes vinculados a la ciberseguridad desde el software hasta el hardware considerando la tipología del dispositivo (local, cloud, médico, móvil), la interconexión a la red y el almacenamiento de los datos.
- ST03: Analizar las metodologías, técnicas y procedimientos de los incidentes de ciberseguridad así como el vector de infección, su detección, mitigación y solución.
- ST04: Utilizar entornos y herramientas que permitan bajo diferentes técnicas/protocolos la detección, identificación, eliminación de intrusos o software malicioso que pueda comprometer la seguridad de la información.
- ST05: Interpretar la legislación nacional e internacional aplicable, los principios éticos y las normas de buen uso que regulan la actividad de los profesionales de la seguridad informática evaluando también las repercusiones legales y económicas derivadas de incidentes de ciberseguridad.
- ST06: Emplear entornos software para el diseño, desarrollo, despliegue de entornos seguros (aplicaciones móviles/web, servicios, bases de datos, sistemas operativos) que sean inmunes delante de incidentes de seguridad y garanticen la privacidad de la información.
- ST07: Probar software malicioso, técnicas de intrusión, análisis de vulnerabilidades, ataques masivos y otros elementos que puedan afectar la seguridad del sistema de información utilizando entornos controlados.
- ST08: Evaluar las decisiones en ciberseguridad mediante un análisis crítico, considerando riesgos, beneficios y cuestiones éticas, y justificando la selección de la solución más adecuada según los objetivos establecidos.
- ST09: Determinar los problemas de ciberseguridad en los sistemas operativos, servicios y aplicaciones desplegadas en máquinas físicas, y virtualizadas.

2.3. Competencias (Competences)

- CT01: Desarrollar proyectos centrados en la evaluación del riesgo, detección, clasificación, mitigación y/o solución de incidentes de seguridad en sistemas de información.
- CT02: Examinar SO, aplicaciones, redes de comunicación y dispositivos/hardware que tengan como valor fundamental la privacidad de la información y que sean susceptibles de ser vulnerada.
- CT03: Generar aplicaciones/servicios/servidores (web, móviles, locales, distribuidas, cloud) seguros, centrados en garantizar la privacidad de la información y la reducción del riesgo ante incidentes de ciberseguridad.
- CT04: Examinar los métodos y mecanismos de ciberseguridad orientados a la protección y privacidad de la información y las implicaciones éticas de los mismos.
- CT05: Examinar técnicas y mecanismos que permitan la detección temprana de incidentes de seguridad y su análisis forense en el caso que ocurran sobre todos los elementos que integran un sistema de información de acuerdo a su despliegue (local/remoto, cloud, distribuido) y a sus implicaciones éticas.
- CT06: Construir entornos de pruebas que permitan la evaluación y análisis de incidentes de seguridad y software malicioso, teniendo en cuenta los diferentes elementos que conforma el sistema.
- CT07: Investigar las desigualdades de género y el impacto ético y social de tecnologías como la inteligencia artificial en la privacidad y dignidad de colectivos vulnerables. Analizar el papel

de la ciberseguridad en su protección, proponiendo medidas de prevención y control para evitar su uso indebido.

3. ADMISIÓN, RECONOCIMIENTO Y MOVILIDAD

3.1. Requisitos de acceso y procedimientos de admisión de estudiantes

3.1.a) Normativa y procedimiento general de acceso

Acceso a los estudios de grado:

Procedimiento UAB:

Vías de acceso a los estudios y sus requisitos

Normativa académica UAB:

Normativa de la UAB aplicable a los estudios universitarios regulados de conformidad con los planes de estudios regulados por el RD 822/2021

Título II. Acceso y admisión
Capítulo I. Enseñanzas de grado
Sección 1a. Disposiciones generales
Artículo 123. Ámbito de aplicación
1. El objeto de este capítulo es regular las condiciones para el acceso y la admisión a las titulaciones de grado de la UAB, en desarrollo del contenido del Real Decreto 534/2024, de 11 de junio, por el que se regulan los requisitos de acceso a las enseñanzas universitarias oficiales de Grado, las características básicas de la prueba de acceso y la normativa básica de los procedimientos de admisión.
2. Pueden ser admitidas a las titulaciones de grado de la UAB, en las condiciones que se determinan en este capítulo y en la legislación de rango superior, las personas que reúnan alguno de los requisitos establecidos en los artículos 4 a 8 del RD 534/2024.
3. Todos los preceptos de este capítulo se interpretan adoptando como principios fundamentales la igualdad, el mérito y la capacidad.

3.1.b) Criterios y procedimiento de admisión a la titulación

No se han previsto pruebas de aptitud personal específicas.

3.2. Criterios para el reconocimiento y transferencias de créditos

Reconocimiento y transferencia de créditos para titulaciones de grado:
https://www.uab.cat/web/estudios/grado/informacion-academica/reconocimiento-de-creditos/creditos-reconocidos-y-transferidos-1345672757413.html

Normativa de la UAB aplicable a los estudios universitarios regulados de conformidad con los planes de estudios regulados por el RD 822/2021
Título IV: Transferencia y reconocimiento de créditos

La contextualización de las decisiones de reconocimiento de créditos responde a la necesidad de adaptarse a la evolución rápida y constante de las tecnologías digitales y las demandas del mercado laboral. El proceso de reconocimiento de créditos permite que los estudiantes obtengan el reconocimiento de habilidades y conocimientos adquiridos en otros estudios o experiencias profesionales previas, siempre que estas sean relevantes y se alineen con los objetivos del programa. La Universidad, en su rol como institución académica, tiene en cuenta criterios tanto académicos como profesionales para evaluar la pertinencia de estas competencias en el marco del programa de ciberseguridad. De esta manera, se garantiza que los estudiantes obtengan una formación integral y actualizada, que les permita enfrentar los desafíos de un campo en continua expansión, facilitando su inserción laboral y promoviendo su desarrollo profesional.

TABLA 3. Criterios específicos para el reconocimiento de créditos

Reconocimiento por enseñanzas superiores no universitarias:	*Número máximo de ECTS*
Breve justificación	
Reconocimiento por títulos propios:	*Número máximo de ECTS*
Breve justificación	
Reconocimiento por experiencia profesional o laboral:	*Número máximo de ECTS ¿?*
Breve justificación Pueden ser objeto de reconocimiento la experiencia laboral y profesional acreditada, siempre que esté relacionada con las competencias inherentes al título. La actividad profesional se puede reconocer siempre que se cumplan los siguientes requisitos: a) Informe favorable del tutor/a o, si no existe, de la coordinación de la titulación. b) Valoración de la acreditación de la empresa que defina las tareas realizadas, certificación de vida laboral de la persona interesada y memoria justificativa en la cual se expongan las competencias conseguidas mediante la actividad laboral. c) Prueba de evaluación adicional cuando lo solicite el tutor/a o, si no existe, la coordinación de la titulación. Los créditos reconocidos en concepto de experiencia laboral se computan en el nuevo expediente como prácticas de la titulación	

3.3. Procedimientos para la organización de la movilidad de los estudiantes propios y de acogida

https://www.uab.cat/web/mobilitat-i-intercanvi-internacional-1345680108534.html

Las acciones de movilidad están diseñadas para fomentar la internacionalización de los estudiantes, ampliando sus perspectivas académicas y profesionales. A través de convenios con universidades y centros de investigación de prestigio en Europa y otros continentes, el programa facilita el acceso a experiencias de aprendizaje en diferentes entornos culturales y académicos. Se prevé que los estudiantes puedan tener la oportunidad de participar en programas de intercambio como el Erasmus, SICUE y UAB Exchange Programme, que les permita cursar asignaturas en instituciones extranjeras y convalidar créditos, enriqueciendo así su formación técnica y profesional en ciberseguridad con visiones globales.

Además, se establecerán acuerdos con empresas, como las incluidas en el Consejo Asesor del Grado (ver Anexo 1), y organizaciones para realizar prácticas en entornos laborales, donde los estudiantes podrán aplicar sus conocimientos en situaciones reales de ciberseguridad, desarrollando habilidades prácticas y de adaptación a diversos contextos laborales y tecnológicos. Estas acciones de movilidad no solo potencian sus competencias técnicas, sino que también fortalecen su capacidad de trabajar en equipos multiculturales y de comprender mejor las diferentes normativas y enfoques en seguridad digital que se aplican globalmente.

4. PLANIFICACIÓN DE LAS ENSEÑANZAS

4.1. Estructura básica de las enseñanzas

Distribución en créditos ECTS a cursar por el estudiante

TIPO DE MATERIA	ECTS
Formación básica	60
Obligatorias	120
Optativas	48
Prácticas Externas (Obligatorias)	0
Trabajo de Fin de Grado	12
ECTS TOTALES	240

4.1.a) Resumen del plan de estudios

Tabla 4a. Resumen del plan de estudios (estructura semestral)

Curso	Semestre	Asignatura	Carácter	ECTS
1	1	*Fundamentos de programación*	*FB*	*6*
		Fundamentos de computadores	*FB*	*6*
		Introducción a la ciberseguridad	*OB*	*6*
		Ética para la ciberseguridad	*FB*	*6*
		Álgebra y matemática discreta	*FB*	*6*
	2	*Programación en C*	*FB*	*6*
		Complejidad, aleatoriedad y números primos	*FB*	*6*
		Criptografía básica	*FB*	*6*
		Sistemas operativos	*FB*	*6*
		Introducción a las redes de comunicación	*FB*	*6*
		Total primer curso		**60**
2	1	*Bases de datos*	*OB*	*6*
		Desarrollo web	*OB*	*6*
		Mecanismos de autentificación	*OB*	*6*
		Servicios para redes seguras	*OB*	*6*
		Fundamentos jurídicos de la ciberseguridad	*FB*	*6*
	2	*Seguridad en bases de datos*	*OB*	*6*
		Técnicas de bajo nivel	*OB*	*6*
		Desarrollo de software seguro	*OB*	*6*
		Conceptos fundamentales de privacidad	*OB*	*6*

		Sistemas distribuidos	*OB*	*6*
		Total segundo curso		**60**
3	**1**	*Auditoria de seguridad del código*	*OB*	*6*
		Virus y software malicioso	*OB*	*6*
		Server hardening	*OB*	*6*
		Digital forensics	*OB*	*6*
		Administración de redes seguras	*OB*	*6*
	2	*Seguridad en hardware*	*OB*	*6*
		Seguridad en servicios de virtualización y cloud	*OB*	*6*
		Penetration testing	*OB*	*6*
		Optativa 1	*OP*	*6*
		Optativa 2	*OP*	*6*
		Total tercer curso		**60**
4	**1**	*Gestión de la ciberseguridad*	*OB*	*6*
		IA aplicada a la ciberseguridad	*OB*	*6*
		Optativa 3	*OP*	*6*
		Optativa 4	*OP*	*6*
		Optativa 5	*OP*	*6*
	2	*Optativa 6*	*OP*	*6*
		Optativa 7	*OP*	*6*
		Optativa 8	*OP*	*6*
	4.0	*Trabajo de Fin de Grado*	*OB*	*12*
		Total cuarto curso		**60**
La oferta de asignaturas optativas se ofrece a partir de 3º y 4 curso. Optatividad:				
	3.2, 4.0	*Criptografía avanzada*	*OP*	*6*
		Programación funcional	*OP*	*6*
		Aspectos de la usabilidad en aplicaciones seguras	*OP*	*6*
		Introducción a la programación en entornos móviles	*OP*	*6*
		Seguridad en sistemas operativos para móviles	*OP*	*6*
		Análisis de redes sociales	*OP*	*6*
		Tecnología blockchain y criptomonedas	*OP*	*6*

Protección de datos y gestión de la privacidad	*OP*	*6*
Adversarial machine learning	*OP*	*6*
Biometría	*OP*	*6*
Seguridad en redes inalámbricas	*OP*	*6*
Seguridad en aplicaciones móviles	*OP*	*6*
Seguridad en eHealth	*OP*	*6*
Tecnología blockchain y smart contracts	*OP*	*6*
Seguridad en industria e infraestructuras críticas	*OP*	*6*
Seguridad en sistemas de control industrial	*OP*	*6*
informática industrial y sistemas basados en PLC	*OP*	*6*
Prácticas Profesionales	*OP*	*12*

4.1.b) Plan de estudios detallado

Tabla resumen de materias	
M1	Formación básica en ciberseguridad
M2	Matemáticas
M3	Programación
M4	Bases de datos
M5	Criptografía
M6	Sistemas operativos
M7	Redes
M8	Gestión de seguridad
M9	Privacidad
M10	Inteligencia artificial
M11	Interfaces de seguridad
M12	Seguridad en entornos móviles
M13	Aspectos de seguridad en industria y aplicaciones
M14	Trabajo de Fin de Grado
M15	Prácticas Profesionales

Tabla 5. Plan de estudios detallado

Materia 1: Formación Básica en Ciberseguridad	
Número de créditos ECTS	30
Tipología	*24 básico, 6 obligatorio*
Ámbito de Conocimiento	Ingeniería informática y de sistemas.
Organización temporal	*1.1, 2.1*
Modalidad	*presencial*
Contenidos de la materia	• Programación Estructurada, Modular y Orientada a Objetos • Sistemas Informáticos y Seguridad • Fundamentos de Ciberseguridad • Marco Normativo en Ciberseguridad • Ética y Buenas Prácticas en Ciberseguridad
Resultados del aprendizaje de la materia	Conocimiento: • KM01: Describir los conceptos básicos de la programación estructurada, modular y orientada a objetos, las herramientas y

	entornos de desarrollo para la creación de software seguro y de calidad. [KT01] • KM02: Describir los componentes básicos de un sistema informático, así como los conceptos principales en un sistema informático y su relación con la seguridad y consumo y rendimiento del sistema. [KT02] • KM03: Definir los principales conceptos de la ciberseguridad, así como los procesos, métodos y acciones involucradas. [KT01] • KM04: Identificar el marco normativo nacional e internacional que regula la ciberseguridad, la protección de datos, el comercio electrónico, la propiedad intelectual, el ciberdelito y la responsabilidad civil y penal de los actores involucrados. [KT02] • KM05: Identificar los principios y valores éticos que guían la actuación de los profesionales de la ciberseguridad, los códigos deontológicos y las buenas prácticas que los regulan. [KT04]
	Habilidades: • SM01: Analizar las necesidades de programación del sistema informático desde el punto de vista de la ciberseguridad. [ST02] • SM02: Determinar los aspectos tecnológicos, humanos y de la organización en un incidente de ciberseguridad y todas las cuestiones vinculadas a su resolución. [ST01] • SM03: Interpretar la legislación pertinente de ámbito nacional/internacional así como los principios éticos y las normas de buen uso que regulan la actividad de los profesionales de seguridad informática y las repercusiones por daños y perjuicios delante de incidentes de ciberseguridad. [ST05]
	Competencias: • CM01: Validar los requisitos del sistema informático, las aplicaciones y los servicios desde el punto de vista de la ciberseguridad y las referencias actuales. [CT01] • CM02: Diseñar entornos que contemplen la ciberseguridad teniendo en cuenta los aspectos tecnológicos, humanos y de la organización frente a los incidentes de seguridad para garantizar la privacidad de la información. [CT02] • CM03: Evaluar los aspectos hardware y software del sistema de información para cumplir los estándares de ciberseguridad y protección de la información. [CT04]

actividades formativas		Dirigidas	Supervisadas	Autónomas
	Horas	247.5	22.5	480
	% Presencialidad	100%	100%	0%

Asignaturas	Denominación	ECTS	Tipología	Semestre	Idioma
	Fundamentos de programación	6	FB	1.1	Castellano/ catalán

Fundamentos de computadores	6	FB	1.1	Castellano/ catalán
Introducción a la ciberseguridad	6	OB	1.1	Castellano/ catalán
Fundamentos jurídicos de la ciberseguridad	6	FB	2.1	Castellano/ catalán
Ética para la ciberseguridad	6	FB	1.1	Castellano/ catalán

Materia 2: Matemáticas	
Número de créditos ECTS	12
Tipología	*12 básico*
Ámbito de Conocimiento	*Matemáticas y Estadística*
Organización temporal	*1.1, 1.2*
Modalidad	*Presencial*
Contenido de la materia	Se abordan conocimientos esenciales para comprender y aplicar conceptos matemáticos fundamentales en el campo de la ciberseguridad, con un enfoque particular en criptografía y análisis de seguridad. • Teoría de Conjuntos y Estructuras Algebraicas • Estadística y Teoría de la Información • Complejidad Computacional
Resultados del aprendizaje de la materia	Conocimiento: • KM06. Reconocer los conceptos y propiedades de conjuntos, relaciones, funciones, operaciones, grupos, anillos, cuerpos y polinomios, así como su aplicación en la criptografía simétrica y asimétrica. [KT03] • KM07. Reconocer los conceptos y métodos de la estadística, la teoría de la información y la complejidad computacional en el diseño y evaluación de los sistemas criptográficos y de seguridad. [KT03]
	Habilidades: • SM04: Utilizar de forma adecuada los métodos, procedimientos y funciones de la estadística, la teoría de la información y la complejidad computacional en el diseño y evaluación de los sistemas criptográficos y de seguridad. [ST01] • SM05: Analizar los diferentes aspectos matemáticos que están involucrados en la criptografía simétrica y asimétrica. [ST01]
	Competencias: • CM04: Evaluar procedimientos y funciones basados en la estadística, la teoría de la información y la complejidad computacional de los sistemas criptográficos y de seguridad utilizados para proteger la información. [CT04]

actividades formativas		**Dirigidas**	**Supervisadas**	**Autónomas**
	Horas	99	9	192
	% Presencialidad	100%	100%	0%

Asignaturas	Denominación	ECTS	Tipología	Semestre	Idioma
	Álgebra y matemática discreta	6	FB	1.1	Castellano/ catalán
	Complejidad, aleatoriedad y números primos	6	FB	1.2	Castellano/ catalán

Materia 3: Programación	
Número de créditos ECTS	42
Tipología	*6 básico, 30 obligatorio, 6 optativo*
Ámbito de Conocimiento	Ingeniería informática y de sistemas.
Organización temporal	*1.2, 2.1, 2.2, 3.1, 3.2, 4.0*
Modalidad	*Presencial*
Contenido de la Materia	Se proporciona una visión integral del desarrollo de software enfocado a la seguridad. • Desarrollo de software seguro • Seguridad en aplicaciones Web • Auditoría de código fuente • Análisis de software malicioso
Resultados del aprendizaje de la materia	Conocimiento: • KM08: Reconocer los principales conceptos del desarrollo de software tanto de alto nivel como de bajo nivel teniendo en cuenta y analizando aspectos de seguridad. [KT02] • KM09: Identificar las mejores prácticas y herramientas para el desarrollo seguro de aplicaciones web y evitando las vulnerabilidades más comunes y la configuración de seguridad defectuosa. [KT04] • KM10: Identificar las metodologías, las herramientas y los estándares para realizar auditorías de seguridad de código fuente considerando las vulnerabilidades que afectan a la confidencialidad, la integridad y la disponibilidad de las aplicaciones. [KT05] • KM11: Identificar las estructuras del software malicioso y los mecanismos utilizados durante su ciclo de vida, así como las vulnerabilidades de las aplicaciones, sistemas operativos, servicios y redes. [KT06]

Habilidades:

- SM06: Experimentar con el diseño, programación, despliegue y test de software seguro a alto y bajo nivel. [ST02]
- SM07: Utilizar diferentes herramientas de análisis y test en el diseño, despliegue y prueba de aplicaciones web seguras. [ST06]
- SM08: Utilizar de forma adecuada los procedimientos, técnicas y herramientas de auditorías de seguridad del código fuente. [ST07]
- SM09: Probar código malicioso durante su ciclo de vida teniendo en cuenta las técnicas utilizadas para su detección, prevención y eliminación. [ST03]

Competencias:

- CM05: Desarrollar servicios y aplicaciones seguros a alto y bajo nivel. [CT01]
- CM06: Desarrollar aplicaciones web seguras que sean resistentes bajo diferentes incidentes de seguridad. [CT03]
- CM07: Evaluar las diferentes técnicas de desarrollo y test del código fuente actuales desde el punto de vista de la seguridad. [CT05]
- CM08: Evaluar diferentes tipos de código malicioso poniendo a prueba las técnicas de evasión, propagación, detección, control y eliminación. [CT06]

actividades formativas

	Dirigidas	**Supervisadas**	**Autónomas**
Horas	247.5	22.5	480
% Presencialidad	100%	100%	0%

Asignaturas

Denominación	ECTS	Tipología	Semestre	Idioma
Programación en C	6	FB	1.2	Castellano/ catalán
Desarrollo web	6	OB	2.1	Castellano/ catalán
Técnicas de bajo nivel	6	OB	2.2	Castellano/ catalán
Desarrollo de software seguro	6	OB	2.2	Castellano/ catalán
Auditoría de seguridad del código	6	OB	3.1	Castellano/ catalán
Virus y software malicioso	6	OB	3.1	Castellano/ catalán
Programación funcional	6	OP	3.2, 4.0	Castellano/ catalán

<table>
<tr><td colspan="2">Materia 4: Bases de Datos</td></tr>
<tr><td>Número de créditos ECTS</td><td>12</td></tr>
<tr><td>Tipología</td><td>12 obligatorio</td></tr>
<tr><td>Organización temporal</td><td>2.1, 2.2</td></tr>
<tr><td>Modalidad</td><td>Presencial</td></tr>
<tr><td>Contenido de la Materia</td><td>En esta materia se estudian las propiedades fundamentales de las bases de datos y los principales modelos de datos, abordando mecanismos de seguridad esenciales.
Propiedades de las bases de datos
Principales modelos de datos
Lenguaje SQL
Mecanismos de seguridad en bases de datos
Recuperación y privacidad de datos</td></tr>
<tr><td rowspan="3">Resultados del aprendizaje de la materia</td><td>Conocimiento:
KM12: Identificar las propiedades de las bases de datos, los principales modelos de datos y el lenguaje SQL. [KT03]
KM13: Reconocer los mecanismos de cifrado, autenticación, autorización, auditoría y recuperación que garantizan la seguridad y la privacidad de los datos almacenados en las bases de datos. [KT04]</td></tr>
<tr><td>Habilidades:
SM10: Analizar el diseño y despliegue de Bases de Datos. [ST02]
SM11: Probar diferentes mecanismos de seguridad aplicados a las bases de datos para preservar su integridad y privacidad. [ST06]</td></tr>
<tr><td>Competencias:
CM9: Evaluar modelos de datos y bases de datos seguras [CT03]
CM10: Validar los diferentes mecanismos actuales de seguridad aplicados a las bases de datos para preservar su integridad y privacidad. [CT04]
CM11: Construir bases de datos seguras que tengan en cuenta los diferentes mecanismos de seguridad. [CT06]</td></tr>
<tr><td>actividades formativas</td><td>
<table>
<tr><td></td><td>Dirigidas</td><td>Supervisadas</td><td>Autónomas</td></tr>
<tr><td>Horas</td><td>99</td><td>9</td><td>192</td></tr>
<tr><td>% Presencialidad</td><td>100%</td><td>100%</td><td>0%</td></tr>
</table>
</td></tr>
<tr><td>Asignaturas</td><td>
<table>
<tr><td>Denominación</td><td>ECTS</td><td>Tipología</td><td>Semestre</td><td>Idioma</td></tr>
<tr><td>Bases de datos</td><td>6</td><td>OB</td><td>2.1</td><td>Castellano/catalán</td></tr>
</table>
</td></tr>
</table>

	Seguridad en bases de datos	6	OB	2.2	Castellano/catalán

Materia 5: Criptografía	
Número de créditos ECTS	18 créditos
Tipología	*6 básico, 6 obligatorio, 6 optativo*
Ámbito de Conocimiento	Ingeniería informática y de sistemas.
Organización temporal	1.2, 2.1, 3.2, 4.0
Modalidad	*Presencial*
Contenido de la Materia	Se tratan los conceptos, algoritmos, y técnicas que conforman las bases de la criptografía actual. Se estudian los fundamentos teóricos y prácticos de las herramientas criptográficas. • Criptografía simétrica y asimétrica • Técnicas criptográficas para garantizar propiedades de confidencialidad, integridad, autenticación y no repudio. • Fundamentos teóricos y prácticos de protocolos criptográficos.
Resultados del aprendizaje de la materia	Conocimiento: • KM14: Identificar los conceptos y algoritmos de la criptografía simétrica y asimétrica y las técnicas que permiten garantizar la confidencialidad, la integridad, la autenticación y el no repudio de los mensajes. [KT03] • KM15: Identificar los fundamentos teóricos y prácticos de los protocolos criptográficos que permiten establecer la autenticación mutua entre las partes. [KT03]
	Habilidades: • SM12: Analizar los diferentes componentes de los mecanismos de seguridad aplicados a la información (criptografía simétrica y asimétrica, cifrado, descifrado, generación de claves, firma digital) [ST04] • SM13: Emplear protocolos de autentificación para determinar su aplicabilidad y robustez delante de situaciones que puedan derivarse en un incidente de seguridad. [ST06]
	Competencias: • CM12: Validar los mecanismos de seguridad aplicados a la información basados en criptografía simétrica y asimétrica, cifrado, descifrado, generación de claves, firma digital. [CT04] • CM13: Construir entornos seguros que implementen protocolos de autentificación a diferentes niveles (aplicación/servicio, SO, base de datos, hardware) que permita garantizar la identidad y rol/permisos del usuario. [CT06]

actividades formativas		**Dirigidas**	**Supervisadas**	**Autónomas**
	Horas	148.5	13.5	288
	% Presencialidad	100%	100%	0%

Asignaturas	Denominación	ECTS	Tipología	Semestre	Idioma
	Criptografía básica	6	FB	1.2	Castellano/catalán
	Mecanismos de autentificación	6	OB	2.1	Castellano/catalán
	Criptografía avanzada	6	OP	3.2, 4.0	Castellano/catalán

Materia 6: Sistemas Operativos	
Número de créditos ECTS	30
Tipología	*6 básico, 24 obligatorio*
Ámbito de Conocimiento	Ingeniería informática y de sistemas.
Organización temporal	1.2, 2.2, 3.1, 3.2
Modalidad	*Presencial*
Contenido de la Materia	En esta materia se trabajan los conceptos fundamentales de los sistemas operativos, incluyendo procesos, servicios, sistemas de ficheros, y dispositivos, abordando aspectos de seguridad en su configuración y gestión. • Conceptos esenciales del sistema operativo • Funcionamiento de servicios distribuidos • Mecanismos de seguridad en aplicaciones virtualizadas y cloud
Resultados del aprendizaje de la materia	Conocimiento: • KM16: Identificar los conceptos esenciales del sistema operativo (procesos, servicios, archivos, dispositivos, entre otros), su configuración y administración segura. [KT01] • KM17: Reconocer el funcionamiento de los servicios distribuidos, identificando sus posibles vulnerabilidades, mecanismos de seguridad y las herramientas de análisis forense para la adquisición de evidencias después de incidentes. [KT02] • KM18: Identificar los mecanismos de seguridad y protección en aplicaciones virtualizadas tanto en sistemas locales como en el cloud analizando su efectividad, viabilidad, costo y consumo energético. [KT05]
	Habilidades:

- SM14: Analizar los sistemas operativos y los servicios distribuidos desde el punto de vista de la seguridad y en relación a su despliegue, configuración y administración. [ST08]
- SM15: Probar diferentes herramientas y configuración en el despliegue y pruebas de servidores seguros y aplicaciones distribuidas seguras. [ST06]
- SM16: Clasificar las diferentes técnicas y herramientas forenses para determinar los puntos de ataques y el daño causado a un sistema de información. [ST09]
- SM17: Analizar las diferentes configuraciones y protocolos para la ejecución segura de máquinas virtuales tanto en infraestructuras locales como en el cloud. [ST09]

Competencias:

- CM14: Desarrollar entornos, servicios y aplicaciones locales/distribuidas seguras. [CT03]
- CM15: Evaluar entornos de servidores seguros desde el hardware, el sistema operativo y el software que se ejecuta sobre él. [CT01]
- CM16: Evaluar las diferentes técnicas forenses determinando su eficacia, valor y capacidad de obtener información después de un incidente de seguridad. [CT05]
- CM17: Desarrollar configuraciones seguras para el despliegue de máquinas virtuales seguras que se ejecuten tanto en infraestructuras locales como en el cloud. [CT05]
- CM18: Evaluar los mecanismos de seguridad que permiten desplegar entornos seguros en el cloud, considerando todos los aspectos/servicios involucrados, y que garantizan la privacidad de la información. [CT03]

actividades formativas

	Dirigidas	**Supervisadas**	**Autónomas**
Horas	247.5	22.5	480
% Presencialidad	100%	100%	0%

Asignaturas

Denominación	ECTS	Tipología	Semestre	Idioma
Sistemas operativos	6	FB	1.2	Castellano/catalán
Sistemas distribuidos	6	OB	2.2	Castellano/catalán
Server hardening	6	OB	3.1	Castellano/catalán
Digital forensics	6	OB	3.1	Castellano/catalán
Seguridad en servicios de virtualización y cloud	6	OB	3.2	Castellano/catalán

Materia 7: Redes	
Número de créditos ECTS	24
Tipología	*6 básico, 18 obligatorio*
Ámbito de Conocimiento	Ingeniería informática y de sistemas.
Organización temporal	1.2, 2.1, 3.1, 3.2
Modalidad	*presencial*
Contenido de la Materia	En esta materia se proporciona una visión profunda de los fundamentos de las redes informáticas, incluida su topología, medios de transmisión y acceso al medio. Se abordan aspectos de seguridad en todos los ámbitos, así como el uso de herramientas y entornos para la gestión y administración segura. • Conceptos básicos de redes • Gestión de seguridad de red • Test de penetración de sistemas informáticos • Selección de herramientas y entornos de gestión de redes
Resultados del aprendizaje de la materia	Conocimiento: • KM19: Identificar los conceptos básicos de las redes de área local y las redes industriales, su topología, el medio de transmisión, el acceso al medio, y sus principales parámetros. [KT02] • KM20: Reconocer los métodos y herramientas para realizar la gestión de seguridad de red, como la detección y resolución de fallos, pérdida de rendimiento, aprovisionamiento de red y mantenimiento de la calidad de servicio. [KT02] • KM21: Identificar las fases y metodologías para realizar un test de penetración de sistemas informáticos utilizando las herramientas y técnicas apropiadas para cada caso. [KT04] • KM22: Seleccionar las herramientas y entornos más adecuados para la gestión y administración de redes de comunicaciones desde el punto de vista de la seguridad y detección de incidentes. [KT07]
	Habilidades: • SM18: Analizar los diferentes aspectos tecnológicos, funcionales y de configuración/administración de redes desde el punto de vista de la seguridad. [ST04] • SM19: Probar métodos, herramientas y procedimientos la penetración de sistemas de información evaluando su seguridad, mitigación y solución. [ST08] • SM20: Analizar la tecnología, herramientas y métodos para la gestión avanzada de seguridad en redes y en la detección de anomalías vinculadas a incidentes de seguridad. [ST09]
	Competencias:

	• CM19: Validar los protocolos de comunicación seguros y los procedimientos/recomendaciones de administración en redes para prevenir, detectar y mitigar los incidentes de seguridad sobre estas. [CT01] • CM20: Evaluar métodos y protocolos que permitan incrementar la seguridad en redes, así como la detección temprana de incidentes y la prevención de ataques. [CT02] • CM21: Desarrollar entornos seguros de redes que permitan hacer ensayos y pruebas sobre procedimientos de penetración, mitigación de ataques, detección de intrusiones y propagación software malicioso. [CT03] • CM22: Construir servicios seguros en redes que permitan la detección de incidentes teniendo en cuenta su administración y gestión continua. [CT04]

actividades formativas		**Dirigidas**	**Supervisadas**	**Autónomas**
	Horas	198	18	384
	% Presencialidad	100%	100%	0%

Asignaturas	Denominación	ECTS	Tipología	Semestre	Idioma
	Introducción a las redes de comunicación	6	FB	1.2	Castellano/catalán
	Servicios para redes seguras	6	OB	2.1	Castellano/catalán
	Administración de redes seguras	6	OB	3.1	Castellano/catalán
	Penetration testing	6	OB	3.2	Castellano/catalán

Materia 8: Gestión de Seguridad	
Número de créditos ECTS	6
Tipología	*6 obligatorio*
Organización temporal	4.1
Modalidad	*presencial*
Contenido de la Materia	Esta materia aborda la gestión de la seguridad. • Principios y metodologías de gestión de riesgos. • Análisis de impacto y evaluación de amenazas. • Selección y aplicación de medidas de mitigación. • Monitorización continua de la seguridad. • Consideraciones de costo y energía.
	Conocimiento:

<table>
<tr><td rowspan="3">Resultados del aprendizaje de la materia</td><td>• KM23: Identificar los principios y metodologías para realizar una gestión de riesgos en ciberseguridad, como el análisis de impacto, la identificación y evaluación de amenazas y vulnerabilidades, la selección y aplicación de medidas de mitigación y la monitorización, la revisión continua del nivel de seguridad, el costo y el consumo energético. [KT08]</td></tr>
<tr><td>Habilidades:
• SM21: Clasificar los métodos y herramientas para la gestión del riesgo, análisis y evaluación de amenazas/vulnerabilidades en un entorno de ciberseguridad. [ST09]
• SM22: Experimentar con métodos y herramientas de detección de vulnerabilidades e intrusos, monitorización, evaluación y mitigación de ataques sobre el sistema de información. [ST04]</td></tr>
<tr><td>Competencias:
• CM23: Evaluar los procedimientos de gestión del riesgo sobre los sistemas de información centrándose en la prevención, detección y gestión continua de los incidentes de seguridad. [CT06]</td></tr>
<tr><td>actividades formativas</td><td>
<table>
<tr><td></td><td>Dirigidas</td><td>Supervisadas</td><td>Autónomas</td></tr>
<tr><td>Horas</td><td>49.5</td><td>4.5</td><td>96</td></tr>
<tr><td>% Presencialidad</td><td>100%</td><td>100%</td><td>0%</td></tr>
</table>
</td></tr>
<tr><td>Asignaturas</td><td>
<table>
<tr><td>Denominación</td><td>ECTS</td><td>Tipología</td><td>Semestre</td><td>Idioma</td></tr>
<tr><td>Gestión de la ciberseguridad</td><td>6</td><td>OB</td><td>4.1</td><td>Castellano/catalán</td></tr>
</table>
</td></tr>
</table>

Materia 9: Privacidad	
Número de créditos ECTS	12
Tipología	*6 obligatorio, 6 optativo*
Organización temporal	*2.2, 3.2, 4.0*
Modalidad	*presencial*
Contenido de la Materia	En esta materia se estudian diferentes aspectos de la privacidad de datos. • Mecanismos para proteger la privacidad de los datos • Cuantificación de la privacidad de los datos • Diseño de sistemas centrados en la protección de la privacidad
Resultados del aprendizaje de la materia	Conocimiento: • KM24: Identificar los mecanismos existentes para proteger y cuantificar la privacidad de los datos teniendo en cuenta las herramientas que permiten el diseño de sistemas centrados en la protección de la privacidad. (KT04)
	Habilidades:

	• SM23: Analizar la toma de decisiones sobre los procesos de protección de la información a aplicar a partir de la evaluación del nivel de privacidad y la pérdida de información/privacidad introducida por un sistema de protección. (ST06)
	Competencias: • CM24: Desarrollar proyectos empresariales atendiendo a requisitos de privacidad, incluyendo mecanismos de seguridad (mecanismos y/o protocolos criptográficos) cuando sea necesario. (CT01)

actividades formativas		**Dirigidas**	**Supervisadas**	**Autónomas**
	Horas	99	9	192
	% Presencialidad	100%	100%	0%

Asignaturas	Denominación	ECTS	Tipología	Semestre	Idioma
	Conceptos fundamentales de privacidad	6	OB	2.2	Castellano/catalán
	Protección de datos y gestión de la privacidad	6	OP	3.2, 4.0	Castellano/catalán

Materia 10: Inteligencia Artificial	
Número de créditos ECTS	12
Tipología	*6 obligatorio, 6 optativo*
Organización temporal	*3.2, 4.1, 4.0*
Modalidad	*presencial*
Contenido de la Materia	Esta materia proporciona una base sólida sobre inteligencia artificial, su seguridad y su aplicación a la ciberseguridad. • Fundamentos de aprendizaje automático en ciberseguridad. • Identificación y aplicación de sistemas de aprendizaje automático. • Ataques a sistemas de aprendizaje automático. • Mitigación de ataques en entornos adversariales.
Resultados del aprendizaje de la materia	Conocimiento: • KM25: Identificar los sistemas de aprendizaje automático y su aplicación en el contexto de la ciberseguridad. (KT07) • KM26: Reconocer los ataques y sistemas de mitigación habituales para sistemas de aprendizaje automático en entornos con adversarios (KT07)
	Habilidades: • SM24: Analizar los modelos de IA más adecuados para la detección, identificación, segregación y mitigación de ataques. (ST06)

	• SM25: Probar diferentes modelos de IA en entornos controlados las principales técnicas de detección y solución de problemas de seguridad en sistemas de información. (ST07)
	Competencias: • CM25: Desarrollar modelos, algoritmos y entornos de IA para la detección de incidentes de seguridad. (CT05)

actividades formativas		**Dirigidas**	**Supervisadas**	**Autónomas**
	Horas	99	9	192
	% Presencialidad	100%	100%	0%

Asignaturas	Denominación	ECTS	Tipología	Semestre	Idioma
	IA aplicada a la ciberseguridad	6	OB	4.1	Castellano/catalán
	Adversarial machine learning	6	OP	3.2, 4.0	Castellano/catalán

Materia 11: Interfaces de Seguridad	
Número de créditos ECTS	18
Tipología	*6 obligatorio, 12 optativo*
Organización temporal	*3.2, 4.0*
Modalidad	*Presencial*
Contenido de la Materia	Esta materia abarca contenidos sobre dispositivos de seguridad, usabilidad y biometría. • Tipos y características de dispositivos de seguridad de software/hardware • Criterios y técnicas para evaluar y mejorar la usabilidad de aplicaciones segur • Fundamentos y técnicas de la biometría
Resultados del aprendizaje de la materia	Conocimiento: • KM27: Identificar los tipos y características de los dispositivos de seguridad del hardware así como su configuración y administración en la prevención de ataques y contramedidas. (KT04) • KM28: Reconocer los criterios y técnicas para evaluar y mejorar la usabilidad de las aplicaciones seguras. (KT05) • KM29: Identificar los fundamentos y las técnicas de la biometría, los dispositivos y su configuración segura y cómo estos se aplican para mejorar la seguridad y la privacidad en los sistemas de información. (KT07)
	Habilidades:

	• SM26: Analizar los requisitos de los dispositivos de seguridad hardware basándose en criterios de grado de seguridad, funcionalidad, eficiencia y administración. (ST04) • SM27: Emplear entornos de diseño, desarrollo y despliegue de aplicaciones centradas en el usuario bajo criterios de seguridad y técnicas biométricas. (ST06)
	Competencias: • CM26: Construir sistemas hardware/software basado en criterios de seguridad y métodos biométricos teniendo en cuenta los requerimientos de los SO/aplicaciones y su usabilidad. (CT06)

actividades formativas		**Dirigidas**	**Supervisadas**	**Autónomas**
	Horas	148.5	13.5	288
	% Presencialidad	100%	100%	0%

Asignaturas	Denominación	ECTS	Tipología	Semestre	Idioma
	Seguridad en Hardware	6	OB	3.2	Castellano/catalán
	Aspectos de la Usabilidad en Aplicaciones Seguras	6	OP	3.2, 4.0	Castellano/catalán
	Biometría	6	OP	3.2, 4.0	Castellano/catalán

Materia 12: Seguridad en Entornos Móviles	
Número de créditos ECTS	24
Tipología	*24 optativo*
Organización temporal	*3.2, 4.0*
Modalidad	*presencial*
Contenido de la Materia	Esta materia abarca el funcionamiento de redes inalámbricas, características y riesgos de sistema operativos móviles y el desarrollo de aplicaciones móviles, haciendo especial énfasis en aspectos de seguridad. • Funcionamiento de las redes inalámbricas • Características de los sistemas operativos móviles (SO) • Desarrollo de aplicaciones móviles seguras
Resultados del aprendizaje de la materia	Conocimiento: • KM30: Identificar el funcionamiento de las redes inalámbricas, sus posibles vulnerabilidades y sus mecanismos de defensa. (KT03) • KM31: Reconocer las características, las vulnerabilidades y los mecanismos de protección de los SO para móviles, así como las mejores prácticas para su administración y uso bajo criterios de seguridad y privacidad. (KT05)

	• KM32: Seleccionar las herramientas más adecuadas para el diseño, desarrollo y despliegue de aplicaciones móviles bajo criterios de seguridad. (KT05)
	Habilidades: • SM28: Analizar los diferentes aspectos vinculados a la seguridad de las redes y los protocolos inalámbricos identificando sus puntos débiles, ataques, infecciones y vulnerabilidades. (ST06) • SM29: Probar herramientas, métodos y procedimientos adecuados para detectar vulnerabilidades y puntos débiles en sistemas operativos móviles. (ST09) • SM30: Emplear entornos de diseño, programación, configuración y gestión de aplicaciones móviles seguras. (ST03)
	Competencias: • CM27: Desarrollar aplicaciones móviles seguras. (CT03) • CM28: Evaluar los parámetros y configuraciones de seguridad de los SO móviles y las redes inalámbricas para la monitorización y prevención de ataques. (CT05)

actividades formativas				
	Dirigidas	**Supervisadas**	**Autónomas**
Horas	198	18	384
% Presencialidad	100%	100%	0%

Asignaturas	Denominación	ECTS	Tipología	Semestre	Idioma
	Introducción a la Programación en Entornos Móviles	6	OP	3.2, 4.0	Castellano/catalán
	Seguridad en Sistemas Operativos para Móviles	6	OP	3.2, 4.0	Castellano/catalán
	Seguridad en Redes Inalámbricas	6	OP	3.2, 4.0	Castellano/catalán
	Seguridad en Aplicaciones Móviles	6	OP	3.2, 4.0	Castellano/catalán

Materia 13: Aspectos de Seguridad en Industria y Aplicaciones	
Número de créditos ECTS	42
Tipología	*30 optativo*
Organización temporal	*3.2, 4.0*
Modalidad	*presencial*
Contenido de la Materia	Los contenidos abarcan los aspectos esenciales en seguridad en la industria y en aplicaciones, proporcionando los conocimientos necesarios para

	comprender y abordar los desafíos de seguridad en diversos entornos tecnológicos. • Principios del análisis de redes sociales • Seguridad en dispositivos médicos • Seguridad en sistemas industriales • Seguridad en infraestructuras críticas • Tecnología blockchain y criptomonedas
Resultados del aprendizaje de la materia	Conocimiento: • KM33: Reconocer los principios y técnicas del análisis de redes sociales, incluyendo la recopilación y análisis de datos, la identificación de patrones y tendencias para mejorar la seguridad y la privacidad en los sistemas informáticos. (KT07) • KM34: Identificar los principales problemas de seguridad de dispositivos médicos, infraestructuras de blockchains, criptomonedas y smart contracts, sistemas industriales e infraestructuras críticas teniendo en cuenta su configuración, uso y administración. (KT04)
	Habilidades: • SM31: Analizar los diferentes aspectos en la recogida de información en redes sociales procesando esta información mediante las herramientas adecuadas para obtener información sensible de futuros objetivos. (ST06) • SM32: Analizar desde el punto de vista de la seguridad los diferentes aspectos vinculados a los sistemas industriales, dispositivos médicos y las infraestructuras críticas. (ST08) • SM33: Clasificar los diferentes aspectos vinculados a las seguridad y vulnerabilidad de las criptomonedas y smart contracts. (ST09)
	Competencias: • CM29: Evaluar aplicaciones, protocolos de comunicación y dispositivos que tengan como valor fundamental la privacidad de la información y que sean susceptibles de ser vulnerada. (CT02) • CM30: Construir entornos seguros basados en tecnología de blockchain. (CT03) • CM31: Desarrollar métodos de análisis de grandes volúmenes de datos que permitan detectar intrusiones y ataques en sistemas de control industrial e infraestructuras críticas. (CT05)
actividades formativas	

	Dirigidas	**Supervisadas**	**Autónomas**
Horas	346.5	31.5	672
% Presencialidad	100%	100%	0%

Asignaturas	Denominación	ECTS	Tipología	Semestre	Idioma
	Análisis de Redes Sociales	6	OP	3.2, 4.0	Castellano/catalán
	Seguridad en EHealth	6	OP	3.2, 4.0	Castellano/catalán

Tecnología Blockchain y Criptomonedas	6	OP	3.2, 4.0	Castellano/catalán
Tecnología Blockchain y Smart Contracts	6	OP	3.2, 4.0	Castellano/catalán
Seguridad en Industria e Infraestructuras Críticas	6	OP	3.2, 4.0	Castellano/catalán
Seguridad en Sistemas de Control Industrial	6	OP	3.2, 4.0	Castellano/catalán
Informática Industrial y Sistemas Basados en PLC	6	OP	3.2, 4.0	Castellano/catalán

Materia 14: Trabajo de Fin de Grado	
Número de créditos ECTS	12
Tipología	*12 obligatorio*
Organización temporal	*4.0*
Modalidad	*presencial*
Contenido de la Materia	Desarrollo de un proyecto basado en los conocimientos adquiridos sobre ciberseguridad.
Resultados del aprendizaje de la materia	Conocimiento: • KM35: Demostrar conocimientos en protocolos, herramientas, estructuras y entornos que gestionen/administren la seguridad de la información. (KT04) • KM36: Definir y diseñar infraestructuras y aplicaciones seguras bajo el criterio de la seguridad de los datos y desplegar entornos en base a la seguridad de la información. (KT07)
	Habilidades: • SM34: Clasificar todos los aspectos, criterios, métodos y requerimientos, desde el hardware hasta el software, que garantizan la protección y privacidad del sistema de información delante de incidentes de seguridad. (ST09) • SM35: Probar herramientas, métodos y protocolos orientados a incrementar la seguridad, proteger la información sobre dispositivos locales, móviles, cloud o médicos o teniendo en cuenta aspecto legales y éticos. (ST07)
	Competencias: • CM32: Desarrollar proyectos empresariales centrados en la evaluación del riesgo, detección, clasificación, mitigación y/o solución de incidentes de seguridad en base al hardware, el SO, aplicaciones, servicios y las redes de comunicación utilizados. (CT01)

	• CM33: Investigar las desigualdades de género y el impacto ético y social de tecnologías como la inteligencia artificial en la privacidad y dignidad de colectivos vulnerables. Analizar el papel de la ciberseguridad en su protección, proponiendo medidas de prevención y control para evitar su uso indebido. [CT07]

actividades formativas		**Dirigidas**	**Supervisadas**	**Autónomas**
	Horas	0	75	225
	% Presencialidad	100%	10%	0%

Asignaturas	Denominación	ECTS	Tipología	Semestre	Idioma
	Trabajo de Fin de Grado	12	TFE	4.0	Castellano/catalán

Materia 15: Prácticas Profesionales	
Número de créditos ECTS	12
Tipología	*12 optativo*
Organización temporal	*3.2, 4.0*
Modalidad	*presencial*
Contenido de la Materia	
Resultados del aprendizaje de la materia	Conocimiento: • KM37: Definir y diseñar infraestructuras y aplicaciones seguras bajo el criterio de la seguridad de los sistemas informáticos y desplegar entornos en base a la seguridad de la información en entornos profesionales concretos. (KT01) • KM38: Demostrar conocimientos de las soluciones apropiadas y comprender la complejidad de los problemas en ciberseguridad y la viabilidad de sus soluciones. (KT07)
	Habilidades: • SM36: Examinar la toma de decisiones en el ámbito de la ciberseguridad a partir de la evaluación critica, considerando los riesgos y beneficios, así como las cuestiones éticas, y seleccionando la mejor solución en función de los objetivos definidos en el entorno concreto de la empresa. (ST08)
	Competencias: • CM34: Desarrollar proyectos empresariales centrados en la evaluación del riesgo, detección, clasificación, mitigación y/o

	solución de incidentes de seguridad en base al hardware, el SO, aplicaciones, servicios y las redes de comunicación utilizados. (CT01)

actividades formativas		**Dirigidas**	**Supervisadas**	**Autónomas**
	Horas	0	75	225
	% Presencialidad	100%	10%	0%

Asignaturas	Denominación	ECTS	Tipología	Semestre	Idioma
	Prácticas Profesionales	12	PRO	3.2, 4.0	Castellano/catalán

Tabla de relación resultados de aprendizaje de Titulación / Materias

	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15
KT01	KM01 KM03					KM16									KM37
KT02	KM02 KM04		KM08			KM17	KM19 KM20								
KT03		KM06 KM07		KM12	KM14 KM15							KM30			
KT04	KM05		KM09	KM13			KM21		KM24		KM27		KM34	KM35	
KT05			KM10			KM18					KM28	KM31 KM32			
KT06			KM11												
KT07							KM22			KM25 KM26	KM29		KM33	KM36	KM38
KT08								KM23							
ST01	SM02	SM04 SM05													
ST02	SM01		SM06	SM10											
ST03			SM09									SM30			
ST04					SM12		SM18	SM22			SM26				
ST05	SM03														
ST06			SM07	SM11	SM13	SM15			SM23	SM24	SM27	SM28	SM31		
ST07			SM08							SM25				SM35	
ST08						SM14	SM19						SM32		SM36
ST09						SM16 SM17	SM20	SM21				SM29	SM33	SM34	
CT01	CM01		CM05			CM15	CM19		CM24					CM32	CM34
CT02	CM02						CM20						CM29		
CT03			CM06	CM9		CM14 CM18	CM21					CM27	CM30		
CT04	CM03	CM04		CM10	CM12		CM22								
CT05			CM07			CM16 CM17				CM25		CM28	CM31		
CT06			CM0~~9~~ 8	CM1	CM13			CM23			CM~~27~~ 26				
CT07														CM33	

TOTAL	**11**	**5**	**12**	**7**	**6**	**12**	**11**	**4**	**3**	**5**	**6**	**8**	**8**	**6**	**4**

4.2. Actividades y metodologías docentes

4.2.a) Materias básicas, obligatorias y optativas

Metodologías docentes

La metodología docente en el grado se basa en el concepto de "aprender haciendo" (l*earning by doing*). Se trabajará para que los estudiantes se enfrenten a proyectos y retos que aborden problemas de aplicación de la ciberseguridad en el mundo profesional o científico, en vez de limitarse a simples casos de laboratorio para fines docentes. En este sentido, se establecerá un marco de colaboración sólido con empresas e instituciones externas mediate el Consejo Asesor del Grado que podrá proporcionar problemas surgidos de su actividad cotidiana. Este enfoque va más allá de la definición de propuestas para trabajos fin de grado o prácticas externas, se busca una implicación más global de las entidades externas en el grado, abarcando cualquier asignatura. En este modelo, las empresas podrán definir casos de uso reales basados en su actividad y proporcionar los datos y la infraestructura necesaria para abordarlos.

De forma resumida, las principales metodologías docentes que se utilizaran en el grado son las siguientes.

En las actividades dirigidas, se utilizarán las siguientes metodologías docentes:

MD1. Aprendizaje basado en proyectos, retos y/o problemas: El alumnado resuelve proyectos prácticos o desafíos reales, aplicando conocimientos teóricos a situaciones concretas para desarrollar habilidades técnicas y de resolución de problemas.

MD2. Resolución de problemas y/o casos prácticos: El alumnado aborda problemas o casos reales o simulados, analizando situaciones complejas y aplicando soluciones prácticas para desarrollar pensamiento crítico y habilidades analíticas.

MD3. Aprendizaje cooperativo: El alumnado trabaja en equipo para lograr objetivos comunes, promoviendo la colaboración, el intercambio de ideas y el aprendizaje mutuo.

MD4. Clases magistrales: El profesorado imparte lecciones teóricas frente al alumnado, proporcionando conocimientos fundamentales y explicando conceptos clave de manera estructurada.

MD5. Aula invertida: El alumnado estudia los contenidos teóricos fuera del aula, generalmente mediante recursos digitales, y el tiempo en clase se dedica a actividades prácticas y discusiones guiadas.

MD6. Prácticas de laboratorio: El alumnado realiza actividades prácticas en entornos controlados, aplicando los conceptos aprendidos a situaciones experimentales, como en el caso de la ciberseguridad, la realización de pruebas en sistemas.

MD7. Debates y desarrollo del pensamiento crítico: El alumnado participa en discusiones estructuradas sobre temas relevantes, promoviendo la reflexión, la argumentación y el análisis crítico de diferentes perspectivas.

MD8. Actividades de evaluación: Se realizan actividades formativas y sumativas para medir el progreso del alumnado, como exámenes, proyectos, pruebas prácticas o presentaciones.

En las actividades supervisadas, se utilizará la siguiente metodología docente:

MS1. Aprendizaje servicio: El alumnado se involucran en proyectos que benefician a la comunidad, aplicando sus conocimientos en situaciones reales para resolver necesidades sociales y al mismo tiempo fortalecer su aprendizaje.

MS2. Tutorías: Sesiones personalizadas entre alumnado y profesorado, donde se abordan dudas, se da orientación académica y se refuerzan los contenidos, permitiendo un seguimiento individualizado del progreso del alumnado.

MS3. Trabajo final de Grado: El alumnado realiza un trabajo bajo la supervisión del tutor/a académico.

MS4. Prácticas Profesionales: El alumnado realiza prácticas curriculares en una empresa del sector.

En las actividades autónomas:

MA1. Elaboración de trabajos: El alumnado realiza investigaciones, elabora proyectos o trabajos escritos y luego los presenta o expone ante la clase, desarrollando habilidades de comunicación y análisis.

MA2. Estudio personal: El alumnado trabaja de forma autónoma, revisando materiales, realizando ejercicios o profundizando en los contenidos para fortalecer su aprendizaje individual.

MA3. Resolución de problemas y casos fuera del aula: El alumnado aborda ejercicios o situaciones prácticas de manera autónoma fuera del aula, aplicando los conocimientos teóricos a contextos reales o simulados.

4.2.b) Prácticas académicas externas (obligatorias)

No se proponen prácticas externas obligatorias.

4.2.c) Trabajo de fin de Grado o Máster

El Trabajo de Fin de Grado (TFG) consiste en un proyecto en el ámbito de la ciberseguridad que se realiza de forma individual bajo la supervisión de una persona tutora y es posteriormente presentado y defendido ante un tribunal universitario.

El trabajo de fin de Grado se regulará con la misma normativa, planificación y seguimiento que el TFG del grado de Ing. Informática. A modo de resumen, se incluyen aquí los puntos principales.

- Oferta: por el profesorado tutor, por empresas o instituciones externas o por el propio estudiantado. El coordinador de Titulación validará que la propuesta cumpla con los requisitos mínimos del TFG.
- Asignación en base a la priorización realizada por el estudiantado.
- Seguimiento periódico del progreso, en función de los objetivos y la planificación definidos al inicio del proyecto (estudiantado y persona tutora).
- Presentación de una memoria o informe y defensa oral ante un tribunal universitario.

La gestión del proceso se realizará con la misma aplicación web que se utiliza para la gestión de los TFG del grado de Ingeniería en Informática.

Para poder cursar el TFG se debe haber superado como mínimo todas las asignaturas de primer curso y dos tercios del total de ECTS del plan de estudios (es decir 160 ECTS).

El trabajo de fin de Grado se regulará de acuerdo con las directrices establecidas en el Sistema de Garantía Interna de Calidad (SGIQ) de la Escuela de Ingeniería.

4.3. Sistemas de evaluación

4.3.a) Evaluación de las materias básicas, obligatorias y optativas

Los sistemas de evaluación que tendrán mayor relevancia en el plan de estudios que certificarán la consecución de los resultados de aprendizaje descritos en la Sección 2 se enumeran a continuación. Entre paréntesis, el mínimo y máximo impacto en la nota final de cada sistema de evaluación.

AE1 Pruebas escritas individuales (20% - 60%).

AE2 Realización de prácticas o proyectos (20% - 50%).

AE3 Resolución de problemas o casos (20% - 40%).

AE4 Entrega de informes y trabajos (0% - 20%).

AE5 Exposición de trabajos (0% - 20%).

Las pruebas escritas individuales están diseñadas para evaluar y verificar que el alumnado ha adquirido los resultados de aprendizaje relacionados con la tipología de conocimientos. Las demás actividades se centran en medir los resultados de aprendizaje relacionados con habilidades y competencias. En un primer nivel, estas actividades evalúan la capacidad de los estudiantes para probar, experimentar y aplicar métodos, técnicas y herramientas concretas. La mayoría de las habilidades descritas en las asignaturas se verifican así, incluyendo la habilidad de los estudiantes para comunicar eficientemente los resultados de su trabajo.

Las prácticas externas, con carácter optativo, se realizarán en empresas relacionadas con la ciberseguridad. El estudiantado cuenta con un tutor en la empresa y un tutor académico en la universidad. El profesorado que tutoriza las prácticas será profesorado de la propia titulación. El alumnado hará un informe final que evaluará el tutor de la universidad. Las entidades en las que se realizaran estas prácticas serán empresas del sector de la ciberseguridad o empresas de otros sectores donde el alumnado realice funciones relacionadas con la ciberseguridad (protección o monitorización de infraestructuras, programación segura, etc.). 4.3.b) Evaluación de las Prácticas académicas externas (obligatorias)

4.3.b) Evaluación de las Prácticas académicas externas (obligatorias)

No se proponen prácticas externas obligatorias.

4.3.c) Evaluación del Trabajo de fin de Grado o Máster

La evaluación del Trabajo de Fin de Grado (TFG) se hará individualmente. Esta evaluación tomará en consideración el progreso del estudiantado a lo largo del semestre, el resultado final del proyecto, la memoria explicativa y la defensa oral. Se utilizarán rúbricas para valorar si el estudiante ha adquirido las competencias del grado a través del contenido del trabajo (incluyendo la capacidad para abordar aspectos éticos, la diversidad y la perspectiva de género), así como la metodología empleada, la dificultad del trabajo, el resultado final (considerando tanto su calidad como el grado de innovación y las conclusiones derivadas), la redacción y otros aspectos formales de la documentación, la presentación oral y las respuestas del estudiantado a las preguntas realizadas durante la defensa del trabajo.

El tribunal encargado de evaluar el TFG estará compuesto por tres miembros, uno de los cuáles podrá ser la persona que ha tutorizado el trabajo. De estos tres miembros, al menos uno deberá ser una persona experta en la temática específica del trabajo, mientras que otra deberá serlo en cualquier temática dentro del ámbito de la ciberseguridad. Además, como mínimo uno de ellos será doctor.

El Coordinador de la titulación o de la asignatura otorgará Matrículas de honor, en caso de ser procedente, basándose en las propuestas del tribunal, que deberá recibir por escrito.

4.4. Estructuras curriculares específicas

No procede

5. PERSONAL ACADÉMICO Y DE APOYO A LA DOCENCIA

5.1. Perfil básico del profesorado

5.1.a) Descripción de la plantilla de profesorado del título

(700 palabras máximo)

Un total de 53 docentes forman la plantilla del Grado en Ciberseguridad. En su mayoría profesorado de tipo “Permanente 1”. La formación básica y obligatoria queda cubierta por este tipo de profesorado, que, junto al profesorado Lectores, suponen un 74% del total de docentes asignados. EL profesorado de las categorías "Permanente 1" y "Lector", cuenta con una amplia experiencia y conocimiento en el área, siendo el 100% de ellos doctores/as acreditados/as. Además, se cuenta con 14 docentes de categoría "Asociado", un 26%, Este profesorado imparte, mayoritariamente, docencia en clases de problemas y apoyo en los laboratorios docentes. Aunque suponen una menor proporción, se trata de profesionales del sector de la ciberseguridad que aportan experiencia profesional en la industria, así como una visión práctica y actual al grado.

El profesorado asociado, que trabaja en empresas del sector, juega un papel clave en el diseño e impartición de asignaturas. Su colaboración asegura que los contenidos académicos estén alineados con las demandas del mercado laboral y las tendencias emergentes en la industria de la ciberseguridad. Además, su experiencia práctica en empresas y organizaciones del sector enriquece la formación de los estudiantes, ofreciéndoles acceso a casos reales que complementan los conceptos teóricos. Esta integración del profesorado asociado fortalece la formación integral de los estudiantes, preparándolos para enfrentar los desafíos profesionales en ciberseguridad con una sólida base tanto técnica como práctica.

Todo el profesorado, independientemente de su área de conocimiento, cuenta con índices de excelencia elevado en lo que respecta su experiencia y calidad investigadora. La gran mayoría de profesorado "Permanente 1" y "Lectores" ostenta sexenios vivos de investigación, participando activamente en proyectos financiados y publicaciones científicas. Para detalles específicos sobre las investigaciones y publicaciones del profesorado, se puede acceder a las webs de los diferentes departamentos que cubren las principales áreas de conocimiento del grado:

- Departamento de Ingeniería de la Información y de las Comunicaciones
- Departamento de Arquitectura de Computadores y Sistemas Operativos
- Departamento de Ciencias de la Computación
- Departamento de Microelectrónica y Sistemas Electrónicos
- Departamento de Telecomunicación e Ingeniería de Sistemas

El profesorado de estos departamentos está distribuido en diferentes grupos de investigación, relacionados con la docencia a impartir de forma directa. Dichos grupos de investigación y su producción científica se pueden consultar a partir de las webs citadas.

5.1.b) Estructura de profesorado

Tabla 6. Resumen del profesorado asignado al título

Categoría	Núm.	ECTS (%)	Doctores/as (%)	Acreditados/as (%)	Sexenios	Quinquenios

Permanentes 1	30	159,61 (56,60%)	30 (100%)	30 (100%)	90	90
Permanentes 2	0	0	0	0	0	0
Lectores	9	47,88 (16,98%)	9 (100%)	9 (100%)	0	0
Asociados	14	74,51 (26,42%)	0	0	0	0
Otros	0	0	0	0	0	0
Total	**53**	**282 (100%)**	**39 (73,58%)**	**39 (100%)**	**90**	**90**

Permanentes 1: profesorado permanente para el que es necesario ser doctor (CC, CU, CEU, TU, agregado y asimilables en centros privados).

Permanentes 2: profesorado permanente para el que no es necesario ser doctor (TEU, colaboradores y asimilables en centros privados).

Otros: profesorado visitante, becarios, etc.

El profesorado funcionario (CU, TU, CEU y TEU) se considerará acreditado.

5.2. Perfil detallado del profesorado

5.2.a) Detalle del profesorado asignado al título por ámbito de conocimiento

Tabla 7a. Detalle del profesorado asignado al título por ámbitos de conocimiento.

Área o ámbito de conocimiento 1: Ciencias de la computación e inteligencia artificial	
Número de profesores/as	24
Número y % de doctores/as	67%
Número y % de acreditados/as	67%
Número de profesores/as por categorías	Permanentes 1: 11 Permanentes 2: 0 Lectores: 5 Asociados: 8 Otros: 0
Materias / asignaturas	Materia 1: Formación básica en ciberseguridad Materia 2: Matemáticas Materia 3: Programación Materia 4: Bases de datos Materia 5: Criptografía Materia 7: Redes Materia 9: Privacidad Materia 10: Inteligencia artificial Materia 11: Interfaces de seguridad

	Materia 13: Aspectos de seguridad en industria y otras aplicaciones
ECTS impartidos (previstos)	123
ECTS disponibles (potenciales)	921,67

Área o ámbito de conocimiento 2: Arquitectura y tecnología de computadores	
Número de profesores/as	18
Número y % de doctores/as	67%
Número y % de acreditados/as	67%
Número de profesores/as por categorías	Permanentes 1:8 Permanentes 2: 0 Lectores: 4 Asociados:6 Otros: 0
Materias / asignaturas	Materia 1: Formación básica en ciberseguridad Materia 3: Programación Materia 6: Sistemas operativos Materia 7: Redes Materia 8: Gestión de seguridad Materia 11: Interfaces de seguridad Materia 12: Seguridad en entornos móviles Materia 13: Aspectos de seguridad en industria y otras aplicaciones
ECTS impartidos (previstos)	102
ECTS disponibles (potenciales)	886,61

Se deben añadir tantas tablas como ámbitos de conocimiento participen en la docencia

Área o ámbito de conocimiento 3: Ingeniería de Sistemas y Automática	
Número de profesores/as	3
Número y % de doctores/as	100%
Número y % de acreditados/as	100%
Número de profesores/as por categorías	Permanentes 1: 3
Materias / asignaturas	Materia 1: Formación básica en ciberseguridad Materia 2: Interfaces de seguridad Materia 3: Seguridad en entornos móviles

	Materia 4: Aspectos de seguridad en industria y otras aplicaciones Materia 11: Interfaces de seguridad Materia 13: Aspectos de seguridad en industria y otras aplicaciones
ECTS impartidos (previstos)	27
ECTS disponibles (potenciales)	67,98

Área o ámbito de conocimiento 4: Teoría de la Señal y Comunicaciones	
Número de profesores/as	2
Número y % de doctores/as	100%
Número y % de acreditados/as	100%
Número de profesores/as por categorías	Permanentes 1: 2
Materias / asignaturas	Materia 12: Seguridad en entornos móviles
ECTS impartidos (previstos)	6
ECTS disponibles (potenciales)	300,55

Área o ámbito de conocimiento 5: Álgebra	
Número de profesores/as	1
Número y % de doctores/as	100 %
Número y % de acreditados/as	100 %
Número de profesores/as por categorías	Permanentes 1: 1
Materias / asignaturas	Materia 1: Matemáticas
ECTS impartidos (previstos)	6
ECTS disponibles (potenciales)	262,24

Área o ámbito de conocimiento 6: Derecho Internacional Público y Relaciones Internacionales	
Número de profesores/as	1
Número y % de doctores/as	100 %
Número y % de acreditados/as	100 %
Número de profesores/as por categorías	Permanentes 1: 1

Materias / asignaturas	Materia 1: Formación básica en ciberseguridad
ECTS impartidos (previstos)	3
ECTS disponibles (potenciales)	516,68

Área o ámbito de conocimiento 7: Historia del Derecho y de las Instituciones	
Número de profesores/as	1
Número y % de doctores/as	100 %
Número y % de acreditados/as	100 %
Número de profesores/as por categorías	Permanentes 1: 1
Materias / asignaturas	Materia 1: Formación básica en ciberseguridad
ECTS impartidos (previstos)	3
ECTS disponibles (potenciales)	177,61

Área o ámbito de conocimiento 8: Lógica y Filosofía de la Ciencia	
Número de profesores/as	1
Número y % de doctores/as	100 %
Número y % de acreditados/as	100 %
Número de profesores/as por categorías	Permanentes 1: 1
Materias / asignaturas	Materia 1: Formación básica en ciberseguridad
ECTS impartidos (previstos)	3
ECTS disponibles (potenciales)	116,34

Área o ámbito de conocimiento 8: Filosofía Moral	
Número de profesores/as	1
Número y % de doctores/as	100 %
Número y % de acreditados/as	100 %
Número de profesores/as por categorías	Permanentes 1: 1
Materias / asignaturas	Materia 1: Formación básica en ciberseguridad
ECTS impartidos (previstos)	3

ECTS disponibles (potenciales)	128,66

Área o ámbito de conocimiento 9: Organización de Empresas	
Número de profesores/as	1
Número y % de doctores/as	100 %
Número y % de acreditados/as	100 %
Número de profesores/as por categorías	Permanentes 1: 1
Materias / asignaturas	Materia 1: Gestión de la Ciberseguridad
ECTS impartidos (previstos)	6
ECTS disponibles (potenciales)	895,04

5.2.b) Méritos docentes del profesorado no acreditado y/o méritos de investigación del profesorado no doctor

La contribución del profesorado no acreditado o no doctor del Grado en Ciberseguridad se basa en una combinación de experiencia práctica profesional y conocimientos especializados. Estos profesionales aportan una valiosa experiencia profesional y méritos docentes que enriquecen significativamente el entorno educativo. Entre el profesorado no acreditado, encontramos a profesionales de la empresa y administración pública que cuentan con amplia experiencia en el campo de la Ciberseguridad. Otros perfiles de profesores no acreditados son Investigadores predoctorales como FPI o de convocatorias internas de la UAB e Investigadores postdoctorales, que están integrados en grupos de investigación relacionados con los campos en los que imparten docencia.

Se trata de profesorado que colabora o ha colaborado recientemente con los diferentes grupos de investigación de los Departamentos de la Universidad Autónoma de Barcelona, y alterna esa actividad de investigación o docencia con una carrera profesional pública o privada, incluyendo profesores de educación secundaria.

5.2.c) Perfil del profesorado necesario y no disponible y plan de contratación

No procede.

5.2.d) Perfil básico de otros recursos de apoyo a la docencia necesarios

La Escuela cuenta con suficiente personal técnico y de administración y servicios especializado de apoyo a la docencia. Parte de estos recursos humanos destinados al soporte de la docencia son de ámbito central de la universidad.

De forma más concreta, la Escuela de Ingeniería cuenta con el apoyo administrativo y técnico de, entre otros, los siguientes servicios de apoyo a la docencia: Servicio de Informática, Administración de Centro, Gestión de la Calidad, Gestión Académica, Gestión Económica, Biblioteca, etc. La lista y los detalles de todos los servicios y su funcionamiento pueden consultarse a través de la página web de información de la Escuela de Ingeniería.

Así mismo, la universidad cuenta con los siguientes servicios: servició de apoyo a los estudiantes con necesidades educativas especificas (PIUNE), servicio asistencial de salud (SAS), unidad de psicología (SPL), servicio de psicología y logopedia (SPL), observatorio de igualdad, servicio de ocupabilidad, unidad de asesoramiento pedagógico, residencia universitaria y alojamiento adaptado en el campus, aulas de estudio, etc. La lista de servicios disponibles en el campus de puede encontrar en la página web de la UAB.

6. RECURSOS PARA EL APRENDIZAJE: MATERIALES E INFRAESTRUCTURALES, PRÁCTICAS Y SERVICIOS

6.1. Recursos materiales y servicios

La Escuela de Ingeniería dispone de la infraestructura docente adecuada para toda su oferta formativa tanto de grado como de postgrado. Cuenta con **20 aulas de docencia, 3 aulas de informática, 12 laboratorios docentes y diversas salas de seminarios y de trabajo en grupo** con los que atender una amplia variedad de actividades y metodologías docentes. Estos espacios cuentan con equipos audiovisuales e informáticos y tienen acceso a Internet, además, de laboratorios y aulas electrificadas. Todos los locales son accesibles para personas con necesidades especiales y las aulas cuentan con extensión de pupitre móvil para alumnos discapacitados.

Para el desarrollo de esta titulación, se utilizarán los siguientes recursos específicos:

- Licencias de software comercial de seguridad, como la detección de intrusiones o ataques.
- Software de protección o prevención.
- Redes y servidores aislados para la realización de pruebas específicas.
- *Sandboxing* para ejecutar y analizar aplicaciones y archivos sospechosos sin riegos por ejemplo en el estudio de análisis de *malware*.
- Sistema *cloud* privado para creación de infraestructura virtual para prácticas de programación, estudio de intrusiones, CTF, DoS, *pentesting*, etc.,
- Entornos para el estudio de mecanismos de protección (*hardening*, *firewalls*, IDSs, etc.)

En el caso de las aulas de informática los servicios de la universidad instalan anualmente en los ordenadores todo el programario que el profesorado solicita para poder realizar adecuadamente la docencia.

En relación a los **servicios de apoyo al estudiantado y profesorado** la Escuela cuenta con la Biblioteca de Ciencia y Tecnología (BCT) y el Servicio de Informática Distribuida (SID). La BCT forma parte del Servicio de Bibliotecas de la UAB y cuenta con la ISO 9001:2015 y el Certificado de Calidad de los Servicios Bibliotecarios ANECA que garantizan un óptimo servicio y una política de mejora continua. La Biblioteca Digital está a disposición de toda la comunidad universitaria para acceder a las principales revistas y manuales de referencia.

El SID da soporte informático a la docencia, investigación y administración del centro y sus titulaciones y gestiona el Campus Virtual, plataforma informática de uso docente, basada en Moodle, que proporciona un Entorno Virtual de Aprendizaje para apoyar en los estudios.

6.2 Procedimiento para la gestión de las prácticas académicas externas

La programación y seguimiento de las prácticas externas se realiza acorde con lo especificado en el proceso PC3: Gestió de les practiques externes i dels projectes final d'estudis (PFE) del SGIQ del centro. La gestión de las Prácticas Profesionales se lleva a cabo por el profesorado responsable de la asignatura y la Gestión académica de la Escuela de Ingeniería, que cuenta con personal especializado.

La información general sobre prácticas externas con normativas, modelos de convenios e informes está publicada en la web de la UAB.

Para información más detallada de las Prácticas Profesionales en el Grado (ver Guía Docente):

Pràctiques - Escola d'Enginyeria - UAB Barcelona

El procedimiento se presenta al alumnado en sesiones específicas: final del curso anterior (funcionamiento general), e inicios de curso (oferta, convenios, tutorías y evaluación).

La gestión de las Prácticas Profesionales se lleva a cabo por el profesorado responsable de la asignatura y la Gestión académica de la Escuela de Ingeniería, que cuenta con personal especializado.

La información general sobre prácticas externas con normativas, modelos de convenios e informes está publicada en la web de la UAB.

Para información más detallada de las Prácticas Profesionales en el Grado (ver Guía Docente):

Pràctiques - Escola d'Enginyeria - UAB Barcelona

El procedimiento se presenta al alumnado en sesiones específicas: final del curso anterior (funcionamiento general), e inicios de curso (oferta, convenios, tutorías y evaluación).

Dado el interés observado en diferentes empresas y la experiencia en grados afines de la Escuela de Ingeniería se prevé que haya un elevado número de destinos a escoger por parte del alumnado. También se incentiva la búsqueda por medios propios. Ello permite atender mejor los intereses del alumnado, así como los aspectos prácticos (proximidad residencia-plaza de destino).

La titulación dispone de una oferta significativa de destinos a escoger (unas 30 plazas por curso), asignados según expediente académico. También se incentiva la búsqueda por medios propios. Ello permite atender mejor los intereses de cada alumno/a, así como los aspectos prácticos (proximidad residencia-plaza de destino).

El grado cuenta con un Consejo Asesor formado por empresas del sector de la ciberseguridad que será ampliado con otras empresas para conformar la oferta final. Esto, junto al éxito de participación por parte de empresas en grados afines de la misma Escuela de Ingeniera (ingeniería informática, inteligencia artificial, ingeniería de datos, etc.), hace prever una oferta de plazas que supere el número de solicitudes por parte del alumnado.

6.3. Previsión de dotación de recursos materiales y servicios

La Escuela de Ingeniería ya dispone de los recursos materiales y los servicios necesarios para impartir y dar soporte a este grado. Sin embargo, de manera periódica la Escuela va destinando parte de su presupuesto a la mejora de los laboratorios y de otras infraestructuras. En este sentido, se prevé que haya dotaciones adicionales para mantener la calidad de los recursos que se destinarán al grado según las necesidades de cada momento.

De forma específica, se puede requerir la compra de programario específico o licencias de software o servicios (software comercial de ciberseguridad, acceso a servicios de cloud, etc.), así como de posibles infraestructuras (creación de redes estancas o aisladas para realización de prácticas con, por ejemplo, simulaciones de ataques y respuestas, etc.).

7. CALENDARIO DE IMPLANTACIÓN

7.1. Cronograma de implantación del título

Se prevé la implantación del Grado como titulación oficial en el curso 2025/26. Se realizará un despliegue secuencial anual, abriendo cada año un nuevo curso.

2025/2026	1r curso oficial
2026/2027	2o curso oficial
2027/2028	3r curso oficial
2028/2029	4o curso oficial

La implantación del nuevo título de Grado en Ciberseguridad será progresiva de acuerdo con el siguiente calendario:

Cronograma de implantación del Título en Ciberseguridad

	2025-2026	2026-2027	2027-2028	2028-2029
Primer curso del Título	X	X	X	X
Segundo curso del Título		X	X	X
Tercer curso del Título			X	X
Cuarto curso del Título				X

7.2 Procedimiento de adaptación

El grado se iniciará como grado oficial y no se requiere ningún procedimiento de adaptación.

7.3 Enseñanzas que se extinguen

La implantación de este grado no comporta la extinción de ningún otro grado o enseñanza

8. SISTEMA INTERNO DE GARANTÍA DE LA CALIDAD

8.1. Sistema Interno de Garantía de la Calidad

SGIQ de l'Escola - Escola d'Enginyeria - UAB Barcelona

8.2. Medios para la información pública

La difusión de información sobre todos los aspectos relacionados con las titulaciones impartidas por la Universidad se realiza a través de:

• Espacio general en la web de la universidad: este espacio contiene información actualizada, exhaustiva y pertinente, en catalán, castellano e inglés, de las características de las titulaciones, tanto de grados como de másteres universitarios, sus desarrollos operativos y resultados. Toda esta información se presenta con un diseño y estructura comunes, para cada titulación, en lo que se conoce como **ficha de la titulación**. Esta ficha incorpora una **pestaña de Calidad** que contiene un apartado relacionado con toda la información de calidad de la titulación y un apartado al Sistema de Indicadores de Calidad (la titulación en cifras) que recoge los indicadores relevantes del título.

• Espacio de centro en la web de la universidad: la facultad dispone de un espacio propio en la web de la universidad donde incorpora la información de interés del centro y de sus titulaciones. Ofrece información ampliada y complementaria de las titulaciones y coordinada con la información del espacio general.

Anexos

1. Anexos de la titulación a la memoria RUCT
   La institución podrá incluir como anexos, en su caso, propuestas de desarrollos particulares para el título de determinadas normativas institucionales de organización académica con relación a especificidades de su naturaleza académica o profesionalizadora.

2. Anexos información complementaria procesos de calidad de titulaciones UAB

2.1 **Resumen de objetivos y resultados de aprendizaje para el Suplemento Europeo al Título**

(máximo 800 caracteres incluyendo los espacios)

El grado en ciberseguridad tiene por finalidad formar profesionales capaces de hacer frente a desafíos en tecnologías de la información. Los estudiantes obtendrán conocimientos matemáticos, algorítmicos y computacionales fundamentales, así como formación específica en técnicas de ciberseguridad, priorizando criptografía, defensa/ataque y privacidad. Se fomentará una cultura de ciberseguridad con énfasis en el pensamiento adversarial. El programa abordará los retos éticos, legales y sociales de la ciberseguridad. El objetivo es preparar a profesionales para liderar, diseñar, desarrollar e implementar soluciones de ciberseguridad en diversos contextos, incluyendo análisis de sistemas, detección de vulnerabilidades y despliegue de soluciones.

(máximo 800 caracteres incluyendo los espacios)

Los resultados de aprendizaje se centran en diversos aspectos de la ciberseguridad y privacidad de la información. Estos incluyen la selección de aspectos tecnológicos y funcionales para desarrollar aplicaciones seguras, comprensión de bases matemáticas y criptográficas, identificación de mecanismos de seguridad de datos y protección de la privacidad, así como la utilización de herramientas para detección y eliminación de intrusos. Los estudiantes aprenderán a analizar incidentes de ciberseguridad, entender la legislación relevante y aplicar metodologías éticas.

Además, se enfocarán en desarrollar proyectos que evalúen y mitiguen riesgos, y en la creación de aplicaciones y servicios seguros.

2.2 **Apartados de PIMPEU**

Àmbits de treball dels futurs titulats

Els titulats del grau tenen la capacitat de triar entre una àmplia gamma d'àmbits professionals amb una alta demanda en diversos sectors industrials. Això els ofereix l'oportunitat de seguir camins professionals que s'ajustin tant als seus interessos personals com a les necessitats del mercat laboral. La versatilitat dels coneixements adquirits durant els seus estudis els permet explorar opcions en àrees com la tecnologia, la salut, l'enginyeria, la gestió empresarial, entre moltes altres. Això proporciona una flexibilitat significativa i la possibilitat d'adaptar-se als canvis del mercat i les oportunitats emergents. Els àmbits amb una alta demanda tant a nivell tècnic com de gestió i direcció per als titulats del grau:

- Sector financer
- Sector mèdic
- Seguretat nacional i defensa
- Companyies tecnològiques
- Sector energètic i infraestructures crítiques
- Sector d'assegurances
- Empreses de logística
- Administració pública

Sortides professionals dels futurs titulats

- Aquest grau forma professionals especialitzats en ciberseguretat, amb capacitat per donar resposta als reptes que s'han d'encarar en relació a les tecnologies de la informació. Els graduats en ciberseguretat estaran habilitats per l'exercici professional dels següents segments professionals:
- Auditoria de seguretat de sistemes d'informació.
- Especialistes en pentesting (de servidors de dades, de sistemes, de xarxes).
- Peritatge forense digital.
- Consultoria especialitzada en ciberseguretat (en comerç electrònic, banca digital, sistemes blockchain, administració electrònica, sistemes biomètrics, intel·ligència artificial, mecanismes d'autenticació, desplegaments criptogràfics, privadesa i protecció de dades).
- Analista o investigador en seguretat.
- Direcció de projectes de seguretat a l'àmbit de les TIC.
- Delegat de protecció de dades (DPO).
- Administració avançada (de xarxes, sistemes o bases de dades).

Perspectives de futur de la titulació

La creació d'aquest grau en ciberseguretat arriba en un moment oportú i respon a una demanda creixent de professionals. La ciberseguretat és una àrea crítica en l'actualitat, amb una demanda extraordinàriament alta de professionals qualificats per afrontar els reptes en constant evolució de la seguretat informàtica. La motivació per la creació d'aquest grau, impulsada per la demanda d'empreses per acollir estudiants en pràctiques o professionals amb formació en ciberseguretat, és una senyal clara de la importància i la necessitat d'aquest tipus de formació en el mercat laboral. A més, els informes sobre la manca de professionals en aquest àmbit a Catalunya subratllen encara més la importància d'aquesta iniciativa.

Per altre banda, si observem la tendència internacional de crear nous graus i programes de formació en ciberseguretat confirma la importància global d'aquesta disciplina i la seva continuïtat com a camp d'estudi i especialització. Això indica un gran potencial futur per al grau.

Preveiem la seva continuïtat i es seu establiment com a grau permanent en el camp de l'enginyeria de cara al futur.

Tres paraules clau

(3 paraules màxim)

Ciberseguridad, Informática, Ingeniería

Idiomes d'impartició de la Titulació

Català 90%

Castellà 5%

Anglès 5%

Breu explicació dels convenis de col·laboració amb empreses i institucions

S'estableixen convenis amb empreses per la realització de practiques externes i la realització del Treball de Final de Grau. Tot i que les pràctiques externes són optatives per l'alumnat, donat l'actual demanda del sector, es preveu que aquestes siguin nombroses. També es preveu fer algun conveni puntual amb caràcter formatiu (impartició de seminaris o tallers) o alguna jornada específica en la fira d'empreses de l'Escola d'Enginyeria de la UAB (MEMEnginy).

Per tal d'articular la col·laboració empresa-universitat i com a llavor de l'establiment de futurs convenis, s'ha constituït un Consell Assessor del Grau en Ciberseguretat, el qual està format per 11 empreses principalment del sector privat. Actualment el formen les següents empreses: Amazon Web Services, DELL Technologies, DXC Technologies, KPMG España, Marsh McLennan, Minsait, NTT Data, Parc Taulí Hospital Universitari, SIRT, Telefonica, i Werfen.

L'objectiu d'aquest consell, a part d'establir la base de futurs convenis de col·laboració, és assessorar de forma contínua a l'Escola d'Enginyeria respecte el grau, els seus continguts, i metodologia per tal de mantenir-lo actualitzat i estratègicament alineat amb la indústria de la

ciberseguretat. També es vol millorar la col·laboració per la realització d'activitats conjuntes universitat-empresa.

Breu explicació del desenvolupament de les pràctiques (metodologia, període, durada, avaluació, etc.)

Les pràctiques externes, amb caràcter optatiu, es realitzaran en empreses relacionades amb la ciberseguretat. Els estudiants compten amb un tutor a l'empresa i un tutor acadèmic a la universitat. El professorat que tutoritza les pràctiques serà professorat de la pròpia titulació. El treball de l'alumnat el supervisen els seus tutors que faran seguiment durant el període de pràctiques. L' alumnat farà un informe final que avaluarà el tutor de la universitat. Les entitats en les quals es realitzaran aquestes pràctiques seran empreses del sector de la ciberseguretat o empreses d'altres sectors on l'alumnat realitzi funcions relacionades amb la ciberseguretat (protecció o monitoratge d'infraestructures, programació segura, etc.). Actualment es disposa d' un Consell Assessor d'empreses que ja han manifestat el seu suport a la realització del grau i el seu interès a acollir alumnat en pràctiques. Concretament aquest consell assessor està format per: Amazon Web Services, DELL Technologies, DXC Technology, KPMG Espanya, Marsh McLennan, Minsait, NTT Data, Parc Taulí Hospital Universitari, SIRT, Telefónica, y Werfen.

2.3 **Tabla de materias y asignaturas**

Materias y asignaturas del grado

	Materias	**ECTS**	**Carácter**	**Asignaturas**	**ECTS**	**Carácter**
1	**Formación básica en ciberseguridad**	**30**	MXT	Fundamentos de programación	6	FB
				Fundamentos de computadores	6	FB
				Introducción a la ciberseguridad	6	OB
				Fundamentos jurídicos de la ciberseguridad	6	FB
				Ética para la ciberseguridad	6	FB
2	**Matemáticas**	12	FB	Álgebra y matemática discreta	6	FB
				Complejidad, aleatoriedad y números primos	6	FB
3	**Programación**	36	MXT	Programación en C	6	FB
				Desarrollo web	6	OB
				Técnicas de bajo nivel	6	OB
				Desarrollo de software seguro	6	OB

				Auditoría de seguridad del código	6	OB
				Virus i software malicioso	6	OB
				Programación funcional	6	OP
4	**Bases de datos**	12	OB	Bases de datos	6	OB
				Seguridad en bases de datos	6	OB
5	**Criptografía**	18	MXT	Criptografía básica	6	FB
				Mecanismos de autentificación	6	OB
				Criptografía avanzada	6	OP
6	**Sistemas operativos**	30	MXT	Sistemas operativos	6	FB
				Sistemas distribuidos	6	OB
				Server hardening	6	OB
				Digital forensics	6	OB
				Seguridad en servicios de virtualización y cloud	6	OB
7	**Redes**	24	MXT	Introducción a las redes de comunicación	6	FB
				Servicios para redes seguras	6	OB
				Administración de redes segures	6	OB
				Penetration testing	6	OB
8	**Gestión de seguridad**	6	OB	Gestión de la ciberseguridad	6	OB
9	**Privacidad**	12	MXT	Conceptos fundamentales de privacidad	6	OB
				Protección de datos y gestión de la privacidad	6	OP
10	**Inteligencia artificial**	12	MXT	IA aplicada a la ciberseguridad	6	OB
				Adversarial machine learning	6	OP
11	**Interfaces de seguridad**	18	MXT	Seguridad en hardware	6	OB

				Aspectos de la usabilidad en aplicaciones seguras	6	OP
				Biometría	6	OP
12	**Seguridad en entornos móviles**	24	OP	Introducción a la programación en entornos móviles	6	OP
				Seguridad en sistemas operativos para móviles	6	OP
				Seguridad en redes inalámbricas	6	OP
				Seguridad en aplicaciones móviles	6	OP
13	**Aspectos de seguridad en industria y aplicaciones**	42	OP	Análisis de redes sociales	6	OP
				Seguridad en eHealth	6	OP
				Tecnología blockchain y criptomonedas	6	OP
				Tecnología blockchain y smart contracts	6	OP
				Seguridad en industria e infraestructuras críticas	6	OP
				Seguridad en sistemas de control industrial	6	OP
				Informática industrial y sistemas basados en PLC	6	OP
14	**Trabajo de Fin de Grado**	12	OB	Trabajo de Fin de Grado	12	OB
15	**Prácticas Profesionales**	12	OP	Prácticas Profesionales	12	OP

*FB: Formación Básica, OB: Obligatoria; OP: Optativa; MXT: FB+OB u OB+OP; TFG: Trabajo de Fin Grado

2.4 Tabla de asignaturas comunes

Titulación origen	Código asignatura	Nombre asignatura	ECTS asignatura	Semestre asignatura

Anexo 1: Listado de Empresas

- Amazon Web Services
- DELL Technologies
- DXC Technology
- KPMG España
- Marsh McLennan
- Minsait
- NTT Data
- Parc Taulí Hospital Universitari
- SIRT
- Telefonica
- Werfen