

IMPRESO SOLICITUD PARA VERIFICACIÓN DE TÍTULOS OFICIALES

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

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

UNIVERSIDAD SOLICITANTE	CENTRO	CÓDIGO CENTRO	
Universidad de Málaga	Escuela Técnica Superior de Ingeniería Informática	29012601	
NIVEL	DENOMINACIÓN CORTA		
Máster	Ciberseguridad		
DENOMINACIÓN ESPECÍFICA			
Máster Universitario en Ciberseguridad por la Universidad de Málaga			
NIVEL MECES			
3			
RAMA DE CONOCIMIENTO	ÁMBITO DE CONOCIMIENTO	CONJUNTO	
Ingeniería y Arquitectura	Ingeniería informática y de sistemas	No	
SOLICITANTE			
NOMBRE Y APELLIDOS	CARGO		
ROCIO PONCE ORTIZ	Vicerrectora		
REPRESENTANTE LEGAL			
NOMBRE Y APELLIDOS	CARGO		
ROCIO PONCE ORTIZ	Vicerrectora		
RESPONSABLE DEL TÍTULO			
NOMBRE Y APELLIDOS	CARGO		
MANUEL NICOLAS ENCISO GARCIA OLIVEROS	Director		
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
Vicerrectorado Doctorado y Posgrado. Pabellón de Gobierno. Campus de Teatinos	29071	Málaga	674237714
E-MAIL	PROVINCIA	FAX	
vrdp@uma.es	Málaga	952134297	
3. PROTECCIÓN DE DATOS PERSONALES			
De acuerdo con lo previsto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se informa que los datos solicitados en este impreso son necesarios para la tramitación de la solicitud y podrán ser objeto de tratamiento automatizado. La responsabilidad del fichero automatizado corresponde al Consejo de Universidades. Los solicitantes, como cedentes de los datos podrán ejercer ante el Consejo de Universidades los derechos de información, acceso, rectificación y cancelación a los que se refiere el Título III de la citada Ley Orgánica 3/2018, de 5 de diciembre, 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 43 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.			
		En: Málaga, AM 27 de septiembre de 2024	
		Firma: Representante legal de la Universidad	



1. DESCRIPCIÓN, OBJETIVOS FORMATIVOS Y JUSTIFICACIÓN DEL TÍTULO

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

NIVEL	DENOMINACIÓN ESPECÍFICA	CONJUNTO	CONVENIO	CONV. ADJUNTO
Máster	Máster Universitario en Ciberseguridad por la Universidad de Málaga	No		Ver Apartado 1: Anexo 1.
RAMA				
Ingeniería y Arquitectura				
ÁMBITO				
Ingeniería informática y de sistemas				
AGENCIA EVALUADORA				
Agencia para la Calidad Científica y Universitaria de Andalucía				
LISTADO DE ESPECIALIDADES				
No existen datos				
MENCIÓN DUAL				
Si				
ADJUNTO CONVENIO MENCIÓN DUAL				
Ver Apartado 1: Anexo 5.				

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

UNIVERSIDAD SOLICITANTE		
Universidad de Málaga		
LISTADO DE UNIVERSIDADES		
CÓDIGO	UNIVERSIDAD	
011	Universidad de Málaga	
LISTADO DE UNIVERSIDADES EXTRANJERAS		
CÓDIGO	UNIVERSIDAD	
No existen datos		
CRÉDITOS TOTALES	CRÉDITOS DE COMPLEMENTOS FORMATIVOS	CRÉDITOS EN PRÁCTICAS EXTERNAS
60		
CRÉDITOS OPTATIVOS	CRÉDITOS OBLIGATORIOS	CRÉDITOS TRABAJO FIN GRADO/ MÁSTER
18	30	12

1.4-1.9 Universidad de Málaga

1.4-1.9.1 CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS			
CÓDIGO	CENTRO	CENTRO RESPONSABLE	CENTRO ACREDITADO INSTITUCIONALMENTE
29012601	Escuela Técnica Superior de Ingeniería Informática	Si	No

1.4-1.9.2 Escuela Técnica Superior de Ingeniería Informática

1.4-1.9.2.1 Datos asociados al centro

MODALIDADES DE ENSEÑANZA EN LAS QUE SE IMPARTE EL TÍTULO		
PRESENCIAL	SEMPRESENCIAL/HÍBRIDA	A DISTANCIA/VIRTUAL
Sí	No	No
PLAZAS POR MODALIDAD		
25		



NÚMERO TOTAL DE PLAZAS	NÚMERO DE PLAZAS DE NUEVO INGRESO PARA PRIMER CURSO	
25	25	
IDIOMAS EN LOS QUE SE IMPARTE		
CASTELLANO	CATALÁN	EUSKERA
Sí	No	No
GALLEGO	VALENCIANO	INGLÉS
No	No	No
FRANCÉS	ALEMÁN	PORTUGUÉS
No	No	No
ITALIANO	OTRAS	
No	No	

1.10 JUSTIFICACIÓN

JUSTIFICACIÓN DEL INTERÉS DEL TÍTULO Y CONTEXTUALIZACIÓN

Ver Apartado 1: Anexo 6.

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

OBJETIVOS FORMATIVOS

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-em-pleo/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

1.14 PERFILES FUNDAMENTALES DE EGRESO Y PROFESIONES REGULADAS

PERFILES DE EGRESO

Profesional

HABILITA PARA EL EJERCICIO DE PROFESIONES REGULADAS

No

NO ES CONDICIÓN DE ACCESO PARA TÍTULO PROFESIONAL

2. RESULTADOS DEL PROCESO DE FORMACIÓN Y DE APRENDIZAJE

RESULTADOS DEL PROCESO DE FORMACIÓN Y DE APRENDIZAJE

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. TIPO: Conocimientos o contenidos

C02 - Al finalizar el aprendizaje, el alumnado será capaz de Identificar riesgos y amenazas que una organización puede afrontar en temas de ciberseguridad para poder seleccionar las mejores estrategias, políticas, técnicas que garanticen la protección de datos (almacenados, procesados o en tránsito), la fiabilidad y seguridad de los componentes, servicios, protocolos y aplicaciones. TIPO: Conocimientos o contenidos

C03 - Al finalizar el aprendizaje, el alumnado será capaz de identificar y analizar problemas y tareas complejas o indefinidas escogiendo las herramientas, tecnologías o metodologías más adecuadas para la obtención de soluciones innovadoras en el campo de la seguridad con especial énfasis en la seguridad desde el diseño. TIPO: Conocimientos o contenidos

C04 - Al finalizar el aprendizaje, el alumnado será capaz de reconocer y comparar aquellos procedimientos relacionados con la gestión continua de riesgos y amenazas, de cara a la integración de procesos para el análisis, correlación, manejo y respuesta de incidentes de ciberseguridad y su información asociada. TIPO: Conocimientos o contenidos

COM01 - 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. TIPO: Competencias

COM02 - 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. TIPO: Competencias

COM03 - 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. TIPO: Competencias

COM04 - 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. TIPO: Competencias

COM05 - 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. TIPO: Competencias

COM06 - 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. TIPO: Competencias

COM07 - 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. TIPO: Competencias

COM08 - 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. TIPO: Competencias

COM09 - 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. TIPO: Competencias

COM10 - 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. TIPO: Competencias



COM11 - 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 sintetizan las competencias adquiridas en las enseñanzas. TIPO: Competencias
COM12 - 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. TIPO: Competencias
COM13 - Llevar a cabo el tratamiento de la sostenibilidad y del cambio climático. TIPO: Competencias
COM14 - Comunicar de forma oral y escrita transmitiendo información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Competencias
COM15 - 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. TIPO: Competencias
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. TIPO: Habilidades o destrezas
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. TIPO: Habilidades o destrezas
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. TIPO: Habilidades o destrezas
HD04 - Al finalizar el aprendizaje, el alumnado será capaz de aplicar conceptos, arquitecturas y modelos avanzados de ciberseguridad en soluciones informáticas. TIPO: Habilidades o destrezas

3. ADMISIÓN, RECONOCIMIENTO Y MOVILIDAD

3.1 REQUISITOS DE ACCESO Y PROCEDIMIENTOS DE ADMISIÓN

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.

La comisión académica decidirá, según la titulación, formación y experiencia del alumnado, las asignaturas que deberá cursar como complementos formativos y que serán seleccionadas de entre las que se relacionan a continuación:

Asignatura	Titulación
Sistemas Operativos	Grado en Ingeniería Informática
Programación Avanzada II	Grado en Ingeniería Informática
Seguridad en Servicios y Protocolos de Internet	Grado en Ciberseguridad e Inteligencia Artificial
Bases de Datos	Grado en Ciberseguridad e Inteligencia Artificial
Ingeniería del Software Seguro	Grado en Ciberseguridad e Inteligencia Artificial



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.

Según el [Reglamento 8/2024 sobre matriculación de estudiantes en actividades formativas correspondientes a planes de estudios conducentes a títulos de carácter oficial de grado y máster universitario de la Universidad de Málaga](#), el estudiantado admitido de forma condicionada en el máster a través del procedimiento general de preinscripción del Distrito Único Universitario Andaluz, al que le reste por superar el TFG y como máximo hasta 9 créditos ECTS del grado que le ha dado acceso, podrá matricularse en dicho máster, si bien la matrícula se entenderá condicionada hasta la finalización de los estudios de grado, y pasará a ser definitiva cuando el estudiante acredite haber abonado los derechos de expedición del título de grado. En ningún caso se podrá obtener el título de máster universitario antes del título de grado que ha dado acceso al máster. El estudiantado de máster universitario con matrícula condicionada tendrá los mismos derechos y deberes que cualquier otro estudiante matriculado en un máster universitario de la Universidad de Málaga, si bien no se expedirán certificaciones académicas oficiales de estos estudios en tanto su matrícula sea condicionada.

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.

El número de plazas en alternancia se establece entre 5 y 10 dependiendo de las empresas y los perfiles de los estudiantes. La comisión mixta establecerá para cada estudiante la mención a realizar.

Para los estudiantes de matrícula condicionada se les considerará, en el expediente académico, la nota media de las asignaturas superadas a la hora de solicitar el ingreso.

3.2 CRITERIOS PARA EL RECONOCIMIENTO Y TRANSFERENCIAS DE CRÉDITOS

Reconocimiento de Créditos cursados en centros de formación profesional de grado superior

MÍNIMO	MÁXIMO
0	0

Adjuntar Convenio

Reconocimiento de Créditos Cursados en Títulos Propios

MÍNIMO	MÁXIMO
0	0

Adjuntar Título Propio

Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional

MÍNIMO	MÁXIMO
0	9

DESCRIPCIÓN

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

La norma reguladora de la Universidad de Málaga es el [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.](#)

Para este título se exige un mínimo de 6 meses de experiencia laboral y/o profesional, debidamente justificada, desarrollando actividades relacionadas con las asignaturas optativas. Cada crédito reconocido corresponderá a un



mínimo de dos meses de desempeño a tiempo completo. Los créditos reconocidos formarán parte de la bolsa de op-tatividad.

3.3 MOVILIDAD DE LOS ESTUDIANTES PROPIOS Y DE ACOGIDA

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

4.1 ESTRUCTURA BÁSICA DE LAS ENSEÑANZAS

DESCRIPCIÓN DEL PLAN DE ESTUDIOS

Ver Apartado 4: Anexo 1.

NIVEL 1: MÓDULO CRÉDITOS OBLIGATORIOS

4.1.1 Datos Básicos del Nivel 1

ECTS NIVEL1	30
-------------	----

NIVEL 2: Tecnologías Emergentes

4.1.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
----------	-------------

ECTS NIVEL 2	3
--------------	---

DESPLIEGUE TEMPORAL: Semestral

ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
------------------	------------------	------------------

3		
---	--	--

ECTS Semestral 4	ECTS Semestral 5	ECTS Semestral 6
------------------	------------------	------------------

ECTS Semestral 7	ECTS Semestral 8	ECTS Semestral 9
------------------	------------------	------------------

ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
-------------------	-------------------	-------------------

--	--	--

NIVEL 3: Seguridad en Computación Cuántica

4.1.1.1.1 Datos Básicos del Nivel 3

CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
----------	-----------------	---------------------

Obligatoria	3	Semestral
-------------	---	-----------

DESPLIEGUE TEMPORAL

ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
------------------	------------------	------------------

3		
---	--	--

ECTS Semestral 4	ECTS Semestral 5	ECTS Semestral 6
------------------	------------------	------------------

ECTS Semestral 7	ECTS Semestral 8	ECTS Semestral 9
------------------	------------------	------------------

--	--	--

ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
-------------------	-------------------	-------------------

--	--	--

4.1.1.2 RESULTADOS DE APRENDIZAJE

COM06 - 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. TIPO: Competencias

COM07 - 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. TIPO: Competencias

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. TIPO: Habilidades o destrezas



HD04 - Al finalizar el aprendizaje, el alumnado será capaz de aplicar conceptos, arquitecturas y modelos avanzados de ciberseguridad en soluciones informáticas. TIPO: Habilidades o destrezas		
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. TIPO: Habilidades o destrezas		
COM09 - 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. TIPO: Competencias		
COM10 - 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. TIPO: Competencias		
COM12 - 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. TIPO: Competencias		
COM13 - Llevar a cabo el tratamiento de la sostenibilidad y del cambio climático. TIPO: Competencias		
COM14 - Comunicar de forma oral y escrita transmitiendo información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Competencias		
COM15 - 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. TIPO: Competencias		
NIVEL 2: Dirección Estratégica en Ciberseguridad		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	13,5	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
4,5	9	
ECTS Semestral 4	ECTS Semestral 5	ECTS Semestral 6
ECTS Semestral 7	ECTS Semestral 8	ECTS Semestral 9
ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
NIVEL 3: Dirección y Gestión de la Ciberseguridad		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Obligatoria	4,5	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
4,5		
ECTS Semestral 4	ECTS Semestral 5	ECTS Semestral 6
ECTS Semestral 7	ECTS Semestral 8	ECTS Semestral 9
ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
NIVEL 3: Auditoría de Seguridad y Análisis de Riesgos		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Obligatoria	4,5	Semestral



DESPLIEGUE TEMPORAL		
ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
	4,5	
ECTS Semestral 4	ECTS Semestral 5	ECTS Semestral 6
ECTS Semestral 7	ECTS Semestral 8	ECTS Semestral 9
ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
NIVEL 3: Ciberinteligencia y Ciberdefensa		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Obligatoria	4,5	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
	4,5	
ECTS Semestral 4	ECTS Semestral 5	ECTS Semestral 6
ECTS Semestral 7	ECTS Semestral 8	ECTS Semestral 9
ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
4.1.1.2 RESULTADOS DE APRENDIZAJE		
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. TIPO: Conocimientos o contenidos		
C02 - Al finalizar el aprendizaje, el alumnado será capaz de Identificar riesgos y amenazas que una organización puede afrontar en temas de ciberseguridad para poder seleccionar las mejores estrategias, políticas, técnicas que garanticen la protección de datos (almacenados, procesados o en tránsito), la fiabilidad y seguridad de los componentes, servicios, protocolos y aplicaciones. TIPO: Conocimientos o contenidos		
C04 - Al finalizar el aprendizaje, el alumnado será capaz de reconocer y comparar aquellos procedimientos relacionados con la gestión continua de riesgos y amenazas, de cara a la integración de procesos para el análisis, correlación, manejo y respuesta de incidentes de ciberseguridad y su información asociada. TIPO: Conocimientos o contenidos		
COM03 - 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. TIPO: Competencias		
COM04 - 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. TIPO: Competencias		
COM06 - 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. TIPO: Competencias		
COM07 - 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. TIPO: Competencias		
COM08 - 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. TIPO: Competencias		
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. TIPO: Habilidades o destrezas		
HD04 - Al finalizar el aprendizaje, el alumnado será capaz de aplicar conceptos, arquitecturas y modelos avanzados de ciberseguridad en soluciones informáticas. TIPO: Habilidades o destrezas		
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. TIPO: Habilidades o destrezas		



COM01 - 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. TIPO: Competencias		
COM02 - 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. TIPO: Competencias		
COM05 - 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. TIPO: Competencias		
COM09 - 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. TIPO: Competencias		
COM10 - 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. TIPO: Competencias		
COM12 - 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. TIPO: Competencias		
COM13 - Llevar a cabo el tratamiento de la sostenibilidad y del cambio climático. TIPO: Competencias		
COM14 - Comunicar de forma oral y escrita transmitiendo información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Competencias		
COM15 - 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. TIPO: Competencias		
NIVEL 2: Seguridad en Entornos Software y Hardware		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	13,5	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
	13,5	
ECTS Semestral 4	ECTS Semestral 5	ECTS Semestral 6
ECTS Semestral 7	ECTS Semestral 8	ECTS Semestral 9
ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
NIVEL 3: Ciberseguridad en Aplicaciones y Servicios Telemáticos de Nueva Generación		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Obligatoria	4,5	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
	4,5	
ECTS Semestral 4	ECTS Semestral 5	ECTS Semestral 6
ECTS Semestral 7	ECTS Semestral 8	ECTS Semestral 9
ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
NIVEL 3: Seguridad en DevOps		
4.1.1.1.1 Datos Básicos del Nivel 3		



CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Obligatoria	4,5	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
	4,5	
ECTS Semestral 4	ECTS Semestral 5	ECTS Semestral 6
ECTS Semestral 7	ECTS Semestral 8	ECTS Semestral 9
ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
NIVEL 3: Seguridad en Sistemas HW y Ciberfísicos		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Obligatoria	4,5	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
	4,5	
ECTS Semestral 4	ECTS Semestral 5	ECTS Semestral 6
ECTS Semestral 7	ECTS Semestral 8	ECTS Semestral 9
ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
4.1.1.2 RESULTADOS DE APRENDIZAJE		
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. TIPO: Conocimientos o contenidos		
C02 - Al finalizar el aprendizaje, el alumnado será capaz de Identificar riesgos y amenazas que una organización puede afrontar en temas de ciberseguridad para poder seleccionar las mejores estrategias, políticas, técnicas que garanticen la protección de datos (almacenados, procesados o en tránsito), la fiabilidad y seguridad de los componentes, servicios, protocolos y aplicaciones. TIPO: Conocimientos o contenidos		
C03 - Al finalizar el aprendizaje, el alumnado será capaz de identificar y analizar problemas y tareas complejas o indefinidas escogiendo las herramientas, tecnologías o metodologías más adecuadas para la obtención de soluciones innovadoras en el campo de la seguridad con especial énfasis en la seguridad desde el diseño. TIPO: Conocimientos o contenidos		
COM04 - 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. TIPO: Competencias		
COM06 - 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. TIPO: Competencias		
COM07 - 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. TIPO: Competencias		
COM08 - 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. TIPO: Competencias		
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. TIPO: Habilidades o destrezas		
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. TIPO: Habilidades o destrezas		
HD04 - Al finalizar el aprendizaje, el alumnado será capaz de aplicar conceptos, arquitecturas y modelos avanzados de ciberseguridad en soluciones informáticas. TIPO: Habilidades o destrezas		



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. TIPO: Habilidades o destrezas		
COM02 - 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. TIPO: Competencias		
COM12 - 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. TIPO: Competencias		
COM13 - Llevar a cabo el tratamiento de la sostenibilidad y del cambio climático. TIPO: Competencias		
COM14 - Comunicar de forma oral y escrita transmitiendo información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Competencias		
COM15 - 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. TIPO: Competencias		
NIVEL 1: MÓDULO CRÉDITOS OPTATIVOS		
4.1.1 Datos Básicos del Nivel 1		
ECTS NIVEL1	36	
NIVEL 2: Tecnologías en Ciberseguridad		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
ECTS NIVEL 2	18	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
18		
ECTS Semestral 4	ECTS Semestral 5	ECTS Semestral 6
ECTS Semestral 7	ECTS Semestral 8	ECTS Semestral 9
ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
NIVEL 3: Gestión de Anomalías e Incidentes de Ciberseguridad		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Optativa	4,5	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
4,5		
ECTS Semestral 4	ECTS Semestral 5	ECTS Semestral 6
ECTS Semestral 7	ECTS Semestral 8	ECTS Semestral 9
ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
NIVEL 3: Diseño y Desarrollo de Software Seguro		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Optativa	4,5	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3



4,5		
ECTS Semestral 4	ECTS Semestral 5	ECTS Semestral 6
ECTS Semestral 7	ECTS Semestral 8	ECTS Semestral 9
ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
NIVEL 3: Técnicas de Pentesting y Análisis Forense		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Optativa	4,5	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
4,5		
ECTS Semestral 4	ECTS Semestral 5	ECTS Semestral 6
ECTS Semestral 7	ECTS Semestral 8	ECTS Semestral 9
ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
NIVEL 3: Análisis de Malware		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Optativa	4,5	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
4,5		
ECTS Semestral 4	ECTS Semestral 5	ECTS Semestral 6
ECTS Semestral 7	ECTS Semestral 8	ECTS Semestral 9
ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
4.1.1.2 RESULTADOS DE APRENDIZAJE		
C02 - Al finalizar el aprendizaje, el alumnado será capaz de Identificar riesgos y amenazas que una organización puede afrontar en temas de ciberseguridad para poder seleccionar las mejores estrategias, políticas, técnicas que garanticen la protección de datos (almacenados, procesados o en tránsito), la fiabilidad y seguridad de los componentes, servicios, protocolos y aplicaciones. TIPO: Conocimientos o contenidos		
C03 - Al finalizar el aprendizaje, el alumnado será capaz de identificar y analizar problemas y tareas complejas o indefinidas escogiendo las herramientas, tecnologías o metodologías más adecuadas para la obtención de soluciones innovadoras en el campo de la seguridad con especial énfasis en la seguridad desde el diseño. TIPO: Conocimientos o contenidos		
COM06 - 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. TIPO: Competencias		
HD04 - Al finalizar el aprendizaje, el alumnado será capaz de aplicar conceptos, arquitecturas y modelos avanzados de ciberseguridad en soluciones informáticas. TIPO: Habilidades o destrezas		
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. TIPO: Habilidades o destrezas		
COM02 - 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. TIPO: Competencias		
COM05 - 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. TIPO: Competencias		
COM09 - 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. TIPO: Competencias

COM10 - 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. TIPO: Competencias

COM12 - 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. TIPO: Competencias

COM13 - Llevar a cabo el tratamiento de la sostenibilidad y del cambio climático. TIPO: Competencias

COM14 - Comunicar de forma oral y escrita transmitiendo información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Competencias

COM15 - 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. TIPO: Competencias

NIVEL 2: Formación en Alternancia

4.1.1.1 Datos Básicos del Nivel 2

CARÁCTER	Optativa
ECTS NIVEL 2	18

DESPLIEGUE TEMPORAL: Semestral

ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
18		
ECTS Semestral 4	ECTS Semestral 5	ECTS Semestral 6
ECTS Semestral 7	ECTS Semestral 8	ECTS Semestral 9
ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12

NIVEL 3: Formación en Alternancia

4.1.1.1.1 Datos Básicos del Nivel 3

CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Optativa	18	Semestral

DESPLIEGUE TEMPORAL

ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
18		
ECTS Semestral 4	ECTS Semestral 5	ECTS Semestral 6
ECTS Semestral 7	ECTS Semestral 8	ECTS Semestral 9
ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12

4.1.1.2 RESULTADOS DE APRENDIZAJE

C02 - Al finalizar el aprendizaje, el alumnado será capaz de Identificar riesgos y amenazas que una organización puede afrontar en temas de ciberseguridad para poder seleccionar las mejores estrategias, políticas, técnicas que garanticen la protección de datos (almacenados, procesados o en tránsito), la fiabilidad y seguridad de los componentes, servicios, protocolos y aplicaciones. TIPO: Conocimientos o contenidos

C03 - Al finalizar el aprendizaje, el alumnado será capaz de identificar y analizar problemas y tareas complejas o indefinidas escogiendo las herramientas, tecnologías o metodologías más adecuadas para la obtención de soluciones innovadoras en el campo de la seguridad con especial énfasis en la seguridad desde el diseño. TIPO: Conocimientos o contenidos

COM06 - 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. TIPO: Competencias

HD04 - Al finalizar el aprendizaje, el alumnado será capaz de aplicar conceptos, arquitecturas y modelos avanzados de ciberseguridad en soluciones informáticas. TIPO: Habilidades o destrezas



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. TIPO: Habilidades o destrezas		
COM02 - 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. TIPO: Competencias		
COM05 - 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. TIPO: Competencias		
COM09 - 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. TIPO: Competencias		
COM10 - 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. TIPO: Competencias		
COM12 - 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. TIPO: Competencias		
COM13 - Llevar a cabo el tratamiento de la sostenibilidad y del cambio climático. TIPO: Competencias		
COM14 - Comunicar de forma oral y escrita transmitiendo información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Competencias		
COM15 - 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. TIPO: Competencias		
NIVEL 1: MÓDULO TRABAJO FIN DE MÁSTER		
4.1.1 Datos Básicos del Nivel 1		
ECTS NIVEL1	12	
NIVEL 2: Trabajo Fin de Máster		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Trabajo Fin de Grado / Máster	
ECTS NIVEL 2	12	
DESPLIEGUE TEMPORAL: Anual		
ECTS Anual 1	ECTS Anual 2	ECTS Anual 3
12		
ECTS Anual 4	ECTS Anual 5	ECTS Anual 6
NIVEL 3: Trabajo Fin de Máster		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Trabajo Fin de Grado / Máster	12	Anual
DESPLIEGUE TEMPORAL		
ECTS Anual 1	ECTS Anual 2	ECTS Anual 3
12		
ECTS Anual 4	ECTS Anual 5	ECTS Anual 6
4.1.1.2 RESULTADOS DE APRENDIZAJE		
COM11 - 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. TIPO: Competencias		



COM12 - 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. TIPO: Competencias

COM13 - Llevar a cabo el tratamiento de la sostenibilidad y del cambio climático. TIPO: Competencias

COM14 - Comunicar de forma oral y escrita transmitiendo información, ideas, problemas y soluciones a un público tanto especializado como no especializado. TIPO: Competencias

COM15 - 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. TIPO: Competencias

4.2 ACTIVIDADES Y METODOLOGÍAS DOCENTES

ACTIVIDADES FORMATIVAS

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.

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.

METODOLOGÍAS DOCENTES

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

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
4.4 ESTRUCTURAS CURRICULARES ESPECÍFICAS		



5. PERSONAL ACADÉMICO Y DE APOYO A LA DOCENCIA

PERSONAL ACADÉMICO
Ver Apartado 5: Anexo 1.
OTROS RECURSOS HUMANOS
Ver Apartado 5: Anexo 2.

6. RECURSOS MATERIALES E INFRAESTRUCTURALES, PRÁCTICAS Y SERVICIOS

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

7. CALENDARIO DE IMPLANTACIÓN

7.1 CRONOGRAMA DE IMPLANTACIÓN	
CURSO DE INICIO	2025
Ver Apartado 7: Anexo 1.	
7.2 PROCEDIMIENTO DE ADAPTACIÓN	
No aplica procedimiento de adaptación	
7.3 ENSEÑANZAS QUE SE EXTINGUEN	
CÓDIGO	ESTUDIO - CENTRO

8. SISTEMA INTERNO DE GARANTÍA DE LA CALIDAD Y ANEXOS

8.1 SISTEMA INTERNO DE GARANTÍA DE LA CALIDAD	
ENLACE	https://www.uma.es/etsi-informatica/cms/base/ver/base/basecontent/10759/plan-de-calidad/
8.2 INFORMACIÓN PÚBLICA	

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.

Normativas de la Universidad de Málaga de aplicación al título.

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.

8.3 ANEXOS

Ver Apartado 8: Anexo 1.

PERSONAS ASOCIADAS A LA SOLICITUD

RESPONSABLE DEL TÍTULO

CARGO	NOMBRE	PRIMER APELLIDO	SEGUNDO APELLIDO
Director	MANUEL NICOLAS	ENCISO	GARCIA OLIVEROS
DOMICILIO	CÓDIGO POSTAL	PROVINCIA	MUNICIPIO
E.T.S. Ingeniería Informática. Campus de Teatinos	29071	Málaga	Málaga
EMAIL	FAX		
director@informatica.uma.es	952132675		

REPRESENTANTE LEGAL

CARGO	NOMBRE	PRIMER APELLIDO	SEGUNDO APELLIDO
Vicerrectora	ROCIO	PONCE	ORTIZ
DOMICILIO	CÓDIGO POSTAL	PROVINCIA	MUNICIPIO
Vicerrectorado Doctorado y Posgrado. Pabellón de Gobierno. Campus de Teatinos	29071	Málaga	Málaga
EMAIL	FAX		
vrp@uma.es	952134297		

El Rector de la Universidad no es el Representante Legal

Ver Personas asociadas a la solicitud: Anexo 1.

SOLICITANTE

El responsable del título no es el solicitante

CARGO	NOMBRE	PRIMER APELLIDO	SEGUNDO APELLIDO
Vicerrectora	ROCIO	PONCE	ORTIZ
DOMICILIO	CÓDIGO POSTAL	PROVINCIA	MUNICIPIO
Vicerrectorado Doctorado y Posgrado. Pabellón de Gobierno. Campus de Teatinos	29071	Málaga	Málaga
EMAIL	FAX		
ordaca@uma.es	952134298		

INFORME PREVIO DE LA COMUNIDAD AUTÓNOMA

Informe previo de la Comunidad Autónoma: Ver Apartado Informe previo de la Comunidad Autónoma: Anexo 1.



Apartado 1: Anexo 5

Nombre : Documentos Mención Dual Máster Ciberseguridad.pdf

HASH SHA1 : E46EB2718C8C558012D5D544E4A0F4F265A4B40F

Código CSV : 805517945475104747656112

Ver Fichero: Documentos Mención Dual Máster Ciberseguridad.pdf



Apartado 1: Anexo 6

Nombre :1_Justificación.pdf

HASH SHA1 :7BCA8CEB65531AE990D8C917C3A35879FE058C1A

Código CSV :862221513091775075600265

Ver Fichero: 1_Justificación.pdf



Apartado 4: Anexo 1

Nombre :4_Planificación enseñanzas.pdf

HASH SHA1 :23AF689EE33590A8A355C08CB66E7DCA1382B6AB

Código CSV :862450176148581005692097

Ver Fichero: 4_Planificación enseñanzas.pdf



Apartado 5: Anexo 1

Nombre :5.1_Personal académico.pdf

HASH SHA1 :817217E4AB63400BCC948762C16B924F1686D846

Código CSV :862235075355243236528781

Ver Fichero: 5.1_Personal académico.pdf



Apartado 5: Anexo 2

Nombre :5.2_Otros recursos humanos.pdf

HASH SHA1 :2E9276F98DE3357F29672AA68376B235CB5E7820

Código CSV :862235134086910573388945

Ver Fichero: 5.2_Otros recursos humanos.pdf



Apartado 6: Anexo 1

Nombre :6_Recursos materiales.pdf

HASH SHA1 :3E225B4E6352E534BDE92757FF16E6B3C9AAD9D3

Código CSV :862235268000582402903937

Ver Fichero: 6_Recursos materiales.pdf



Apartado 7: Anexo 1

Nombre :7_Calendario implantación.pdf

HASH SHA1 :A1AB8FABD07767FA6C0CE1545B03A6EF8BC8D5E0

Código CSV :862235371900275656044858

Ver Fichero: 7_Calendario implantación.pdf



Apartado 8: Anexo 1

Nombre :8.3_Respuesta informe provisional.pdf

HASH SHA1 :E895A2707778A94879633EE4160949383FC635E4

Código CSV :862376019058869414875883

Ver Fichero: 8.3_Respuesta informe provisional.pdf



Apartado Personas asociadas a la solicitud: Anexo 1

Nombre :Delegación firma_Rocío Ponce_verificación y modificación planes estudio.pdf

HASH SHA1 :2B617E52AC949035AB76FF70FBA5215DE7119D70

Código CSV :801062732248639301917226

Ver Fichero: Delegación firma_Rocío Ponce_verificación y modificación planes estudio.pdf



Apartado Informe previo de la Comunidad Autónoma: Anexo 1

Nombre :INFORME PREVIO VERIFICACION JULIO 2024.pdf

HASH SHA1 :987EE99C7A93F9B5697C0E3A992C6FF1775A6B9F

Código CSV :801058802578100469269166

Ver Fichero: INFORME PREVIO VERIFICACION JULIO 2024.pdf



