IMPRESO SOLICITUD PARA VERIFICACIÓN DE TÍTULOS OFICIALES

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

De conformidad con el Real Decreto 1393/2007, por el que se establece la ordenación de las Enseñanzas Universitarias Oficiales

UNIVERSIDAD SOLICITANTE	CENTRO	CÓDIGO CENTRO
Universidad de Murcia	Facultad de Informática	30011715
NIVEL	**DENOMINACIÓN CORTA**	
Máster	Ciberseguridad / Master in Cybersecurity	
DENOMINACIÓN ESPECÍFICA		
Máster Universitario Ciberseguridad / Master in Cybersecurity por la Universidad de Murcia		
RAMA DE CONOCIMIENTO	**CONJUNTO**	
Ingeniería y Arquitectura	No	
HABILITA PARA EL EJERCICIO DE PROFESIONES REGULADAS	**NORMA HABILITACIÓN**	
No		
SOLICITANTE		
NOMBRE Y APELLIDOS	**CARGO**	
ANTONIO FLORES GIL	DECANO DE LA FACULTAD DE INFORMÁTICA	
Tipo Documento	**Número Documento**	
NIF	34786541F	
REPRESENTANTE LEGAL		
NOMBRE Y APELLIDOS	**CARGO**	
SONIA MADRID CANOVAS	VICERRECTORA DE ESTUDIOS	
Tipo Documento	**Número Documento**	
NIF	48392224V	
RESPONSABLE DEL TÍTULO		
NOMBRE Y APELLIDOS	**CARGO**	
ANTONIO FLORES GIL	DECANO DE LA FACULTAD DE INFORMÁTICA	
Tipo Documento	**Número Documento**	
NIF	34786541F	

2. DIRECCIÓN A EFECTOS DE NOTIFICACIÓN

A los efectos de la práctica de la NOTIFICACIÓN de todos los procedimientos relativos a la presente solicitud, las comunicaciones se dirigirán a la dirección que figure en el presente apartado.

DOMICILIO	CÓDIGO POSTAL	MUNICIPIO	TELÉFONO
AVENIDA TENIENTE FLOMESTA Nº 5 (RECTORADO UNIVERSIDAD DE MURCIA)	30003	Murcia	868883513
E-MAIL	**PROVINCIA**		**FAX**
vicestudios@um.es	Murcia		868883506

3. PROTECCIÓN DE DATOS PERSONALES
De acuerdo con lo previsto en la Ley Orgánica 5/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa que los datos solicitados en este impreso son necesarios para la tramitación de la solicitud y podrán ser objeto de tratamiento automatizado. La responsabilidad del fichero automatizado corresponde al Consejo de Universidades. Los solicitantes, como cedentes de los datos podrán ejercer ante el Consejo de Universidades los derechos de información, acceso, rectificación y cancelación a los que se refiere el Título III de la citada Ley 5-1999, sin perjuicio de lo dispuesto en otra normativa que ampare los derechos como cedentes de los datos de carácter personal.
El solicitante declara conocer los términos de la convocatoria y se compromete a cumplir los requisitos de la misma, consintiendo expresamente la notificación por medios telemáticos a los efectos de lo dispuesto en el artículo 59 de la 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en su versión dada por la Ley 4/1999 de 13 de enero.

	En: Murcia, AM 3 de noviembre de 2022
	Firma: Representante legal de la Universidad

1. DESCRIPCIÓN DEL TÍTULO

1.1. DATOS BÁSICOS

NIVEL	DENOMINACIÓN ESPECIFICA	CONJUNTO	CONVENIO	CONV. ADJUNTO
Máster	Máster Universitario Ciberseguridad / Master in Cybersecurity por la Universidad de Murcia	No		Ver Apartado 1: Anexo 1.

LISTADO DE ESPECIALIDADES
No existen datos

RAMA	ISCED 1	ISCED 2
Ingeniería y Arquitectura	Ciencias de la computación	Ingeniería y profesiones afines

NO HABILITA O ESTÁ VINCULADO CON PROFESIÓN REGULADA ALGUNA
AGENCIA EVALUADORA
Agencia Nacional de Evaluación de la Calidad y Acreditación
UNIVERSIDAD SOLICITANTE
Universidad de Murcia

LISTADO DE UNIVERSIDADES	
CÓDIGO	UNIVERSIDAD
012	Universidad de Murcia

LISTADO DE UNIVERSIDADES EXTRANJERAS	
CÓDIGO	UNIVERSIDAD
No existen datos	

LISTADO DE INSTITUCIONES PARTICIPANTES
No existen datos

1.2. DISTRIBUCIÓN DE CRÉDITOS EN EL TÍTULO

CRÉDITOS TOTALES	CRÉDITOS DE COMPLEMENTOS FORMATIVOS	CRÉDITOS EN PRÁCTICAS EXTERNAS
90	0	0
CRÉDITOS OPTATIVOS	**CRÉDITOS OBLIGATORIOS**	**CRÉDITOS TRABAJO FIN GRADO/ MÁSTER**
18	48	24

LISTADO DE ESPECIALIDADES	
ESPECIALIDAD	CRÉDITOS OPTATIVOS
No existen datos	

1.3. Universidad de Murcia

1.3.1. CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS	
CÓDIGO	CENTRO
30011715	Facultad de Informática

1.3.2. Facultad de Informática

1.3.2.1. Datos asociados al centro

TIPOS DE ENSEÑANZA QUE SE IMPARTEN EN EL CENTRO		
PRESENCIAL	SEMIPRESENCIAL	A DISTANCIA
No	No	Sí

PLAZAS DE NUEVO INGRESO OFERTADAS	
PRIMER AÑO IMPLANTACIÓN	SEGUNDO AÑO IMPLANTACIÓN
50	50

	TIEMPO COMPLETO	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	30.0	66.0
RESTO DE AÑOS	30.0	66.0
	TIEMPO PARCIAL	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	18.0	30.0
RESTO DE AÑOS	18.0	30.0
NORMAS DE PERMANENCIA		
https://www.um.es/web/estudios/normativa/permanencia		
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

2. JUSTIFICACIÓN, ADECUACIÓN DE LA PROPUESTA Y PROCEDIMIENTOS

Ver Apartado 2: Anexo 1.

3. COMPETENCIAS

3.1 COMPETENCIAS BÁSICAS Y GENERALES
BÁSICAS
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
GENERALES
CG1 - Que los estudiantes sean capaces de analizar métodos y técnicas de ciberataques y ciberdefensa.
CG2 - Que los estudiantes sean capaces de diseñar, desplegar y mantener sistemas de ciberseguridad.
CG3 - Que los estudiantes sean capaces de identificar la normativa y legislación aplicable en el ámbito de la ciberseguridad.
CG4 - Que los estudiantes sean capaces de elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.
CG5 - Que los estudiantes conozcan los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, considerando la definición de estrategias, políticas y normas para la seguridad corporativa.
3.2 COMPETENCIAS TRANSVERSALES
No existen datos
3.3 COMPETENCIAS ESPECÍFICAS
CE1 - Que los estudiantes sean capaces de gestionar los procesos asociados a vulnerabilidades, amenazas y riesgos dentro de una organización.
CE2 - Que los estudiantes sean capaces de proyectar, diseñar e implantar productos, procesos, servicios e infraestructuras inteligentes en ámbitos de la ciberseguridad.
CE3 - Ser capaz de diseñar, monitorizar y evaluar arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.
CE4 - Aplicar técnicas de seguridad de datos y software.
CE5 - Identificar y conocer las nuevas tendencias, buenas prácticas, normas, regulación y aspectos humanos relacionados con la ciberseguridad.

4. ACCESO Y ADMISIÓN DE ESTUDIANTES

4.1 SISTEMAS DE INFORMACIÓN PREVIO

Ver Apartado 4: Anexo 1.

4.2 REQUISITOS DE ACCESO Y CRITERIOS DE ADMISIÓN

El acceso y admisión a las titulaciones oficiales de máster viene regulado en el artículo 18 del **RD 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 y en el artículo 17 del **Reglamento** por el que se regulan los estudios universitarios oficiales de Grado y Máster universitario de la Universidad de Murcia, aprobado en Consejo de Gobierno de 22 de Julio de 2022.

ACCESO

1. La posesión de un título universitario oficial de graduada o graduado español o equivalente es condición para acceder a un máster universitario, o en su caso disponer de otro título de máster universitario, o títulos del mismo nivel que el título español de grado o máster expedidos por universidades e instituciones de educación superior de un país del EEES que en dicho país permita el acceso a los estudios de máster.

2. De igual modo, podrán acceder a un máster universitario del sistema universitario español personas en posesión de títulos procedentes de sistemas educativos que no formen parte del EEES, que equivalgan al título de grado, sin necesidad de homologación del título, pero sí de comprobación por parte de la universidad del nivel de formación que implican, siempre y cuando en el país donde se haya expedido dicho título permita acceder a estu-

dios de nivel de postgrado universitario. En ningún caso el acceso por esta vía implicará la homologación del título previo del que disponía la persona interesada ni su reconocimiento a otros efectos que el de realizar los estudios de máster.

Los alumnos podrán acceder al Máster Universitario en Ciberseguridad / Master in Cybersecurity estando en posesión de titulaciones oficiales cuyos perfiles más adecuados serían los grados en ingeniería relacionados con la Informática, en particular: el Grado en Ingeniería Informática y el Grado en Ciencia e Ingeniería de Datos, o sus equivalentes extranjeros del Espacio Europeo de Educación Superior o de cualquier otro espacio, previa comprobación del nivel de formación equivalente para el acceso. De igual modo, tendrán acceso quienes hayan cursado el Grado en Ingeniería Telemática, Grado en Ingeniería del Software, Grado en Ingeniería de Computadores o el Grado en Ingeniería en Sistemas de Telecomunicación. También serán admitidos aquellos profesionales que se encuentren en posesión de títulos extinguidos relacionados con los grados anteriores, como Ingeniero Superior en Informática, Ingeniero Técnico en Informática de Gestión e Ingeniero Técnico en Informática de Sistemas. En el caso de otros grados españoles o extranjeros, la comisión académica estudiará caso por caso si son equiparables a los anteriores o si la formación complementaria y experiencia laboral son adecuadas para el acceso.

La Facultad de Informática ofrece este título en modalidad bilingüe. De este modo las lenguas utilizadas son español e inglés. En relación con el nivel de inglés exigible para poder acceder a la titulación, el estudiante deberá cumplir con alguno de los siguientes requisitos:

- Ser hablante nativo de inglés (deberá presentar pasaporte o tarjeta de identificación como nacional de un país de habla inglesa).
- Tener certificado acreditativo de nivel B2 o superior de inglés o superar una prueba de nivel.

ADMISIÓN.

3. La Universidad de Murcia garantiza una información transparente y accesible sobre los procedimientos de admisión, y dispone de sistemas de orientación al estudiantado. Asimismo, dicha información y los procedimientos de admisión tienen en cuenta al estudiantado con diversidad funcional o con necesidades específicas, y dispone de servicios de apoyo y asesoramiento adecuados.

4. La Universidad de Murcia podrá establecer excepcionalmente en sus normas de admisión, procedimientos de matrícula condicionada para el acceso a un máster universitario, y garantizará la prioridad en la matrícula de los estudiantes que dispongan del título universitario oficial de graduada o graduado.

5. La Universidad de Murcia regulará la admisión en las enseñanzas de máster universitario, estableciendo requisitos específicos y, en caso de ser necesarios, complementos formativos, cuya carga en créditos no podrá superar el equivalente al 20 % de la carga crediticia del título. Los créditos de complementos formativos tendrán la misma consideración que el resto de los créditos del plan de estudios del título de máster universitario.

6. La Universidad de Murcia reservará, al menos, un 5 % de las plazas ofertadas en los títulos universitarios oficiales de máster universitario para estudiantes que tengan reconocido un grado de discapacidad igual o superior al 33 %, así como para estudiantes con necesidades de apoyo educativo permanentes asociadas a circunstancias personales de discapacidad, que en sus estudios anteriores hayan precisado de recursos y apoyos para su plena inclusión educativa.

7. La admisión en un máster la decidirá el centro que lo oferta a propuesta de la Comisión Académica del correspondiente máster. A estos efectos, la Comisión Académica del Máster utilizará los criterios previamente establecidos en la memoria oficial de la titulación y que servirán para establecer una relación de solicitantes admitidos a partir de la valoración de:

a. El currículo académico;

b. Los méritos de especial relevancia o significación en relación al máster solicitado;

c. Cualquier otro criterio o procedimiento que permita constatar la idoneidad para seguir los estudios que solicita.

8. Una vez recibida la propuesta de la Comisión Académica del Máster, el centro hará públicas las listas de solicitantes admitidos y excluidos.

9. Los estudiantes deberán presentar solicitud de admisión a enseñanzas oficiales de Máster, y tras la admisión en el máster correspondiente, procederán a formalizar su matrícula en la forma, plazos y con los requisitos que se establezcan en las normas e instrucciones de admisión y matrícula que a estos efectos se aprobarán mediante resolución del rector de la Universidad de Murcia para cada curso académico.

Dados los criterios de acceso establecidos en el punto anterior no se considera necesario establecer criterios específicos de admisión. Asimismo, se evaluará la necesidad de posibles adaptaciones curriculares, itinerarios o estudios alternativos en el caso de estudiantes con necesidades educativas específicas derivadas de discapacidad previendo, en tal caso, los servicios de apoyo y asesoramiento adecuados a dicha situación. En el supuesto de existir mayor número de solicitudes que de plazas ofertadas, la selección de los admitidos se producirá con arreglo al siguiente porcentaje: **expediente académico (60%)**, **experiencia profesional (20%), experiencia investigadora (20%).**

De acuerdo con el RD 822/2021, artículo 18.4, *"Las universidades podrán excepcionalmente establecer, a partir de normativas específicas aprobadas por sus órganos de Gobierno, procedimientos de matrícula condicionada para el acceso a un Máster Universitario. Esta consistirá en permitir que uno una estudiante de Grado al que le reste por superar el TFG y como máximo hasta 9 créditos ECTS, podrá acceder y matricularse en un Máster Universitario, si bien en ningún caso podrá obtener el título de Máster si previamente no ha obtenido el título de Grado. Las universidades garantizarán la prioridad en la matrícula de los y las estudiantes que dispongan del título universitario oficial de Graduada o Graduado. En este procedimiento podrán ser tenidos en cuenta los créditos pendientes de reconocimiento o transferencia en el título de Grado, o la exigencia de superación de un determinado nivel de conocimiento de un idioma extranjero para la obtención del título."*

La opción de la admisión condicionada ya ha sido empleada por la Universidad de Murcia en el curso 2021/22, con un procedimiento establecido mediante resolución rectoral. Si esta opción continuara disponible en cursos próximos, la Comisión Académica del Máster en Ciberseguridad / Master in Cybersecurity podría optar por hacer uso de la misma en el proceso de admisión.

4.3 APOYO A ESTUDIANTES

Además de lo referido en el apartado 4.1, la Universidad de Murcia cuenta con variados instrumentos al servicio del apoyo y orientación del estudiante en los ámbitos académico, personal, ciudadano y deportivo. Así, además de los servicios centrales de la Universidad de Murcia dedicados a tal fin (sobre los cuales se puede obtener mayor información en las direcciones **https://www.um.es/web/universidad/estructura/servicios** y **https://**

www.um.es/web/vic-estudiantes-scu/), los estudiantes de la Universidad de Murcia cuentan con el apoyo que se presta desde el máximo órgano de representación estudiantil, el **Consejo de Estudiantes** así como con la asistencia que, en su caso, les ofrece el **Defensor del Universitario**. Entre los referidos servicios universitarios merecen especial mención los que se prestan desde la Unidad de apoyo a los estudiantes con discapacidad integrado en el Servicio de Atención a la Diversidad y Voluntariado (**ADYV**) a través de la cual, coordinando los esfuerzos del profesorado, el personal de administración y servicios y el alumnado que se implica en tareas de voluntariado universitario, se da soporte a los estudiantes con discapacidad física y sensorial que lo soliciten para garantizar la igualdad de condiciones con el resto de estudiantes y su integración en la Universidad de Murcia en todos los aspectos que afectan a la vida académica.

Hay que destacar también que la Universidad de Murcia aprobó el 6 de julio de 2009 una Propuesta de colaboración entre el Centro de Orientación e Información de Empleo (**COIE**) y el Servicio de Atención a la Diversidad y Voluntariado y las Facultades y Escuelas de esta Universidad, en la programación y desarrollo de actividades dentro de los procesos clave del SAIC. Estos servicios de orientación y empleo cuentan con una dilatada experiencia en la organización y puesta en marcha de actuaciones de orientación para universitarios. La orientación se entiende como un proceso en el que se debe definir poco a poco el objetivo profesional, planificando los pasos necesarios para lograr dicho objetivo. Debido a esta condición de proceso, ha de entenderse que la orientación es necesaria en todas las etapas del estudiante universitario. Así se realizan actividades dirigidas a estudiantes de primer curso, a estudiantes en el ecuador de su carrera y a estudiantes de último curso, tanto de orientación académica como de orientación profesional.

También, como oferta general y primordial para el correcto desarrollo de nuestro programa de formación, la comunidad universitaria cuenta con un **campus virtual** integrado por las plataformas MI CAMPUS y una plataforma oficial de docencia (e-learning) AULA VIRTUAL (basada en el proyecto educativo de software libre SAKAI)Este último se ha revelado como una potente herramienta de apoyo al estudiante que será utilizada en este Máster como soporte fundamental para la docencia on-line ya que dota a la Universidad de Murcia de un ámbito de comunicación virtual entre alumnado y profesorado (docentes y tutores), mediante el cual se puede acceder a documentación que ofrece el profesor, se puede interactuar con éste, consultar las calificaciones, entregar los trabajos, y demás herramientas telemáticas que nutren el desarrollo de los procesos de enseñanza y aprendizaje en un entorno virtual.

A continuación se muestra un resumen de los amplios servicios que ofrecen ambas plataformas, MI CAMPUS y Aula Virtual:

MI CAMPUS

Este portal otorga el máximo protagonismo a nuestros usuarios ofreciéndoles desde un único sitio la posibilidad de relacionarse de forma digital con la Universidad. Te permite entre otras muchas actividades realizar gestiones y trámites, consultar información y, acceder en línea a los servicios que necesitan en el día a día de su actividad educativa, investigadora y administrativa.

Es un nuevo entorno, más intuitivo y amigable que propone un diseño y funcionalidad más en la línea de las actuales plataformas populares. Simplifica los procesos, agiliza trámites, integra analítica de datos y facilita canales de comunicación y colaboración. Una vez que te hayas identificado, puedes acceder a información personalizada y al catálogo de aplicaciones, trámites y servicios que la Universidad de Murcia pone a tu disposición. El contenido que te ofrecerá cambiará dependiendo de la relación que tengas con la universidad y de tus intereses, preferencias, necesidades y hábitos de uso. De navegación rápida y cómoda, adaptada a dispositivos móviles y con un diseño simplificado e intuitivo, este sitio web estará en continua evolución para poder proporcionar cada día una mejor experiencia

Entre los servicios a los que se puede acceder en el portal MI CAMPUS destacan las siguientes:

- Consulta de expediente.
- Servicios de Tarjeta Universitaria (TUI): solicitud y activación TUI, y obtención código QR.
- Acceso al portal de Recursos Humanos.
- Reserva de Aula de Libre Acceso.
- Reserva de actividades e instalaciones deportivas.
- Servicio de impresión centralizado (DALI).
- Acceso al Aula Virtual.
- Acceso a **UMUBox**.

El Aula Virtual institucional de la Universidad de Murcia es la plataforma oficial de docencia virtual donde el profesorado y alumnado disponen de diversas herramientas telemáticas que facilitan el desarrollo de los procesos de enseñanza y aprendizaje. Entre las herramientas que se disponen en el Aula Virtual se destacan las siguientes:

- Guías Docentes, calendario, recursos y contenidos.
- Mensajes Privados.
- Anuncios.
- Foros.
- Agenda.
- Tareas.
- Exámenes, llamamientos de exámenes y calificaciones.
- Videoconferencia síncrona.
- Videoclases.
- Galería Multimedia.

La principal funcionalidad del Aula Virtual será la de ofrecer los contenidos de la asignatura, calendarios, avisos o mensajes personalizados, que serán necesarios para la adquisición de competencias y conceptos identificados en el programa. Los profesores del Máster Universitario y el Coordinador del mismo utilizarán las herramientas del Campus Virtual de la Universidad de Murcia no sólo con fines docentes, sino también para facilitar todo tipo de información a los estudiantes, a través de su tablón de anuncios, del correo electrónico y de las tutorías.

Debido a la modalidad de enseñanza del Máster, para los estudiantes de nuevo ingreso, el coordinador responsable del Máster Universitario organizará una reunión de bienvenida virtual en la que se les explicarán los aspectos que deben conocer de las herramientas informáticas que se van a utilizar en el desarrollo las actividades formativas, como el Aula Virtual de la Universidad de Murcia. Se informará de todos los aspectos del Máster Universitario que los estudiantes deben conocer para poder planificar su aprendizaje en el Máster sin problemas (estructura del Máster Universitario, metodología de trabajo, calendarios académicos, fechas de evaluación, trabajo fin de Máster, etc.). Además, también informará de otros aspectos de la Universidad de Murcia que como estudiantes les afecten, como el uso de las herramientas de las bibliotecas, el Servicio de Información Universitario, el Servicio de Idiomas de la Universidad de Murcia, los órganos de representación y toma de decisiones, las estructuras de representación estudiantil y el Defensor del Universitario.

Por otro lado, la Universidad de Murcia organiza una **Semana de Bienvenida Universitaria** (SBU) en la que se explica a los estudiantes de nuevo ingreso todo aquello que necesitan saber para desenvolverse en la Universidad de Murcia durante el periodo de duración de sus estudios. Además, como hemos comentado, la Universidad de Murcia dispone de una **página web** en la que los estudiantes pueden consultar cualquier información que les interese relativa al Máster o a otros asuntos universitarios.

El **SIU** (Servicio de Información Universitario), junto con el Vicerrectorado que en cada momento tenga atribuidas las competencias en materia de gestión de estudios oficiales, mantienen a través de la WEB de la Universidad, folletos institucionales y diversa información que permiten orientar y reconducir las dudas de los estudiantes ya matriculados. Desde el centro se ofrecen a lo largo del curso varias actividades de orientación académica y profesional, unas específicas desde la coordinación del máster, y otras en colaboración con el COIE.

El Máster Universitario en Ciberseguridad / Master in Cybersecurity por la Universidad de Murcia , además de contar con los procedimientos de acogida y orientación a estudiantes de nuevo ingreso, establecerá un Plan de Acción Tutorial, principalmente enfocado al proceso de enseñanza virtual. En este plan se contempla que los estudiantes tengan un apoyo directo en su proceso de toma de decisiones y el seguimiento continuo a través de la coordinación del Máster, de Decanato y de Secretaría. La tarea básica en este Plan de Acción Tutorial será informar, orientar y asesorar al estudiante respecto a todo aquello que es competencia del plan de estudios y el *sistema de apoyo permanente a los estudiantes* una vez matriculados, que consistirá en un seguimiento directo del estudiante durante todos sus estudios de Posgrado. En la carta de admisión al Máster se informará de este sistema.

A la información de todos estos Servicios, los estudiantes pueden acceder a través de la web de la Universidad de Murcia o acudiendo personalmente para realizar su consulta, si así lo desea. Hacemos mención especial de los servicios que presta a los estudiantes con discapacidad el servicio de atención a la diversidad y voluntariado (ADyV), realizando asesoramiento psicológico y pedagógico a los estudiantes y profesores en aquellas cuestiones relacionadas con la discapacidad y los estudios universitarios, organizando acciones de formación específica para el profesorado sobre estrategias pedagógico-didácticas que deben utilizar en clases con presencia de estudiantes con discapacidad, asesorando a los estudiantes sobre el uso de ayudas técnicas que faciliten su acceso a los estudios y canalizando al voluntariado universitario hacia acciones dirigidas a cubrir las necesidades de estos estudiantes. Además de la información que aparece en la página web de la Universidad de Murcia, todos los Servicios de estudiantes de la Universidad de Murcia poseen dípticos explicativos que se colocan en los puntos de recogida de información de estudiantes de los distintos Centros, y en los tablones de anuncios de estos, y se reponen con regularidad para que la información esté al alcance de todos los estudiantes.

Finalmente, a nivel de centro, anualmente se realizan charlas para estudiantes relacionadas con orientación profesional y empleo (JOPE), programas de movilidad nacionales e internacionales, prácticas curriculares y extracurriculares, etc.

Todo el trabajo aquí realizado, así como su continua mejora viene garantizado en el Sistema de Aseguramiento Interno de la Calidad de la Facultad, y en concreto por los procedimientos documentados PC04 Orientación a estudiantes en los Centros de la UMU, PC05 Resultados Académicos y PC09 Información pública y rendición de cuentas.

Los sistemas de apoyo y orientación se completan con algunos servicios específicos de la Universidad de Murcia:

1. Centro de Orientación e Información de Empleo (**COIE**). Se trata de una oficina universitaria para canalizar la realización de prácticas extracurriculares en empresas.
2. Área Científica y Técnica de Investigación (**ACTI**).
3. Servicio de Idiomas (**SIDI**), que ofrece a la comunidad universitaria formación lingüística instrumental en varios idiomas. Todos los cursos están enfocados al aprendizaje instrumental de la lengua y la metodología empleada responde a los principios de los enfoques comunicativos.
4. Área de Relaciones Internacionales (**ARI**). Da cobertura a los programas de movilidad internacional de nuestros estudiantes. Actualmente, el alumnado de la Titulación tiene la posibilidad de acogerse al Programa Erasmus Plus o al programa ILA para cursar un cuatrimestre o un año completo en diversas universidades europeas o latinoamericanas respectivamente; asimismo, también lo puede hacer al ISEP (International Student Exchange Program). El programa permite la movilidad de estudiantes de pregrado y posgrado entre la Universidad de Murcia y más de 120 instituciones de los Estados Unidos, incluyendo una oferta que abarca la mayoría de las áreas de estudio. Por su parte, SICUE es un programa de movilidad nacional de estudiantes universitarios que permite cursar un cuatrimestre o un año completo en otra universidad española, con garantías de reconocimiento académico y aprovechamiento de los estudios realizados semejantes a los de la Universidad de Murcia (**https://sicue.um.es)**.
5. Servicio de Atención a la Diversidad y Voluntariado (**https://www.um.es/web/adyv)**. Supone la oportunidad para el alumnado de resolver problemas relacionados con el aprovechamiento de la oferta docente desde el punto de vista pedagógico y, en el caso de alumnado con necesidades educativas especiales, supone el nexo de mejora de comunicación entre éste y el profesorado, pues se da soporte a los estudiantes con discapacidad física y sensorial que lo soliciten para garantizar la igualdad de condiciones con el resto de estudiantes y su integración en la Universidad de Murcia en todos los aspectos que afectan a la vida académica.
6. Biblioteca Universitaria (**https://www.um.es/web/biblioteca)**. Informa de los procesos de uso y préstamo de los fondos bibliográficos y de los distintos servicios de apoyo al autoaprendizaje que ofrece.
7. Servicio de Actividades Deportivas (**https://www.um.es/web/deportes)**
8. Consejo de Estudiantes de la Universidad de Murcia (**CEUM**). Es el máximo órgano de representación estudiantil de la Universidad de Murcia. Se trata de una estructura en la cual los representantes de estudiantes pueden debatir todos aquellos temas que afectan a los estudiantes a nivel general de la Universidad. El CEUM está compuesto por las delegaciones de estudiantes de cada facultad y escuela, así como por representantes en el Claustro Universitario. De sus opiniones y decisiones salen las líneas de actuación para llevar a cabo la defensa efectiva de los derechos de los estudiantes.

4.4 SISTEMA DE TRANSFERENCIA Y RECONOCIMIENTO DE CRÉDITOS

Reconocimiento de Créditos Cursados en Enseñanzas Superiores Oficiales no Universitarias

MÍNIMO	MÁXIMO
0	0

Reconocimiento de Créditos Cursados en Títulos Propios

MÍNIMO	MÁXIMO
0	0

Adjuntar Título Propio

Ver Apartado 4: Anexo 2.

Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional

MÍNIMO	MÁXIMO
0	12

El reconocimiento consiste en la aceptación por parte de la Universidad de Murcia de los créditos que, habiendo sido obtenidos en esta u otra Universidad, son computados a efectos de la obtención de un título oficial de la misma. Por su parte, la transferencia de créditos consiste en la consignación, a petición del interesado, de los créditos superados por el estudiante en enseñanzas oficiales universitarias del mismo nivel (Grado, Máster o Doctorado) que no puedan ser reconocidos.

El artículo 10 del RD 822/2021 establece que las universidades aprobarán normativas específicas para regular estos procedimientos. La Universidad de Murcia da cumplida cuenta de este mandato en su "**Reglamento sobre Reconocimiento y Transferencia de Créditos en Enseñanzas de Grado y Máster conducentes a la obtención de los correspondientes títulos oficiales de la Universidad de Murcia"** aprobado en Consejo de Gobierno de 25 de mayo de 2009, y modificado en sesiones de Consejo de Gobierno de 22 de octubre de 2010, 28 de julio de 2011 y 6 de julio de 2012 y 28 de octubre de 2016. El sistema de transferencia y reconocimiento de créditos propuesto por la Universidad de Murcia para las enseñanzas de máster queda explicitado en el artículo 8 del mencionado reglamento.

Dicho Reglamento establece que se podrá reconocer a los alumnos los créditos cursados en enseñanzas oficiales en ésta u otra universidad, siempre que guarden relación con el presente título de Máster. A estos efectos, el art. 8 del Reglamento por el que se regulan los Estudios Universitarios Oficiales de Máster de la Universidad de Murcia (Última modificación aprobada en consejo de gobierno de 22 de Julio de 2016) remite a lo dispuesto en los artículos 6.4 y 8 del "Reglamento sobre reconocimiento y transferencia de créditos en las enseñanzas de grado y de máster conducentes a la obtención de los correspondientes títulos oficiales de la Universidad de Murcia", o norma que lo sustituya.

El sistema de transferencia y reconocimiento de créditos propuesto por la Universidad de Murcia para las enseñanzas de Máster queda explicitado en el artículo 6 y 8 del Reglamento sobre Reconocimiento y Transferencia de Créditos en las Enseñanzas de Grado y Máster conducentes a la obtención de los correspondientes títulos oficiales de la Universidad de Murcia (Aprobado en Consejo de Gobierno de 25 de mayo de 2009 y modificado en Consejo de Gobierno de 22 de octubre de 2010, 6 de julio de 2012 y 28 de Octubre de 2016). Dicho documento recoge lo siguiente:

Artículo 8. RECONOCIMIENTO DE CRÉDITOS EN LAS ENSEÑANZAS DE MÁSTER

1. Reglas generales

a. A criterio de las Comisiones Académicas de los Másteres, se podrán reconocer créditos de las enseñanzas oficiales realizadas en esta u otras universidades, siempre que guarden relación con el título de Máster en el que se desean reconocer los créditos.

b. Asimismo los estudiantes que hayan cursado estudios parciales de doctorado en el marco de lo dispuesto en el Real Decreto 778/1998 o normas anteriores podrán solicitar el reconocimiento de los créditos correspondientes a cursos y trabajos de iniciación a la investigación previamente realizados.

c. El reconocimiento se solicitará a la Comisión Académica del Máster que, a la vista de la documentación aportada, elevará una propuesta para su resolución por los Decanos/Decanas o Directores/Directoras de centro al que se encuentran adscritos estos estudios.

d. En las normas e instrucciones de admisión y matrícula se establecerán el procedimiento y la documentación a aportar para la solicitud del reconocimiento de créditos.

2. Con el fin de evitar diferencias entre Másteres, se dictan las siguientes reglas:

a. Reconocimiento de créditos procedentes de otros Másteres. Se podrán reconocer en un máster créditos superados en otros másteres, a juicio de la Comisión Académica del mismo, siempre que guarden relación con las asignaturas del máster y provengan de un título del mismo nivel en el contexto nacional o internacional.

b. Reconocimiento de créditos procedentes de Programas de Doctorado regulados por normas anteriores al RD-1393/2007. Como en el caso anterior, se podrán reconocer en un máster créditos superados en otros másteres, a juicio de la Comisión Académica del mismo, que podrá ser la totalidad de los créditos, salvo el TFM, cuando el máster provenga del mismo Programa de Doctorado.

c. Reconocimiento de créditos por experiencia profesional, laboral o de enseñanzas no oficiales. El número de créditos que sean objeto de reconocimiento no podrá ser superior, en su conjunto, al 15 por ciento del total de los créditos que constituyen el plan de estudios.

d. No obstante lo anterior, los créditos procedentes de títulos propios de la Universidad de Murcia podrán, excepcionalmente, ser objeto de reconocimiento en un porcentaje superior al señalado en el apartado anterior o, en su caso, ser objeto de reconocimiento en su totalidad siempre que el correspondiente título haya sido extinguido y sustituido por un título oficial y así se haga constar expresamente en la memoria de verificación del nuevo plan de estudios.

e. Reconocimiento de créditos superados en Licenciaturas, Arquitecturas o Ingenierías. En este caso se podrá reconocer hasta el 20% de créditos, siempre que concurran todas las siguientes condiciones:

- Cuando la licenciatura o la ingeniería correspondiente figure como titulación de acceso al máster.

- Los créditos solicitados para reconocimiento tendrán que formar parte necesariamente del segundo ciclo de estas titulaciones.
- Los créditos reconocidos tendrán que guardar relación con las materias del máster.

3. El Trabajo Fin de Máster (TFM) nunca podrá ser objeto de reconocimiento, al estar orientado a la evaluación de las competencias asociadas al título correspondiente de la Universidad de Murcia.

Por otra parte, atendiendo al requisito que figura en el **R.D 822/2021**, Artículo 2, punto 2, que exige a las universidades la inclusión y justificación de los criterios de reconocimiento de créditos en la memoria de los planes de estudios que presenten a verificación, la Comisión Académica del Máster Universitario establecerá la siguiente aplicación en el reconocimiento de experiencia profesional previa y de enseñanzas universitarias no oficiales conducentes a títulos propios:

Por lo que se refiere a la experiencia profesional y laboral, ésta podrá ser reconocida siempre y cuando el tipo de experiencia obtenida, las funciones desarrolladas en el desempeño del puesto de trabajo y las competencias adquiridas, en un periodo de tiempo suficiente y debidamente acreditadas, tengan correspondencia con las competencias de las materias de la titulación de destino. **En el caso de reconocimiento de créditos por acreditación de experiencia laboral y profesional se contempla la posibilidad de reconocimientos sólo en las siguientes asignaturas que se consideran pueden tener asociación con formación básica en principios de ciberseguridad hasta un máximo de 12 créditos:**

- **Técnicas de Ciberataques Hacking Ético.**
- **Técnicas de Ciberdefensa.**
- **Técnicas de Ciberseguridad y Comunicaciones.**
- **Técnicas de Gestión de la Ciberseguridad.**

Para realizar el reconocimiento se exigirá que se demuestre al menos 1 año de experiencia profesional en actividades relacionadas con el contenido y competencias de la asignatura correspondiente y no pudiéndose en ningún caso realizar un reconocimiento que abarque a más de dos asignaturas. Estas asignaturas son las introductorias a los diferentes contenidos del máster por lo que entendemos que pueden corresponder a los perfiles profesionales más frecuentes hoy en día.

Para el reconocimiento de los créditos procedentes de enseñanzas universitarias no oficiales conducentes a la obtención de otros títulos, entendiendo por tales, según lo establecido en el artículo 34.1 de la Ley Orgánica 6/2001 de Universidades, los títulos propios de Máster, Especialista Universitario y similares, la Comisión Académica elaborará una propuesta teniendo en cuenta las competencias adquiridas con los créditos cursados en la titulación de origen y su posible correspondencia con las competencias de las materias de la titulación de destino.

EFECTOS DEL RECONOCIMIENTO DE CRÉDITOS

1. En el proceso de reconocimiento quedarán reflejadas de forma explícita aquellas materias o asignaturas que no deberán ser cursadas por el estudiante. Se entenderá en este caso que dichas materias o asignaturas ya han sido superadas y no serán susceptibles de nueva evaluación.
2. La calificación de las materias o asignaturas superadas como consecuencia de un proceso de reconocimiento será equivalente a la calificación de las materias o asignaturas que han dado origen a éste. Cuando varias materias o asignaturas conlleven el reconocimiento de una sola en la titulación de destino se realizará la media ponderada en función del número de créditos de aquéllas.
3. No obstante, el reconocimiento de créditos a partir de experiencia profesional o laboral y los obtenidos en enseñanzas no oficiales, no incorporará calificación de los mismos, por lo que no computarán a efectos de baremación del expediente.
4. Los créditos reconocidos por actividades universitarias, culturales, deportivas, de representación estudiantil, solidarias y de cooperación, figurarán con la calificación de apto y no se computarán a efectos del cálculo de la nota media del expediente.

PLAZOS Y SOLICITUD

La presentación de solicitudes para el reconocimiento y transferencia de créditos, así como el calendario para la resolución y notificación al interesado de las mismas, coincidirán con las fechas establecidas por la Universidad de Murcia en sus "Instrucciones y Normas de Matrícula para cada curso académico". La solicitud se presentará en la secretaría del centro al que se encuentre adscrito el título objeto de reconocimiento en modelo unificado de la Universidad de Murcia. El estudiante solicitará a la Comisión Académica el reconocimiento de créditos presentando una instancia donde se reflejen las materias cursadas, con sus correspondientes programas. En los estudios de máster, la Comisión Académica del mismo será la encargada de elaborar la propuesta de reconocimiento y transferencia de créditos, para su posterior resolución por los Decanos/Decanas o Directores/Directoras de centro al que se encuentran adscritos estos estudios.

TRANSFERENCIA DE CRÉDITOS

Se entenderá por **transferencia** la consignación en los documentos académicos oficiales acreditativos de las enseñanzas seguidas por cada estudiante de todos los créditos obtenidos en enseñanzas oficiales, cursados con anterioridad a la obtención del título oficial.

Por lo que se refiere a la transferencia de créditos, el artículo 6, en sus apartados 4 y 5, del Reglamento sobre Reconocimiento y Transferencia de créditos en las Enseñanzas de Grado y Máster conducentes a la obtención de los correspondientes títulos oficiales de la Universidad de Murcia, recoge lo siguiente:

4. En relación con la transferencia de créditos:

a) Los créditos superados por el estudiante en enseñanzas oficiales universitarias del mismo nivel (Grado, Máster, Doctorado) que no sean constitutivos de reconocimiento para la obtención del título oficial o que no hayan conducido a la obtención de otro título, deberán consignarse, a solicitud del interesado, en el expediente del estudiante. En el impreso normalizado previsto en el artículo 4.2 de este Reglamento, se habilitará un apartado en el que haga constar su voluntad al respecto.

b) La transferencia se realizará consignando el literal, el número de créditos y la calificación original de las materias cursadas que aporte el estudiante. En ningún caso computarán para el cálculo de la nota media del expediente.

5. Incorporación de créditos al expediente académico: Todos los créditos obtenidos por el estudiante en enseñanzas oficiales cursados en cualquier universidad, los transferidos, los reconocidos y los superados para la obtención del correspondiente título, serán incluidos en su expediente académico.

4.6 COMPLEMENTOS FORMATIVOS

En este Máster no hay materias de nivelación o complementos de formación de los recogidos en el art. 17.5 del **Reglamento por el que se regulan los estudios oficales de Grado y Máster Universitario de la Universidad de Murcia**.

5. PLANIFICACIÓN DE LAS ENSEÑANZAS

5.1 DESCRIPCIÓN DEL PLAN DE ESTUDIOS
Ver Apartado 5: Anexo 1.
5.2 ACTIVIDADES FORMATIVAS
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.
Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica, resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).
Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.
Sesiones asíncronas de laboratorio: Se proporciona contenido didáctico práctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.
Casos prácticos: Las asignaturas pueden incluir casos prácticos con el objetivo pedagógico final de que el estudiante detecte situaciones relevantes, analice la información complementaria, tome decisiones en relación con el escenario que se plantea y proponga soluciones o indique cómo mejorar la situación de partida.
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.
Trabajo colaborativo: Las habilidades propias del trabajo colaborativo pueden ponerse en práctica con el apoyo del profesor de la asignatura, mediante el uso de herramientas que la Universidad pone a disposición del estudiantado. Incluye trabajos en grupo, tormenta de ideas, etc.
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.
5.3 METODOLOGÍAS DOCENTES
Lección Magistral: Exposición oral de un tema estructurado para facilitar los contenidos sobre la materia objeto de estudio de forma organizada. Se realizan a través de sesiones síncronas de teoría online o sesiones síncronas de laboratorio online.
Estudio de Casos: Análisis de un problema o suceso real para conocerlo, interpretarlo, resolverlo, generar hipótesis, contrastar datos, reflexionar, completar conocimientos, diagnosticarlo y buscar las soluciones.
Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.
Aprendizaje Basado en Problemas (ABP): A partir de un problema diseñado por el profesor, el estudiante ha de resolverlo para desarrollar determinadas competencias previamente definidas. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.
Aprendizaje Orientado a Proyectos (AOP): Los estudiantes llevan a cabo la realización de un proyecto en un tiempo determinado abordando una tarea mediante la planificación, diseño y realización de una serie de actividades. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.
Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

Contrato de Aprendizaje: Acuerdo establecido entre el profesor y el estudiante para la consecución de unos aprendizajes a través de una propuesta de trabajo autónomo, con la supervisión del profesor. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, tutorías grupales, etc.
5.4 SISTEMAS DE EVALUACIÓN
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).
Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.
Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.
Informe TFM: Este instrumento incluye los resultados de actividades relacionadas con el desarrollo del Trabajo Fin de Máster, junto con su memoria descriptiva.
Exposición y Defensa TFM: Este instrumento se refiere a la presentación o exposición oral del Trabajo Fin de Máster realizada de forma individual ante uno o varios profesores a modo de tribunal, y posibles turnos en los que los candidatos respondan a preguntas relacionadas con el trabajo.
5.5 SIN NIVEL 1
NIVEL 2: TÉCNICAS DE CIBERATAQUES Y HACKING ÉTICO
5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	6

DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
6		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**

LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

NO CONSTAN ELEMENTOS DE NIVEL 3
5.5.1.2 RESULTADOS DE APRENDIZAJE

- Identificar los principales aspectos a comunicar a la hora de presentar los resultados de un estudio o análisis relacionado con la ciberseguridad y al público al que va dirigido.
- Analizar métodos y técnicas de ciberataques y ciberdefensa.
- Diseñar, desplegar y mantener sistemas de ciberseguridad.
- Identificar la normativa y legislación aplicable en el ámbito de la ciberseguridad.
- Elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.
- Enumerar e identificar los distintos tipos de vulnerabilidades, amenazas y riesgos dentro de la organización, así como posibles soluciones a aplicar.
- Realizar procesos de análisis de vulnerabilidades y de riesgos.
- Clasificar las vulnerabilidades, amenazas y riesgos dentro de la organización para determinar su importancia. teniendo en cuenta el contexto.

5.5.1.3 CONTENIDOS

- Introducción a Ethical hacking.
  - Conceptos básicos.
  - Normativa y legislación asociada.
- Evaluaciones de seguridad.
  - Tipos de evaluaciones.

- Metodologías.
- Entrenamiento.

- Proceso de ethical hacking.
  - Despliegue de escenario y realización de proceso de ethical hacking.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Que los estudiantes sean capaces de analizar métodos y técnicas de ciberataques y ciberdefensa.

CG2 - Que los estudiantes sean capaces de diseñar, desplegar y mantener sistemas de ciberseguridad.

CG3 - Que los estudiantes sean capaces de identificar la normativa y legislación aplicable en el ámbito de la ciberseguridad.

CG4 - Que los estudiantes sean capaces de elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.

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

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE1 - Que los estudiantes sean capaces de gestionar los procesos asociados a vulnerabilidades, amenazas y riesgos dentro de una organización.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	9	0
Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica, resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).	9	0
Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	9	0

Sesiones asíncronas de laboratorio: Se proporciona contenido didáctico práctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	9	0
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	4	0
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	4	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	102	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	4	0

5.5.1.7 METODOLOGÍAS DOCENTES

Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.

Aprendizaje Orientado a Proyectos (AOP): Los estudiantes llevan a cabo la realización de un proyecto en un tiempo determinado abordando una tarea mediante la planificación, diseño y realización de una serie de actividades. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.

Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	10.0	60.0

Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0
Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.	20.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	10.0	30.0

NIVEL 2: TÉCNICAS DE CIBERDEFENSA		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
6		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Identificar los principales problemas actuales en el ámbito de la ciberseguridad en escenarios concretos.
- Analizar de forma detallada escenarios, soluciones o sistemas de ciberseguridad para detectar posibles aspectos de mejora.
- Aplicar métodos, protocolos, técnicas criptográficas o herramientas software para resolver problemas en entornos nuevos o poco conocidos relacionados con la ciberseguridad.
- Identificar los distintos aspectos multidisciplinares (legales, sociales, éticos) a tener en cuenta a la hora de abordar un problema relacionado con un escenario de ciberseguridad.
- Aplicar métodos, técnicas criptográficas, herramientas software o metodologías relacionadas con la ciberseguridad que permitan tener en cuenta aspectos multi-disciplinares.
- Formular juicios de valor a partir de la información recopilada que, siendo incompleta o limitada, incluya razonamiento crítico sobre las responsabilidades sociales y éticas de la aplicación de métodos, técnicas criptográficas, herramientas software o metodologías para abordar problemas relacionados con la ciberseguridad.
- Identificar los principales aspectos a comunicar a la hora de presentar los resultados de un estudio o análisis relacionado con la ciberseguridad y al público al que va dirigido.
- Diseñar una presentación que incluye las principales ideas a comunicar y los materiales audiovisuales que permitirán reforzar los mensajes a transmitir con respecto a un escenario de ciberseguridad.
- Exponer sus conocimientos de una forma clara, concisa, sin ambigüedades y adaptándose al tiempo establecido para la presentación.
- Analizar métodos y técnicas de ciberataques y ciberdefensa.
- Elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.
- Identificar las características y funciones de los elementos que forman parte de las arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.
- Identificar nuevas y emergentes tecnologías, buenas prácticas, aspectos normativos, legislativos y humanos relacionados con la ciberseguridad y los mecanismos para detectar estos cambios.

5.5.1.3 CONTENIDOS

Herramientas de defensa y monitorización de la red, diseño de arquitectura de red, sistemas de detección y prevención de intrusiones, gestión de incidentes, informática forense, modelos y procesos forenses, buenas prácticas y principios forenses, extracción y manipulación de evidencias, análisis de evidencias digitales, elaboración de informes, herramientas forenses.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Que los estudiantes sean capaces de analizar métodos y técnicas de ciberataques y ciberdefensa.

CG4 - Que los estudiantes sean capaces de elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.

CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

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

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

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

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE3 - Ser capaz de diseñar, monitorizar y evaluar arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.

CE5 - Identificar y conocer las nuevas tendencias, buenas prácticas, normas, regulación y aspectos humanos relacionados con la ciberseguridad.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	9	0
Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica, resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).	8	0
Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando	9	0

diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.		
Sesiones asíncronas de laboratorio: Se proporciona contenido didáctico práctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	8	0
Casos prácticos: Las asignaturas pueden incluir casos prácticos con el objetivo pedagógico final de que el estudiante detecte situaciones relevantes, analice la información complementaria, tome decisiones en relación con el escenario que se plantea y proponga soluciones o indique cómo mejorar la situación de partida.	3	0
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	2	0
Trabajo colaborativo: Las habilidades propias del trabajo colaborativo pueden ponerse en práctica con el apoyo del profesor de la asignatura, mediante el uso de herramientas que la Universidad pone a disposición del estudiantado. Incluye trabajos en grupo, tormenta de ideas, etc.	3	0
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	2	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	102	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en	4	0

la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.		

5.5.1.7 METODOLOGÍAS DOCENTES
Lección Magistral: Exposición oral de un tema estructurado para facilitar los contenidos sobre la materia objeto de estudio de forma organizada. Se realizan a través de sesiones síncronas de teoría online o sesiones síncronas de laboratorio online.
Estudio de Casos: Análisis de un problema o suceso real para conocerlo, interpretarlo, resolverlo, generar hipótesis, contrastar datos, reflexionar, completar conocimientos, diagnosticarlo y buscar las soluciones.
Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.
Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	10.0	60.0
Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0
Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.	20.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	10.0	30.0

NIVEL 2: TÉCNICAS DE CIBERSEGURIDAD Y COMUNICACIONES		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
6		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	

No	No

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Identificar los principales problemas actuales en el ámbito de la ciberseguridad en escenarios concretos.
- Analizar de forma detallada escenarios, soluciones o sistemas de ciberseguridad para detectar posibles aspectos de mejora.
- Aplicar métodos, protocolos, técnicas criptográficas o herramientas software para resolver problemas en entornos nuevos o poco conocidos relacionados con la ciberseguridad.
- Evaluar los métodos, protocolos seguros, técnicas criptográficas o herramientas software a utilizar para acometer la resolución de un problema en un entorno nuevo o poco conocido en el ámbito de la ciberseguridad.
- Utilizar los conocimientos para investigar nuevas tecnologías y metodologías aplicadas al ámbito de la ciberseguridad y contribuir así a su desarrollo.
- Aplicar métodos, técnicas criptográficas, herramientas software o metodologías relacionadas con la ciberseguridad que permitan tener en cuenta aspectos multi-disciplinares.
- Planifica tareas de trabajo autónomo y procesos de autoaprendizaje ejecutándolos en los tiempos previstos.
- Diseñar una presentación que incluye las principales ideas a comunicar y los materiales audiovisuales que permitirán reforzar los mensajes a transmitir con respecto a un escenario de ciberseguridad.
- Exponer sus conocimientos de una forma clara, concisa, sin ambigüedades y adaptándose al tiempo establecido para la presentación.
- Diseñar soluciones a problemas de ciberseguridad utilizando pensamiento creativo.
- Colaborar a la hora de resolver un problema del ámbito de la ciberseguridad, trabajo en equipo y liderazgo.
- Analizar métodos y técnicas de ciberataques y ciberdefensa.
- Elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.
- Identificar las características y funciones de los elementos que forman parte de las arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.
- Discutir sobre la funcionalidad de los elementos incorporados en las arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.
- Describir las primitivas criptográficas, los protocolos seguros y los mecanismos software que permitan la protección de datos.
- Diferenciar las distintas propiedades de seguridad que ofrecen las primitivas criptográficas, los protocolos que hacen uso de ellas y los métodos para el desarrollo de software seguro.
- Emplear el uso de primitivas criptográficas, protocolos seguros y modelos software para proteger datos en escenario de ciberseguridad.
- Identificar nuevas y emergentes tecnologías, buenas prácticas, aspectos normativos, legislativos y humanos relacionados con la ciberseguridad y los mecanismos para detectar estos cambios.
- Diferenciar los aspectos más relevantes de las nuevas tendencias, buenas prácticas, normas, leyes y aspectos humanos con respecto a los ya existentes.

5.5.1.3 CONTENIDOS

- Protocolos de red y vulnerabilidades: modelos de adversario, tipos de ataque.
- Seguridad a nivel de aplicación (gestión de claves simétrica y clave pública, protección a nivel de aplicación (SSH, S/MIME), seguridad en servicios de aplicación).
- Seguridad a nivel de transporte (TLS, DTLS, QUIC).
- Seguridad a nivel de red (ACLs, seguridad en IPv6, seguridad en los protocolos de enrutamiento, VPNs).
- Seguridad a nivel de enlace: seguridad a nivel inalámbrico (IEEE 802.1X, EAP, RADIUS, DIAMETER, WPA) ataques en switches ethernet, ataques a nivel MAC.
- Herramientas de defensa no criptográficas (filtrado de paquetes, firewall, DMZ, IDS, IPS, etc.).
- Tópicos avanzados de seguridad (SDN, NFV, IoT).
- Estándares en seguridad en las comunicaciones (cómo se especifican y documentan protocolos se seguridad).

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Que los estudiantes sean capaces de analizar métodos y técnicas de ciberataques y ciberdefensa.

CG4 - Que los estudiantes sean capaces de elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.

CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

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

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

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

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE3 - Ser capaz de diseñar, monitorizar y evaluar arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.

CE4 - Aplicar técnicas de seguridad de datos y software.
CE5 - Identificar y conocer las nuevas tendencias, buenas prácticas, normas, regulación y aspectos humanos relacionados con la ciberseguridad.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	9	0
Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica, resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).	9	0
Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	9	0
Sesiones asíncronas de laboratorio: Se proporciona contenido didáctico práctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	9	0
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	4	0

Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	4	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	102	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	4	0

5.5.1.7 METODOLOGÍAS DOCENTES

Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.

Aprendizaje Orientado a Proyectos (AOP): Los estudiantes llevan a cabo la realización de un proyecto en un tiempo determinado abordando una tarea mediante la planificación, diseño y realización de una serie de actividades. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.

Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	10.0	60.0
Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0
Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.	20.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	10.0	30.0

NIVEL 2: TÉCNICAS DE GESTIÓN DE LA CIBERSEGURIDAD

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	6

DESPLIEGUE TEMPORAL: Cuatrimestral

ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3

6		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Identificar de forma holística los distintos problemas relacionados con un área concreta de la ciberseguridad.
- Identificar los distintos aspectos multidisciplinares (legales, sociales, éticos) a tener en cuenta a la hora de abordar un problema relacionado con un escenario de ciberseguridad.
- Identificar, organizar y planificar las tecnologías a estudiar y/o recursos bibliográficos a analizar para abordar un determinado problema dentro del ámbito de la ciberseguridad.
- Identificar la normativa y legislación aplicable en el ámbito de la ciberseguridad.
- Planificar tareas de trabajo autónomo y procesos de autoaprendizaje ejecutándose en los tiempos previstos.
- Enumerar e identificar los distintos tipos de vulnerabilidades, amenazas y riesgos dentro de la organización, así como posibles soluciones a aplicar.
- Describir los principios de la gestión de riesgos, cómo aplicarlos y posibles herramientas a utilizar.
- Describir los principales elementos y funciones que forman parte de los servicios, productos e infraestructuras inteligentes en ámbitos de la ciberseguridad.
- Explicar los distintos aspectos relacionados con la gobernanza de la seguridad de la organización, la gestión de proyectos de seguridad, el diseño y la implantación de productos, servicios e instalaciones en escenarios de ciberseguridad.
- Diferenciar los aspectos más relevantes de la nuevas tendencias, buenas prácticas, normas, leyes y aspectos humanos con respecto a los ya existentes.

5.5.1.3 CONTENIDOS

- Gestión de sistemas de seguridad de la información.
  - Ciberseguridad y Esquema Nacional de Seguridad (ENS) en España: objetivos y ámbito de aplicación, requisitos del ENS, medidas de seguridad.
  - Sistemas de Gestión de la Seguridad de la Información (SGSI). Familia ISO 27000.
  - Implantación y auditoría de los SGSI según las etapas del ciclo de Deming: planificar, hacer, verificar, actuar.
  - Planes de seguridad y continuidad de negocio. Familia ISO 22300.
- Identificación, análisis y gestión de los riesgos de seguridad.
  - Análisis y gestión de riesgos: vulnerabilidades, amenazas, programas maliciosos.
  - Metodologías de identificación y análisis de riesgos: NIST SP 800, MAGERIT, ISACA.
  - Casos prácticos para la gestión de los riesgos de seguridad: proyección y despliegue de controles y medidas de salvaguarda para la reducción del riesgo.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG3 - Que los estudiantes sean capaces de identificar la normativa y legislación aplicable en el ámbito de la ciberseguridad.

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

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

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE1 - Que los estudiantes sean capaces de gestionar los procesos asociados a vulnerabilidades, amenazas y riesgos dentro de una organización.

CE2 - Que los estudiantes sean capaces de proyectar, diseñar e implantar productos, procesos, servicios e infraestructuras inteligentes en ámbitos de la ciberseguridad.
CE5 - Identificar y conocer las nuevas tendencias, buenas prácticas, normas, regulación y aspectos humanos relacionados con la ciberseguridad.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	9	0
Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica, resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).	9	0
Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	9	0
Sesiones asíncronas de laboratorio: Se proporciona contenido didáctico práctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	9	0
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los	4	0

estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.		
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	4	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	102	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	4	0

5.5.1.7 METODOLOGÍAS DOCENTES

Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.

Aprendizaje Basado en Problemas (ABP): A partir de un problema diseñado por el profesor, el estudiante ha de resolverlo para desarrollar determinadas competencias previamente definidas. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.

Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	10.0	60.0
Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0
Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.	20.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	10.0	30.0

NIVEL 2: CRIPTOGRAFÍA

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	3
DESPLIEGUE TEMPORAL: Cuatrimestral	

ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3

3		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Aplicar métodos, protocolos, técnicas criptográficas o herramientas software para resolver problemas en entornos nuevos o poco conocidos relacionados con la ciberseguridad.
- Evaluar los métodos, protocolos seguros, técnicas criptográficas o herramientas software a utilizar para acometer la resolución de un problema en un entorno nuevo o poco conocido en el ámbito de la ciberseguridad.
- Utilizar los conocimientos para investigar nuevas tecnologías y metodologías aplicadas al ámbito de la ciberseguridad y contribuir así a su desarrollo.
- Recopilar y analizar datos de investigación para afrontar nuevos problemas en el ámbito de la ciberseguridad.
- Analizar métodos y técnicas de ciberataques y ciberdefensa.
- Describir las primitivas criptográficas, los protocolos seguros y los mecanismos software que permitan la protección de datos.
- Diferenciar las distintas propiedades de seguridad que ofrecen las primitivas criptográficas, los protocolos que hacen uso de ellas y los métodos para el desarrollo de software seguro.
- Emplear el uso de primitivas criptográficas, protocolos seguros y modelos software para proteger datos en escenario de ciberseguridad.
- Analizar escenarios donde es necesario proporcionar software y mecanismos protección de los datos de la organización respetando la normativa existente.
- Proponer el uso de primitivas criptográficas, protocolos seguros y metodologías de desarrollo de software seguro en función de los escenarios planteados considerando tanto aspectos técnicos como de negocio.
- Evaluar la seguridad de los datos y del software desarrollado en base a las primitivas criptográficas empleadas, protocolos seguros utilizados y los análisis de vulnerabilidades realizados.

5.5.1.3 CONTENIDOS

- Se dará una visión amplia de la criptografía, estudiando tanto los aspectos matemáticos y teóricos hasta los aspectos relativos a la implementación de los mismos en entornos especiales.
- Modelos de seguridad criptográfica. Sistemas de compartición de secretos. Criptografía simétrica (cifrados de bloques, cifrados de flujo, funciones de resumen digital, códigos de autenticación de mensajes, árboles de Merkle y cadenas de bloques), criptografía de clave pública (construcciones basadas en RSA, en curvas elípticas y en retículos, firmas digitales), protocolos criptográficos (autenticación, intercambio de claves, conocimiento cero, computación segura multipartita), aspectos avanzados de criptografía (firmas basadas en grupos/anillos, cifrados basados en la identidad, criptografía homomórfica, ataques de canal lateral, implementaciones en entornos con requerimientos especiales).

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Que los estudiantes sean capaces de analizar métodos y técnicas de ciberataques y ciberdefensa.

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

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE4 - Aplicar técnicas de seguridad de datos y software.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la	4.5	0

metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.		
Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica, resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).	4.5	0
Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	4.5	0
Sesiones asíncronas de laboratorio: Se proporciona contenido didáctico práctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	4.5	0
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	2	0
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	1	0

Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	51	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	3	0

5.5.1.7 METODOLOGÍAS DOCENTES

Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.

Aprendizaje Orientado a Proyectos (AOP): Los estudiantes llevan a cabo la realización de un proyecto en un tiempo determinado abordando una tarea mediante la planificación, diseño y realización de una serie de actividades. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.

Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	10.0	60.0
Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0
Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.	20.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	10.0	30.0

NIVEL 2: SEMINARIO SOBRE INNOVACIÓN Y EMPRENDIMIENTO I

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	3

DESPLIEGUE TEMPORAL: Cuatrimestral

ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
3		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**

LENGUAS EN LAS QUE SE IMPARTE

CASTELLANO	CATALÁN	EUSKERA
Sí	No	No

GALLEGO	VALENCIANO	INGLÉS
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Aplicar métodos, técnicas criptográficas, herramientas software o metodologías relacionadas con la ciberseguridad que permitan tener en cuenta aspectos multidisciplinares.
- Diseñar una presentación que incluye las principales ideas a comunicar y los materiales audiovisuales que permitirán reforzar los mensajes a transmitir con respecto a un escenario de ciberseguridad.
- Identificar, organizar y planificar las tecnologías a estudiar y/o recursos bibliográficos a analizar para abordar un determinado problema dentro del ámbito de la ciberseguridad.
- Identificar modelos de gestión de la ciberseguridad y procesos asociados para llevar a cabo el seguimiento y la gestión de la ciberseguridad dentro de una organización.
- Identificar nuevas y emergentes tecnologías, buenas prácticas, aspectos normativos, legislativos y humanos relacionados con la ciberseguridad y los mecanismos para detectar estos cambios.
- Diferenciar los aspectos más relevantes de las nuevas tendencias, buenas prácticas, normas, leyes y aspectos humanos con respecto a los ya existentes.

5.5.1.3 CONTENIDOS

- El objetivo es acercar los problemas y soluciones más acuciantes en cada momento de la industria, administración, defensa e investigación a los alumnos. A través de una serie de seminarios, presentaciones y exposiciones que se propongan a los alumnos, éstos podrán tener acceso a la experiencia de profesionales de reconocido prestigio cuya labor profesional está relacionada con la ciberseguridad en sus facetas legales, administrativas y de gestión y legales.
- Por otra parte, los seminarios más académicos pondrán a los alumnos en contacto con el estado de la técnica en conceptos, protocolos, desarrollos y herramientas en temas concretos relacionados con la ciberseguridad. Por tanto, los seminarios podrán encuadrarse dentro de cualquiera de las materias del máster.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG5 - Que los estudiantes conozcan los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, considerando la definición de estrategias, políticas y normas para la seguridad corporativa.

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

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

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE5 - Identificar y conocer las nuevas tendencias, buenas prácticas, normas, regulación y aspectos humanos relacionados con la ciberseguridad.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	8	0
Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de	4	0

actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.		
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	4	0
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	6	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	51	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	2	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección Magistral: Exposición oral de un tema estructurado para facilitar los contenidos sobre la materia objeto de estudio de forma organizada. Se realizan a través de sesiones síncronas de teoría online o sesiones síncronas de laboratorio online.

Estudio de Casos: Análisis de un problema o suceso real para conocerlo, interpretarlo, resolverlo, generar hipótesis, contrastar datos, reflexionar, completar conocimientos, diagnosticarlo y buscar las soluciones.

Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.

Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	20.0	60.0
Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0

Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	20.0	40.0

NIVEL 2: TECNOLOGÍAS DE ATAQUES Y MALWARE		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	3	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	3	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Aplicar métodos, técnicas criptográficas, herramientas software o metodologías relacionadas con la ciberseguridad que permitan tener en cuenta aspectos multi-disciplinares.
- Diseñar soluciones a problemas de ciberseguridad utilizando pensamiento creativo.
- Analizar métodos y técnicas de ciberataques y ciberdefensa.
- Enumerar e identificar los distintos tipos de vulnerabilidades, amenazas y riesgos dentro de la organización así como posibles soluciones a aplicar.
- Clasificar las vulnerabilidades, amenazas y riesgos dentro de la organización para determinar su importancia teniendo en cuenta el contexto.
- Proponer el uso de primitivas criptográficas, protocolos seguros y metodologías de desarrollo de software seguro en función de los escenarios planteados consi-derando tanto aspectos técnicos como de negocio.
- Evaluar la seguridad de los datos y del software desarrollado en base a las primitivas criptográficas empleadas, protocolos seguros utilizados y los análisis de vulnerabilidades realizados.

5.5.1.3 CONTENIDOS

- Taxonomía de malware. Dimensiones y características.
- Actividades maliciosas del malware.
- Análisis de malware. Técnicas de análisis, entornos de análisis. Técnicas de evasión de análisis.
- Detección de malware. Identificar presencia, detección de ataques.
- Respuesta a un malware. Detener operaciones. Identificación.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Que los estudiantes sean capaces de analizar métodos y técnicas de ciberataques y ciberdefensa.

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

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

5.5.1.5.2 TRANSVERSALES

No existen datos		
5.5.1.5.3 ESPECÍFICAS		
CE1 - Que los estudiantes sean capaces de gestionar los procesos asociados a vulnerabilidades, amenazas y riesgos dentro de una organización.		
CE4 - Aplicar técnicas de seguridad de datos y software.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	4.5	0
Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica, resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).	4.5	0
Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	4.5	0
Sesiones asíncronas de laboratorio: Se proporciona contenido didáctico práctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	4.5	0
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas	2	0

particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.		
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	1	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	51	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	3	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección Magistral: Exposición oral de un tema estructurado para facilitar los contenidos sobre la materia objeto de estudio de forma organizada. Se realizan a través de sesiones síncronas de teoría online o sesiones síncronas de laboratorio online.

Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.

Aprendizaje Orientado a Proyectos (AOP): Los estudiantes llevan a cabo la realización de un proyecto en un tiempo determinado abordando una tarea mediante la planificación, diseño y realización de una serie de actividades. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.

Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	10.0	60.0
Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0
Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.	20.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	10.0	30.0

NIVEL 2: RÉGIMEN JURÍDICO DE LA CIBERSEGURIDAD

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria	
ECTS NIVEL 2	3	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	3	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Identificar los principales problemas actuales en el ámbito de la ciberseguridad en escenarios concretos.
- Identificar de forma holística los distintos problemas relacionados con un área concreta de la ciberseguridad.
- Identificar los distintos aspectos multidisciplinares (legales, sociales, éticos) a tener en cuenta a la hora de abordar un problema relacionado con un escenario de ciberseguridad.
- Formular juicios de valor a partir de la información recopilada que, siendo incompleta o limitada, incluya razonamiento crítico sobre las responsabilidades sociales y éticas de la aplicación de métodos, técnicas criptográficas, herramientas software o metodologías para abordar problemas relacionados con la ciberseguridad.
- Identificar los principales aspectos a comunicar a la hora de presentar los resultados de un estudio o análisis relacionado con la ciberseguridad y al público al que va dirigido.
- Identificar, organizar y planificar las tecnologías a estudiar y/o recursos bibliográficos a analizar para abordar un determinado problema dentro del ámbito de la ciberseguridad.
- Identificar la normativa y legislación aplicable en el ámbito de la ciberseguridad.
- Elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.
- Identificar modelos de gestión de la ciberseguridad y procesos asociados para llevar a cabo el seguimiento y la gestión de la ciberseguridad dentro de una organización.
- Identificar nuevas y emergentes tecnologías, buenas prácticas, aspectos normativos, legislativos y humanos relacionados con la ciberseguridad y los mecanismos para detectar estos cambios.
- Diferenciar los aspectos más relevantes de las nuevas tendencias, buenas prácticas, normas, leyes y aspectos humanos con respecto a los ya existentes.
- Adaptar escenarios de ciberseguridad conforme a las nuevas tendencias, buenas prácticas, normas, regulación y aspectos humanos.
- Analizar de forma detallada nuevas tendencias, buenas prácticas, normas, regulación y aspectos humanos relacionados con la ciberseguridad.
- Argumentar y asesorar sobre las razones de la introducción de nuevas tecnologías, buenas prácticas, normas, regulación y aspectos en un escenario de ciberseguridad.
- Evaluar las implicaciones de la adopción de nuevas tecnologías, buenas prácticas, normas, regulación y aspectos humanos de la ciberseguridad en escenarios concretos de negocio.

5.5.1.3 CONTENIDOS

- Seguridad de las redes y sistemas de información.
- Protección de las infraestructuras críticas.
- Protección de datos de carácter personal.
- Control de los servicios financieros y medios de pago.
- Servicios de confianza.
- Identidad digital.
- Esquema Nacional de Seguridad.
- Regulación de aspectos penales.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG3 - Que los estudiantes sean capaces de identificar la normativa y legislación aplicable en el ámbito de la ciberseguridad.

CG4 - Que los estudiantes sean capaces de elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.

CG5 - Que los estudiantes conozcan los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, considerando la definición de estrategias, políticas y normas para la seguridad corporativa.
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
5.5.1.5.2 TRANSVERSALES
No existen datos
5.5.1.5.3 ESPECÍFICAS
CE5 - Identificar y conocer las nuevas tendencias, buenas prácticas, normas, regulación y aspectos humanos relacionados con la ciberseguridad.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	5	0
Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	5	0
Sesiones asíncronas de laboratorio: Se proporciona contenido didáctico práctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden	3	0

ir suministrando conforme avance la asignatura.		
Casos prácticos: Las asignaturas pueden incluir casos prácticos con el objetivo pedagógico final de que el estudiante detecte situaciones relevantes, analice la información complementaria, tome decisiones en relación con el escenario que se plantea y proponga soluciones o indique cómo mejorar la situación de partida.	6	0
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	2	0
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	1	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	51	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	2	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección Magistral: Exposición oral de un tema estructurado para facilitar los contenidos sobre la materia objeto de estudio de forma organizada. Se realizan a través de sesiones síncronas de teoría online o sesiones síncronas de laboratorio online.

Estudio de Casos: Análisis de un problema o suceso real para conocerlo, interpretarlo, resolverlo, generar hipótesis, contrastar datos, reflexionar, completar conocimientos, diagnosticarlo y buscar las soluciones.

Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.

Aprendizaje Orientado a Proyectos (AOP): Los estudiantes llevan a cabo la realización de un proyecto en un tiempo determinado abordando una tarea mediante la planificación, diseño y realización de una serie de actividades. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.

Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	10.0	60.0

Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0
Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.	20.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	10.0	30.0

NIVEL 2: SEGURIDAD SOFTWARE Y CICLO DE VIDA DEL SOFTWARE SEGURO

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	3

DESPLIEGUE TEMPORAL: Cuatrimestral

ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	3	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**

LENGUAS EN LAS QUE SE IMPARTE

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

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Analizar de forma detallada escenarios, soluciones o sistemas de ciberseguridad para detectar posibles aspectos de mejora.
- Identificar de forma holística los distintos problemas relacionados con un área concreta de la ciberseguridad.
- Aplicar métodos, técnicas criptográficas, herramientas software o metodologías de vanguardia relacionadas con la ciberseguridad que permitan tener en cuenta aspectos multidisciplinares.
- Identificar modelos de gestión de la ciberseguridad y procesos asociados para llevar a cabo el seguimiento y la gestión de la ciberseguridad dentro de una organización.
- Diferenciar las distintas propiedades de seguridad que ofrecen las primitivas criptográficas, los protocolos que hacen uso de ellas y los métodos para el desarrollo de software seguro.
- Analizar escenarios donde es necesario proporcionar software y mecanismos protección de los datos de la organización respetando la normativa existente.
- Proponer el uso de primitivas criptográficas, protocolos seguros y metodologías de desarrollo de software seguro en función de los escenarios planteados considerando tanto aspectos técnicos como de negocio.
- Evaluar la seguridad de los datos y del software desarrollado en base a las primitivas criptográficas empleadas, protocolos seguros utilizados y los análisis de vulnerabilidades realizados.

5.5.1.3 CONTENIDOS

- **DESARROLLO DE SOFTWARE SEGURO**
  - Gestión del riesgo en la seguridad: análisis de riesgos, modelado de amenazas y su documentación para desarrollar un plan de riesgos de ciberseguridad software.
  - Técnicas de desarrollo de software seguro.
  - Diseño, validación y verificación de requisitos de seguridad.
  - El paradigma DevSecOps.
  - CI/CD y la automatización de detección de problemas de seguridad mediante SDLC.
- **ASEGURAMIENTO DEL CICLO DE VIDA DEL SOFTWARE SEGURO**
  - Chequeo de la seguridad.
  - Estándares para el desarrollo seguro y su planificación documental.
  - Sistemas de certificación de la seguridad.
- **PREVENCIÓN Y DETECCIÓN DE VULNERABILIDADES**

- Prevención y detección.
- Mitigación de la explotación de vulnerabilidades.
- Vulnerabilidades y mitigación en el lado del cliente y del servidor.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG5 - Que los estudiantes conozcan los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, considerando la definición de estrategias, políticas y normas para la seguridad corporativa.

CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

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

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

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE4 - Aplicar técnicas de seguridad de datos y software.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	4.5	0
Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica, resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).	4.5	0
Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	4.5	0

Sesiones asíncronas de laboratorio: Se proporciona contenido didáctico práctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	4.5	0
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	2	0
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	1	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	51	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	3	0

5.5.1.7 METODOLOGÍAS DOCENTES

Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.

Aprendizaje Basado en Problemas (ABP): A partir de un problema diseñado por el profesor, el estudiante ha de resolverlo para desarrollar determinadas competencias previamente definidas. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.

Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	10.0	60.0

Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0
Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.	20.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	10.0	30.0

NIVEL 2: INFRAESTRUCTURAS DE AUTENTICACIÓN Y AUTORIZACIÓN

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	3

DESPLIEGUE TEMPORAL: Cuatrimestral

ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	3	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**

LENGUAS EN LAS QUE SE IMPARTE

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

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Aplicar métodos, protocolos, técnicas criptográficas o herramientas software para resolver problemas en entornos nuevos o poco conocidos relacionados con la ciberseguridad.
- Identificar modelos de gestión de la ciberseguridad y procesos asociados para llevar a cabo el seguimiento y la gestión de la ciberseguridad dentro de una organización.
- Identificar nuevas y emergentes tecnologías, buenas prácticas, aspectos normativos, legislativos y humanos relacionados con la ciberseguridad y los mecanismos para detectar estos cambios.
- Planificar tareas de trabajo autónomo y procesos de autoaprendizaje ejecutándose en los tiempos previstos.
- Diseñar una presentación que incluye las principales ideas a comunicar y los materiales audiovisuales que permitirán reforzar los mensajes a transmitir con respecto a un escenario de ciberseguridad.
- Exponer sus conocimientos de una forma clara, concisa, sin ambigüedades y adaptándose al tiempo establecido para la presentación.
- Colaborar a la hora de resolver un problema del ámbito de la ciberseguridad, trabajo en equipo y liderazgo.
- Identificar de forma holística los distintos problemas relacionados con un área concreta de la ciberseguridad.

5.5.1.3 CONTENIDOS

- Autenticación, Autorización y Contabilidad: definición, modelos, etc.
- Autenticación de usuarios (passwords, biometría, tokens de autenticación, comportamiento, 2FA, etc.). Modelos de gestión y procesos de autenticación y autorización. Tendencias actuales en procesos de autenticación. Normativa y regulación.
- Autenticación en sistemas distribuidos. Descripción de los principales sistemas distribuidos, como Kerberos, SAML, OpenID Connect, etc. Características, funcionalidad y evaluación de las arquitecturas para la autenticación.
- Sistemas de control de acceso y autorización. Descripción de los principales sistemas de control de acceso y autenticación, como OAuth o XACML. Características, funcionalidad y evaluación de las arquitecturas para control de acceso y autorización.
- Gestión de la Contabilidad (privacidad, logs, etc.) para la monitorización de sistemas e infraestructuras.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES
CG5 - Que los estudiantes conozcan los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, considerando la definición de estrategias, políticas y normas para la seguridad corporativa.
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
5.5.1.5.2 TRANSVERSALES
No existen datos
5.5.1.5.3 ESPECÍFICAS
CE5 - Identificar y conocer las nuevas tendencias, buenas prácticas, normas, regulación y aspectos humanos relacionados con la ciberseguridad.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	4.5	0
Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica, resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).	4.5	0
Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	4.5	0
Sesiones asíncronas de laboratorio: Se proporciona contenido didáctico práctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse	4.5	0

en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.		
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	2	0
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	1	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	51	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	3	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección Magistral: Exposición oral de un tema estructurado para facilitar los contenidos sobre la materia objeto de estudio de forma organizada. Se realizan a través de sesiones síncronas de teoría online o sesiones síncronas de laboratorio online.

Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.

Aprendizaje Orientado a Proyectos (AOP): Los estudiantes llevan a cabo la realización de un proyecto en un tiempo determinado abordando una tarea mediante la planificación, diseño y realización de una serie de actividades. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.

Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	10.0	60.0
Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0

Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.	20.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	10.0	30.0

NIVEL 2: LABORATORIO DE PROYECTOS EN CIBERSEGURIDAD

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	6

DESPLIEGUE TEMPORAL: Cuatrimestral

ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	6	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**

LENGUAS EN LAS QUE SE IMPARTE

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

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Identificar los principales problemas actuales en el ámbito de la ciberseguridad en escenarios concretos.
- Aplicar métodos, protocolos, técnicas criptográficas o herramientas software para resolver problemas en entornos nuevos o poco conocidos relacionados con la ciberseguridad.
- Aplicar métodos, técnicas criptográficas, herramientas software o metodologías relacionadas con la ciberseguridad que permitan tener en cuenta aspectos multidisciplinares.
- Formular juicios de valor a partir de la información recopilada que, siendo incompleta o limitada, incluya razonamiento crítico sobre las responsabilidades sociales y éticas de la aplicación de métodos, técnicas criptográficas, herramientas software o metodologías para abordar problemas relacionados con la ciberseguridad.
- Diseñar una presentación que incluye las principales ideas a comunicar y los materiales audiovisuales que permitirán reforzar los mensajes a transmitir con respecto a un escenario de ciberseguridad.
- Exponer sus conocimientos de una forma clara, concisa, sin ambigüedades y adaptándose al tiempo establecido para la presentación.
- Colaborar a la hora de resolver un problema del ámbito de la ciberseguridad, trabajo en equipo y liderazgo.
- Analizar métodos y técnicas de ciberataques y ciberdefensa.
- Enumerar e identificar los distintos tipos de vulnerabilidades, amenazas y riesgos dentro de la organización, así como posibles soluciones a aplicar.
- Realizar procesos de análisis de vulnerabilidades y de riesgos.
- Discutir sobre la funcionalidad de los elementos incorporados en las arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.
- Desplegar elementos de monitorización en arquitecturas y servicios de seguridad, infraestructuras críticas y redes de comunicaciones.
- Analizar la información de seguridad recopilada mediante procesos de monitorización de arquitecturas de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.

5.5.1.3 CONTENIDOS

Esta asignatura tendrá una estructura en donde los alumnos por grupo deberán resolver problemas en grupo, formando un equipo de respuesta y donde tengan que poner en colaboración técnicas y herramientas aprendidas en las asignaturas anteriores, de forma que puedan poner en funcionamiento de forma práctica la integración de diferentes herramientas. La conformación de equipos se hará de forma que puedan interaccionar entre alumnos con perfiles diferentes de forma que los equipos puedan abarcar diferentes aspectos de la resolución de problemas de ciberseguridad. Se focalizará en realizar ejercicios simulados de ataques y de reacción donde equipos diferentes podrán ejercer en diferentes roles.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS
5.5.1.5.1 BÁSICAS Y GENERALES
CG1 - Que los estudiantes sean capaces de analizar métodos y técnicas de ciberataques y ciberdefensa.
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
5.5.1.5.2 TRANSVERSALES
No existen datos
5.5.1.5.3 ESPECÍFICAS
CE1 - Que los estudiantes sean capaces de gestionar los procesos asociados a vulnerabilidades, amenazas y riesgos dentro de una organización.
CE3 - Ser capaz de diseñar, monitorizar y evaluar arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	4	0
Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica, resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).	6	0
Casos prácticos: Las asignaturas pueden incluir casos prácticos con el objetivo pedagógico final de que el estudiante detecte situaciones relevantes, analice la información complementaria, tome decisiones en relación con el escenario que se plantea y proponga soluciones o indique cómo mejorar la situación de partida.	4	0
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los	4	0

estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.		
Trabajo colaborativo: Las habilidades propias del trabajo colaborativo pueden ponerse en práctica con el apoyo del profesor de la asignatura, mediante el uso de herramientas que la Universidad pone a disposición del estudiantado. Incluye trabajos en grupo, tormenta de ideas, etc.	22	0
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	4	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	102	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	4	0

5.5.1.7 METODOLOGÍAS DOCENTES

Estudio de Casos: Análisis de un problema o suceso real para conocerlo, interpretarlo, resolverlo, generar hipótesis, contrastar datos, reflexionar, completar conocimientos, diagnosticarlo y buscar las soluciones.

Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

Contrato de Aprendizaje: Acuerdo establecido entre el profesor y el estudiante para la consecución de unos aprendizajes a través de una propuesta de trabajo autónomo, con la supervisión del profesor. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, tutorías grupales, etc.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	20.0	60.0
Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.	20.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	0.0	40.0

NIVEL 2: SEGURIDAD EN SISTEMAS IoT, 5G Y CIBERFÍSICOS

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Optativa

ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	6	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NO CONSTAN ELEMENTOS DE NIVEL 3		

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Evaluar los métodos, protocolos seguros, técnicas criptográficas o herramientas software a utilizar para acometer la resolución de un problema en un entorno nuevo o poco conocido en el ámbito de la ciberseguridad.
- Recopilar y analizar datos de investigación para afrontar nuevos problemas en el ámbito de la ciberseguridad.
- Aplicar métodos, técnicas criptográficas, herramientas software o metodologías relacionadas con la ciberseguridad que permitan tener en cuenta aspectos multi-disciplinares.
- Diseñar soluciones a problemas de ciberseguridad utilizando pensamiento creativo.
- Diseñar, desplegar y mantener sistemas de ciberseguridad.
- Identificar la normativa y legislación aplicable en el ámbito de la ciberseguridad.
- Identificar modelos de gestión de la ciberseguridad y procesos asociados para llevar a cabo el seguimiento y la gestión de la ciberseguridad dentro de una organización.
- Describir los principales elementos y funciones que forman parte de los servicios, productos e infraestructuras inteligentes en ámbitos de la ciberseguridad.
- Diseñar e implantar procesos de gestión de la seguridad, de productos, servicios e instalaciones desde la perspectiva de la seguridad de estos y considerando aspectos de negocio (regulación, normativa, económicos, etc).
- Analizar escenarios en el ámbito de la ciberseguridad desde el punto de vista de gobernanza de la seguridad de la organización, la gestión de la ciberseguridad y de la seguridad de productos, servicios e instalaciones.
- Evaluar críticamente los procesos de gobernanza de la seguridad, gestión de la seguridad, diseño de productos, procesos, servicios e infraestructuras inteligentes en ámbitos de ciberseguridad teniendo en cuenta requisitos, soluciones existentes, normas, estándares y buenas prácticas.
- Desplegar elementos de monitorización en arquitecturas y servicios de seguridad, infraestructuras críticas y redes de comunicaciones.
- Analizar la información de seguridad recopilada mediante procesos de monitorización de arquitecturas de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.
- Diseñar arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones que estén de acuerdo a las políticas de la organización, consideren aspectos técnicos, de negocio (económicos, legales, medioambientales, etc) y de innovación.
- Evaluar arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones que estén de acuerdo a las políticas de la organización, considerando aspectos técnicos, de negocio (económicos, legales, medioambientales, etc) y de innovación.

5.5.1.3 CONTENIDOS

- Seguridad a nivel de capa física en las principales tecnologías de comunicación. Vulnerabilidades en comunicaciones radio: Redes celulares, Sistemas de Navegación por Satélite (GNSS), Sistemas de Identificación por Radiofrecuencia (RFID), redes de sensores, sistemas de comunicaciones en el ámbito del transporte, etc.
- Ciberseguridad en el ámbito de Internet de las cosas (IoT) y de los Sistemas Ciberfísicos (CPS). Gestión de identidad, privacidad y control de acceso en despliegues IoT y CPS, conforme a normativa vigente.
- Diseño e implementación de sistemas de ciberseguridad inteligentes en entornos IoT.
- La ciberseguridad en los Sistemas Control Industrial (ICS). Análisis de vulnerabilidades. Gestión de incidentes. Seguridad en equipos industriales, etc.
- Seguridad en arquitecturas de redes celulares: 5G.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG2 - Que los estudiantes sean capaces de diseñar, desplegar y mantener sistemas de ciberseguridad.

CG3 - Que los estudiantes sean capaces de identificar la normativa y legislación aplicable en el ámbito de la ciberseguridad.

CG5 - Que los estudiantes conozcan los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, considerando la definición de estrategias, políticas y normas para la seguridad corporativa.
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
5.5.1.5.2 TRANSVERSALES
No existen datos
5.5.1.5.3 ESPECÍFICAS
CE2 - Que los estudiantes sean capaces de proyectar, diseñar e implantar productos, procesos, servicios e infraestructuras inteligentes en ámbitos de la ciberseguridad.
CE3 - Ser capaz de diseñar, monitorizar y evaluar arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	16	0
Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica, resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).	16	0
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	6	0
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	6	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los	102	0

contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.		
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	4	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección Magistral: Exposición oral de un tema estructurado para facilitar los contenidos sobre la materia objeto de estudio de forma organizada. Se realizan a través de sesiones síncronas de teoría online o sesiones síncronas de laboratorio online.

Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.

Aprendizaje Basado en Problemas (ABP): A partir de un problema diseñado por el profesor, el estudiante ha de resolverlo para desarrollar determinadas competencias previamente definidas. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	10.0	60.0
Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0
Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.	20.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	10.0	30.0

NIVEL 2: TÉCNICAS AVANZADAS DE CIBER INTELIGENCIA

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Optativa
ECTS NIVEL 2	6

DESPLIEGUE TEMPORAL: Cuatrimestral

ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
	6	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**

LENGUAS EN LAS QUE SE IMPARTE

CASTELLANO	CATALÁN	EUSKERA
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**

No	No	No
ITALIANO	**OTRAS**	
No	No	

LISTADO DE ESPECIALIDADES

No existen datos

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Identificar los principales problemas actuales en el ámbito de la ciberseguridad en escenarios concretos.
- Analizar de forma detallada escenarios, soluciones o sistemas de ciberseguridad para detectar posibles aspectos de mejora.
- Diseñar escenarios, soluciones, o sistemas de ciberseguridad incluyendo aspectos originales o innovadores.
- Identificar de forma holística los distintos problemas relacionados con un área concreta de la ciberseguridad.
- Aplicar métodos, protocolos, técnicas criptográficas o herramientas software para resolver problemas en entornos nuevos o poco conocidos relacionados con la ciberseguridad.
- Evaluar los métodos, protocolos seguros, técnicas criptográficas o herramientas software a utilizar para acometer la resolución de un problema en un entorno nuevo o poco conocido en el ámbito de la ciberseguridad.
- Utilizar los conocimientos para investigar nuevas tecnologías y metodologías aplicadas al ámbito de la ciberseguridad y contribuir así a su desarrollo.
- Recopilar y analizar datos de investigación para afrontar nuevos problemas en el ámbito de la ciberseguridad.
- Identificar los principales aspectos a comunicar a la hora de presentar los resultados de un estudio o análisis relacionado con la ciberseguridad y al público al que va dirigido.
- Diseñar una presentación que incluye las principales ideas a comunicar y los materiales audiovisuales que permitirán reforzar los mensajes a transmitir con respecto a un escenario de ciberseguridad.
- Identificar, organizar y planificar las tecnologías a estudiar y/o recursos bibliográficos a analizar para abordar un determinado problema dentro del ámbito de la ciberseguridad.
- Diseñar soluciones a problemas de ciberseguridad utilizando pensamiento creativo.
- Analizar métodos y técnicas de ciberataques y ciberdefensa.
- Diseñar, desplegar y mantener sistemas de ciberseguridad.
- Identificar las características y funciones de los elementos que forman parte de las arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.
- Discutir sobre la funcionalidad de los elementos incorporados en las arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.
- Desplegar elementos de monitorización en arquitecturas y servicios de seguridad, infraestructuras críticas y redes de comunicaciones.
- Analizar la información de seguridad recopilada mediante procesos de monitorización de arquitecturas de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.
- Analizar escenarios donde es necesario proporcionar software y mecanismos protección de los datos de la organización respetando la normativa existente.

5.5.1.3 CONTENIDOS

- **Gestión de información de ciber inteligencia**
  - Arquitecturas, fases y procesos asociados a la ciber inteligencia.
  - Técnicas automáticas de captación, intercambio y gestión de información de ciber inteligencia.
  - Formatos y representación de información de ciber inteligencia.
  - Privacidad y confidencialidad en el intercambio de información de ciber inteligencia.
- **Procesamiento avanzado de información de ciber-inteligencia**
  - Detección de ciberataques y amenazas basada en Inteligencia Artificial.
  - Sistemas de ciber inteligencia basados en IA escalables y federados.
  - Técnicas computacionales avanzadas para la detección de anomalías.
  - Análisis de datos de Redes sociales y otras fuentes para Ciber-inteligencia.
  - Diseño y gestión de los sistemas de ciber inteligencia: casos prácticos.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Que los estudiantes sean capaces de analizar métodos y técnicas de ciberataques y ciberdefensa.

CG2 - Que los estudiantes sean capaces de diseñar, desplegar y mantener sistemas de ciberseguridad.

CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

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

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

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE3 - Ser capaz de diseñar, monitorizar y evaluar arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.

CE4 - Aplicar técnicas de seguridad de datos y software.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	9	0
Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica, resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).	9	0
Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	9	0
Sesiones asíncronas de laboratorio: Se proporciona contenido didáctico práctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	9	0
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	4	0
Seminarios: Se imparten de modo virtual para la resolución de aquellas	4	0

cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.		
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	102	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	4	0

5.5.1.7 METODOLOGÍAS DOCENTES

Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.

Aprendizaje Orientado a Proyectos (AOP): Los estudiantes llevan a cabo la realización de un proyecto en un tiempo determinado abordando una tarea mediante la planificación, diseño y realización de una serie de actividades. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.

Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	10.0	60.0
Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0
Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.	20.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	10.0	30.0

NIVEL 2: FACTORES HUMANOS EN LA SEGURIDAD, PRIVACIDAD Y DERECHOS EN INTERNET

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Optativa
ECTS NIVEL 2	3

DESPLIEGUE TEMPORAL: Cuatrimestral

ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
	3	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**

ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

LISTADO DE ESPECIALIDADES

No existen datos

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Identificar de forma holística los distintos problemas relacionados con un área concreta de la ciberseguridad.
- Aplicar métodos, protocolos, técnicas criptográficas o herramientas software para resolver problemas en entornos nuevos o poco conocidos relacionados con la ciberseguridad.
- Identificar los distintos aspectos multidisciplinares (legales, sociales, éticos) a tener en cuenta a la hora de abordar un problema relacionado con un escenario de ciberseguridad.
- Aplicar métodos, técnicas criptográficas, herramientas software o metodologías relacionadas con la ciberseguridad que permitan tener en cuenta aspectos multi-disciplinares.
- Planifica tareas de trabajo autónomo y procesos de autoaprendizaje ejecutándolos en los tiempos previstos.
- Identificar los principales aspectos a comunicar a la hora de presentar los resultados de un estudio o análisis relacionado con la ciberseguridad y al público al que va dirigido.
- Exponer sus conocimientos de una forma clara, concisa, sin ambigüedades y adaptándose al tiempo establecido para la presentación.
- Elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.
- Describir las primitivas criptográficas, los protocolos seguros y los mecanismos software que permitan la protección de datos.
- Emplear el uso de primitivas criptográficas, protocolos seguros y modelos software para proteger datos en escenario de ciberseguridad.
- Analizar escenarios donde es necesario proporcionar software y mecanismos protección de los datos de la organización respetando la normativa existente.
- Identificar nuevas y emergentes tecnologías, buenas prácticas, aspectos normativos, legislativos y humanos relacionados con la ciberseguridad y los mecanismos para detectar estos cambios.

5.5.1.3 CONTENIDOS

- Aspectos humanos de la ciberseguridad.
- Privacidad y derechos en Internet.
- Técnicas y tecnologías de privacidad.
  - Primitivas y protocolos.
  - Tecnologías.
- Tendencias en factores Humanos en la Seguridad, Privacidad y Derechos en Internet.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG4 - Que los estudiantes sean capaces de elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.

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

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

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

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE4 - Aplicar técnicas de seguridad de datos y software.

CE5 - Identificar y conocer las nuevas tendencias, buenas prácticas, normas, regulación y aspectos humanos relacionados con la ciberseguridad.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	4.5	0
Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica, resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).	4.5	0
Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	4.5	0
Sesiones asíncronas de laboratorio: Se proporciona contenido didáctico práctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	4.5	0
Casos prácticos: Las asignaturas pueden incluir casos prácticos con el objetivo pedagógico final de que el estudiante detecte situaciones relevantes, analice la información complementaria, tome decisiones en relación con el escenario que	2	0

se plantea y proponga soluciones o indique cómo mejorar la situación de partida.		
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	1	0
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	1	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	51	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	2	0

5.5.1.7 METODOLOGÍAS DOCENTES

Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.

Aprendizaje Orientado a Proyectos (AOP): Los estudiantes llevan a cabo la realización de un proyecto en un tiempo determinado abordando una tarea mediante la planificación, diseño y realización de una serie de actividades. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.

Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	10.0	60.0
Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0
Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.	20.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	10.0	30.0

NIVEL 2: SEGURIDAD HARDWARE

5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
ECTS NIVEL 2	3	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	3	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NO CONSTAN ELEMENTOS DE NIVEL 3		

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Identificar los principales problemas actuales en el ámbito de la ciberseguridad en escenarios concretos.
- Analizar de forma detallada escenarios, soluciones o sistemas de ciberseguridad para detectar posibles aspectos de mejora.
- Diseñar escenarios, soluciones, o sistemas de ciberseguridad incluyendo aspectos originales o innovadores.
- Identificar de forma holística los distintos problemas relacionados con un área concreta de la ciberseguridad.
- Aplicar métodos, protocolos, técnicas criptográficas o herramientas software para resolver problemas en entornos nuevos o poco conocidos relacionados con la ciberseguridad.
- Evaluar los métodos, protocolos seguros, técnicas criptográficas o herramientas software a utilizar para acometer la resolución de un problema en un entorno nuevo o poco conocido en el ámbito de la ciberseguridad.
- Utilizar los conocimientos para investigar nuevas tecnologías y metodologías aplicadas al ámbito de la ciberseguridad y contribuir así a su desarrollo.
- Recopilar y analizar datos de investigación para afrontar nuevos problemas en el ámbito de la ciberseguridad.
- Identificar los principales aspectos a comunicar a la hora de presentar los resultados de un estudio o análisis relacionado con la ciberseguridad y al público al que va dirigido.
- Diseñar una presentación que incluye las principales ideas a comunicar y los materiales audiovisuales que permitirán reforzar los mensajes a transmitir con respecto a un escenario de ciberseguridad.
- Exponer sus conocimientos de una forma clara, concisa, sin ambigüedades y adaptándose al tiempo establecido para la presentación.
- Analizar métodos y técnicas de ciberataques y ciberdefensa.
- Enumerar e identificar los distintos tipos de vulnerabilidades, amenazas y riesgos dentro de la organización, así como posibles soluciones a aplicar.
- Realizar procesos de análisis de vulnerabilidades y de riesgos.
- Identificar las características y funciones de los elementos que forman parte de las arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.
- Discutir sobre la funcionalidad de los elementos incorporados en las arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.

5.5.1.3 CONTENIDOS

- Introducción a las principales fuentes de vulnerabilidad en dispositivos hardware a través de la capa física.
- Evaluación de la seguridad hardware. Principales estándares y su certificación.
- Plataformas hardware seguras: Módulos HSM, TPM, elementos seguros, smartcards, etc.
- Revisión de técnicas básicas relativas a la seguridad hardware:
  - Métodos invasivos: Clonado y manipulación del hardware a nivel de chip.
  - Métodos no invasivos: Acoplamiento electromagnético
- Técnicas para implementaciones seguras.
  - Secure boot y memorias OTP Prog
  - Sistemas anti tamper.
  - Elementos seguros.
- Fuentes de entropía mediante dispositivos hardware: Funciones Físicamente Unclonables (PUF), generadores de números aleatorios.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Que los estudiantes sean capaces de analizar métodos y técnicas de ciberataques y ciberdefensa.
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
5.5.1.5.2 TRANSVERSALES
No existen datos
5.5.1.5.3 ESPECÍFICAS
CE1 - Que los estudiantes sean capaces de gestionar los procesos asociados a vulnerabilidades, amenazas y riesgos dentro de una organización.
CE3 - Ser capaz de diseñar, monitorizar y evaluar arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.
5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	7	0
Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica, resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).	7	0
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	3	0
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	5	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la	51	0

asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.		
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	2	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección Magistral: Exposición oral de un tema estructurado para facilitar los contenidos sobre la materia objeto de estudio de forma organizada. Se realizan a través de sesiones síncronas de teoría online o sesiones síncronas de laboratorio online.

Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.

Aprendizaje Basado en Problemas (ABP): A partir de un problema diseñado por el profesor, el estudiante ha de resolverlo para desarrollar determinadas competencias previamente definidas. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	10.0	60.0
Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0
Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.	20.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	10.0	30.0

NIVEL 2: SEGURIDAD EN SISTEMAS DISTRIBUIDOS

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Optativa
ECTS NIVEL 2	3

DESPLIEGUE TEMPORAL: Cuatrimestral

ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
	3	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**

LENGUAS EN LAS QUE SE IMPARTE

CASTELLANO	CATALÁN	EUSKERA
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No

ITALIANO	OTRAS
No	No

LISTADO DE ESPECIALIDADES

No existen datos

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Identificar los principales problemas actuales en el ámbito de la ciberseguridad en escenarios concretos.
- Analizar de forma detallada escenarios, soluciones o sistemas de ciberseguridad para detectar posibles aspectos de mejora.
- Identificar de forma holística los distintos problemas relacionados con un área concreta de la ciberseguridad.
- Identificar los distintos aspectos multidisciplinares (legales, sociales, éticos) a tener en cuenta a la hora de abordar un problema relacionado con un escenario de ciberseguridad.
- Planifica tareas de trabajo autónomo y procesos de autoaprendizaje ejecutándolos en los tiempos previstos.
- Identificar los principales aspectos a comunicar a la hora de presentar los resultados de un estudio o análisis relacionado con la ciberseguridad y al público al que va dirigido.
- Diseñar una presentación que incluye las principales ideas a comunicar y los materiales audiovisuales que permitirán reforzar los mensajes a transmitir con respecto a un escenario de ciberseguridad.
- Diseñar soluciones a problemas de ciberseguridad utilizando pensamiento creativo.
- Colaborar a la hora de resolver un problema del ámbito de la ciberseguridad, trabajo en equipo y liderazgo.
- Diseñar, desplegar y mantener sistemas de ciberseguridad.
- Identificar modelos de gestión de la ciberseguridad y procesos asociados para llevar a cabo el seguimiento y la gestión de la ciberseguridad dentro de una organización.
- Identificar las características y funciones de los elementos que forman parte de las arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.
- Discutir sobre la funcionalidad de los elementos incorporados en las arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.
- Describir las primitivas criptográficas, los protocolos seguros y los mecanismos software que permitan la protección de datos.
- Emplear el uso de primitivas criptográficas, protocolos seguros y modelos software para proteger datos en escenario de ciberseguridad.

5.5.1.3 CONTENIDOS

- **Clases de Sistemas Distribuidos y vulnerabilidades**
  - P2P: modelos, arquitecturas, diseño y despliegue.
  - Tipos de arquitecturas P2P. Diseños no estructurados, estructurados, híbridos y jerárquicos.
- **Ataques a sistemas P2P**
  - Evaluación y monitorización en escenarios P2P.
- **Coordinación de recursos:**
  - Modelo cliente servidor, modelos multi-nivel y multi-tenant, agregación de recursos elástica bajo demanda y geo-dispersa.
  - Microservicios.
  - Implicaciones de los ataques en la coordinación de recursos.
- **Coordinación de Servicios**
  - Servicio Web, distribución de claves, Almacenamiento Atributo-Valor (KVS), Bases de datos, Tecnologías de libro mayor distribuido(DLT)/Criptomonedas.
  - Habilitadores de seguridad basados en posicionamiento.
  - Implicaciones de ataques a la coordinación de servicios.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG2 - Que los estudiantes sean capaces de diseñar, desplegar y mantener sistemas de ciberseguridad.

CG5 - Que los estudiantes conozcan los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, considerando la definición de estrategias, políticas y normas para la seguridad corporativa.

CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

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

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

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

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE3 - Ser capaz de diseñar, monitorizar y evaluar arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.		
CE4 - Aplicar técnicas de seguridad de datos y software.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	4.5	0
Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica, resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).	4.5	0
Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	4.5	0
Sesiones asíncronas de laboratorio: Se proporciona contenido didáctico práctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	4.5	0
Casos prácticos: Las asignaturas pueden incluir casos prácticos con el objetivo pedagógico final de que el estudiante detecte situaciones relevantes, analice la información complementaria, tome	1	0

decisiones en relación con el escenario que se plantea y proponga soluciones o indique cómo mejorar la situación de partida.		
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	2	0
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	1	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	51	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	2	0

5.5.1.7 METODOLOGÍAS DOCENTES

Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.

Aprendizaje Basado en Problemas (ABP): A partir de un problema diseñado por el profesor, el estudiante ha de resolverlo para desarrollar determinadas competencias previamente definidas. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.

Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	10.0	60.0
Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0
Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.	20.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	10.0	30.0

NIVEL 2: ASPECTOS AVANZADOS DE LA GESTIÓN DE LA CIBERSEGURIDAD

5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
ECTS NIVEL 2	3	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	3	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NO CONSTAN ELEMENTOS DE NIVEL 3		

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Recopilar y analizar datos de investigación para afrontar nuevos problemas en el ámbito de la ciberseguridad.
- Identificar los distintos aspectos multidisciplinares (legales, sociales, éticos) a tener en cuenta a la hora de abordar un problema relacionado con un escenario de ciberseguridad.
- Formular juicios de valor a partir de la información recopilada que, siendo incompleta o limitada, incluya razonamiento crítico sobre las responsabilidades sociales y éticas de la aplicación de métodos, técnicas criptográficas, herramientas software o metodologías para abordar problemas relacionados con la ciberseguridad.
- Diseñar, desplegar y mantener sistemas de ciberseguridad.
- Identificar la normativa y legislación aplicable en el ámbito de la ciberseguridad.
- Aplicar los conceptos asociados a gobernanza de la organización, la gestión de proyectos, diseño e implantación de productos, servicios e instalaciones en escenarios de ciberseguridad.
- Analizar escenarios en el ámbito de la ciberseguridad desde el punto de vista de gobernanza de la seguridad de la organización, la gestión de la ciberseguridad y de la seguridad de productos, servicios e instalaciones.
- Explicar los distintos aspectos relacionados con la gobernanza de la seguridad de la organización, la gestión de proyectos de seguridad, el diseño y la implantación de productos, servicios e instalaciones en escenarios de ciberseguridad.
- Evaluar críticamente los procesos de gobernanza de la seguridad, gestión de la seguridad, diseño de productos, procesos, servicios e infraestructuras inteligentes en ámbitos de ciberseguridad teniendo en cuenta requisitos, soluciones existentes, normas, estándares y buenas prácticas.
- Evaluar y definir las distintas medidas a aplicar (planes de contingencia, etc.) en función de vulnerabilidades, amenazas y riesgos considerando tanto aspectos técnicos como de negocio (económicos y políticos).
- Analizar informes forenses, y definir planes de acción y su aplicación.
- Definir el alcance e impacto ocasionado por un determinado ciberincidente.

5.5.1.3 CONTENIDOS

- **Catalogación de elementos y activos TIC y de ciberseguridad**
  - Tipos de activos.
  - Dimensiones de valoración.
  - Criterios de valoración.
  - Amenazas y Salvaguardas.
- **Operativas de Ciberseguridad**
  - Identificación.
  - Protección.
  - Detección.
  - Respuesta.
  - Recuperación.
- **Diseño y Planificación de Sistemas de CIberseguridad**
  - Planificación de la ciberseguridad.
  - Continuidad de negocio, recuperación de desastres y gestión de incidentes.
- **Diseño de arquitecturas y servicios seguridad de sistemas: ejemplos para infraestructura críticas y redes de comunicación**
  - Definición de un modelo de protección de la información en un SGSI (Sistema de gestión de Seguridad de la Información)
- **Aspectos legales y normativas económicos , innovación y medioambientales ligado al intercambio de datos y su impacto en el diseño de los sistemas y servicios de seguridad**
- **Buenas prácticas en el diseño y despliegue**
  - Caza de amenazas cibernéticas.
  - CTI con preservación de la privacidad.

- Ciberejercicios y plataformas de simulación.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG2 - Que los estudiantes sean capaces de diseñar, desplegar y mantener sistemas de ciberseguridad.

CG3 - Que los estudiantes sean capaces de identificar la normativa y legislación aplicable en el ámbito de la ciberseguridad.

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

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

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE2 - Que los estudiantes sean capaces de proyectar, diseñar e implantar productos, procesos, servicios e infraestructuras inteligentes en ámbitos de la ciberseguridad.

CE3 - Ser capaz de diseñar, monitorizar y evaluar arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	4.5	0
Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica, resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).	4.5	0
Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	4.5	0

Sesiones asíncronas de laboratorio: Se proporciona contenido didáctico práctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	4.5	0
Casos prácticos: Las asignaturas pueden incluir casos prácticos con el objetivo pedagógico final de que el estudiante detecte situaciones relevantes, analice la información complementaria, tome decisiones en relación con el escenario que se plantea y proponga soluciones o indique cómo mejorar la situación de partida.	1	0
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	2	0
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	1	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	51	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	2	0

5.5.1.7 METODOLOGÍAS DOCENTES

Estudio de Casos: Análisis de un problema o suceso real para conocerlo, interpretarlo, resolverlo, generar hipótesis, contrastar datos, reflexionar, completar conocimientos, diagnosticarlo y buscar las soluciones.

Aprendizaje Basado en Problemas (ABP): A partir de un problema diseñado por el profesor, el estudiante ha de resolverlo para desarrollar determinadas competencias previamente definidas. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.

Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA

Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	10.0	60.0
Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0
Informe práctico de laboratorio: Evaluación de informes o memorias relacionadas con los contenidos de prácticas de laboratorio de la asignatura.	20.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	10.0	30.0

NIVEL 2: INTRODUCCIÓN A LA INVESTIGACIÓN		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
		6
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NO CONSTAN ELEMENTOS DE NIVEL 3		

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Diseñar escenarios, soluciones, o sistemas de ciberseguridad incluyendo aspectos originales o innovadores.
- Evaluar los métodos, protocolos seguros, técnicas criptográficas o herramientas software a utilizar para acometer la resolución de un problema en un entorno nuevo o poco conocido en el ámbito de la ciberseguridad.
- Utilizar los conocimientos para investigar nuevas tecnologías y metodologías aplicadas al ámbito de la ciberseguridad y contribuir así a su desarrollo.
- Planifica tareas de trabajo autónomo y procesos de autoaprendizaje ejecutándolos en los tiempos previstos.
- Exponer sus conocimientos de una forma clara, concisa, sin ambigüedades y adaptándose al tiempo establecido para la presentación.
- Colaborar a la hora de resolver un problema del ámbito de la ciberseguridad, trabajo en equipo y liderazgo.
- Elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.
- Identificar modelos de gestión de la ciberseguridad y procesos asociados para llevar a cabo el seguimiento y la gestión de la ciberseguridad dentro de una organización.
- Diferenciar los aspectos más relevantes de las nuevas tendencias, buenas prácticas, normas, leyes y aspectos humanos con respecto a los ya existentes.
- Analizar de forma detallada nuevas tendencias, buenas prácticas, normas, regulación y aspectos humanos relacionados con la ciberseguridad.
- Evaluar las implicaciones de la adopción de nuevas tecnologías, buenas prácticas, normas, regulación y aspectos humanos de la ciberseguridad en escenarios concretos de negocio.

5.5.1.3 CONTENIDOS

Se pretende (a) repasar y profundizar los fundamentos de la gestión de proyectos tradicional y ágil, a través de un conjunto de métodos, técnicas y herramientas aplicables al diseño, planificación y seguimiento de proyectos de I+D+i, (b) identificar las principales áreas de investigación en la ciberseguridad y su impacto en los sistemas y organizaciones, así como (c) transmitir al alumnado una visión general de la carrera investigadora.

- Introducción a la gestión de proyectos.
- Elaboración y planificación de proyectos de investigación.
- Difusión de la investigación: publicaciones y presentaciones.
- La Tesis Doctoral y la carrera investigadora.
- Aspectos éticos y de ciencia abierta.
- Métodos de investigación en ciberseguridad.
- Técnicas y herramientas para la investigación en ciberseguridad.
- Ciberseguridad y su impacto en las organizaciones y los retos de investigación y tecnológicos actuales asociados y las políticas de innovación.
- Definición de estrategias, políticas y normas para la seguridad corporativa.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG4 - Que los estudiantes sean capaces de elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.

CG5 - Que los estudiantes conozcan los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, considerando la definición de estrategias, políticas y normas para la seguridad corporativa.

CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

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

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

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

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE5 - Identificar y conocer las nuevas tendencias, buenas prácticas, normas, regulación y aspectos humanos relacionados con la ciberseguridad.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	10	0
Sesiones síncronas de laboratorio online: Consisten en sesiones prácticas presenciales impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde, dependiendo de la metodología, el profesorado expone aspectos relacionados con la práctica,	7	0

resuelve dudas del alumnado, y realiza seguimiento de las prácticas realizadas por el alumnado (de forma individualizada o en grupo).		
Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	10	0
Sesiones asíncronas de laboratorio: Se proporciona contenido didáctico práctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	7	0
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	4	0
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	6	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	102	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	4	0
5.5.1.7 METODOLOGÍAS DOCENTES		
Lección Magistral: Exposición oral de un tema estructurado para facilitar los contenidos sobre la materia objeto de estudio de forma organizada. Se realizan a través de sesiones síncronas de teoría online o sesiones síncronas de laboratorio online.		

Estudio de Casos: Análisis de un problema o suceso real para conocerlo, interpretarlo, resolverlo, generar hipótesis, contrastar datos, reflexionar, completar conocimientos, diagnosticarlo y buscar las soluciones.
Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.
Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	20.0	60.0
Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	20.0	40.0

NIVEL 2: SEMINARIO SOBRE INNOVACIÓN Y EMPRENDIMIENTO II

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Optativa
ECTS NIVEL 2	6

DESPLIEGUE TEMPORAL: Cuatrimestral

ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
		6
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**

LENGUAS EN LAS QUE SE IMPARTE

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

LISTADO DE ESPECIALIDADES

No existen datos

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Analizar de forma detallada escenarios, soluciones o sistemas de ciberseguridad para detectar posibles aspectos de mejora.
- Diseñar escenarios, soluciones, o sistemas de ciberseguridad incluyendo aspectos originales o innovadores.
- Formular juicios de valor a partir de la información recopilada que, siendo incompleta o limitada, incluya razonamiento crítico sobre las responsabilidades sociales y éticas de la aplicación de métodos, técnicas criptográficas, herramientas software o metodologías para abordar problemas relacionados con la ciberseguridad.

- Exponer sus conocimientos de una forma clara, concisa, sin ambigüedades y adaptándose al tiempo establecido para la presentación.
- Identificar, organizar y planificar las tecnologías a estudiar y/o recursos bibliográficos a analizar para abordar un determinado problema dentro del ámbito de la ciberseguridad.
- Identificar modelos de gestión de la ciberseguridad y procesos asociados para llevar a cabo el seguimiento y la gestión de la ciberseguridad dentro de una organización.
- Adaptar escenarios de ciberseguridad conforme a las nuevas tendencias, buenas prácticas, normas, regulación y aspectos humanos.
- Analizar de forma detallada nuevas tendencias, buenas prácticas, normas, regulación y aspectos humanos relacionados con la ciberseguridad.

5.5.1.3 CONTENIDOS

El objetivo es realizar una serie de seminarios, presentaciones y exposiciones relacionados con las posibilidades de innovación y emprendimiento en el ámbito de la ciberseguridad. Se invitarán expertos de empresas, así como docentes en el ámbito de los estudios de económicas y empresariales que permitan a los alumnos analizar diferentes aspectos tanto legales o económicos desde diferentes perspectivas. Además, se contará con la oficina de emprendimiento de la Universidad de Murcia para impartir algunas sesiones.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG5 - Que los estudiantes conozcan los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, considerando la definición de estrategias, políticas y normas para la seguridad corporativa.

CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

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

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

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE5 - Identificar y conocer las nuevas tendencias, buenas prácticas, normas, regulación y aspectos humanos relacionados con la ciberseguridad.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones síncronas de teoría online: Consisten en sesiones presenciales teóricas impartidas por profesores a través del Aula Virtual (clases en tiempo real) donde el profesorado, dependiendo de la metodología docente, explica contenidos, realiza actividades de debate en grupo, resuelve y debate las dudas que los estudiantes puedan plantear gracias a la interacción en tiempo real, etc.	16	0
Sesiones asíncronas de teoría: Se proporciona contenido teórico didáctico impartido por especialistas en su área de actividad. Se facilitan a los estudiantes como material y pueden desarrollarse en entornos distintos, presentando diversos formatos: lecciones magistrales, entrevistas, análisis de ejemplos y/o casos reales, animaciones multimedia, etc. Están permanentemente accesibles a los estudiantes en el repositorio documental de la titulación y se pueden ir suministrando conforme avance la asignatura.	8	0

Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	8	0
Seminarios: Se imparten de modo virtual para la resolución de aquellas cuestiones más complejas que surgen en la elaboración de los trabajos, con elementos comunes que sirven de orientación para la mayor parte de los estudiantes. También pueden consistir en seminarios específicos formativos como análisis de datos o gestión de bibliografía por poner algunos ejemplos.	12	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	102	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	4	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección Magistral: Exposición oral de un tema estructurado para facilitar los contenidos sobre la materia objeto de estudio de forma organizada. Se realizan a través de sesiones síncronas de teoría online o sesiones síncronas de laboratorio online.

Estudio de Casos: Análisis de un problema o suceso real para conocerlo, interpretarlo, resolverlo, generar hipótesis, contrastar datos, reflexionar, completar conocimientos, diagnosticarlo y buscar las soluciones.

Resolución de Ejercicios y Problemas: Ejercitar, ensayar y poner en práctica los conocimientos previos. Suele utilizarse como complemento de la lección magistral. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, herramientas interactivas, casos prácticos, etc.

Aprendizaje Invertido: El profesor dejará disponible para los estudiantes recursos didácticos audiovisuales. Estos recursos deberán ser revisados por los estudiantes y se dedicarán una serie de sesiones síncronas de teoría o laboratorio online para resolver dudas o realizar ejercicios sobre el material didáctico proporcionado.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación continua: La calificación de cada una de las asignaturas se obtiene teniendo en cuenta la realización de pruebas de distinto tipo a lo largo del cuatrimestre (ver apartado 5.1).	20.0	60.0
Informe teórico: Evaluación de informes o memorias de teoría relacionadas con los contenidos teóricos de la asignatura.	0.0	60.0
Entrevista personal o en grupo: Evaluación de entrevista individual o en grupo sobre trabajos teóricos o de prácticas de laboratorio.	20.0	40.0

NIVEL 2: TRABAJO FIN DE MÁSTER

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Trabajo Fin de Grado / Máster
ECTS NIVEL 2	24

DESPLIEGUE TEMPORAL: Cuatrimestral

ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
		24
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**

LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

LISTADO DE ESPECIALIDADES

No existen datos

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Diseñar escenarios, soluciones, o sistemas de ciberseguridad incluyendo aspectos originales o innovadores.
- Planifica tareas de trabajo autónomo y procesos de autoaprendizaje ejecutándose en los tiempos previstos.
- Identificar los principales aspectos a comunicar a la hora de presentar los resultados de un estudio o análisis relacionado con la ciberseguridad y al público al que va dirigido.
- Diseñar una presentación que incluye las principales ideas a comunicar y los materiales audiovisuales que permitirán reforzar los mensajes a transmitir con respecto a un escenario de ciberseguridad.
- Exponer sus conocimientos de una forma clara, concisa, sin ambigüedades y adaptándose al tiempo establecido para la presentación.
- Identificar, organizar y planificar las tecnologías a estudiar y/o recursos bibliográficos a analizar para abordar un determinado problema dentro del ámbito de la ciberseguridad.
- Diseñar soluciones a problemas de ciberseguridad utilizando pensamiento creativo.
- Colaborar a la hora de resolver un problema del ámbito de la ciberseguridad, trabajo en equipo y liderazgo.
- Elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.
- Identificar modelos de gestión de la ciberseguridad y procesos asociados para llevar a cabo el seguimiento y la gestión de la ciberseguridad dentro de una organización.
- Diseñar arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones que estén de acuerdo a las políticas de la organización, consideren aspectos técnicos, de negocio (económicos, legales, medioambientales, etc) y de innovación.
- Argumentar y asesorar sobre las razones de la introducción de nuevas tecnologías, buenas prácticas, normas, regulación y aspectos en un escenario de ciberseguridad.
- Evaluar las implicaciones de la adopción de nuevas tecnologías, buenas prácticas, normas, regulación y aspectos humanos de la ciberseguridad en escenarios concretos de negocio.

5.5.1.3 CONTENIDOS

- Se realiza bajo el asesoramiento y orientación del Profesor, siguiendo las directrices marcadas por el Reglamento de Trabajos de y de Fin de Máster (TFM).
- Elaboración, diseño y defensa pública de un caso teórico o práctico sobre seguridad informática, donde el estudiante deberá demostrar sus habilidades y conocimientos en relación a uno o varios de los siguientes aspectos:
  - Análisis exhaustivo de sistemas informáticos complejos, en los que la seguridad resulte un elemento crítico para su correcto funcionamiento.
  - Identificación de las potenciales amenazas, debilidades y elementos inseguros, tanto externos como internos. Estos pueden pertenecer tanto al plano técnico, como administrativo, legal, o una combinación de los mismos.
  - Realización de un análisis detallado de las amenazas, debilidades y elementos inseguros; para la posterior realización de un informe con posibles soluciones, así como con recomendaciones para mejorar el sistema desde el punto de vista de la seguridad informática.
  - Presentación del plan de implantación para las soluciones anteriormente descritas.
- Cada TFM debe ser original y puede enfocarse de forma distinta y sobre distintos aspectos de la ciberseguridad, por lo que cada uno ahondará en una temática distinta, contenida o ampliando lo estudiado en las asignaturas impartidas.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG4 - Que los estudiantes sean capaces de elaborar documentación clara, concisa y razonada sobre aspectos relacionados con el ámbito de la ciberseguridad.

CG5 - Que los estudiantes conozcan los conceptos y tecnologías utilizadas en la implantación de la Ciberseguridad en una organización, considerando la definición de estrategias, políticas y normas para la seguridad corporativa.

CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
5.5.1.5.2 TRANSVERSALES
No existen datos
5.5.1.5.3 ESPECÍFICAS
CE3 - Ser capaz de diseñar, monitorizar y evaluar arquitecturas y servicios de seguridad de sistemas, infraestructuras críticas y redes de comunicaciones.
CE5 - Identificar y conocer las nuevas tendencias, buenas prácticas, normas, regulación y aspectos humanos relacionados con la ciberseguridad.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Tutorías: Tutorías individuales o grupales donde el profesorado resuelve dudas particulares, orienta, apoya y ayuda a los estudiantes en el desarrollo de su trabajo y en la adquisición de competencias.	18	0
Trabajo autónomo: Dedicación del estudiante a revisar y estudiar los contenidos teórico/prácticos de la asignatura, búsqueda de información bibliográfica, realización de lecturas, etc.	580	0
Pruebas de evaluación: Incluye cualquier tipo de evaluación que sea necesaria en la asignatura, como pruebas parciales o finales, ya sean de teoría o prácticas.	2	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección Magistral: Exposición oral de un tema estructurado para facilitar los contenidos sobre la materia objeto de estudio de forma organizada. Se realizan a través de sesiones síncronas de teoría online o sesiones síncronas de laboratorio online.
Estudio de Casos: Análisis de un problema o suceso real para conocerlo, interpretarlo, resolverlo, generar hipótesis, contrastar datos, reflexionar, completar conocimientos, diagnosticarlo y buscar las soluciones.
Aprendizaje Orientado a Proyectos (AOP): Los estudiantes llevan a cabo la realización de un proyecto en un tiempo determinado abordando una tarea mediante la planificación, diseño y realización de una serie de actividades. Se pueden realizar a través de sesiones síncronas de teoría o laboratorio online, la utilización de recursos didácticos audiovisuales, casos prácticos, tutorías grupales, etc.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Informe TFM: Este instrumento incluye los resultados de actividades relacionadas con el desarrollo del Trabajo Fin de Máster, junto con su memoria descriptiva.	40.0	60.0
Exposición y Defensa TFM: Este instrumento se refiere a la presentación o exposición oral del Trabajo Fin de Máster realizada de forma individual ante uno o varios profesores a modo de tribunal, y posibles turnos en los que los candidatos respondan a preguntas relacionadas con el trabajo.	40.0	60.0

6. PERSONAL ACADÉMICO

6.1 PROFESORADO Y OTROS RECURSOS HUMANOS				
Universidad	**Categoría**	**Total %**	**Doctores %**	**Horas %**
Universidad de Murcia	Catedrático de Universidad	22.7	100	20,2
Universidad de Murcia	Profesor Titular de Universidad	45.5	100	41,7
Universidad de Murcia	Ayudante Doctor	4.6	100	8,4
Universidad de Murcia	Profesor Contratado Doctor	4.6	100	4,8
Universidad de Murcia	Otro personal docente con contrato laboral	4.6	100	2,4
Universidad de Murcia	Profesor Asociado (incluye profesor asociado de C.C.: de Salud)	13.6	100	15,5
Universidad de Murcia	Profesor colaborador Licenciado	4.6	100	7,1

PERSONAL ACADÉMICO

Ver Apartado 6: Anexo 1.

6.2 OTROS RECURSOS HUMANOS

Ver Apartado 6: Anexo 2.

7. RECURSOS MATERIALES Y SERVICIOS

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

8. RESULTADOS PREVISTOS

8.1 ESTIMACIÓN DE VALORES CUANTITATIVOS		
TASA DE GRADUACIÓN %	**TASA DE ABANDONO %**	**TASA DE EFICIENCIA %**
85	10	90
CODIGO	**TASA**	**VALOR %**
No existen datos		

Justificación de los Indicadores Propuestos:

Ver Apartado 8: Anexo 1.

8.2 PROCEDIMIENTO GENERAL PARA VALORAR EL PROCESO Y LOS RESULTADOS

La Universidad de Murcia no tiene establecido un procedimiento específico para valorar el progreso de los resultados de aprendizaje de los estudiantes. Se entiende que dicha valoración queda garantizada como consecuencia de la suma de las valoraciones de las diferentes materias que configuran el Plan de Estudios. Los resultados son analizados y se transforman en las correspondientes acciones de mejora siguiendo los diferentes procesos que configuran el SAIC de los centros de la Universidad de Murcia.

Nuestro Sistema de Aseguramiento Interno de Calidad contiene, entre otros, los procedimientos documentados PC01-*Planificación y desarrollo de las enseñanzas. Evaluación del aprendizaje* y PC05-*Resultados académicos*.

El procedimiento PC01 establece el modo por el cual los centros de la Universidad de Murcia garantizan que las enseñanzas oficiales de grado y máster que ofertan se imparten de acuerdo con lo indicado en sus memorias de verificación aprobadas, para lo que planifican, implantan y desarrollan sus programas formativos de modo que los estudiantes puedan alcanzar los objetivos establecidos en los diferentes planes de estudio. Dentro de esta planificación y seguimiento del desarrollo de su impartición, dado su carácter singular, se dedica interés especial a garantizar que la evaluación del aprendizaje de sus estudiantes se lleva a cabo tal y como se indica en las correspondientes guías docentes de las asignaturas aprobadas y difundidas.

El procedimiento PC05 recoge cómo los centros de la Universidad de Murcia garantizan que se miden y analizan los resultados del aprendizaje, y cómo, a partir de los mismos, se toman las decisiones para la mejora de la calidad de las enseñanzas impartidas en el centro.

Además, de cada procedimiento del SAIC deriva un análisis que obliga a las titulaciones a comprobar que se han cumplido todos los requerimientos marcados en los diferentes procedimientos del SAIC, incluyendo la revisión de dicho sistema.

Por otro lado, la existencia de un Trabajo Fin de Máster, con una duración prevista de 30 ECTS, permite valorar, como el *RD 822/2021 indica*, que se han alcanzado los resultados de aprendizaje asociados al título.

PC01:

PLANIFICACIÓN Y DESARROLLO DE LAS ENSEÑANZAS. EVALUACIÓN DEL APRENDIZAJE

ÍNDICE

1. OBJETO

Este documento tiene por objeto establecer el modo por el cual los Centros de la Universidad de Murcia garantizan que las enseñanzas oficiales de grado y máster que ofertan se imparten de acuerdo con lo indicado en sus memorias de verificación aprobadas. Para ello, planifican, implantan y desarrollan sus programas formativos de modo que los estudiantes puedan alcanzar los objetivos establecidos en los diferentes planes de estudio. Igualmente se debe garantizar la coordinación, tanto vertical como horizontal, así como entre las diferentes metodologías de enseñanza. Dentro de esta planificación y seguimiento del desarrollo, se dedica interés especial a garantizar que la evaluación del aprendizaje de sus estudiantes se lleva a cabo tal y como se indica en las correspondientes guías docentes de las asignaturas.

2. PARTICIPANTES Y RESPONSABILIDADES

Coordinador/a de Calidad (CC): Propietario/a del proceso. Comprobar la publicación en la página Web de las guías docentes de cada una de las asignaturas de todas las titulaciones oficiales del Centro (apoyado por los/las Coordinadores/as de titulación, si los/las hubiese).

Coordinador/a de Titulación: Comprobar que se encuentran públicas las guías docentes de cada una de las asignaturas de la titulación que coordina. Asegurar que se aplican los mecanismos de coordinación docente que permiten tanto una adecuada asignación de carga de trabajo del estudiante, como una adecuada planificación temporal. Asegurar la adquisición de los resultados de aprendizaje.

Comisión de Aseguramiento de Calidad (CAC): Ser informada de la planificación y analizar el desarrollo de las enseñanzas y las incidencias que puedan producirse, teniendo especial relevancia aquellas relacionadas con la evaluación del aprendizaje.

Comisiones de Titulación/Coordinación (en su caso): Realizar los análisis y propuestas a nivel de titulación y reportar a la CAC.

Consejo de Gobierno: Elaborar anualmente la planificación de las enseñanzas y el calendario académico del curso siguiente.

Junta de Centro (JC): Aprobar la programación docente anual del Centro. Aprobar horario y calendario académicos del Centro, incluyendo evaluaciones. Velar por el correcto desarrollo de la impartición de las enseñanzas oficiales ofertadas.

Consejos de Departamento: Aprobar el Plan de Ordenación Docente de su Departamento. Aprobar las guías docentes de las asignaturas bajo su responsabilidad y enviarlas al Equipo de Dirección del Centro. Velar por la calidad de la docencia asignada al Departamento.

Equipo de Dirección (ED): Realizar la difusión de toda la información relativa a la planificación docente.

Profesorado: Actualizar las guías docentes de las asignaturas que imparten y aplicarlas en todo su contenido.

3. DESARROLLO

3.1 Planificación y desarrollo de las enseñanzas

El Consejo de Gobierno elabora anualmente la planificación de las enseñanzas y el calendario académico del curso siguiente, quedando así establecida la oferta formativa de la UM, que ha de ser difundida convenientemente. A partir de dicha planificación cada centro ha de proceder a planificar e implantar las enseñanzas que tiene a su cargo.

Para ello, los Consejos de Departamento han de aprobar su Plan de Ordenación Docente, así como coordinar y aprobar las guías docentes de las asignaturas que tienen adscritas, en las que se especificaran los objetivos docentes, los resultados de aprendizaje esperados, los contenidos, la metodología y el sistema y las características de la evaluación. También han de velar por su cumplimiento en todos los grupos docentes en que se impartan.

Se prestará especial atención a que el contenido de las guías docentes se corresponda con lo indicado en la Memoria de la titulación verificada. Por otro lado, la Junta de Centro ha de aprobar el horario de clases y el calendario de exámenes, conocer e informar el Plan de Ordenación Docente y demás propuestas de los Consejos de Departamento que impartan docencia en el Centro. Igual que los Departamentos, la Junta de Centro ha de velar

por la calidad de la docencia de las titulaciones bajo su responsabilidad así como de su gestión. Antes del inicio del periodo de matrícula de cada curso académico, el/la coordinador/a de calidad, o el/la coordinador/a de titulación, ha de comprobar la disponibilidad pública de las guías docentes de cada asignatura.

3.2. Coordinación

Los mecanismos de coordinación docente deben ir encaminados a conseguir unas adecuadas: asignación de carga de trabajo del estudiante y planificación temporal. Se debe realizar una coordinación tanto vertical como horizontal y una coordinación entre las diferentes metodologías de enseñanza. En el caso de que el título cuente con prácticas externas o clínicas, debe haber necesariamente una coordinación entre la universidad y los tutores de prácticas (PC07 Prácticas externas).

Se prestará especial atención a la coordinación en el caso de que el título se imparta en varios centros de la UM, sea un título interuniversitario, y/o en el caso de los planes de estudios simultáneos.

En las actas deben quedar reflejados los acuerdos y conclusiones de la coordinación entre materias, asignaturas o equivalentes, en todos los aspectos: globales y de metodología.

4. MEDIDAS, ANÁLISIS Y MEJORA CONTINUA

El/la Coordinador/a de Calidad del Centro ha de aportar a la Comisión de Aseguramiento de Calidad información sistemática sobre la planificación y el desarrollo de la docencia y las acciones de coordinación de los títulos de grado y máster impartidos por el centro para su análisis y propuesta, en su caso, de las acciones de mejora que se consideren adecuadas.

5. EVIDENCIAS

Identificación de las evidencias	Soporte de archivo	Punto de archivo de la evidencia	Tiempo de conservación
Actas de aprobación de las guías docentes del Centro (Junta de Centro)	Informático	Aplicación informática UNICA	6 años
Actas donde se recojan las conclusiones de la coordinación entre materias, asignaturas o equivalentes, en aspectos globales y/o metodológicos.	Informático	Aplicación informática UNICA	6 años
Informe planificación enseñanzas	Informático	Aplicación informática UNICA	6 año

PC05:

RESULTADOS ACADÉMICOS

ÍNDICE

1. OBJETO

El objeto del presente documento es definir cómo los Centros de la Universidad de Murcia garantizan que se miden y analizan los resultados académicos, se comparan con las estimaciones realizadas en la Memoria verificada por el Consejo de Universidades y cómo se toman decisiones a partir de dicho análisis para la mejora de la calidad de las enseñanzas oficiales.

2. PARTICIPANTES Y RESPONSABILIDADES

Coordinador/a de Calidad (CC): Propietario/a del proceso. Facilitar la información a la CAC referente a los resultados académicos de cada una de las titulaciones oficiales de grado y máster del Centro.

Comisión de Aseguramiento de Calidad (CAC)*:* Analizar la documentación facilitada, elaborar un informe anual sobre los resultados académicos incluyendo un plan de mejoras sobre los mismos. Enviar dicho informe al Claustro para su conocimiento.

Unidad para la Calidad (UC): Proponer los indicadores a utilizar y asegurar que llega la información al Centro.

ATICA: Gestionar la aplicación informática a través de la cual se obtienen los indicadores de resultados académicos.

Gestión Académica: Aportar información a la aplicación informática, a través de las bases de datos que gestionan.

3. DESARROLLO

3.1. Indicadores a analizar

La Unidad para la Calidad, a partir de la experiencia de años anteriores, de la opinión recogida de los diferentes Centros de la UM y del protocolo para el seguimiento y acreditación de las titulaciones oficiales, propone y revisa la propuesta de los indicadores a utilizar para el análisis de los resultados académicos de las titulaciones oficiales impartidas en la Universidad de Murcia.

En su propuesta, la UC aporta la definición y ficha para el cálculo de los indicadores de resultados académicos y vela para que estén disponibles los valores correspondientes a los seis últimos cursos académicos para todas las titulaciones de grado y máster impartidas en el Centro.

3.2. Recogida de datos y revisión

El valor de los diferentes indicadores se obtiene a curso cerrado para garantizar su validez, por medio de una aplicación informática que extrae la información directamente de las bases de datos del Área de Gestión Académica de la Universidad de Murcia.

En el momento de elaborar este documento, los indicadores son obtenidos por la aplicación UNICA, que elabora y archiva el informe de Resultados Académicos para todos los Centros de la UM. Los/las Coordinadores/ras de Calidad remiten este informe a la CAC y/o comisiones de titulación para su análisis.

3.3. Informe de resultados académicos

La CAC, o las comisiones de titulación en su caso, analizan los resultados académicos y los comparan con los valores estimados en la Memoria verificada. En caso de que se considere pertinente, se proponen las acciones de mejora que se incluyen en el Informe de Análisis de Resultados Académicos del Centro. Éste informe se envía a la comisión de Calidad del Claustro por mandato de los Estatutos de la Universidad de Murcia. Estas acciones de mejora han de ser aprobadas en Junta de Centro e incluidas en el Informe de Seguimiento Manual de Calidad).

4. MEDIDAS, ANÁLISIS Y MEJORA CONTINUA

Para el análisis de los resultados académicos, los indicadores propuestos se indican a continuación y las fichas para su cálculo se incluyen en los anexos del proceso:

- Anexo 1.IN01-PC05 Tasa de rendimiento.
- Anexo 2.IN02-PC05 Tasa de éxito.
- Anexo 3.IN03.1-PC05 Tasa de graduación en la duración del plan de estudios, n Anexo 4 IN03.2-PC05 Tasa de graduación (n+1) (RD 1393/2007).
- Anexo 5 IN04.1-PC05 Tasa de abandono (RD).
- Anexo 6 IN04.2-PC05 Tasa de abandono (REACU).
- Anexo 7 IN04.3-PC05 Tasa de abandono en el curso siguiente al de ingreso Anexo 8 IN05-PC05 Tasa de eficiencia.
- Anexo 9 IN06-PC05 Duración media de los estudios.
- Anexo 10 IN08-PC05 Número de estudiantes matriculados.
- A medida que se puedan obtener datos sobre "tiempo parcial" en los indicadores que procedan, se irán incorporando al informe de resultados.

5. EVIDENCIAS

Identificación de la evidencia Soporte de archivo Punto de archivo de la evidencia Tiempo de conservación Informe Resultados Académicos Informático Aplicación informática UNICA 6 años Tasas de éxito y rendimiento por asignaturas Informática Aplicación informática UNICA 6 años Informe del análisis de los Resultados Académicos del Centro (CAC)

Identificación de la evidencia	Soporte de archivo	Punto de archivo de la evidencia	Tiempo de conservación
Informe resultados académicos	Informático	Aplicación informática UNICA	6 años
Tasas de éxito y rendimiento por asignaturas	Informático	Aplicación informática UNICA	6 años
Informe del análisis de los resultados académicos del centro (CAC)	Informático	Aplicación informática UNICA	6 años

9. SISTEMA DE GARANTÍA DE CALIDAD

ENLACE	https://www.um.es/web/informatica/calidad

10. CALENDARIO DE IMPLANTACIÓN

10.1 CRONOGRAMA DE IMPLANTACIÓN	
CURSO DE INICIO	2023
Ver Apartado 10: Anexo 1.	
10.2 PROCEDIMIENTO DE ADAPTACIÓN	

No procedes ya que el Máster Universitario en Ciberseguridad / Master in Cybersecurity por la Universidad de Murcia es de nueva implantación y no extingue ningún título.

10.3 ENSEÑANZAS QUE SE EXTINGUEN	
CÓDIGO	**ESTUDIO - CENTRO**

11. PERSONAS ASOCIADAS A LA SOLICITUD

11.1 RESPONSABLE DEL TÍTULO			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
34786541F	ANTONIO	FLORES	GIL
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
FACULTAD DE INFORMÁTICA, CAMPUS DE ESPINARDO, EDIFICIO 32	30100	Murcia	Murcia
EMAIL	**MÓVIL**	**FAX**	**CARGO**
decano.inf@um.es	868884311	868884151	DECANO DE LA FACULTAD DE INFORMÁTICA

11.2 REPRESENTANTE LEGAL			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
48392224V	SONIA	MADRID	CANOVAS
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
AVENIDA TENIENTE FLOMESTA Nº 5 (RECTORADO UNIVERSIDAD DE MURCIA)	30003	Murcia	Murcia
EMAIL	**MÓVIL**	**FAX**	**CARGO**
vicestudios@um.es	868883513	868883506	VICERRECTORA DE ESTUDIOS
El Rector de la Universidad no es el Representante Legal			
Ver Apartado 11: Anexo 1.			

11.3 SOLICITANTE			
El responsable del título es también el solicitante			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
34786541F	ANTONIO	FLORES	GIL
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
FACULTAD DE INFORMÁTICA, CAMPUS DE ESPINARDO, EDIFICIO 32	30100	Murcia	Murcia
EMAIL	**MÓVIL**	**FAX**	**CARGO**
decano.inf@um.es	868884311	868884151	DECANO DE LA FACULTAD DE INFORMÁTICA

Apartado 2: Anexo 1

Nombre : Criterio 2.1 Justificacion.pdf

HASH SHA1 :08AFBBCD0050CD045B1D1BDD26B8AE76B68F1120

Código CSV :557731977501513917027530

Ver Fichero: Criterio 2.1 Justificacion.pdf

Apartado 4: Anexo 1

Nombre : Criterio 4.1 Sistemas de información previo.pdf

HASH SHA1 :BD542638D3169E45F900225EFB29A7C68A1D6F0F

Código CSV :559216309144461507673053

Ver Fichero: Criterio 4.1 Sistemas de información previo.pdf

Apartado 5: Anexo 1

Nombre : Criterio 5.1 Descripcion del plan de estudios.pdf

HASH SHA1 :B286379807FB3F288240F40AD10A65EB1647193B

Código CSV :565504129203353159246886

Ver Fichero: Criterio 5.1 Descripcion del plan de estudios.pdf

Apartado 6: Anexo 1

Nombre : Criterio 6.1 Profesorado.pdf

HASH SHA1 :5638DADE357CD42C7386CC045C54C8DED30E463E

Código CSV :557732458753206256777283

Ver Fichero: Criterio 6.1 Profesorado.pdf

Apartado 6: Anexo 2

Nombre : Criterio 6.2 Otros Recursos Humanos.pdf

HASH SHA1 :40CD367FD5BEA25C32AE417EC4B2DE4C5B093AAB

Código CSV :557732537824571969074859

Ver Fichero: Criterio 6.2 Otros Recursos Humanos.pdf

Apartado 7: Anexo 1

Nombre : Criterio 7.1 Justificacion de los medios materiales disponibles.pdf

HASH SHA1 :6E3151D1D04E0A526D04BC92D3181C56842197A2

Código CSV :557732559006680339308240

Ver Fichero: Criterio 7.1 Justificacion de los medios materiales disponibles.pdf

Apartado 8: Anexo 1

Nombre : Criterio 8.1 Justificacion de la estimacion de valores cuantitativos.pdf

HASH SHA1 :F195C00703D88BA8713EB5FF29BA3BB6BCD76BE4

Código CSV :557732589510093050048028

Ver Fichero: Criterio 8.1 Justificacion de la estimacion de valores cuantitativos.pdf

Apartado 10: Anexo 1

Nombre : Criterio 10.1 Cronograma de implantación.pdf

HASH SHA1 :C9B487CCDE83CE59D982651B1B04EC05BE36E1D8

Código CSV :557732631141731978971737

Ver Fichero: Criterio 10.1 Cronograma de implantación.pdf

Apartado 11: Anexo 1

Nombre : DelegacionFirma2022.pdf

HASH SHA1 :68080A682D3330C6D55ADF62897F30D6EEA67621

Código CSV :539241499495140003618175

Ver Fichero: DelegacionFirma2022.pdf