MEMORIA DE VERIFICACIÓN DEL TÍTULO UNIVERSITARIO OFICIAL

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

Universidad solicitante: UNIVERSIDAD DE MÁLAGA

Centro responsable: E.T.S. INGENIERÍA INFORMÁTICA

Contenido

1. Descripción, objetivos formativos y justificación del título (ESG 1.2)

1.1.- Descripción general

1.1. Denominación del Título	**MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD**		
1.2. Nivel MECES:	3		
1.3. Rama:	Ingeniería y Arquitectura		
1.4. Ámbito de conocimiento:	Ingeniería Informática y de Sistemas		
1.4.a) Universidad Responsable:	UNIVERSIDAD DE MÁLAGA		
1.4.b) Cód. RUCT y denominación del Centro de impartición responsable:	29012601 Escuela Técnica Superior de Ingeniería Informática		
1.4.c) Centro acreditado institucionalmente	NO		
1.6.a) Título conjunto:	NO		
1.6.b) Convenio (TC nacional)**:**			
1.6.c) Universidades Participantes:			
1.6.d) Código RUCT y Denominación de los Centros de impartición			
1.7 Menciones/Especialidades *(denominación y ECTS):*	DUAL (30 ECTS, incluyendo TFM) GENERAL (30 ECTS, incluyendo TFM)		
1.7.a) Mención dual:	SI		
1.7.b) Convenio Mención dual:	Convenio de Colaboración para Desarrollo Programa de Formación Dual en Máster en Ciberseguridad		
1.8. Número total de créditos:	60		
Información Referente al centro en el que se imparte el Título:			
1.9. Modalidad de enseñanza *(marcar lo que proceda)*	**X**	**Presencial**	Núm. Plazas: 25
		Híbrida (semipresencial)	Núm. Plazas:
		Virtual (No presencial)	Núm. Plazas:
1.9. Número total de plazas:	25		
1.9.a) Número de plazas de nuevo ingreso para primer curso:	25		
1.10. Idiomas de impartición:	Español		

En esta titulación se aplicarán las Normas reguladoras del progreso y la permanencia de los estudiantes en estudios de grado y máster de la Universidad de Málaga, así como el Reglamento 9/2024, de 27 de junio, de la Universidad de Málaga, que regula la condición de estudiante a tiempo parcial.

La siguiente tabla recoge la horquilla de créditos ECTS mínimos y máximos de los que el estudiantado se debe matricular para cada categoría en los diferentes cursos:

	ESTUDIANTE A TIEMPO COMPLETO		ESTUDIANTE A TIEMPO PARCIAL	
	ECTS matrícula mínima	ECTS matrícula máxima	ECTS matrícula mínima	ECTS matrícula máxima
PRIMER CURSO	60	60	24	60
SUCESIVOS CURSOS	24	60	24	60

El Reglamento 8/2024, de 27 de junio, de la Universidad de Málaga, sobre matriculación de estudiantes en actividades formativas correspondientes a planes de estudios conducentes a títulos de carácter oficial de grado y máster universitario, actualmente vigente en la Universidad de Málaga, recoge, en su artículo 5, que el estudiantado que continúa sus estudios conducentes a títulos de grado o máster universitario deberá matricular

un mínimo de 24 créditos, salvo que el número de créditos que resten para finalizar los respectivos estudios sea inferior, en cuyo caso se deberá matricular dicho número restante.

El estudiantado que formalice matrícula por segunda o sucesivas veces deberá atenerse a lo establecido en las Normas reguladoras del progreso y la permanencia de los estudiantes de grado y máster de la Universidad de Málaga así como en la Guía para la matriculación de estudiantes de estudios de Máster publicada por la UMA para cada curso académico.

1.2.- Justificación del interés del título y contextualización

Este título forma parte de una remodelación más amplia de la oferta formativa de la ETSI Informática de la UMA. Así, la creación del Máster en Ciberseguridad se realiza conjuntamente con la modificación del actual Máster de Ingeniería Informática. Ese máster contenía una especialidad en Ciberseguridad que ha sido extinguida y en su lugar se ha desarrollado este nuevo máster, que propone una formación más específica en Ciberseguridad. Cabe señalar que, debido al contexto local y regional, este nuevo máster contará con una mención dual para, como se establece en el RD 822/2021, tener como objetivo una más adecuada capacitación del estudiantado que mejore su formación integral y su empleabilidad.

Esta modificación de la oferta de másteres no supone una modificación significativa de la capacidad docente de las áreas de conocimiento involucradas, pues se combina con la cancelación de la carga docente que la Universidad de Málaga tenía en el máster interuniversitario en Transformación Digital de Empresas. En la siguiente tabla se representa la situación anterior y posterior de la oferta de másteres y se observa que tan solo supone un aumento de 17,5 créditos ECTS pero que es asumible dentro de la capacidad docente de las áreas de conocimiento.

	Planes en 2024		Planes en 2025		
	MUII	MTDE	MUII	MCIBER	Diferencia
LENGUAJES Y SISTEMAS INFORMÁTICOS	42	27,5	54	18	2,5
CIENCIA DE LA COMPUTACIÓN E INTELIGENCIA ARTIFICIAL	10,5	0	13,5	4,5	7,5
INGENIERÍA TELEMÁTICA	22,5	3	4,5	25,5	4,5
MATEMÁTICA APLICADA	7,5	0	7,5	0	0
ARQUITECTURA Y TECNOLOGÍA DE COMPUTADOREDS	22,5	0	25,5	0	3
					17,5

MTDE: Máster en Transformación Digital de Empresas
MUII: Máster en Ingeniería Informática
MCIBER: Máster en Ciberseguridad

En el **Anexo I** se describe con detalle la justificación del título y su contextualización.

1.3.- Objetivos formativos

Principales objetivos formativos del título

El objetivo fundamental es formar a profesionales especializados que dispongan de conocimientos y competencias en Ciberseguridad y que puedan aplicarlas en el contexto laboral y también en el científico. Desde un punto de vista más específico se pretende que el plan de estudios forme profesionales que en la finalización de esos estudios puedan:

- Ser capaz de garantizar la seguridad en la cadena de suministro de software, gestionando adecuadamente las dependencias y componentes de terceros para mitigar los riesgos asociados con vulnerabilidades externas.

- Ser capaz de desarrollar estrategias para proteger el ecosistema de desarrollo de software, incluyendo la protección del código fuente, las herramientas de desarrollo, y los entornos de prueba contra amenazas y vulnerabilidades.
- Ser capaz de identificar, evaluar y mitigar vulnerabilidades de seguridad específicas del hardware, utilizando técnicas y herramientas adecuadas para prevenir ataques y asegurar la integridad de los sistemas ciberfísicos.
- Ser capaz de asegurar entornos IT/OT integrando soluciones de seguridad que protejan tanto la información (IT) como las operaciones (OT), reconociendo la necesidad de salvaguardar contra amenazas dirigidas a infraestructuras críticas.
- Ser capaz de implementar protección basada en componentes hardware seguros, seleccionando y utilizando dispositivos y tecnologías que ofrezcan robustez frente a intentos de intrusión y ataques, tanto en el diseño como en la implementación de sistemas seguros.
- Ser capaz de identificar la relación entre ciberseguridad y ciberdefensa, incluyendo las principales estrategias y organismos existentes orientados al resguardo del bienestar público.
- Ser capaz de aplicar los principales mecanismos para la adquisición y compartición de ciberinteligencia e inteligencia de amenazas en el contexto de la defensa de las infraestructuras críticas en el ámbito de la seguridad nacional.
- Ser capaz de extraer información de evidencias digitales procedentes de un ciberataque siguiendo las directrices de la legislación vigente.
- Ser capaz de determinar los mecanismos de defensa más óptimos para proteger el ciclo de vida de una solución de inteligencia artificial ante las amenazas más tradicionales en entornos informáticos existentes.

Objetivos formativos de las menciones o especialidades

Las especialidades que se pueden obtener con el título son:

- Mención DUAL
- Itinerario GENERAL

La mención Dual se corresponde con lo reglamentado en el artículo 22 del real decreto 822/2021 por el que se establece la organización de las enseñanzas universitarias y del procedimiento de aseguramiento de su calidad. Se deberá firmar el contrato Formativo para la Formación en Alternancia:

https://www.sepe.es/HomeSepe/es/que-es-el-sepe/comunicacion-institucional/publicaciones/publicaciones-oficiales/listado-pub-empleo/guia-contratos/guia-contratos-introduccion/contrato-para-la-formacion-y-el-aprendizaje.html

Se ha incluido un **Anexo III** donde se detalla en profundidad la estructura del plan de estudios. Los objetivos formativos de la mención DUAL y el itinerario GENERAL se diferencian en la forma de adquirir los resultados de aprendizaje. Mientras en la primera se obtienen con metodologías propias de la formación en alternancia, en la última se produce un proceso de enseñanza-aprendizaje habitual mediante asignaturas.

Los objetivos formativos específicos de ambas especialidades son:

- Ser capaz de aplicar pruebas automatizadas de software para identificar vulnerabilidades y problemas de seguridad desde las etapas iniciales del desarrollo, utilizando herramientas y técnicas para asegurar la calidad y seguridad del software.
- Ser capaz de implementar controles de seguridad efectivos durante el proceso de despliegue de software, incluyendo la configuración de entornos seguros y la gestión de actualizaciones de seguridad.
- Ser capaz de aplicar principios de programación segura y de ingeniería del software para desarrollar aplicaciones y sistemas que cumplan con estándares de seguridad y privacidad desde su concepción hasta su despliegue.
- Ser capaz de aplicar técnicas y herramientas de pentesting y hacking contra sistemas para el descubrimiento de debilidades dentro del contexto de una organización.

- Ser capaz de aplicar diversas técnicas de análisis del comportamiento de un malware y su interacción con el entorno para obtener información que sirva de apoyo a la toma de decisiones.

El número de créditos de la mención DUAL es de 18 ECTS para la formación en alternancia y de 12 en el TFM , lo que corresponde al 50% de los créditos del máster, cumpliendo lo establecido en el real decreto 822/2021.

Estructuras curriculares específicas y Estrategias metodológicas de innovación docente específicas y justificación de sus objetivos

En el documento **Anexo III** se detalla la estructura del plan de estudios, que contempla como hemos indicado una mención dual. Además, se indican las correspondencias de las asignaturas del máster adaptadas al perfil de acceso al máster.

Perfiles fundamentales de egreso a los que se orientan las enseñanzas y profesiones reguladas

Perfiles de egreso:	• Chief Information Security Officer (CISO): Responsable de la seguridad de la información. • Ingeniero de Ciberseguridad: Encargado de diseñar, implementar y mantener soluciones de seguridad. • Analista de Ciberseguridad: Analiza amenazas y vulnerabilidades para proteger sistemas y redes. • Ingeniero de Redes: Se enfoca en la seguridad de las redes y su infraestructura. • Auditor de Ciberseguridad o Hacker Ético: Evalúa la seguridad de sistemas y aplicaciones. • Gerente de Seguridad Lógica: Supervisa políticas y procedimientos de seguridad.
Habilita para profesión regulada:	[no]
Profesión regulada:	
Acuerdo:	
Norma:	
Condición de acceso para título profesional:	[no]
Título profesional:	

2. Resultados del proceso de formación y de aprendizaje (ESG 1.2)

Código *(C/COM/HD)*		**Tipo** *Conocimientos o contenidos (C) Competencias (COM) Habilidades o Destrezas (HD)*
C01	Al finalizar el aprendizaje, el alumnado será capaz de interpretar leyes y regulaciones aplicables en materia de ciberseguridad y privacidad tanto en entorno de organizaciones como para la sociedad en general.	*Conocimientos o contenidos (C)*
COM01	Al finalizar el aprendizaje, el alumnado será capaz de concebir soluciones integrales de computación, equipamiento (hardware), aplicaciones, interacción y servicios (software) en empresas y centros tecnológicos, de acuerdo a criterios técnicos, económicos, medioambientales, de garantía de calidad y homologación de los productos, y de seguridad para las personas y los bienes según la normativa vigente y asegurando la calidad del servicio.	*Competencias (COM)*
COM02	Al finalizar el aprendizaje, el alumnado será capaz de elaborar pliegos técnicos razonados de características de equipamientos hardware o software adaptadas a necesidades definidas para participar en contratos competitivos como cliente o proveedor.	*Competencias (COM)*
COM03	Al finalizar el aprendizaje, el alumnado será capaz de organizar su propio trabajo para ser autónomo e independiente, demostrando autoorganización, iniciativa, responsabilidad, y capacidad para el aprendizaje permanente y el desarrollo profesional continuo, aplicando los principios del cuerpo disciplinar y la ordenación de la Ingeniería Informática.	*Competencias (COM)*
COM04	Al finalizar el aprendizaje, el alumnado será capaz de liderar la transformación digital de empresas y centros tecnológicos por medio de la participación en la elaboración, planificación, dirección, gestión y/o coordinación de proyectos del ámbito de la ingeniería informática, en particular de su área de conocimiento.	*Competencias (COM)*
COM05	Al finalizar el aprendizaje, el alumnado será capaz de liderar equipos de trabajo en ámbitos específicos y/o multidisciplinares en entornos críticos, de alto impacto, fiabilidad o interés, como empresas o centros tecnológicos que afronten problemas informáticos complejos, ejerciendo si es necesario las funciones de dirección general, dirección técnica y/o planificación estratégica.	*Competencias (COM)*
COM06	Capacidad para la puesta en marcha, dirección y gestión de procesos de fabricación de equipos informáticos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.	*Competencias (COM)*
COM07	Al finalizar el aprendizaje, el alumnado será capaz de demostrar una conducta profesional y ética, de acuerdo a un código deontológico y al contexto legal, comercial, industrial y/o social.	*Competencias (COM)*
COM08	Al finalizar el aprendizaje, el alumnado será capaz de concebir metodologías originales o adaptaciones novedosas de metodologías conocidas para la resolución de problemas en entornos con especificaciones inciertas o incompletas.	*Competencias (COM)*
COM09	Al finalizar el aprendizaje, el alumnado será capaz de evaluar la calidad de los desarrollos, procesos, sistemas, servicios, aplicaciones y productos informáticos participando en el diseño, desarrollo y gestión de mecanismos de homologación, certificación y procesos de auditoría atendiendo a la normativa y legislación vigente, así como a aspectos técnicos, corporativos o estratégicos.	*Competencias (COM)*
COM10	Al finalizar el aprendizaje, el alumnado será capaz de evaluar riesgos y amenazas que una organización puede afrontar en temas de ciberseguridad para poder seleccionar las mejores estrategias, políticas, técnicas y herramientas que garanticen la protección de datos (almacenados, procesados o en tránsito), la fiabilidad y seguridad de los componentes, servicios, protocolos y aplicaciones.	*Competencias (COM)*
COM11	Al finalizar el aprendizaje, el alumnado será capaz de proponer políticas y técnicas acordes a los retos y las repercusiones que las diferentes ciberamenazas representan para la sociedad consciente de los riesgos e implicaciones sociales y éticas que conllevan.	*Competencias (COM)*

COM12	Realización, presentación y defensa, una vez obtenidos todos los créditos del plan de estudios, de un ejercicio original realizado individualmente ante un tribunal universitario, consistente en un proyecto integral de Ingeniería en Informática de naturaleza profesional en el que se sinteticen las competencias adquiridas en las enseñanzas.	*Competencias (COM)*
COM13	Respetar los derechos humanos y derechos fundamentales; los valores democráticos, la libertad de pensamiento y de cátedra, la tolerancia y el reconocimiento y respeto a la diversidad, la equidad de todas las ciudadanas y de todos los ciudadanos, con respeto a la igualdad de género, la eliminación de todo contenido o práctica discriminatoria por razón de nacimiento, origen nacional o étnico, religión, convicción u opinión, edad, discapacidad, orientación sexual, identidad o expresión de género, características sexuales, enfermedad, situación socioeconómica o cualquier otra condición o circunstancia personal o social, la cultura de la paz y de la participación, entre otros.	*Competencias (COM)*
COM14	Llevar a cabo el tratamiento de la sostenibilidad y del cambio climático.	*Competencias (COM)*
COM15	Comunicar de forma oral y escrita transmitiendo información, ideas, problemas y soluciones a un público tanto especializado como no especializado.	*Competencias (COM)*
COM16	Capacidad para desenvolverse en un entorno laboral, incluyendo el trabajo en equipo, la capacidad de liderazgo y el respeto a los principios de accesibilidad universal y diseño para todas las personas.	*Competencias (COM)*
HD01	Al finalizar el aprendizaje, el alumnado será capaz de analizar problemas y tareas complejas o indefinidas escogiendo las herramientas o metodologías más adecuadas para la obtención de soluciones innovadoras en su campo o campos afines.	*Habilidades o Destrezas (H-D)*
HD02	Al finalizar el aprendizaje, el alumnado será capaz de adaptar las tecnologías nuevas o emergentes en informática a la resolución de problemas en nuevas áreas o que impliquen el uso de otras disciplinas contribuyendo al desarrollo de la informática como disciplina.	*Habilidades o Destrezas (H-D)*
HD03	Al finalizar el aprendizaje, el alumnado será capaz de aplicar los principios de la economía y de la gestión de recursos humanos y proyectos, así como la legislación, regulación y normalización de la informática.	*Habilidades o Destrezas (H-D)*
HD04	Al finalizar el aprendizaje, el alumnado será capaz de analizar problemas y tareas complejas o indefinidas escogiendo las herramientas o metodologías más adecuadas para la obtención de soluciones innovadoras en su campo o campos afines.	*Habilidades o Destrezas (H-D)*
HD05	Al finalizar el aprendizaje, el alumnado será capaz de aplicar conceptos, arquitecturas y modelos avanzados de ciberseguridad en soluciones informáticas.	*Habilidades o Destrezas (H-D)*

3. Admisión, reconocimiento y movilidad (ESG 1.4)

3.1.- Requisitos de acceso y procedimientos de admisión

¿Cumple requisitos de acceso según legislación vigente? SI

Requisitos de acceso

De acuerdo con las previsiones del art. 75 de la Ley 15/2003, Andaluza de Universidades, a los únicos efectos del ingreso en los centros universitarios, todas las Universidades públicas andaluzas se constituyen en un distrito único. En consecuencia, los procesos de admisión se realizan de acuerdo con los criterios que establezca la Comisión de Distrito Único Andaluz, considerándose en los mismos la existencia de estudiantes con necesidades educativas específicas derivadas de discapacidad.

En este máster se establecen 4 vías de acceso:

- Vía 1: Podrá acceder al Máster quien haya cursado un grado en ciberseguridad o bien un grado en el ámbito de la Ingeniería Informática y de Sistemas y con amplia formación o experiencia específica en ciberseguridad.
- Vía 2: Asimismo, se permitirá el acceso al Máster cuando el título de grado que avala la solicitud pertenezca al ámbito de la Ingeniería Informática y de Sistemas con formación o experiencia básica en ciberseguridad.
- Vía 3: También podrán acceder a este Máster quienes estén en posesión de un título de grado con competencias en tecnologías de la información sin experiencia ni formación en ciberseguridad.
- Vía 4. Excepcionalmente, se podrán admitir en el máster egresados de cualquier grado que tengan una dilatada experiencia especializada en el ámbito de la ciberseguridad.

En las Vías 3 o 4, la Comisión Académica del Título podrá establecer individualmente los complementos de formación que estime necesarios relacionados con el perfil concreto de ingreso. Estos complementos consistirán en asignaturas del grado en Ingeniería Informática o del grado en Ciberseguridad e Inteligencia Artificial impartidos en la E.T.S.I. Informática de la Universidad de Málaga. De acuerdo con el Real Decreto 822/2021, de 28 de septiembre, el número de créditos no excederá del 20% del total de créditos del Máster, es decir, 12 créditos. Los complementos se podrán cursar de forma simultánea al desarrollo de los estudios de máster.

Es importante destacar que la asignación de las vías de acceso de cada estudiante y, sobre todo, la posibilidad de cursar o no una formación en alternancia, será llevada a cabo por la Comisión Mixta (universidad-empresa) que velará porque la formación previa de los solicitantes aporte garantías de poder abordar satisfactoriamente el proceso de enseñanza-aprendizaje.

Los estudiantes de nacionalidad extranjera procedentes de países no hispanoparlantes deben acreditar un nivel B2 de español. La acreditación debe estar expedida por el Instituto Cervantes (DELE o SIELE) o alguna institución de acreditación lingüística similar.

Procedimiento y criterios de Admisión

Se ordenarán las solicitudes según las vías de acceso anteriormente citadas, atendiendo primero las solicitudes de preferencia alta (vías 1 y 2 indistintamente), siguiendo con las de preferencia media (vías 3 y 4).

Considerando el orden anterior y a igualdad de condiciones, se tendrá en cuenta:

- Expediente académico: 60%
- Otros méritos (dominio de segundo idioma -preferentemente inglés-, experiencia profesional, adecuación de la titulación de acceso, etc.): 40%

Adicionalmente se podrá realizar una entrevista a las personas solicitantes, especialmente para comprobar el nivel de idioma requerido y también en el caso de que quiera optar a una de las menciones del título de formación en alternancia.

Dependiendo del número de plazas disponibles de la formación en alternancia y de la elección solicitada , la comisión mixta establecerá para cada estudiante la mención a realizar.

3.2.- Criterios para el reconocimiento y transferencia de créditos

Tipos de reconocimiento	Mínimo	Máximo	Documento
Créditos cursados en Centros de formación profesional de grado superior	**0**	**0**	
Créditos cursados en Títulos propios	**0**	**0**	
Créditos cursados por Acreditación Experiencia Laboral y Profesional	**0**	**9**	Reconocimiento por optatividad

Las normas reguladoras de la Universidad de Málaga de los reconocimientos de estudios o actividades, y de la experiencia laboral o profesional, a efectos de la obtención de títulos universitarios oficiales de graduado y máster universitario, así como de la transferencia de créditos se pueden consultar en el siguiente enlace:

Reglamento 4/2023, de 18 de julio de 2023, sobre reconocimientos de estudios o actividades, y de la experiencia laboral o profesional, a efectos de la obtención de títulos universitarios oficiales de Graduado y Máster Universitario, así como de la transferencia de créditos

3.3.- Procedimiento para la organización de la movilidad de estudiantes propios y de acogida

En el siguiente enlace web se pueden consultar los diferentes programas y normativa relacionados con la movilidad en la Universidad de Málaga.

En el **Anexo II** se describe la movilidad en nuestro Centro: charlas informativas, talleres para la realización del currículum, entrevistas en inglés y acuerdos con empresas multinacionales con sede en Málaga. Otra peculiaridad del Centro es la existencia de un Contrato Académico, para evitar posibles confusiones en los reconocimientos. Actualmente nuestra Escuela tiene acuerdos de movilidad internacional con 68 universidades extranjeras.

4. Planificación de las Enseñanzas (ESG 1.3)

4.1.- Estructura del plan de estudios

El plan de estudios completo se detalla en el **Anexo III** . La estructura del máster en Ciberseguridad por la Universidad de Málaga se configura mediante 30 créditos ECTS formativos obligatorios, 12 ECTS del trabajo fin de máster (TFM) y 18 créditos ECTS que pueden cubrirse mediante la formación en alternancia (mención DUAL) o mediante el itinerario general alternativo, cursando las asignaturas correspondientes.

Los procedimientos de coordinación del centro se describen en el siguiente enlace (**Anexo IV Coordinación**)

Tabla 1. Estructura del plan de estudios

Créditos obligatorios	30
Créditos optativos	18
Créditos de Trabajo Fin de Grado o Máster	12
Total Créditos ECTS	**60**

Tabla 2. Resumen del plan de estudios (estructura semestral/trimestral)

Semestre/Trimestre (en este caso se añadirá una columna más)	
Semestre 1/Trimestre 1	Semestre 2/Trimestre 2
ECTS: 30 Materias/asignaturas: -Seguridad en Computación Cuántica -Dirección y Gestión de la Ciberseguridad Tipología (carácter): Obligatoria Modalidad: Presencial Lengua: Español Materias/asignaturas: -Gestión de Anomalías e Incidentes de Ciberseguridad -Diseño y Desarrollo de Software Seguro -Técnicas de Pentesting y Análisis Forense -Análisis de Malware -Formación en Alternancia Tipología (carácter): Optativo Modalidad: Presencial Lengua: Español	ECTS: 30 Materias/asignaturas: -Ciberseguridad en Aplicaciones y Servicios Telemáticos de Nueva Generación -Seguridad en DevOps -Auditoría de Seguridad y Análisis de Riesgos -Ciberinteligencia y Ciberdefensa -Seguridad en sistemas hardware y ciberfísicos Tipología (carácter): Obligatorio Modalidad: presencial Lengua: Español
Trabajo fin de Máster. Anual, Español	

Tabla 3. Estructura de las menciones/especialidades

Menciones / Especialidades	Materias/asignaturas	Semestre / Trimestre	Créditos ECTS
Mención Dual	Formación en Alternancia	1	18 (450 horas)
Itinerario General	• Gestión de Anomalías e Incidentes de Ciberseguridad • Diseño y Desarrollo de Software Seguro • Técnicas de Pentesting y Análisis Forense • Análisis de Malware	1	18

Tabla 4. Plan de estudios detallado

Materia 1: Tecnologías Emergentes	
Número de créditos ECTS	3 ECTS
Tipología	*obligatorio*
Organización temporal	*Semestre nº 1*
Modalidad	*presencial*
Resultados del proceso de formación y aprendizaje	*HD01- Al finalizar el aprendizaje, el alumnado será capaz de analizar problemas y tareas complejas o indefinidas escogiendo las herramientas o metodologías más adecuadas para la obtención de soluciones innovadoras en su campo o campos afines* *HD02- Al finalizar el aprendizaje, el alumnado será capaz de adaptar las tecnologías nuevas o emergentes en informática a la resolución de problemas en nuevas áreas o que impliquen el uso de otras disciplinas contribuyendo al desarrollo de la informática como disciplina* *COM07- Al finalizar el aprendizaje, el alumnado será capaz de demostrar una conducta profesional y ética, de acuerdo a un código deontológico y al contexto legal, comercial, industrial y/o social* *COM08- Al finalizar el aprendizaje, el alumnado será capaz de concebir metodologías originales o adaptaciones novedosas de metodologías conocidas para la resolución de problemas en entornos con especificaciones inciertas o incompletas.* *COM10- Al finalizar el aprendizaje, el alumnado será capaz de evaluar riesgos y amenazas que una organización puede afrontar en temas de ciberseguridad para poder seleccionar las mejores estrategias, políticas, técnicas y herramientas que garanticen la protección de datos (almacenados, procesados o en tránsito), la fiabilidad y seguridad de los componentes, servicios, protocolos y aplicaciones,* *COM11- Al finalizar el aprendizaje, el alumnado será capaz de proponer políticas y técnicas acordes a los retos y las repercusiones que las diferentes ciberamenazas representan para la sociedad consciente de los riesgos e implicaciones sociales y éticas que conllevan.* *HD05- Al finalizar el aprendizaje, el alumnado será capaz de aplicar conceptos, arquitecturas y modelos avanzados de ciberseguridad en diferentes entornos que requieran el uso de la informática*
Asignaturas	*Seguridad en Computación Cuántica, semestre 1, 3 ECTS, Español*
Lenguas	*Español/Inglés*
Contenidos propios del módulo/materia/asignatura	*Fundamentos de seguridad en computación cuántica.* *Mecanismos y protocolos criptográficos post-cuánticos.* *Seguridad en la Internet cuántica.* *Mecanismos criptográficos cuánticos.*
Actividades formativas/Metodologías docentes	*MD01 Lecciones magistrales* *MD05 Seminarios* *MD08 Análisis o estudios de casos* *MD09 Realización de proyectos* *AF01 Actividades expositivas: Lección magistral, conferencia, charla, exposiciones por parte del alumnado, etc.* *AF02 Actividades prácticas en aula docente o en instalaciones específicas. En aula docente: Resolución de problemas, actividades de diseño, ejercicios de simulación y/o demostración, realización de informes profesionales y/o técnicos, realización de proyectos, revisión bibliográfica o documental, etc; en instalaciones específicas: Prácticas de laboratorio, prácticas en talleres, etc.* *AF03 Seminarios/Talleres de estudio, revisión, debate, actividades de seguimiento, tutorización y evaluación, etc.: Debates, estudio/discusión de casos, revisión/exposición de trabajos, actividades de seguimiento y evaluación, etc.* *AF05 Actividades prácticas no presenciales: Resolución de problemas, estudios de casos,* *proyectos, etc.* *AF07 Actividades de elaboración de documentos: Elaboración de informes, elaboración de memorias, elaboración de portafolios.* *AF09 Estudio personal.*

Sistemas de evaluación	*SE01- Trabajos individuales o grupales (proyectos, diseños, ensayos, informes, investigaciones, resolución de casos…).* *SE02- Valoración de ejercicios concretos, individuales y/o grupales, que se proponen y realizan durante el desarrollo de la materia (solución de problemas, análisis de texto, prácticas concretas …).* *SE07- Presentación pública de producciones, individuales o grupales.* *SE10- Pruebas de adquisición de conocimientos.*
Observaciones	

Materia 2: Dirección Estratégica en Ciberseguridad	
Número de créditos ECTS	13.5 ECTS
Tipología	*obligatorio*
Organización temporal	*Semestre nº 1 y 2*
Modalidad	*presencial*
Resultados del proceso de formación y aprendizaje	*COM01- Al finalizar el aprendizaje, el alumnado será capaz de concebir soluciones integrales de computación, equipamiento (hardware), aplicaciones, interacción y servicios (software) en empresas y centros tecnológicos, de acuerdo a criterios técnicos, económicos, medioambientales, de garantía de calidad y homologación de los productos, y de seguridad para las personas y los bienes según la normativa vigente y asegurando la calidad del servicio* *COM02- Al finalizar el aprendizaje, el alumnado será capaz de elaborar pliegos técnicos razonados de características de equipamientos hardware o software adaptadas a necesidades definidas para participar en contratos competitivos como cliente o proveedor.* *COM04- Al finalizar el aprendizaje, el alumnado será capaz de liderar la transformación digital de empresas y centros tecnológicos por medio de la participación en la elaboración, planificación, dirección, gestión y/o coordinación de proyectos del ámbito de la ingeniería informática, en particular de su área de conocimiento* *COM03- Al finalizar el aprendizaje, el alumnado será capaz de organizar su propio trabajo para ser autónomo e independiente, demostrando autoorganización, iniciativa, responsabilidad, y capacidad para el aprendizaje permanente y el desarrollo profesional continuo, aplicando los principios del cuerpo disciplinar y la ordenación de la Ingeniería Informáticas.* *COM05- Al finalizar el aprendizaje, el alumnado será capaz de liderar equipos de trabajo en ámbitos específicos y/o multidisciplinares en entornos críticos, de alto impacto, fiabilidad o interés, como empresas o centros tecnológicos que afronten problemas informáticos complejos, ejerciendo si es necesario las funciones de dirección general, dirección técnica y/o planificación estratégica* *COM06- Capacidad para la puesta en marcha, dirección y gestión de procesos de fabricación de equipos informáticos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.* *COM07- Al finalizar el aprendizaje, el alumnado será capaz de demostrar una conducta profesional y ética, de acuerdo a un código deontológico y al contexto legal, comercial, industrial y/o social originales o adaptaciones novedosas de metodologías conocidas para la resolución de problemas en entornos con especificaciones inciertas o incompletas.* *COM09– Al finalizar el aprendizaje, el alumnado será capaz de evaluar la calidad de los desarrollos, procesos, sistemas, servicios, aplicaciones y productos informáticos participando en el diseño, desarrollo y gestión de mecanismos de homologación, certificación y procesos de auditoría atendiendo a la normativa y legislación vigente, así como a aspectos técnicos, corporativos o estratégicos.* *COM10- Al finalizar el aprendizaje, el alumnado será capaz de evaluar riesgos y amenazas que una organización puede afrontar en temas de ciberseguridad para poder seleccionar las mejores estrategias, políticas, técnicas y herramientas que garanticen la protección de datos (almacenados, procesados o en tránsito), la fiabilidad y seguridad de los componentes, servicios, protocolos y aplicaciones.* *COM11- Al finalizar el aprendizaje, el alumnado será capaz de proponer políticas y técnicas acordes a los retos y las repercusiones que las diferentes ciberamenazas representan para la sociedad consciente de los riesgos e implicaciones sociales y éticas que conllevan.*

	HD02- Al finalizar el aprendizaje, el alumnado será capaz de adaptar las tecnologías nuevas o emergentes en informática a la resolución de problemas en nuevas áreas o que impliquen el uso de otras disciplinas contribuyendo al desarrollo de la informática como disciplina *HD03- Al finalizar el aprendizaje, el alumnado será capaz de aplicar los principios de la economía y de la gestión de recursos humanos y proyectos, así como la legislación, regulación y normalización de la informática.* *HD05- Al finalizar el aprendizaje, el alumnado será capaz de aplicar conceptos, arquitecturas y modelos avanzados de ciberseguridad en diferentes entornos que requieran el uso de la informática.* *C01 - Al finalizar el aprendizaje, el alumnado será capaz de interpretar leyes y regulaciones aplicables en materia de ciberseguridad y privacidad tanto en entorno de organizaciones como para la sociedad en general.*
Asignaturas	*Dirección y Gestión de la Ciberseguridad, semestre 1, 4.5 ECTS, Español* *Auditoría de Seguridad y Análisis de Riesgos, semestre 2, 4.5 ECTS, Español* *Ciberinteligencia y Ciberdefensa, semestre 2, 4.5 ECTS, Español*
Lenguas	*Español/Inglés*
Contenidos propios del módulo/materia/asignatura	*Gestión de riesgos de ciberseguridad* *Políticas y procedimientos de ciberseguridad* *Gobierno y cumplimiento normativo* *Liderazgo y dirección estratégica en ciberseguridad* *Ética y responsabilidad en ciberseguridad* *Programas de certificación y estándares de auditoría y riesgo* *Desarrollo de informes de auditoría* *Análisis de riesgos, evaluación y gestión de las ciberamenazas* *Supervisión y gestión de incidentes* *Introducción a la ciberdefensa y ciberinteligencia* *Métodos y herramientas de ciberinteligencia* *Inteligencia de ciberamenazas* *Simulaciones de ciberdefensa y ciberguerra*
Actividades formativas/Metodologías docentes	*MD01 Lecciones magistrales* *MD02 Prácticas de laboratorio* *MD03 Resolución de problemas* *MD04 Aprendizaje basado en proyectos* *MD05 Seminarios* *MD06 Talleres* *MD08 Análisis o estudios de casos* *MD09 Realización de proyectos* *MD10 Revisión y exposición de trabajos* *AF01 Actividades expositivas: Lección magistral, conferencia, charla, exposiciones por parte del alumnado, etc.* *AF03 Seminarios/Talleres de estudio, revisión, debate, actividades de seguimiento, tutorización y evaluación, etc.: Debates, estudio/discusión de casos, revisión/exposición de trabajos, actividades de seguimiento y evaluación, etc.* *AF02 Actividades prácticas en aula docente o en instalaciones específicas. En aula docente: Resolución de problemas, actividades de diseño, ejercicios de simulación y/o demostración, realización de informes profesionales y/o técnicos, realización de proyectos, revisión bibliográfica o documental, etc; en instalaciones específicas: Prácticas de laboratorio, prácticas en talleres, etc.* *AF05 Actividades prácticas no presenciales: Resolución de problemas, estudios de casos,* *proyectos, etc.* *AF07 Actividades de elaboración de documentos: Elaboración de informes, elaboración de memorias, elaboración de portafolios.* *AF09 Estudio personal*
Sistemas de evaluación	*SE01- Trabajos individuales o grupales (proyectos, diseños, ensayos, informes, investigaciones, resolución de casos…).*

	SE02- Valoración de ejercicios concretos, individuales y/o grupales, que se proponen y realizan durante el desarrollo de la materia (solución de problemas, análisis de texto, prácticas concretas …). *SE07- Presentación pública de producciones, individuales o grupales.* *SE10- Pruebas de adquisición de conocimientos.*
Observaciones	

Materia 3: Seguridad en Entornos Software y Hardware	
Número de créditos ECTS	13.5 ECTS
Tipología	*obligatorio*
Organización temporal	*Semestre nº 2*
Modalidad	*presencial*
Resultados del proceso de formación y aprendizaje	*COM01-Al finalizar el aprendizaje, el alumnado será capaz de concebir soluciones integrales de computación, equipamiento (hardware), aplicaciones, interacción y servicios (software) en empresas y centros tecnológicos, de acuerdo a criterios técnicos, económicos, medioambientales, de garantía de calidad y homologación de los productos, y de seguridad para las personas y los bienes según la normativa vigente y asegurando la calidad del servicio* *COM03- Al finalizar el aprendizaje, el alumnado será capaz de organizar su propio trabajo para ser autónomo e independiente, demostrando autoorganización, iniciativa, responsabilidad, y capacidad para el aprendizaje permanente y el desarrollo profesional continuo, aplicando los principios del cuerpo disciplinar y la ordenación de la Ingeniería Informáticas.* *COM05- Al finalizar el aprendizaje, el alumnado será capaz de liderar equipos de trabajo en ámbitos específicos y/o multidisciplinares en entornos críticos, de alto impacto, fiabilidad o interés, como empresas o centros tecnológicos que afronten problemas informáticos complejos, ejerciendo si es necesario las funciones de dirección general, dirección técnica y/o planificación estratégica* *COM07- Al finalizar el aprendizaje, el alumnado será capaz de demostrar una conducta profesional y ética, de acuerdo a un código deontológico y al contexto legal, comercial, industrial y/o social* *COM08- Al finalizar el aprendizaje, el alumnado será capaz de concebir metodologías originales o adaptaciones novedosas de metodologías conocidas para la resolución de problemas en entornos con especificaciones inciertas o incompletas.* *COM09 – Al finalizar el aprendizaje, el alumnado será capaz de evaluar la calidad de los desarrollos, procesos, sistemas, servicios, aplicaciones y productos informáticos participando en el diseño, desarrollo y gestión de mecanismos de homologación, certificación y procesos de auditoría atendiendo a la normativa y legislación vigente, así como a aspectos técnicos, corporativos o estratégicos.* *C01- Al finalizar el aprendizaje, el alumnado será capaz de interpretar leyes y regulaciones aplicables en materia de ciberseguridad y privacidad tanto en entorno de organizaciones como para la sociedad en general.* *HD01- Al finalizar el aprendizaje, el alumnado será capaz de analizar problemas y tareas complejas o indefinidas escogiendo las herramientas o metodologías más adecuadas para la obtención de soluciones innovadoras en su campo o campos afines* *HD02- Al finalizar el aprendizaje, el alumnado será capaz de adaptar las tecnologías nuevas o emergentes en informática a la resolución de problemas en nuevas áreas o que impliquen el uso de otras disciplinas contribuyendo al desarrollo de la informática como disciplina* *HD03- Al finalizar el aprendizaje, el alumnado será capaz de aplicar los principios de la economía y de la gestión de recursos humanos y proyectos, así como la legislación, regulación y normalización de la informática.* *HD04- Al finalizar el aprendizaje, el alumnado será capaz de analizar problemas y tareas complejas o indefinidas escogiendo las herramientas o metodologías más adecuadas para la obtención de soluciones innovadoras en su campo o campos afines.*

	HD05- Al finalizar el aprendizaje, el alumnado será capaz de aplicar conceptos, arquitecturas y modelos avanzados de ciberseguridad en diferentes entornos que requieran el uso de la informática.
Asignaturas	*Ciberseguridad en Aplicaciones y Servicios Telemáticos de Nueva Generación, semestre 2, 4.5 ECTS, Español* *Seguridad en DevOps, semestre 2 , 4.5 ECTS, Español* *Seguridad en Sistemas HW y Ciberfísicos, semestre 2, 4.5 ECTS, Español*
Lenguas	*Español/Inglés*
Contenidos propios del módulo/materia/asignatura	*Seguridad en entornos IoT/Edge* *Seguridad en vehículos conectados y autónomos* *Seguridad en redes 5G/6G* *Seguridad en sistemas aeroespaciales* *Introducción a DevOps y DevSecOps* *Plataformas de soporte a DevSecOps* *Introducción a las pruebas automatizadas de software* *Controles de seguridad en el despliegue* *Seguridad en la cadena de suministro de software* *Implementación de SBOM (Software Bill of Material)* *Protección del ecosistema de desarrollo del software* *Cumplimiento de certificaciones de seguridad* *Vulnerabilidades y amenazas en sistemas ciberfísicos* *Seguridad en entornos IT/OT* *Protección basada en componentes hardware seguros* *Seguridad Operacional de Sistemas*
Actividades formativas/Metodologías docentes	*MD01 Lecciones magistrales* *MD02 Prácticas de laboratorio* *MD03 Resolución de problemas* *MD04 Aprendizaje basado en proyectos* *MD05 Seminarios* *MD08 Análisis o estudios de casos* *MD09 Realización de proyectos* *MD10 Revisión y exposición de trabajos* *AF01 Actividades expositivas: Lección magistral, conferencia, charla, exposiciones por parte del alumnado, etc.* *AF03 Seminarios/Talleres de estudio, revisión, debate, actividades de seguimiento, tutorización y evaluación, etc.: Debates, estudio/discusión de casos, revisión/exposición de trabajos, actividades de seguimiento y evaluación, etc.* *AF02 Actividades prácticas en aula docente o en instalaciones específicas. En aula docente: Resolución de problemas, actividades de diseño, ejercicios de simulación y/o demostración, realización de informes profesionales y/o técnicos, realización de proyectos, revisión bibliográfica o documental, etc; en instalaciones específicas: Prácticas de laboratorio, prácticas en talleres, etc.* *AF05 Actividades prácticas no presenciales: Resolución de problemas, estudios de casos, proyectos, etc.* *AF07 Actividades de elaboración de documentos: Elaboración de informes, elaboración de memorias, elaboración de portafolios.* *AF09 Estudio personal*
Sistemas de evaluación	*SE01- Trabajos individuales o grupales (proyectos, diseños, ensayos, informes, investigaciones, resolución de casos…).* *SE02- Valoración de ejercicios concretos, individuales y/o grupales, que se proponen y realizan durante el desarrollo de la materia (solución de problemas, análisis de texto, prácticas concretas …).* *SE07- Presentación pública de producciones, individuales o grupales.* *SE10- Pruebas de adquisición de conocimientos.*
Observaciones	

Materia 4: Tecnologías en Ciberseguridad	
Número de créditos ECTS	18 ECTS
Tipología	*optativo*
Organización temporal	*Semestre nº 1*
Modalidad	*presencial*
Resultados del proceso de formación y aprendizaje	*COM01-Al finalizar el aprendizaje, el alumnado será capaz de concebir soluciones integrales de computación, equipamiento (hardware), aplicaciones, interacción y servicios (software) en empresas y centros tecnológicos, de acuerdo a criterios técnicos, económicos, medioambientales, de garantía de calidad y homologación de los productos, y de seguridad para las personas y los bienes según la normativa vigente y asegurando la calidad del servicio.* *COM03- Al finalizar el aprendizaje, el alumnado será capaz de organizar su propio trabajo para ser autónomo e independiente, demostrando autoorganización, iniciativa, responsabilidad, y capacidad para el aprendizaje permanente y el desarrollo profesional continuo, aplicando los principios del cuerpo disciplinar y la ordenación de la Ingeniería Informática* *COM06- Capacidad para la puesta en marcha, dirección y gestión de procesos de fabricación de equipos informáticos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.* *COM07- Al finalizar el aprendizaje, el alumnado será capaz de demostrar una conducta profesional y ética, de acuerdo a un código deontológico y al contexto legal, comercial, industrial y/o social.* *COM10 - Al finalizar el aprendizaje, el alumnado será capaz de evaluar riesgos y amenazas que una organización puede afrontar en temas de ciberseguridad para poder seleccionar las mejores estrategias, políticas, técnicas y herramientas que garanticen la protección de datos (almacenados, procesados o en tránsito), la fiabilidad y seguridad de los componentes, servicios, protocolos y aplicaciones.* *COM11- Al finalizar el aprendizaje, el alumnado será capaz de proponer políticas y técnicas acordes a los retos y las repercusiones que las diferentes ciberamenazas representan para la sociedad consciente de los riesgos e implicaciones sociales y éticas que conllevan.* *HD02-Al finalizar el aprendizaje, el alumnado será capaz de adaptar las tecnologías nuevas o emergentes en informática a la resolución de problemas en nuevas áreas o que impliquen el uso de otras disciplinas contribuyendo al desarrollo de la informática como disciplina* *HD04– Al finalizar el aprendizaje, el alumnado será capaz de analizar problemas y tareas complejas o indefinidas escogiendo las herramientas o metodologías más adecuadas para la obtención de soluciones innovadoras en su campo o campos afines,* *HD05- Al finalizar el aprendizaje, el alumnado será capaz de aplicar conceptos, arquitecturas y modelos avanzados de ciberseguridad en diferentes entornos que requieran el uso de la informática.*
Asignaturas	*Gestión de Anomalías e Incidentes de Ciberseguridad, semestre 1, 4.5 ECTS, Español* *Diseño y Desarrollo de Software Seguro, semestre 1, 4.5 ECTS, Español* *Técnicas de Pentesting y Análisis Forense, semestre 1, 4.5 ECTS, Español* *Análisis de Malware, semestre 1, 4.5 ECTS, Español*
Lenguas	*Español/Inglés*
Contenidos propios del módulo/materia/asignatura	*Fundamentos de seguridad en protocolos y redes telemáticas* *Diseño y configuración de redes de comunicación* *Detección de anomalías, intrusiones e incidentes de seguridad* *Respuesta contra anomalías e intrusiones* *Sistema de gestión de eventos e información de seguridad* *Centro de Operaciones de Seguridad* *Principios de Programación Segura y de Ingeniería del Software* *Tratamiento de errores y vulnerabilidades* *Herramientas de Programación Segura* *Ingeniería de Requisitos* *Diseño, modelado, y desarrollo de Software Seguro* *Verificación y pruebas*

	Descubrimiento, monitorización y explotación de vulnerabilidades *Técnicas de Hacking y Herramientas* *Evidencias forenses generadas por ciberataques* *Adquisición de evidencias forenses* *Análisis de evidencias forenses* *Introducción al análisis de malware* *Análisis estático y dinámico de malware* *Análisis dinámico de malware* *Análisis automático de malware*
Actividades formativas/Metodologías docentes	*MD01 Lecciones magistrales* *MD02 Prácticas de laboratorio* *MD03 Resolución de problemas* *MD04 Aprendizaje basado en proyectos* *MD05 Seminarios* *MD08 Análisis o estudios de casos* *MD09 Realización de proyectos* *MD10 Revisión y exposición de trabajos* *AF01 Actividades expositivas: Lección magistral, conferencia, charla, exposiciones por parte del alumnado, etc.* *AF03 Seminarios/Talleres de estudio, revisión, debate, actividades de seguimiento, tutorización y evaluación, etc.: Debates, estudio/discusión de casos, revisión/exposición de trabajos, actividades de seguimiento y evaluación, etc.* *AF02 Actividades prácticas en aula docente o en instalaciones específicas. En aula docente: Resolución de problemas, actividades de diseño, ejercicios de simulación y/o demostración, realización de informes profesionales y/o técnicos, realización de proyectos, revisión bibliográfica o documental, etc; en instalaciones específicas: Prácticas de laboratorio, prácticas en talleres, etc.* *AF05 Actividades prácticas no presenciales: Resolución de problemas, estudios de casos, proyectos, etc.* *AF07 Actividades de elaboración de documentos: Elaboración de informes, elaboración de memorias, elaboración de portafolios.* *AF09 Estudio personal*
Sistemas de evaluación	*SE01- Trabajos individuales o grupales (proyectos, diseños, ensayos, informes, investigaciones, resolución de casos…).* *SE02- Valoración de ejercicios concretos, individuales y/o grupales, que se proponen y realizan durante el desarrollo de la materia (solución de problemas, análisis de texto, prácticas concretas …).* *SE07- Presentación pública de producciones, individuales o grupales.* *SE10- Pruebas de adquisición de conocimientos.*
Observaciones	
Aquellos estudiantes que sigan el itinerario general deberán matricularse de esta materia.	

Materia 5: Formación en Alternancia	
Número de créditos ECTS	18 ECTS
Tipología	*optativo*
Organización temporal	*Semestre nº 1*
Modalidad	*presencial*
Resultados del proceso de formación y aprendizaje	*COM01-Al finalizar el aprendizaje, el alumnado será capaz de concebir soluciones integrales de computación, equipamiento (hardware), aplicaciones, interacción y servicios (software) en empresas y centros tecnológicos, de acuerdo a criterios técnicos, económicos, medioambientales, de garantía de calidad y homologación de los productos, y de seguridad para las personas y los bienes según la normativa vigente y asegurando la calidad del servicio.* *COM03- Al finalizar el aprendizaje, el alumnado será capaz de organizar su propio trabajo para ser autónomo e independiente, demostrando autoorganización, iniciativa, responsabilidad, y capacidad para el aprendizaje permanente y el desarrollo profesional*

	continuo, aplicando los principios del cuerpo disciplinar y la ordenación de la Ingeniería Informática *COM06- Capacidad para la puesta en marcha, dirección y gestión de procesos de fabricación de equipos informáticos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.* *COM07- Al finalizar el aprendizaje, el alumnado será capaz de demostrar una conducta profesional y ética, de acuerdo a un código deontológico y al contexto legal, comercial, industrial y/o social.* *COM10 - Al finalizar el aprendizaje, el alumnado será capaz de evaluar riesgos y amenazas que una organización puede afrontar en temas de ciberseguridad para poder seleccionar las mejores estrategias, políticas, técnicas y herramientas que garanticen la protección de datos (almacenados, procesados o en tránsito), la fiabilidad y seguridad de los componentes, servicios, protocolos y aplicaciones.* *COM11- Al finalizar el aprendizaje, el alumnado será capaz de proponer políticas y técnicas acordes a los retos y las repercusiones que las diferentes ciberamenazas representan para la sociedad consciente de los riesgos e implicaciones sociales y éticas que conllevan.* *HD02-Al finalizar el aprendizaje, el alumnado será capaz de adaptar las tecnologías nuevas o emergentes en informática a la resolución de problemas en nuevas áreas o que impliquen el uso de otras disciplinas contribuyendo al desarrollo de la informática como disciplina* *HD04– Al finalizar el aprendizaje, el alumnado será capaz de analizar problemas y tareas complejas o indefinidas escogiendo las herramientas o metodologías más adecuadas para la obtención de soluciones innovadoras en su campo o campos afines,* *HD05- Al finalizar el aprendizaje, el alumnado será capaz de aplicar conceptos, arquitecturas y modelos avanzados de ciberseguridad en diferentes entornos que requieran el uso de la informática.*
Asignaturas	*Formación en alternancia, semestre 1, 18 ECTS, Español*
Lenguas	*Español/Inglés*
Contenidos propios del módulo/materia/asignatura	*Fundamentos de seguridad en protocolos y redes telemáticas* *Diseño y configuración de redes de comunicación* *Detección de anomalías, intrusiones e incidentes de seguridad* *Respuesta contra anomalías e intrusiones* *Sistema de gestión de eventos e información de seguridad* *Centro de Operaciones de Seguridad* *Principios de Programación Segura y de Ingeniería del Software* *Tratamiento de errores y vulnerabilidades* *Herramientas de Programación Segura* *Ingeniería de Requisitos* *Diseño, modelado, y desarrollo de Software Seguro* *Verificación y pruebas* *Descubrimiento, monitorización y explotación de vulnerabilidades* *Técnicas de Hacking y Herramientas* *Evidencias forenses generadas por ciberataques* *Adquisición de evidencias forenses* *Análisis de evidencias forenses* *Introducción al análisis de malware* *Análisis estático y dinámico de malware* *Análisis dinámico de malware* *Análisis automático de malware*
Actividades formativas/Metodologías docentes	*MD05 Seminarios* *MD08 Análisis o estudios de casos* *MD09 Realización de proyectos* *MD10 Revisión y exposición de trabajos* *AF01 Actividades expositivas: Lección magistral, conferencia, charla, exposiciones por parte del alumnado, etc.* *AF03 Seminarios/Talleres de estudio, revisión, debate, actividades de seguimiento, tutorización y evaluación, etc.: Debates, estudio/discusión de casos, revisión/exposición de trabajos, actividades de seguimiento y evaluación, etc.*

	AF07 Actividades de elaboración de documentos: Elaboración de informes, elaboración de memorias, elaboración de portafolios. *AF09 Estudio personal*
Sistemas de evaluación	*SE01- Trabajos individuales o grupales (proyectos, diseños, ensayos, informes, investigaciones, resolución de casos…).* *SE08- Entrevistas, individuales y/o en pequeño grupo, sobre el proceso de aprendizaje del alumnado.* *SE11- Seguimiento de las actividades durante la estancia en la empresa por parte de la persona que ejerce de tutor*
Observaciones	
Aquellos estudiantes que sigan la mención dual deberán matricularse de esta materia.	

Materia 6: Trabajo Fin de Máster	
Número de créditos ECTS	12
Tipología	*TFM*
Organización temporal	*Semestre nº 1 y 2*
Modalidad	*presencial*
Resultados del proceso de formación y aprendizaje	*COM13 - Respetar los derechos humanos y derechos fundamentales, los valores democráticos, la libertad de pensamiento y de cátedra, la tolerancia y el reconocimiento y respeto a la diversidad, la equidad de todas las ciudadanas y de todos los ciudadanos, la eliminación de todo contenido o práctica discriminatoria, la cultura de la paz y de la participación, entre otros.* *COM14 - Llevar a cabo el tratamiento de la sostenibilidad y del cambio climático.* *COM15 - Comunicar de forma oral y escrita transmitiendo información, ideas, problemas y soluciones a un público tanto especializado como no especializado.* *COM16 - Capacidad para desenvolverse en un entorno laboral, incluyendo el trabajo en equipo y la capacidad de liderazgo .* *COM12 - Realización, presentación y defensa, una vez obtenidos todos los créditos del plan de estudios, de un ejercicio original realizado individualmente ante un tribunal universitario, consistente en un proyecto integral de Ingeniería en Informática de naturaleza profesional en el que se sinteticen las competencias adquiridas en las enseñanzas.*
Asignaturas	*Trabajo Fin de Máster*
Lenguas	*Español*
Contenidos propios del módulo/materia/asignatura	*El Trabajo Fin de Máster supone la realización, presentación y defensa, una vez obtenidos todos los créditos del plan de estudios, de un ejercicio original realizado individualmente ante un tribunal universitario. Consiste por lo tanto en un proyecto integral de Ingeniería Informática de naturaleza profesional en el que se sinteticen las competencias adquiridas en las enseñanzas.*
Actividades formativas/Metodologías docentes	*AF05 Actividades prácticas no presenciales: Resolución de problemas, estudios de casos, proyectos, etc.* *AF06 Actividades de documentación: Búsqueda bibliográfica, etc.* *AF07 Actividades de elaboración de documentos: Elaboración de informes, elaboración de memorias, elaboración de portafolios.* *AF09 Estudio personal.* *MD09 Realización de proyectos* *MD10 Revisión y exposición de trabajos*
Sistemas de evaluación	*SE01- Trabajos individuales o grupales (proyectos, diseños, ensayos, informes, investigaciones, resolución de casos…).* *SE07- Presentación pública de producciones, individuales o grupales.*
Observaciones	
Requisitos previos: El Trabajo Fin de Máster no podrá defenderse sin cumplir los requisitos establecidos en el Reglamento de Trabajo Fin de Máster aplicable, sin perjuicio de lo que pueda disponer la normativa de carácter general que establezca la Universidad de Málaga.	

Debido a la naturaleza dual del título, El Trabajo fin de Máster para el estudiantado que esté asociado a una formación en alternancia (mención dual) se desarrollará en el ámbito de la empresa o institución donde esté desarrollado la mención. En este caso, los 12 ECTS se corresponderá con una estancia de 300 horas en dicha empresa o institución, en las mismas condiciones laborales que ya tuvo en su estancia de formación en alternancia.
Si la relación laboral que dio lugar a la estancia para el estudiantado en alternancia se viese interrumpida, se garantizará que el alumnado pueda desarrollar un TFM académico, al igual que los estudiantes que han cursado el itinerario general. En este caso, no se podrá especificar al acabar el título que haya obtenido la mención dual, que queda reservada al estudiantado que cubren la estancia en empresa y el TFM en alternancia.
El procedimiento seguido para la evaluación está regulado en la Normativa sobre Trabajos de Fin de Máster de la Universidad de Málaga, accesible a través del siguiente enlace:
https://www.uma.es/secretaria-general-uma/navegador_de_ficheros/boletin/descargar/2024/julio/20240702_31531.pdf

4.2.- Actividades y metodologías Docentes

En la información que se incluye para cada materia se establecen las actividades formativas que se organizan en cada caso. A continuación, se relacionan las diversas actividades consideradas, su metodología de enseñanza y aprendizaje, y una estimación de la dedicación del estudiantado (**Anexo V**).

La Universidad de Málaga recomienda una distribución de la dedicación para cada tipo de actividad. La cuantificación de la dedicación se ha realizado en horas de trabajo del alumnado, asumiendo una dedicación de 25 horas por cada crédito ECTS distribuidas entre 7,5 y 10 horas de docencia presencial, y entre 15 y 17,5 horas para el resto del trabajo del alumnado, incluida la evaluación.

Código	Metodología
MD01	Lecciones magistrales
MD02	Prácticas de laboratorio
MD03	Resolución de problemas
MD04	Aprendizaje basado en proyectos
MD05	Seminarios
MD06	Talleres
MD07	Debates
MD08	Análisis o estudios de casos
MD09	Realización de proyectos
MD10	Revisión y exposición de trabajos
MD11	Salidas de estudio

Considerando las recomendaciones de la Universidad de Málaga para la elaboración de las guías docentes, a continuación, se presenta el listado de actividades formativas que se sugieren:

Código	Actividad formativa
AF01	Actividades expositivas: Lección magistral, conferencia, charla, exposiciones por parte del alumnado, etc.
AF02	Actividades prácticas en aula docente o en instalaciones específicas. En aula docente: Resolución de problemas, actividades de diseño, ejercicios de simulación y/o demostración, realización de informes profesionales y/o técnicos, realización de proyectos, revisión bibliográfica o documental, etc; en instalaciones específicas: Prácticas de laboratorio, prácticas en talleres, etc.
AF03	Seminarios/Talleres de estudio, revisión, debate, actividades de seguimiento, tutorización y evaluación, etc.: Debates, estudio/discusión de casos, revisión/exposición de trabajos, actividades de seguimiento y evaluación, etc.
AF04	Actividades fuera de la Universidad: Prácticas en instituciones, prácticas en empresas, visitas a Centros/Instituciones, etc.
AF05	Actividades prácticas no presenciales: Resolución de problemas, estudios de casos, proyectos, etc.
AF06	Actividades de documentación: Búsqueda bibliográfica, etc.
AF07	Actividades de elaboración de documentos: Elaboración de informes, elaboración de memorias, elaboración de portafolios.
AF08	Actividades de discusión, debate, etc.: Participación en foros, participación en wiki, participación en chat, seminarios virtuales.
AF09	Estudio personal.

4.3.- Sistemas de evaluación

En la planificación docente se describen los sistemas de evaluación que se aplicarán en cada una de las materias. Aunque el procedimiento final dependerá del profesorado que imparta la docencia, las alternativas de evaluación cumplen la Normativa de la Universidad de Málaga.

El sistema de calificaciones a aplicar será el que establezca la legislación vigente, actualmente el recogido en el Real Decreto 1125/2003, publicado en el B. O. E. el 18 de septiembre de 2003.

Materia Formación en Alternancia:

Sistema de evaluación	Ponderación Mínima (%)	Ponderación Máxima(%)
SE01- Trabajos individuales o grupales (proyectos, diseños, ensayos, informes, investigaciones, resolución de casos…).	30	90
SE08- Entrevistas, individuales y/o en pequeño grupo, sobre el proceso de aprendizaje del alumnado.	10	30
SE11- Seguimiento de las actividades durante la estancia en la empresa por parte de la persona que ejerce de tutor	30	90

Materia Trabajo Fin de Máster:

Sistema de evaluación	Ponderación Mínima (%)	Ponderación Máxima(%)
SE01- Trabajos individuales o grupales (proyectos, diseños, ensayos, informes, investigaciones, resolución de casos…).	60	90
SE07- Presentación pública de producciones, individuales o grupales.	10	40

Resto de Materias:

Sistema de evaluación	Ponderación Mínima (%)	Ponderación Máxima(%)
SE01- Trabajos individuales o grupales (proyectos, diseños, ensayos, informes, investigaciones, resolución de casos…).	0	90
SE02- Valoración de ejercicios concretos, individuales y/o grupales, que se proponen y realizan durante el desarrollo de la materia (solución de problemas, análisis de texto, prácticas concretas …).	0	90
SE03- Participación en clase.	0	5
SE04- Participación a través del Campus Virtual.	0	10
SE05- Ejecución de portafolios.	0	10
SE06- Ejecución del diario del estudiante.	0	5
SE07- Presentación pública de producciones, individuales o grupales.	0	10
SE08- Entrevistas, individuales y/o en pequeño grupo, sobre el proceso de aprendizaje del alumnado.	0	40
SE09- Valoración de la asistencia a eventos de carácter académico, científico, y/o cultural	0	10
SE10- Pruebas de adquisición de conocimientos.	0	90

5. Personal académico y de apoyo a la docencia (ESG 1.5)

5.1.- Descripción de los perfiles de profesorado y otros recursos Humanos

El título cuenta con una plantilla de profesorado experimentada, implicada por su labor y suficientemente preparada, como muestra no sólo los puestos que desempeñan, sino también datos objetivos como los niveles de satisfacción del alumnado, la participación en proyectos de innovación educativa y la participación en cursos de formación. Además, los equipos docentes de las asignaturas cuentan con personas integradas en grupos de investigación consolidados y fuertemente relacionados con las materias propuestas.

En relación al procedimiento de evaluación de la actividad docente del profesorado, en sesión ordinaria de 28 de mayo de 2021 del Consejo de Gobierno de la Universidad de Málaga se acuerda aprobar el Programa "DOCENTIA-UMA", procedimiento para la evaluación de la actividad docente del profesorado de la Universidad de Málaga. Posteriormente a la aprobación por Consejo de Gobierno, se remite el procedimiento a la Dirección General de Evaluación y Acreditación de la Agencia Andaluza del Conocimiento (DEVA), con objeto de verificar su diseño y obtener informe de evaluación.

También cabe destacar la implicación del profesorado en medidas encaminadas a mejorar la calidad docente. Entre un 25% y un 35% del profesorado realiza cursos de formación cada año y prácticamente un cuarto de los profesores participan en uno o más proyectos de innovación educativa. La mayoría de estos proyectos suelen incluir a varias asignaturas, y en algunos casos se trata de proyectos de innovación que afectan a toda la escuela.

Tabla 5. Resumen del profesorado asignado al título (incluir al menos la siguiente información)

Categoría	Número	ECTS	Doctores/as	Acreditados/as	Sexenio	Quinquenio
Catedrático de Universidad	2	9	2	2	9	11
Titular de Universidad	9	39	9	9	22	31
Total	**11**	**48**	**11**	**11**	**31**	**42**

Tabla 6. Detalle del profesorado asignado al título por área de conocimiento.

Área de conocimiento: Ciencia de la Computación e Inteligencia Artificial	
Número de profesorado	*1*
Número de doctores/as	*1*
Categorías	*Catedrático de Universidad: 1*
Número de Profesorado acreditado	*1*
Materias / asignaturas	*Dirección y Gestión de la Ciberseguridad*
ECTS impartidos (previstos)	*4,5*
ECTS disponibles (potenciales)	*80*

Área de conocimiento: Lenguajes y Sistemas Informáticos	
Número de profesorado	*4*
Número de doctores/as	*4*
Categorías	*Titular de Universidad: 4*
Número de Profesorado acreditado	*4*
Materias / asignaturas	*Seguridad en DevOps* *Auditoría de Seguridad y Análisis de Riesgos* *Diseño y Desarrollo de Software Seguro* *Análisis de Malware*
ECTS impartidos (previstos)	*18*
ECTS disponibles (potenciales)	*337*

Área de conocimiento: Ingeniería Telemática	
Número de profesorado	*6*
Número de doctores/as	*6*
Categorías	*Catedrático de Universidad:1* *Titular de Universidad: 5*
Número de Profesorado acreditado	*6*
Materias / asignaturas	*Seguridad en Computación Cuántica* *Seguridad en Sistemas HW y Ciberfísicos* *Ciberinteligencia y Ciberdefensa* *Ciberseguridad en Aplicaciones y Servicios Telemáticos de Nueva Generación* *Gestión de Anomalías e Incidentes de Ciberseguridad* *Técnicas de Pentesting y Análisis Forense*
ECTS impartidos (previstos)	*25,5*
ECTS disponibles (potenciales)	*80,7*

Tabla 7. Personal disponible para impartir el título

Denominación del título: **MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD**
Universidad/es (si es título conjunto): **UNIVERSIDAD DE MÁLAGA**

												Dedicación al Título		Dedicación a otros títulos	
Universidad [1]	Identificador del profesor/a	Denominación asignatura	N º ECTs asignatura	Modalidad de enseñanza [2]	Área de Conocimiento del Profesorado [3]	Nivel de idioma [4]	Categoría [5]	Doctor/a (S/N)	Experiencia docente [6] (años)	Experiencia investigadora [7] (sexenios)	Experiencia profesional (años)	Dedicación (TC ó TP) [8]	Tiempo (horas/semana)	Denominación de título/s [9]	Tiempo total de dedicación a otro/s título/s (horas/semana)
El Contenido de esta tabla se puede encontrar en el **Anexo VI Profesorado**															
	Núm. Total prof. diferentes **11**							**100%** de Doctores sobre el total de profesorado diferente del título							

(1) Universidad de origen a la que pertenece el profesor o profesora
(2) Tipo de enseñanza en la que se oferta la asignatura (presencial/híbrida/virtual)
(3) Área de conocimiento del profesorado que implarte la asignatura
(4) Nivel de idioma del profesor o profesora, en caso de que la asignatura se oferte en un idioma diferente al castellano
(5) Categorías académicas (CU, TU, CEU, TEU, Ayudante, asociado, etc…) o Categorías profesionales dentro del Grupo al que pertenezca, personal de administración y servicios (Técnico de laboratorio, Técnico de apoyo a la docencia, etc.…)
(6) Experiencia docente en número de años no quinquenios. Cuando el tipo de enseñanza de la asignatura sea "híbrida" o "virtual" se incluirá además el número de años de experiencia docente en esta modalidad (Ejemplo: 20 / 4)
(7) Experiencia investigadora en número de sexenios
(8) Dedicación al Título: TP -Tiempo parcial ; TC - Tiempo completo
(9) Incluirla denominación de todos los títulos en los que esté implicado con docencia

Se podrán añadir tantas filas como sean necesarias para la correcta cumplimentación de las tablas.

Se elaborará una tabla con la misma información en el caso de informar del Personal no disponible y se pretenda incorporar (Tabla. Personal adicional necesario para poder impartir el título)

Tabla 8. Detalle del profesorado de empresa asignado al título por área de conocimiento. (Formación dual)

Área de conocimiento: Ingeniería Telemática	
Número de profesorado	10
Número de doctores/as	0
Número de prof. nivel máster	6
Experiencia profesional (años)	100
Materias / asignaturas	Formación en Alternancia
ECTS impartidos (previstos)	18

Perfil del profesorado necesario y no disponible y plan de contratación

Este máster se impartirá con los recursos actuales. Se ha propuesto una modificación del Máster Universitario de Ingeniería Informática eliminando la mención de Ciberseguridad y desplazando esos créditos al máster que se propone.

Perfil del profesorado de empresa que participa en la mención dual

Nombre de la Empresa	**Apellidos, Nombre de TUTOR**	**E-mail TUTOR**	**Titulación de TUTOR**	**Breve CV de TUTOR**	**Pdf con CV de Tutor propuesto:**
Babel	Casado Mancha, Mario	mario.casado@babelgroup.com	Ingeniero de Telecomunicación	https://www.linkedin.com/in/mariocasado/	https://drive.google.com/open?id=1pHo3qGsC_NIK6hBrAd9PEFbols6vLIt2
ACCENTURE	CORTÉS DANTA, CARLOS	carlos.cortes@accenture.com	Grado en Ingeniería de Sistemas de Telecomunicación	https://www.linkedin.com/in/ccdanta/	https://drive.google.com/open?id=1aXF46nVTuBxOe0lqPSUNnCtfwX8RVBeJ
Sofistic	Fernando Denis Ramírez Guerrero	framirez@sofistic.com	Técnico Superior en Desarrollo de Aplicaciones Informáticas	https://www.linkedin.com/in/fernando-denis-ramirez-guerrero/	https://drive.google.com/open?id=1gR-PfBXmrPQH_8sSJ1ZaNCsdkMWw71vg
jtsec Beyond IT Security	TALLON GUERRI, JAVIER	jtallon@jtsec.es	Ingeniero Informático	https://www.linkedin.com/in/javitallon/	https://drive.google.com/open?id=12KSdVZli_FYteaoLkTLQtJm4YYJvzSa1
Cybercrin	Rida Lkhluf	rida@cybercrin.com	Ingeniero en telecomunicación sistemas electrónicos/ máster en ciberseguridad	https://www.linkedin.com/in/ridalkhluf/	https://drive.google.com/open?id=1Bt7HZK94uqC8616VWezCcWftCPYZV2jE
Mercedes-Benz Group Services Madrid	Andres Romero Sanchez	andres.romero_sanchez@mercedes-benz.com	Ingeniero de Telecomunicaciones	https://www.linkedin.com/in/andr%C3%A9s-romero-s%C3%A1nchez-b4841424/	https://drive.google.com/open?id=1qBuvcZSHmTYCNThwxzHgk-1VD9jY0wVe
Hispasec Sistemas	Miguel Tobaria, Luciano	lmiguel@hispasec.com	Grado en Imagen y Sonido (UMA) + Máster de Profesorado (UMA)	https://www.linkedin.com/in/lmtobaria/	https://drive.google.com/open?id=1a0stYfXs6BCK4iIBtybzmdLZb412Ge0W

Nombre de la Empresa	Apellidos, Nombre de TUTOR	E-mail TUTOR	Titulación de TUTOR	Breve CV de TUTOR	Pdf con CV de Tutor propuesto:
Capgemini España S.L.	Munoz Martínez, Jesús	jesus.munoz-martinez@capgemini.com	Master SEEI y Graduado en Ing. Electrónica Industrial.	https://www.linkedin.com/in/jmm-5b80b315a/	https://drive.google.com/open?id=1RD9VzKr_QpHp--l4MizMdB6jfIKHia9d
Telefónica Tech	Sergio de los Santos	sergio.delossantosvilchez@telefonica.com			
INDRA	Fco Javier Cano Fernández	fjcano@minsait.com			

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

Recogidos en el punto 6.1.- Justificación de la adecuación de los medios materiales y servicios disponibles.

6. Recursos para el aprendizaje: materiales e infraestructuras, prácticas y servicios (ESG 1.6)

6.1.- Justificación de la adecuación de los medios materiales y servicios disponibles

La Escuela comparte espacio con la ETS de Ingeniería de Telecomunicación. El edificio está compuesto por 5 módulos, 3 con plantas para aulas, laboratorios docentes y de investigación y despachos. El cuarto módulo está dedicado a aulas docentes y el quinto a gestión y servicios.

Aulas docentes: 5 pequeñas, 6 medianas, 8 grandes y 3 muy grandes con capacidades de 32, 72, 119 y 192 estudiantes respectivamente.

Laboratorios:

Departamento	Laboratorios	Puestos por laboratorio
Lenguajes y Ciencias de la Computación	11	32

Servicio de Biblioteca y Hemeroteca con más de 500 puestos de estudio. Servicio de préstamos físicos y virtuales a través de aplicación web centralizada de la UMA. Existen dos aulas adicionales de ordenadores (58 y 28 puestos) y un aula de docencia avanzada.

El Salón de Actos cuenta con más de 500 plazas y equipamiento audiovisual de gama alta. Existen 3 Salas de Grado para reuniones, presentación y defensas de TFEs y tesis doctorales

El alumnado dispone de comedor/sala de esparcimiento en la que pueden tomar su propia comida.

Se puede consultar información más detallada en el siguiente enlace.

Entre el personal de apoyo disponible para el desarrollo de las actividades de soporte técnico y administrativo asociadas a los grados que ya se imparten en la E.T.S.I. y al nuevo propuesto por la E.T.S.I. Informática, se incluye el personal de administración y servicios siguientes:

- Secretaría del Centro, encargada de la gestión de expedientes y apoyo al equipo de dirección de la Escuela: 7 personas con una antigüedad de 27 a 5 años.
- Servicio de Atención Informática al Complejo Tecnológico (SAICT), encargado de labores de apoyo técnico, relativas al mantenimiento de las instalaciones informáticas: 3 personas con experiencia de 28 a 20 años.
- Biblioteca de la ETSI Informática compartida con la ETSI de Telecomunicación: 11 personas con experiencia de 34 a 22 años.
- Servicio de Información, Conserjería y Atención al Usuario (SICAU), compartido con la ETSI Telecomunicación, encargado de la atención a la persona usuario, soporte a la docencia, investigación y a los servicios, supervisión de la conservación de las infraestructuras: 12 personas con una experiencia de 21 a 12 años.
- Los departamentos que participan en la docencia del Título propuesto cuentan con seis puestos administrativos con 9 años de experiencia de media, tres Técnicos Especialista de Laboratorio (Grupo III) con 16 años, 5 Técnicos de Grado Medio de Apoyo a la Docencia y a la Investigación (Grupo II) con 18 años y un Técnico Superior de apoyo a la docencia e investigación con 7 años de antigüedad.
- EVLT: El Servicio de Enseñanza Virtual y Laboratorios Tecnológicos, apuesta por la introducción de las nuevas tecnologías en la docencia como apoyo a la enseñanza presencial, creando asignaturas semipresenciales y cursos on-line. Se trata de facilitar a los alumnos el acceso a los materiales docentes y explotar las posibilidades formativas y los mecanismos de comunicación que ofrece Internet.
- Aulas TIC que existen en los Centros se ofrece a profesores y alumnos apoyo técnico para la utilización del entorno virtual de aprendizaje y de los recursos necesarios.

6.2.- Gestión de las Prácticas externas

Este Máster no oferta prácticas externas curriculares.

Tabla 10. Información sobre Prácticas externas

Nº de créditos de prácticas académicas externas obligatorias:		Nº total de plazas ofertadas (desglosar en su caso, las plazas si se ofertan las prácticas en varios idiomas):	
Nº de créditos de prácticas optativas (de especialidad, mención o itinerario):		Nº total de plazas ofertadas (desglosar en su caso, las plazas si se ofertan las prácticas en varios idiomas):	

6.3.- Previsión de dotación de recursos materiales y servicios

No se han detectado recursos adicionales necesarios a nivel de personal docente al tratarse de una reestructuración de planes de estudio que afecta al Máster Universitario de Ingeniería Informática y este título. Además, esta renovación de la oferta de máster ha respetado las adscripciones anteriores de los títulos.

Dado que no se plantea un aumento del número de plazas, tampoco se precisarán de otros recursos adicionales como espacios, equipamiento y personal de administración y servicios.

7. Calendario de implantación

7.1.- Cronograma de implantación

Curso de inicio:	**2025/26**
Cronograma:	En el curso 2025-2026 se implantará la titulación completa

7.2.- Procedimiento de adaptación

No aplica procedimiento de adaptación

7.3.- Enseñanzas que se extinguen

Cod. RUCT	
Denominación título y Centro	

8. Sistema Interno de Garantía de la Calidad (ESG 1.1/1.7/1.8/1.9/1.10)

8.1.- Sistema interno de garantía de calidad

El Sistema de Garantía de Calidad de la UMA está descrito en el documento accesible desde la página web de calidad de la Universidad de Málaga, en el que se siguen los criterios y directrices para el aseguramiento de la Calidad en el Espacio Europeo de Educación Superior.

La calidad en los centros de la UMA está descrita en el siguiente enlace, mientras que el Sistema de Garantía de Calidad de la ETSI Informática está descrita en la página de la Escuela.

La Comisión Académica del Máster es la encargada de: asesorar al Coordinador o Coordinadora del Máster durante el proceso de admisión de estudiantes, cuando le sea requerido; aprobar los anteproyectos de Trabajo Fin de Máster presentados; informar sobre los reconocimientos solicitados; organizar la evaluación los Trabajos Fin de Máster; y cualesquiera otras que se establezcan en la memoria de verificación del título del Máster. Su reglamento será aprobado antes de la implantación de estos estudios.

Además, se constituirá una Comisión Mixta Universidad-Entidades del programa de formación en alternancia que realizará la asignación de las vías de acceso de cada estudiante y la posibilidad de cursar o no una formación en alternancia, diseñará los ejes del itinerario de esta formación así como los posibles temas a desarrollar en los trabajos fin de máster; establecerá los mecanismos de coordinación, integración y supervisión de las actividades desarrolladas en la entidad y las impartidas en el aula; analizará indicadores, incidencias y evidencias detectadas en el desarrollo del programa de formación en alternancia; garantizará el seguimiento del alumnado trabajador en el proceso de enseñanza-aprendizaje en alternancia, y ejercerá las funciones de control y seguimiento del convenio específico resolviendo, en su caso, las incidencias de interpretación y ejecución que pudieran plantearse en el desarrollo de las actividades.

8.2.- Medios para la información pública

La publicación de información actualizada de las actividades y programas de la E.T.S.I. Informática se realiza sobre varios canales y medios de comunicación:

- Web del Centro: Recoge información en español e inglés (parcialmente) sobre el centro, oferta de grado y posgrado (másteres, doctorado y titulaciones propias), calendario académico por titulaciones y servicios. También incluye espacios a movilidad, calidad y acciones con empresas e igualdad.
- Campus Virtuales de apoyo a la docencia (Grado, Máster y Doctorado)-
- Acceso a distintas web institucionales de la UMA con información estratificada por Centros (Servicio de Calidad, Servicio de PDI, Servicio de Ordenación Académica con las programaciones docentes de Grado y Máster).

Para la comunicación interna se dispone de:

- Sala de profesorado Espacio virtual utilizado para la coordinación y la comunicación e interacción con el profesorado.
- Sala de Estudiantes (por curso lectivo) Para publicación e interacción relacionada con el estudiantado.
- Listas de correo internas: docentes@Informática.uma.es
- Para la comunicación externa el centro publica en Redes Sociales: Twitter, Instagram, Youtube, y Telegram.

A través de estos medios, se garantiza que los programas formativos y resto de actividades que tienen lugar en la E.T.S.I. Informática están actualizados con información precisa y fácilmente accesibles para todos los colectivos de interés.

Apoyo y orientación a estudiantes, una vez matriculados

En el siguiente enlace se describe el proceso de apoyo, orientación y tutorización.

8.3.- Anexos

- **Anexo I** - Justificación
- **Anexo II** - Movilidad
- **Anexo III** - Plan de estudios
- **Anexo IV** - Coordinación
- **Anexo V** - Actividades formativas
- **Anexo VI** - Profesorado

Informe previo de la comunidad autónoma

INFORME PREVIO A LA VERIFICACIÓN DE LAS DE ENSEÑANZAS UNIVERSITARIAS SOLICITADAS POR LA UNIVERSIDAD DE MÁLAGA

El artículo 57.2 del Texto Refundido de la Ley Andaluza de Universidades, aprobado por Decreto Legislativo 1/2013, de 8 de enero, establece que la Consejería competente en materia de Universidades deberá emitir informe favorable sobre la adecuación de los planes de estudios a los objetivos y criterios establecidos en la programación universitaria de Andalucía para que los planes de estudios puedan ser remitidos para su verificación.

De otro lado, el Real Decreto 822/2021, de 28 de septiembre, por el que se establece la organización de las enseñanzas universitarias y del procedimiento de aseguramiento de su calidad dispone en su artículo 26.3 que las Comunidades Autónomas en el ejercicio de sus competencias sobre la programación universitaria y la ordenación del mapa de titulaciones oficiales de su ámbito territorial, realizarán un informe preceptivo sobre la necesidad y viabilidad académica y social de la implantación del título universitario oficial previo al inicio del procedimiento de verificación de tal manera que en caso de informe favorable, la universidad podrá iniciar el procedimiento de verificación del título.

Por su parte, el artículo 14 del Decreto 154/2023, de 27 de junio, de ordenación de las enseñanzas universitarias oficiales en el ámbito de la Comunidad Autónoma de Andalucía, en el marco de los procedimientos para la ordenación de las enseñanzas universitarias, regula la emisión del informe previo de adecuación, necesidad y viabilidad de los planes de estudios, así como la información acreditativa de la adecuación del plan de estudios a la programación universitaria de la Junta de Andalucía y de la necesidad y viabilidad académica y social del título previo a la verificación.

Mediante Resolución de 8 de abril de 2024, de la Dirección General de Coordinación Universitaria, de conformidad con lo establecido en el artículo 57.2 del Texto Refundido de la Ley Andaluza de Universidades, aprobado por Decreto Legislativo 1/2013, de 8 de enero y en el artículo 26.3 del Real Decreto 822/2021, de 28 de septiembre, por el que se establece la organización de las enseñanzas universitarias y del procedimiento de aseguramiento de su calidad, se acordó el plazo de presentación para la solicitud de informe previo a la verificación de los títulos que se prevé impartir en el curso 2025-2026.

El órgano competente para la emisión del presente informe es la Dirección General de Coordinación Universitaria, de conformidad con lo previsto en el artículo 9 del Decreto 158/2022, de 9 de agosto, por el que se regula la estructura orgánica de la Consejería de Universidad, Investigación e Innovación, que al respecto dispone que le corresponde a este centro directivo el control, evaluación y seguimiento de la Programación Universitaria del Sistema Universitario Andaluz.

Dando cumplimiento en tiempo y forma a la Resolución de 8 de abril de 2024, de la Dirección General de Coordinación Universitaria, la Universidad de Málaga ha presentado la solicitud para la emisión de informe previo a verificación para los títulos universitarios que a continuación se relacionan:

1. Máster Universitario en Biotecnología y Biología Vegetal por la UNIA y la Universidad de Málaga.
2. Máster Universitario en Ciberseguridad por la Universidad de Málaga.
3. Máster Universitario en Derecho Digital por la Universidad de Almería, la Universidad de Cádiz, la Universidad de Córdoba, la Universidad de Málaga y la Universidad de Jaén.

4. Máster Universitario en Estudios Avanzados en Trabajo Social por la Universidad de Málaga.

5. Máster Universitario en Gestión Ejecutiva de Alojamientos Turísticos por la Universidad de Córdoba y la Universidad de Málaga.

6. Máster Universitario en Intervención e Investigación Logopédicas por la Universidad de Chile y Universidad de Málaga.

7. Máster Universitario en Materiales Avanzados por la Universidad de Alicante, Universidad Politécnica de Valencia, Universidad Autónoma de Madrid, Universidad de Zaragoza, Universidad de Barcelona, Universidad de Castilla La Mancha, Universidad de Málaga, Universidad Santiago de Compostela y Universidad de Valencia.

8. Máster Universitario en Salud Global por la Universidad de Almería, la Universidad de Islas Baleares y la Universidad de Málaga.

9. Máster Universitario en Tecnologías para el Mundo Conectado / MSc Connected World Technologies por la Universidad de Málaga.

10. Programa de Doctorado en Estudios Sociales y del Trabajo por la Universidad de Málaga.

Para la necesaria valoración sobre la necesidad y viabilidad académica y social de los títulos a implantar, y la adaptación del plan de estudios propuesto a la Programación Universitaria de Andalucía, aprobada por Orden de la Consejería de Universidad, Investigación e Innovación, el 7 de mayo de 2024 (BOJA núm. 93, de 15 de mayo), teniendo en cuenta las orientaciones estratégicas de la Universidad se han tenido en cuenta los criterios establecidos en el Anexo II del Decreto 154/2023, de 27 de junio:

- La afectación del nuevo título al tejido productivo andaluz, valorando para ello la impartición de títulos con formación dual.

-La justificación sobre la viabilidad de la nueva titulación.

- El equilibrio territorial en la oferta de enseñanzas.

- La valoración de la nueva enseñanza como título conjunto.

- La valoración de la nueva enseñanza como título internacional.

- El principio de especialización de la universidad y complementariedad de la programación universitaria.

- La suficiencia de recursos de personal e infraestructuras para la implantación de la nueva titulación.

- La solvencia y viabilidad económica para la puesta en marcha del nuevo plan de estudios.

- La impartición del nuevo título en un centro cuyo sistema de garantía de calidad esté certificado o que cuente con acreditación institucional.

- El calendario propuesto para la implantación de la nueva titulación.

De acuerdo con los criterios establecidos, y una vez analizada la solicitud y previa valoración de la viabilidad académica y social de los planes de estudios propuestos por la Universidad de Málaga, desde esta Dirección General de Coordinación Universitaria se informa lo siguiente:

Se emite informe FAVORABLE previo a la verificación para los títulos:

1. Máster Universitario en Biotecnología y Biología Vegetal por la UNIA y la Universidad de Málaga.
2. Máster Universitario en Ciberseguridad por la Universidad de Málaga.

3. Máster Universitario en Derecho Digital por la Universidad de Almería, la Universidad de Cádiz, la Universidad de Córdoba, la Universidad de Málaga y la Universidad de Jaén.

4. Máster Universitario en Estudios Avanzados en Trabajo Social por la Universidad de Málaga.

5. Máster Universitario en Gestión Ejecutiva de Alojamientos Turísticos por la Universidad de Córdoba y la Universidad de Málaga.

6. Máster Universitario en Intervención e Investigación Logopédicas por la Universidad de Chile y Universidad de Málaga.

7. Máster Universitario en Materiales Avanzados por la Universidad de Alicante, Universidad Politécnica de Valencia, Universidad Autónoma de Madrid, Universidad de Zaragoza, Universidad de Barcelona, Universidad de Castilla La Mancha, Universidad de Málaga, Universidad Santiago de Compostela y Universidad de Valencia.

8. Máster Universitario en Salud Global por la Universidad de Almería, la Universidad de Islas Baleares y la Universidad de Málaga.

9. Máster Universitario en Tecnologías para el Mundo Conectado / MSc Connected World Technologies por la Universidad de Málaga.

10. Programa de Doctorado en Estudios Sociales y del Trabajo por la Universidad de Málaga.

EL DIRECTOR GENERAL DE COORDINACIÓN UNIVERSITARIA