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 Salamanca	Facultad de Derecho	37007924

NIVEL	DENOMINACIÓN CORTA
Máster	Cibercriminalidad

DENOMINACIÓN ESPECÍFICA
Máster Universitario en Cibercriminalidad por la Universidad de Salamanca

NIVEL MECES
3

RAMA DE CONOCIMIENTO	CAMPO DE ESTUDIO	CONJUNTO
Ciencias Sociales y Jurídicas	Derecho y especialidades jurídicas	No

SOLICITANTE

NOMBRE Y APELLIDOS	CARGO
Javier Peña González	Director Académico de Postgrado

REPRESENTANTE LEGAL

NOMBRE Y APELLIDOS	CARGO
María Teresa Escribano Bailón	Delegada del Rector para Estudios de Postgrado y Formación Permanente

RESPONSABLE DEL TÍTULO

NOMBRE Y APELLIDOS	CARGO
Federico Bueno de Mata	Director del Máster

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
Hospedería Fonseca, Fonseca, nº 2, 1ª planta	37002	Salamanca	686443690
E-MAIL	**PROVINCIA**		**FAX**
delegadapostgrado@usal.es	Salamanca		

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: Salamanca, AM 30 de septiembre de 2024
	Firma: Representante legal de la Universidad

1. DESCRIPCIÓN, OBJETIVOS FORMATIVOS Y JUSTIFICACIÓN DEL TÍTULO

1.1-1.3 DENOMINACIÓN, CAMPO DE ESTUDIO, MENCIONES/ESPECIALIDADES Y OTROS DATOS BÁSICOS

NIVEL	DENOMINACIÓN ESPECIFICA	CONJUNTO	CONVENIO	CONV. ADJUNTO
Máster	Máster Universitario en Cibercriminalidad por la Universidad de Salamanca	No		Ver Apartado 1: Anexo 1.

RAMA
Ciencias Sociales y Jurídicas
CAMPO DE ESTUDIO
Derecho y especialidades jurídicas
AGENCIA EVALUADORA
Agencia para la Calidad del Sistema Universitario de Castilla y León
LISTADO DE ESPECIALIDADES
Especialidad en Aspectos jurídicos de la cibercriminalidad
Especialidad en Aspectos criminológicos de la cibercriminalidad
MENCIÓN DUAL
No

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

UNIVERSIDAD SOLICITANTE	
Universidad de Salamanca	
LISTADO DE UNIVERSIDADES	
CÓDIGO	**UNIVERSIDAD**
014	Universidad de Salamanca
LISTADO DE UNIVERSIDADES EXTRANJERAS	
CÓDIGO	**UNIVERSIDAD**
No existen datos	

CRÉDITOS TOTALES	CRÉDITOS DE COMPLEMENTOS FORMATIVOS	CRÉDITOS EN PRÁCTICAS EXTERNAS
60	0	0
CRÉDITOS OPTATIVOS	**CRÉDITOS OBLIGATORIOS**	**CRÉDITOS TRABAJO FIN GRADO/ MÁSTER**
18	36	6

1.4-1.9 Universidad de Salamanca

1.4-1.9.1 CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS			
CÓDIGO	**CENTRO**	**CENTRO RESPONSABLE**	**CENTRO ACREDITADO INSTITUCIONALMENTE**
37007924	Facultad de Derecho	Si	No

1.4-1.9.2 Facultad de Derecho

1.4-1.9.2.1 Datos asociados al centro

MODALIDADES DE ENSEÑANZA EN LAS QUE SE IMPARTE EL TITULO		
PRESENCIAL	**SEMIPRESENCIAL/HÍBRIDA**	**A DISTANCIA/VIRTUAL**
Sí	No	No
PLAZAS POR MODALIDAD		
30		
NÚMERO TOTAL DE PLAZAS	**NÚMERO DE PLAZAS DE NUEVO INGRESO PARA PRIMER CURSO**	

30	30	
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

1.3.1.a) Principales objetivos formativos del título

Este MU pretende formar de un modo teórico, práctico y técnico, a profesionales, tanto en el ámbito criminológico como jurídico, para poder enfrentarse laboralmente al estudio, investigación, persecución y tratamiento de las diferentes manifestaciones de la ciberdelincuencia, así como a las consecuencias desencadenadas por ésta, como la reparación del daño ocasionado, la atención a las víctimas, la reinserción de los ciberdelincuentes, entre otras cuestiones.

Los principales objetivos formativos del título son:

- Proporcionar una formación avanzada y multidisciplinar sobre el fenómeno de la cibercriminalidad, desde la doble perspectiva de la víctima y del delincuente, con la finalidad de comprender el ciberdelito en su totalidad en la sociedad digitalizada actual y futura.
- Formar criminólogos/as y juristas capaces de actuar ante las particularidades delictivas de la cibercriminalidad, atendiendo al conjunto de rasgos que caracterizan a las víctimas, a los victimarios y a la sociedad actual.
- Formar profesionales que se enfrenten al fenómeno de la cibercriminalidad desde diferentes perspectivas, contribuyendo al desarrollo de los estudios en cibercriminalidad, a su investigación social, psicológica y jurídica, a su persecución y represión, y al tratamiento y cese de determinados resultados.
- Ofrecer a las y a los estudiantes un entorno de aprendizaje teórico-práctico que favorezca la actuación ante diferentes tipologías de cibercriminalidad, posibilitando la exposición y defensa de desarrollos y aplicaciones de ideas de forma crítica.

1.3.1.b) Objetivos formativos de las especialidades

OBJETIVOS DE LA ESPECIALIDAD EN ASPECTOS JURÍDICOS DE LA CIBERCRIMINALIDAD

- Formar profesionales con conocimientos avanzados y especializados en investigación y enjuiciamiento de la cibercriminalidad (profesionales de la judicatura, asesoría jurídica, auditoría y seguridad informática, entre otros)
- Formar abogados/as, procuradores/as y peritos/as en el marco de la defensa de las garantías, derechos y en materia de prueba, para que sean capaces de intervenir en procesos incoados por motivo de un ciberdelito, incluyendo el ámbito internacional.

OBJETIVOS DE LA ESPECIALIDAD EN ASPECTOS CRIMINOLÓGICOS DE LA CIBERCRIMINALIDAD

- Formar criminólogos/as con conocimientos avanzados y especializados en el análisis y evaluación de la cibercriminalidad, y en la elaboración de planes y políticas de prevención e intervención.
- Formar expertos capaces de atender de modo profesional a las víctimas y a los autores de la cibercriminalidad, poniendo especial énfasis en los agentes del sistema policial y judicial.

ESTRUCTURAS CURRICULARES ESPECÍFICAS Y ESTRATEGIAS METODOLÓGICAS DE INNOVACIÓN DOCENTE

1.14 PERFILES FUNDAMENTALES DE EGRESO Y PROFESIONES REGULADAS

PERFILES DE EGRESO		
Ver perfiles de egreso al final del apdo 1.1 Justificación		
HABILITA PARA EL EJERCICIO DE PROFESIONES REGULADAS	No	
NO ES CONDICIÓN DE ACCESO PARA TITULO PROFESIONAL		

2. RESULTADOS DEL PROCESO DE FORMACIÓN Y DE APRENDIZAJE

RESULTADOS DEL PROCESO DE FORMACIÓN Y DE APRENDIZAJE
C1 - Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática. TIPO: Conocimientos o contenidos
C10. E2 - Evaluar las particularidades de las víctimas en este tipo de criminalidad y las necesidades de intervención que se derivan tras estos delitos. TIPO: Conocimientos o contenidos

C2 - Examinar el funcionamiento de las tecnologías disruptivas utilizadas por delincuentes y por profesionales que actúan ante la cibercriminalidad, así como los principios básicos de ciberespacio. TIPO: Conocimientos o contenidos
C3 - Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada. TIPO: Conocimientos o contenidos
C4 - Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos. TIPO: Conocimientos o contenidos
C5 - Interpretar la normativa nacional e internacional que regula la ciberdelincuencia, así como las funciones de autoridades y profesionales en el marco de detección, prevención, actuación e intervención en casos de ciberdelincuencia. TIPO: Conocimientos o contenidos
C6 - Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos. TIPO: Conocimientos o contenidos
C7 - Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica TIPO: Conocimientos o contenidos
C8. E1 - Seleccionar conocimientos jurídicos especializados de los diferentes tipos de ciberdelincuencia para poder asesorar a los profesionales que intervienen en el proceso penal, así como a otras instituciones públicas o privadas. TIPO: Conocimientos o contenidos
C9. E2 - Comparar conocimientos específicos para elaborar estudios e informes criminológicos en el ámbito de la ciberdelincuencia y profundizar en las teorías criminológicas que explican el delito en el ciberespacio, así como otros factores relacionados con el proceso penal. TIPO: Conocimientos o contenidos
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas
H10. E2 - Desarrollar estrategias de prevención e intervención ante ciberataques u otro tipo de ciberdelitos, razonando y argumentando la propuesta con un enfoque interdisciplinar y teniendo en cuenta las particularidades de las víctimas para que la propuesta responda a las necesidades de éstas. TIPO: Habilidades o destrezas
H2 - Identificar el funcionamiento técnico de las ciberamenazas y ciberdelitos, en relación con las herramientas técnicas y legales disponibles para su cese y represión. TIPO: Habilidades o destrezas
H3 - Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos. TIPO: Habilidades o destrezas
H4 - Evaluar la viabilidad de diferentes herramientas y medidas de investigación en atención al tipo de delictivo presentado, las autoridades involucradas y el momento procesal del caso. TIPO: Habilidades o destrezas
H5 - Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos. TIPO: Habilidades o destrezas
H6 - Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad. TIPO: Habilidades o destrezas
H7. E1 - Ante casos específicos de ciberdelincuencia, elaborar, exponer y defender una solución jurídicamente fundamentada y adecuada al caso, de la que se deriven actuaciones concretas ante el delito. TIPO: Habilidades o destrezas
H8. E1 - Argumentar los derechos, garantías y principios que deben primar en atención al tipo delictivo concreto, así como las autoridades competentes para la práctica de diferentes funciones TIPO: Habilidades o destrezas
H9. E2 - Ante casos específicos de cibercriminalidad, elaborar, exponer y defender informes criminológicos jurídicamente fundamentados adecuados al caso y en relación con las exigencias procedimentales. TIPO: Habilidades o destrezas
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias
K10. E2 - Determinar, tras su evaluación, el tratamiento individualizado de las víctimas de un cibercrimen, así como planes de prevención para hacer frente a los riesgos derivados de este tipo de criminalidad en diferentes sectores de la población. TIPO: Competencias
K2 - Aprender a actualizar de modo autónomo los conocimientos sobre las últimas tecnologías y herramientas de seguridad informática. TIPO: Competencias
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias
K4 - Aplicar el ordenamiento jurídico español y la normativa internacional, con todas las garantías, ante riesgos, amenazas y ciberdelitos concretos. TIPO: Competencias

K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias
K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias
K7. E1 - Seleccionar los conocimientos específicos y cualidades más idóneos necesarios para garantizar y salvaguardar los derechos y principios jurídicos que favorezcan la intervención eficaz de diferentes autoridades en casos de ciberdelincuencia nacional e internacional. TIPO: Competencias
K8. E1 - Realizar análisis críticos, auditorías y asesoramiento jurídico ante ciberamenazas, ciberataques u otro tipo de riesgos detectados. TIPO: Competencias
K9. E2 - Elaborar informes criminológicos relacionados con el ciberdelito, en los que se seleccione los conocimientos específicos y las cualidades más idóneos y en los que se identifiquen los factores que favorecen la criminalidad y se defina y reconstruya el modus operandi o la actuación posterior. TIPO: Competencias

3. ADMISIÓN, RECONOCIMIENTO Y MOVILIDAD

3.1 REQUISITOS DE ACCESO Y PROCEDIMIENTOS DE ADMISIÓN

3.1 Requisitos de acceso y procedimientos de admisión de estudiantes

3.1.a) Requisitos de acceso

El perfil de ingreso recomendado es el de aquellas personas en posesión de ~~un grado en alguna de~~ los siguientes grados~~ en ciencias sociales y/o jurídicas, además de técnico~~:

- Grado en Criminología
- Grado en Derecho
- ~~Grado en Ingeniería Informática~~
- ~~Grado en Psicología~~
- ~~Grado en Sociología~~
- ~~Grado en Trabajo Social~~

En caso de que haya plazas disponibles se valorará la posibilidad de admitir estudiantes de otros grados que tengan relación con los perfiles de egreso en este MU en Cibercriminalidad **y que cuenten con la formación básica necesaria para poder cumplir con la programación prevista.**

Este Máster Universitario está dirigido preferentemente a Graduados/as en Criminología y en Derecho~~, y, en menor medida a Graduados/as en Ingeniería Informática, en Psicología, en Sociología y en Trabajo Social;~~ con buen expediente académico. Además, se precisa:

- Tener un nivel de español, en aquellos casos en que su lengua materna no sea este idioma, de ~~C1~~ **B2** del Marco Común Europeo de Referencia para Lenguas (MCERL).
- Tener al menos un nivel de inglés científico, equivalente al nivel B2 del Marco Común Europeo de Referencia para Lenguas (MCERL) para el manejo de bibliografía en este idioma.
- Tener interés por el estudio, persecución y tratamiento de la ciberdelincuencia

Para el acceso al máster se tendrá en cuenta lo establecido en el artículo 18 del Real Decreto 822/2021, de 28 de septiembre, que señala que #la posesión de un título universitario oficial de Graduada o Graduado español o equivalente es condición para acceder a un Máster Universitario, o en su caso disponer de otro título de Máster Universitario, o títulos del mismo nivel que el título español de Grado o Máster expedidos por universidades e instituciones de educación superior de un país del EEES que en dicho país permita el acceso a los estudios de Máster. Una explicación detallada aparece en la web https://www.usal.es/preinscripcion-masteres

De igual modo, podrán acceder a un Máster Universitario del sistema universitario español personas en posesión de títulos procedentes de sistemas educativos que no formen parte del EEES, que equivalgan al título de Grado, sin necesidad de homologación del título, pero sí de comprobación por parte de la universidad del nivel de formación que implican, siempre y cuando en el país donde se haya expedido dicho título permita acceder a estudios de nivel de postgrado universitario. En ningún caso el acceso por esta vía implicará la homologación del título previo del que disponía la persona interesada ni su reconocimiento a otros efectos que el de realizar los estudios de Máster#.

Por otro lado, es imprescindible dominar el español que es la lengua básica sobre la que se desarrollará la docencia. En caso de que su lengua materna no sea el español, será obligatorio la acreditación documental del nivel B2 del Marco Común Europeo de Referencia para Lenguas (MECERL).#

En este título no hay pruebas especiales de acceso.

3.1.b) Procedimiento y criterios de admisión

Las personas interesadas en la admisión en el máster deberán formalizar la correspondiente solicitud, acreditando que están en posesión de alguno de los títulos que permite el ingreso en estos estudios de postgrado (consultar el siguiente enlace **http://www.usal.es/preinscripcion-Másteres**). La solicitud debe ir acompañada de la siguiente documentación: expediente académico y título del Grado que permite el acceso al máster (valorándose de manera preferente aquellos expedientes con una nota media mínima de 7/10 puntos); acreditación, en su caso, de experiencia profesional relacionada con el contenido del máster; carta de motivación; y acreditación de un nivel ~~C1~~ B2 de dominio del español en el caso de hablantes no nativos. Se recomienda presentar Currículum Vitae que refleje los méritos y carta de recomendación.

La admisión de los estudiantes, hasta completar las plazas ofertadas, se realizará atendiendo al orden que se ocupe en un listado (ordenado de mayor a menor puntuación), resultante de la aplicación de los siguientes criterios de valoración objetiva:

1. Adecuación de la titulación (40%), **Grado en Derecho y Grado en Criminología**. ~~con el siguiente orden de prelación:~~
   a. ~~Grado en Criminología o en Derecho (4 puntos)~~

b. ~~Grado en Ingeniería informática, Psicología, Sociología o Trabajo social (3 puntos)~~
c. ~~Otras titulaciones 0-2 puntos en atención a la relación con la formación del MU~~

2. Expediente académico (40%)
3. Otros méritos (formación complementaria, investigación previa, idiomas, experiencia profesional relacionada con el MU) (20%)

La Comisión Académica del Título será la responsable de realizar la selección de las preinscripciones, con base en todos los criterios mencionados. Estará formada por el director/a de la titulación, tres docentes y un estudiante del título.

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
1	6

Adjuntar Título Propio

Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional

MÍNIMO	MÁXIMO
3	9

DESCRIPCIÓN

3.2 Criterios para el reconocimiento y transferencia de créditos

Para el reconocimiento de créditos se seguirá lo establecido en el artículo 10 del RD 822/2021, tal como se refleja en las Normas sobre Reconocimiento y Transferencia de Créditos de la Universidad de Salamanca, aprobadas por el Consejo de Gobierno en su sesión de 24/03/2023.

Para ello, establece en su art. 22.1 que la Comisión Académica del Máster debe aprobar la composición de la Comisión de Transferencia y Reconocimiento de Créditos (COTRARET) del Máster. La Comisión Académica, como máximo órgano de decisión en la que se encuentran representados los diferentes sectores del Máster Universitario en Criminalidad diseñará unas normas sobre composición y funcionamiento de su propia COTRARET.

Reconocimiento de ECTS cursados por Acreditación de Experiencia Laboral y Profesional

Nº mínimo de ECTS reconocidos: 3

Nº máximo de ECTS reconocidos: 9

La experiencia laboral y profesional acreditada podrá ser reconocida en forma de créditos académicos, siempre que dicha experiencia esté claramente relacionada con los conocimientos, habilidades y competencias especificadas en el plan de estudios. Como norma general, se podrá reconocer hasta un crédito ECTS por cada cuarenta horas de experiencia laboral o profesional acreditada.

Reconocimiento de ECTS cursados en Títulos Propios (TP) o de formación permanente

Nº mínimo ECTS reconocidos: 1

Nº máximo ECTS reconocidos: 6

3.3 MOVILIDAD DE LOS ESTUDIANTES PROPIOS Y DE ACOGIDA

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

En este título no se establecen programas de movilidad específicos. De hecho, no está previsto que se produzca la movilidad de los estudiantes durante el mismo ya que no es necesario para alcanzar los resultados de aprendizaje previstos. No obstante, si en un futuro se firman convenios de movilidad, estos atenderán a la Normativa de movilidad académica internacional de estudiantes de la USAL, disponible en **https://rel-int.usal.es/es/**

4. PLANIFICACIÓN DE LAS ENSEÑANZAS

4.1 ESTRUCTURA BÁSICA DE LAS ENSEÑANZAS		
DESCRIPCIÓN DEL PLAN DE ESTUDIOS		
Ver Apartado 4: Anexo 1.		
4.1 SIN NIVEL 1		
NIVEL 2: Aspectos legales de la ciberdelincuencia		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
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**
NO CONSTAN ELEMENTOS DE NIVEL 3		
4.1.1.2 RESULTADOS DE APRENDIZAJE		
C1 - Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática. TIPO: Conocimientos o contenidos		
C4 - Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos. TIPO: Conocimientos o contenidos		
C5 - Interpretar la normativa nacional e internacional que regula la ciberdelincuencia, así como las funciones de autoridades y profesionales en el marco de detección, prevención, actuación e intervención en casos de ciberdelincuencia. TIPO: Conocimientos o contenidos		
C6 - Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos. TIPO: Conocimientos o contenidos		
C7 - Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica TIPO: Conocimientos o contenidos		
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas		
H2 - Identificar el funcionamiento técnico de las ciberamenazas y ciberdelitos, en relación con las herramientas técnicas y legales disponibles para su cese y represión. TIPO: Habilidades o destrezas		
H3 - Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos. TIPO: Habilidades o destrezas		
H4 - Evaluar la viabilidad de diferentes herramientas y medidas de investigación en atención al tipo de delictivo presentado, las autoridades involucradas y el momento procesal del caso. TIPO: Habilidades o destrezas		
H6 - Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad. TIPO: Habilidades o destrezas		
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias		
K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias		
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias		
K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias		

K7. E1 - Seleccionar los conocimientos específicos y cualidades más idóneos necesarios para garantizar y salvaguardar los derechos y principios jurídicos que favorezcan la intervención eficaz de diferentes autoridades en casos de ciberdelincuencia nacional e internacional. TIPO: Competencias		
NIVEL 2: Ciberdelincuencia y Derecho penal		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
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**
NO CONSTAN ELEMENTOS DE NIVEL 3		
4.1.1.2 RESULTADOS DE APRENDIZAJE		
C1 - Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática. TIPO: Conocimientos o contenidos		
C3 - Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada. TIPO: Conocimientos o contenidos		
C7 - Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica TIPO: Conocimientos o contenidos		
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas		
H3 - Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos. TIPO: Habilidades o destrezas		
H5 - Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos. TIPO: Habilidades o destrezas		
H6 - Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad. TIPO: Habilidades o destrezas		
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias		
K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias		
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias		
K4 - Aplicar el ordenamiento jurídico español y la normativa internacional, con todas las garantías, ante riesgos, amenazas y ciberdelitos concretos. TIPO: Competencias		
K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias		
NIVEL 2: Fundamentos de la Seguridad Informática		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
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**
NO CONSTAN ELEMENTOS DE NIVEL 3		
4.1.1.2 RESULTADOS DE APRENDIZAJE		
C1 - Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática. TIPO: Conocimientos o contenidos		
C2 - Examinar el funcionamiento de las tecnologías disruptivas utilizadas por delincuentes y por profesionales que actúan ante la cibercriminalidad, así como los principios básicos de ciberespacio. TIPO: Conocimientos o contenidos		
C3 - Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada. TIPO: Conocimientos o contenidos		
C4 - Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos. TIPO: Conocimientos o contenidos		
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas		
H2 - Identificar el funcionamiento técnico de las ciberamenazas y ciberdelitos, en relación con las herramientas técnicas y legales disponibles para su cese y represión. TIPO: Habilidades o destrezas		
H4 - Evaluar la viabilidad de diferentes herramientas y medidas de investigación en atención al tipo de delictivo presentado, las autoridades involucradas y el momento procesal del caso. TIPO: Habilidades o destrezas		
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias		
K2 - Aprender a actualizar de modo autónomo los conocimientos sobre las últimas tecnologías y herramientas de seguridad informática. TIPO: Competencias		
K4 - Aplicar el ordenamiento jurídico español y la normativa internacional, con todas las garantías, ante riesgos, amenazas y ciberdelitos concretos. TIPO: Competencias		
K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias		
NIVEL 2: Ciberperfilación criminológica		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
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**
NO CONSTAN ELEMENTOS DE NIVEL 3		
4.1.1.2 RESULTADOS DE APRENDIZAJE		
C1 - Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática. TIPO: Conocimientos o contenidos		
C2 - Examinar el funcionamiento de las tecnologías disruptivas utilizadas por delincuentes y por profesionales que actúan ante la cibercriminalidad, así como los principios básicos de ciberespacio. TIPO: Conocimientos o contenidos		
C3 - Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada. TIPO: Conocimientos o contenidos		
C6 - Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos. TIPO: Conocimientos o contenidos		

H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas
H4 - Evaluar la viabilidad de diferentes herramientas y medidas de investigación en atención al tipo de delictivo presentado, las autoridades involucradas y el momento procesal del caso. TIPO: Habilidades o destrezas
H5 - Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos. TIPO: Habilidades o destrezas
H6 - Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad. TIPO: Habilidades o destrezas
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias
K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias

NIVEL 2: La víctima en el ciberespacio: cuestiones penales y procesales		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
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**
NO CONSTAN ELEMENTOS DE NIVEL 3		

4.1.1.2 RESULTADOS DE APRENDIZAJE
C1 - Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática. TIPO: Conocimientos o contenidos
C3 - Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada. TIPO: Conocimientos o contenidos
C6 - Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos. TIPO: Conocimientos o contenidos
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas
H3 - Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos. TIPO: Habilidades o destrezas
H4 - Evaluar la viabilidad de diferentes herramientas y medidas de investigación en atención al tipo de delictivo presentado, las autoridades involucradas y el momento procesal del caso. TIPO: Habilidades o destrezas
H6 - Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad. TIPO: Habilidades o destrezas
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias
K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias

K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias		
NIVEL 2: Victimización de mujeres y menores en Internet: cuestiones penales		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
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**
NO CONSTAN ELEMENTOS DE NIVEL 3		
4.1.1.2 RESULTADOS DE APRENDIZAJE		
H7. E1 - Ante casos específicos de ciberdelincuencia, elaborar, exponer y defender una solución jurídicamente fundamentada y adecuada al caso, de la que se deriven actuaciones concretas ante el delito. TIPO: Habilidades o destrezas		
C1 - Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática. TIPO: Conocimientos o contenidos		
C3 - Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada. TIPO: Conocimientos o contenidos		
C6 - Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos. TIPO: Conocimientos o contenidos		
C7 - Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica TIPO: Conocimientos o contenidos		
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas		
H3 - Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos. TIPO: Habilidades o destrezas		
H5 - Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos. TIPO: Habilidades o destrezas		
H6 - Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad. TIPO: Habilidades o destrezas		
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias		
K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias		
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias		
K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias		
C8. E1 - Seleccionar conocimientos jurídicos especializados de los diferentes tipos de ciberdelincuencia para poder asesorar a los profesionales que intervienen en el proceso penal, así como a otras instituciones públicas o privadas. TIPO: Conocimientos o contenidos		
K7. E1 - Seleccionar los conocimientos específicos y cualidades más idóneos necesarios para garantizar y salvaguardar los derechos y principios jurídicos que favorezcan la intervención eficaz de diferentes autoridades en casos de ciberdelincuencia nacional e internacional. TIPO: Competencias		
NIVEL 2: Derecho penal y ciberdelincuencia económica		

4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
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**
NO CONSTAN ELEMENTOS DE NIVEL 3		
4.1.1.2 RESULTADOS DE APRENDIZAJE		
H7. E1 - Ante casos específicos de ciberdelincuencia, elaborar, exponer y defender una solución jurídicamente fundamentada y adecuada al caso, de la que se deriven actuaciones concretas ante el delito. TIPO: Habilidades o destrezas		
K8. E1 - Realizar análisis críticos, auditorías y asesoramiento jurídico ante ciberamenazas, ciberataques u otro tipo de riesgos detectados. TIPO: Competencias		
C1 - Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática. TIPO: Conocimientos o contenidos		
C3 - Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada. TIPO: Conocimientos o contenidos		
C5 - Interpretar la normativa nacional e internacional que regula la ciberdelincuencia, así como las funciones de autoridades y profesionales en el marco de detección, prevención, actuación e intervención en casos de ciberdelincuencia. TIPO: Conocimientos o contenidos		
C6 - Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos. TIPO: Conocimientos o contenidos		
C7 - Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica TIPO: Conocimientos o contenidos		
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas		
H3 - Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos. TIPO: Habilidades o destrezas		
H5 - Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos. TIPO: Habilidades o destrezas		
H6 - Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad. TIPO: Habilidades o destrezas		
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias		
K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias		
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias		
K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias		
C8. E1 - Seleccionar conocimientos jurídicos especializados de los diferentes tipos de ciberdelincuencia para poder asesorar a los profesionales que intervienen en el proceso penal, así como a otras instituciones públicas o privadas. TIPO: Conocimientos o contenidos		

K7. E1 - Seleccionar los conocimientos específicos y cualidades más idóneos necesarios para garantizar y salvaguardar los derechos y principios jurídicos que favorezcan la intervención eficaz de diferentes autoridades en casos de ciberdelincuencia nacional e internacional. TIPO: Competencias		
NIVEL 2: Aspectos probatorios de la cibercriminalidad		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
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**
NO CONSTAN ELEMENTOS DE NIVEL 3		
4.1.1.2 RESULTADOS DE APRENDIZAJE		
H8. E1 - Argumentar los derechos, garantías y principios que deben primar en atención al tipo delictivo concreto, así como las autoridades competentes para la práctica de diferentes funciones TIPO: Habilidades o destrezas		
C1 - Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática. TIPO: Conocimientos o contenidos		
C2 - Examinar el funcionamiento de las tecnologías disruptivas utilizadas por delincuentes y por profesionales que actúan ante la cibercriminalidad, así como los principios básicos de ciberespacio. TIPO: Conocimientos o contenidos		
C4 - Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos. TIPO: Conocimientos o contenidos		
C7 - Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica TIPO: Conocimientos o contenidos		
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas		
H3 - Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos. TIPO: Habilidades o destrezas		
H5 - Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos. TIPO: Habilidades o destrezas		
H6 - Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad. TIPO: Habilidades o destrezas		
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias		
K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias		
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias		
K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias		
C8. E1 - Seleccionar conocimientos jurídicos especializados de los diferentes tipos de ciberdelincuencia para poder asesorar a los profesionales que intervienen en el proceso penal, así como a otras instituciones públicas o privadas. TIPO: Conocimientos o contenidos		
K7. E1 - Seleccionar los conocimientos específicos y cualidades más idóneos necesarios para garantizar y salvaguardar los derechos y principios jurídicos que favorezcan la intervención eficaz de diferentes autoridades en casos de ciberdelincuencia nacional e internacional. TIPO: Competencias		
NIVEL 2: Cooperación procesal internacional en materia de cibercrimen		

4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
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**
NO CONSTAN ELEMENTOS DE NIVEL 3		
4.1.1.2 RESULTADOS DE APRENDIZAJE		
H7. E1 - Ante casos específicos de ciberdelincuencia, elaborar, exponer y defender una solución jurídicamente fundamentada y adecuada al caso, de la que se deriven actuaciones concretas ante el delito. TIPO: Habilidades o destrezas		
H8. E1 - Argumentar los derechos, garantías y principios que deben primar en atención al tipo delictivo concreto, así como las autoridades competentes para la práctica de diferentes funciones TIPO: Habilidades o destrezas		
K8. E1 - Realizar análisis críticos, auditorías y asesoramiento jurídico ante ciberamenazas, ciberataques u otro tipo de riesgos detectados. TIPO: Competencias		
C1 - Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática. TIPO: Conocimientos o contenidos		
C2 - Examinar el funcionamiento de las tecnologías disruptivas utilizadas por delincuentes y por profesionales que actúan ante la cibercriminalidad, así como los principios básicos de ciberespacio. TIPO: Conocimientos o contenidos		
C4 - Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos. TIPO: Conocimientos o contenidos		
C7 - Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica TIPO: Conocimientos o contenidos		
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas		
H3 - Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos. TIPO: Habilidades o destrezas		
H5 - Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos. TIPO: Habilidades o destrezas		
H6 - Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad. TIPO: Habilidades o destrezas		
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias		
K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias		
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias		
K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias		
C8. E1 - Seleccionar conocimientos jurídicos especializados de los diferentes tipos de ciberdelincuencia para poder asesorar a los profesionales que intervienen en el proceso penal, así como a otras instituciones públicas o privadas. TIPO: Conocimientos o contenidos		
K7. E1 - Seleccionar los conocimientos específicos y cualidades más idóneos necesarios para garantizar y salvaguardar los derechos y principios jurídicos que favorezcan la intervención eficaz de diferentes autoridades en casos de ciberdelincuencia nacional e internacional. TIPO: Competencias		
NIVEL 2: Medidas de investigación tecnológicas		

4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
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**
NO CONSTAN ELEMENTOS DE NIVEL 3		
4.1.1.2 RESULTADOS DE APRENDIZAJE		
C2 - Examinar el funcionamiento de las tecnologías disruptivas utilizadas por delincuentes y por profesionales que actúan ante la cibercriminalidad, así como los principios básicos de ciberespacio. TIPO: Conocimientos o contenidos		
C3 - Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada. TIPO: Conocimientos o contenidos		
C4 - Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos. TIPO: Conocimientos o contenidos		
C5 - Interpretar la normativa nacional e internacional que regula la ciberdelincuencia, así como las funciones de autoridades y profesionales en el marco de detección, prevención, actuación e intervención en casos de ciberdelincuencia. TIPO: Conocimientos o contenidos		
C7 - Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica TIPO: Conocimientos o contenidos		
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas		
H2 - Identificar el funcionamiento técnico de las ciberamenazas y ciberdelitos, en relación con las herramientas técnicas y legales disponibles para su cese y represión. TIPO: Habilidades o destrezas		
H4 - Evaluar la viabilidad de diferentes herramientas y medidas de investigación en atención al tipo de delictivo presentado, las autoridades involucradas y el momento procesal del caso. TIPO: Habilidades o destrezas		
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias		
K2 - Aprender a actualizar de modo autónomo los conocimientos sobre las últimas tecnologías y herramientas de seguridad informática. TIPO: Competencias		
K4 - Aplicar el ordenamiento jurídico español y la normativa internacional, con todas las garantías, ante riesgos, amenazas y ciberdelitos concretos. TIPO: Competencias		
K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias		
NIVEL 2: Auditoría y herramientas de seguridad informática basadas en IA		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
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**

NO CONSTAN ELEMENTOS DE NIVEL 3
4.1.1.2 RESULTADOS DE APRENDIZAJE
H7. E1 - Ante casos específicos de ciberdelincuencia, elaborar, exponer y defender una solución jurídicamente fundamentada y adecuada al caso, de la que se deriven actuaciones concretas ante el delito. TIPO: Habilidades o destrezas
H8. E1 - Argumentar los derechos, garantías y principios que deben primar en atención al tipo delictivo concreto, así como las autoridades competentes para la práctica de diferentes funciones TIPO: Habilidades o destrezas
K8. E1 - Realizar análisis críticos, auditorías y asesoramiento jurídico ante ciberamenazas, ciberataques u otro tipo de riesgos detectados. TIPO: Competencias
C1 - Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática. TIPO: Conocimientos o contenidos
C2 - Examinar el funcionamiento de las tecnologías disruptivas utilizadas por delincuentes y por profesionales que actúan ante la cibercriminalidad, así como los principios básicos de ciberespacio. TIPO: Conocimientos o contenidos
C4 - Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos. TIPO: Conocimientos o contenidos
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas
H3 - Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos. TIPO: Habilidades o destrezas
H5 - Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos. TIPO: Habilidades o destrezas
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias
K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias
K2 - Aprender a actualizar de modo autónomo los conocimientos sobre las últimas tecnologías y herramientas de seguridad informática. TIPO: Competencias
K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias
C8. E1 - Seleccionar conocimientos jurídicos especializados de los diferentes tipos de ciberdelincuencia para poder asesorar a los profesionales que intervienen en el proceso penal, así como a otras instituciones públicas o privadas. TIPO: Conocimientos o contenidos
K7. E1 - Seleccionar los conocimientos específicos y cualidades más idóneos necesarios para garantizar y salvaguardar los derechos y principios jurídicos que favorezcan la intervención eficaz de diferentes autoridades en casos de ciberdelincuencia nacional e internacional. TIPO: Competencias
NIVEL 2: Talleres de actualización jurídica
4.1.1.1 Datos Básicos del Nivel 2

CARÁCTER	Optativa
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**

NO CONSTAN ELEMENTOS DE NIVEL 3
4.1.1.2 RESULTADOS DE APRENDIZAJE
H7. E1 - Ante casos específicos de ciberdelincuencia, elaborar, exponer y defender una solución jurídicamente fundamentada y adecuada al caso, de la que se deriven actuaciones concretas ante el delito. TIPO: Habilidades o destrezas

H8. E1 - Argumentar los derechos, garantías y principios que deben primar en atención al tipo delictivo concreto, así como las autoridades competentes para la práctica de diferentes funciones TIPO: Habilidades o destrezas
C3 - Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada. TIPO: Conocimientos o contenidos
C4 - Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos. TIPO: Conocimientos o contenidos
C6 - Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos. TIPO: Conocimientos o contenidos
C7 - Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica TIPO: Conocimientos o contenidos
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas
H3 - Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos. TIPO: Habilidades o destrezas
H5 - Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos. TIPO: Habilidades o destrezas
H6 - Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad. TIPO: Habilidades o destrezas
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias
K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias
K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias
C8. E1 - Seleccionar conocimientos jurídicos especializados de los diferentes tipos de ciberdelincuencia para poder asesorar a los profesionales que intervienen en el proceso penal, así como a otras instituciones públicas o privadas. TIPO: Conocimientos o contenidos

NIVEL 2: Teorías criminológicas y ciberespacio		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
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**
NO CONSTAN ELEMENTOS DE NIVEL 3		
4.1.1.2 RESULTADOS DE APRENDIZAJE		
K10. E2 - Determinar, tras su evaluación, el tratamiento individualizado de las víctimas de un cibercrimen, así como planes de prevención para hacer frente a los riesgos derivados de este tipo de criminalidad en diferentes sectores de la población. TIPO: Competencias		
H9. E2 - Ante casos específicos de cibercriminalidad, elaborar, exponer y defender informes criminológicos jurídicamente fundamentados adecuados al caso y en relación con las exigencias procedimentales. TIPO: Habilidades o destrezas		

C3 - Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada. TIPO: Conocimientos o contenidos
C5 - Interpretar la normativa nacional e internacional que regula la ciberdelincuencia, así como las funciones de autoridades y profesionales en el marco de detección, prevención, actuación e intervención en casos de ciberdelincuencia. TIPO: Conocimientos o contenidos
C6 - Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos. TIPO: Conocimientos o contenidos
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas
H3 - Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos. TIPO: Habilidades o destrezas
H5 - Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos. TIPO: Habilidades o destrezas
H6 - Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad. TIPO: Habilidades o destrezas
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias
K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias
K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias
C9. E2 - Comparar conocimientos específicos para elaborar estudios e informes criminológicos en el ámbito de la ciberdelincuencia y profundizar en las teorías criminológicas que explican el delito en el ciberespacio, así como otros factores relacionados con el proceso penal. TIPO: Conocimientos o contenidos

NIVEL 2: Principales explicaciones sociocriminológicas del ciberdelito		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
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**
NO CONSTAN ELEMENTOS DE NIVEL 3		
4.1.1.2 RESULTADOS DE APRENDIZAJE		
K10. E2 - Determinar, tras su evaluación, el tratamiento individualizado de las víctimas de un cibercrimen, así como planes de prevención para hacer frente a los riesgos derivados de este tipo de criminalidad en diferentes sectores de la población. TIPO: Competencias		
H9. E2 - Ante casos específicos de cibercriminalidad, elaborar, exponer y defender informes criminológicos jurídicamente fundamentados adecuados al caso y en relación con las exigencias procedimentales. TIPO: Habilidades o destrezas		
H10. E2 - Desarrollar estrategias de prevención e intervención ante ciberataques u otro tipo de ciberdelitos, razonando y argumentando la propuesta con un enfoque interdisciplinar y teniendo en cuenta las particularidades de las víctimas para que la propuesta responda a las necesidades de éstas. TIPO: Habilidades o destrezas		

C3 - Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada. TIPO: Conocimientos o contenidos
C5 - Interpretar la normativa nacional e internacional que regula la ciberdelincuencia, así como las funciones de autoridades y profesionales en el marco de detección, prevención, actuación e intervención en casos de ciberdelincuencia. TIPO: Conocimientos o contenidos
C6 - Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos. TIPO: Conocimientos o contenidos
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas
H3 - Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos. TIPO: Habilidades o destrezas
H5 - Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos. TIPO: Habilidades o destrezas
H6 - Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad. TIPO: Habilidades o destrezas
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias
K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias
K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias
C9. E2 - Comparar conocimientos específicos para elaborar estudios e informes criminológicos en el ámbito de la ciberdelincuencia y profundizar en las teorías criminológicas que explican el delito en el ciberespacio, así como otros factores relacionados con el proceso penal. TIPO: Conocimientos o contenidos

NIVEL 2: Factor humano del ciberdelito		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
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**
NO CONSTAN ELEMENTOS DE NIVEL 3		
4.1.1.2 RESULTADOS DE APRENDIZAJE		
K10. E2 - Determinar, tras su evaluación, el tratamiento individualizado de las víctimas de un cibercrimen, así como planes de prevención para hacer frente a los riesgos derivados de este tipo de criminalidad en diferentes sectores de la población. TIPO: Competencias		
H9. E2 - Ante casos específicos de cibercriminalidad, elaborar, exponer y defender informes criminológicos jurídicamente fundamentados adecuados al caso y en relación con las exigencias procedimentales. TIPO: Habilidades o destrezas		
H10. E2 - Desarrollar estrategias de prevención e intervención ante ciberataques u otro tipo de ciberdelitos, razonando y argumentando la propuesta con un enfoque interdisciplinar y teniendo en cuenta las particularidades de las víctimas para que la propuesta responda a las necesidades de éstas. TIPO: Habilidades o destrezas		

C3 - Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada. TIPO: Conocimientos o contenidos
C4 - Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos. TIPO: Conocimientos o contenidos
C5 - Interpretar la normativa nacional e internacional que regula la ciberdelincuencia, así como las funciones de autoridades y profesionales en el marco de detección, prevención, actuación e intervención en casos de ciberdelincuencia. TIPO: Conocimientos o contenidos
C6 - Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos. TIPO: Conocimientos o contenidos
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas
H3 - Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos. TIPO: Habilidades o destrezas
H5 - Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos. TIPO: Habilidades o destrezas
H6 - Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad. TIPO: Habilidades o destrezas
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias
K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias
K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias
C9. E2 - Comparar conocimientos específicos para elaborar estudios e informes criminológicos en el ámbito de la ciberdelincuencia y profundizar en las teorías criminológicas que explican el delito en el ciberespacio, así como otros factores relacionados con el proceso penal. TIPO: Conocimientos o contenidos
K9. E2 - Elaborar informes criminológicos relacionados con el ciberdelito, en los que se seleccione los conocimientos específicos y las cualidades más idóneos y en los que se identifiquen los factores que favorecen la criminalidad y se defina y reconstruya el modus operandi o la actuación posterior. TIPO: Competencias

NIVEL 2: Análisis y gestión de riesgos del cibercrimen		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
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**
NO CONSTAN ELEMENTOS DE NIVEL 3		
4.1.1.2 RESULTADOS DE APRENDIZAJE		
K10. E2 - Determinar, tras su evaluación, el tratamiento individualizado de las víctimas de un cibercrimen, así como planes de prevención para hacer frente a los riesgos derivados de este tipo de criminalidad en diferentes sectores de la población. TIPO: Competencias		

H10. E2 - Desarrollar estrategias de prevención e intervención ante ciberataques u otro tipo de ciberdelitos, razonando y argumentando la propuesta con un enfoque interdisciplinar y teniendo en cuenta las particularidades de las víctimas para que la propuesta responda a las necesidades de éstas. TIPO: Habilidades o destrezas
C1 - Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática. TIPO: Conocimientos o contenidos
C2 - Examinar el funcionamiento de las tecnologías disruptivas utilizadas por delincuentes y por profesionales que actúan ante la cibercriminalidad, así como los principios básicos de ciberespacio. TIPO: Conocimientos o contenidos
C4 - Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos. TIPO: Conocimientos o contenidos
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas
H3 - Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos. TIPO: Habilidades o destrezas
H5 - Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos. TIPO: Habilidades o destrezas
H6 - Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad. TIPO: Habilidades o destrezas
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias
K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias
K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias
C9. E2 - Comparar conocimientos específicos para elaborar estudios e informes criminológicos en el ámbito de la ciberdelincuencia y profundizar en las teorías criminológicas que explican el delito en el ciberespacio, así como otros factores relacionados con el proceso penal. TIPO: Conocimientos o contenidos

NIVEL 2: Prueba electrónica e informes periciales en el proceso penal		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
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**

NO CONSTAN ELEMENTOS DE NIVEL 3
4.1.1.2 RESULTADOS DE APRENDIZAJE
K10. E2 - Determinar, tras su evaluación, el tratamiento individualizado de las víctimas de un cibercrimen, así como planes de prevención para hacer frente a los riesgos derivados de este tipo de criminalidad en diferentes sectores de la población. TIPO: Competencias
H9. E2 - Ante casos específicos de cibercriminalidad, elaborar, exponer y defender informes criminológicos jurídicamente fundamentados adecuados al caso y en relación con las exigencias procedimentales. TIPO: Habilidades o destrezas
H10. E2 - Desarrollar estrategias de prevención e intervención ante ciberataques u otro tipo de ciberdelitos, razonando y argumentando la propuesta con un enfoque interdisciplinar y teniendo en cuenta las particularidades de las víctimas para que la propuesta responda a las necesidades de éstas. TIPO: Habilidades o destrezas

C1 - Defender las bases conceptuales de la ciberdelincuencia, ciberamenazas y la seguridad informática. TIPO: Conocimientos o contenidos
C2 - Examinar el funcionamiento de las tecnologías disruptivas utilizadas por delincuentes y por profesionales que actúan ante la cibercriminalidad, así como los principios básicos de ciberespacio. TIPO: Conocimientos o contenidos
C4 - Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos. TIPO: Conocimientos o contenidos
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas
H3 - Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos. TIPO: Habilidades o destrezas
H5 - Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos. TIPO: Habilidades o destrezas
H6 - Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad. TIPO: Habilidades o destrezas
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias
K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias
K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias
C9. E2 - Comparar conocimientos específicos para elaborar estudios e informes criminológicos en el ámbito de la ciberdelincuencia y profundizar en las teorías criminológicas que explican el delito en el ciberespacio, así como otros factores relacionados con el proceso penal. TIPO: Conocimientos o contenidos
K9. E2 - Elaborar informes criminológicos relacionados con el ciberdelito, en los que se seleccione los conocimientos específicos y las cualidades más idóneos y en los que se identifiquen los factores que favorecen la criminalidad y se defina y reconstruya el modus operandi o la actuación posterior. TIPO: Competencias

NIVEL 2: Talleres de actualización criminológica		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
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**
NO CONSTAN ELEMENTOS DE NIVEL 3		
4.1.1.2 RESULTADOS DE APRENDIZAJE		
K10. E2 - Determinar, tras su evaluación, el tratamiento individualizado de las víctimas de un cibercrimen, así como planes de prevención para hacer frente a los riesgos derivados de este tipo de criminalidad en diferentes sectores de la población. TIPO: Competencias		
H9. E2 - Ante casos específicos de cibercriminalidad, elaborar, exponer y defender informes criminológicos jurídicamente fundamentados adecuados al caso y en relación con las exigencias procedimentales. TIPO: Habilidades o destrezas		
H10. E2 - Desarrollar estrategias de prevención e intervención ante ciberataques u otro tipo de ciberdelitos, razonando y argumentando la propuesta con un enfoque interdisciplinar y teniendo en cuenta las particularidades de las víctimas para que la propuesta responda a las necesidades de éstas. TIPO: Habilidades o destrezas		

C3 - Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada. TIPO: Conocimientos o contenidos
C4 - Evaluar las herramientas técnicas y legales necesarias para analizar y hacer frente a diferentes riesgos, ciberamenazas y ciberdelitos. TIPO: Conocimientos o contenidos
C6 - Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos. TIPO: Conocimientos o contenidos
C7 - Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica TIPO: Conocimientos o contenidos
H1 - Identificar riesgos asociados a la cibercriminalidad en diferentes contextos, a nivel nacional e internacional, individualizar el tipo delictivo y analizar las particularidades de los nuevos escenarios virtuales. TIPO: Habilidades o destrezas
H3 - Practicar con pericia la búsqueda de legislación y jurisprudencia a través de diferentes técnicas que puedan favorecer la investigación, la prueba y la intervención ante ciberdelitos. TIPO: Habilidades o destrezas
H5 - Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos. TIPO: Habilidades o destrezas
H6 - Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad. TIPO: Habilidades o destrezas
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias
K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias
K1 - Discriminar los tipos de ciberdelito, comprendiendo los nuevos espacios virtuales y, en atención a ellos, aplicar la normativa vigente y las resoluciones jurisprudenciales vinculantes en cada caso en cuestión. TIPO: Competencias
K6 - Discriminar las funciones de cada una de las autoridades y profesionales que intervienen en casos de ciberdelincuencia, identificando los requisitos formales que van ligados a todas ellas para poder poner en práctica las mismas. TIPO: Competencias
C9. E2 - Comparar conocimientos específicos para elaborar estudios e informes criminológicos en el ámbito de la ciberdelincuencia y profundizar en las teorías criminológicas que explican el delito en el ciberespacio, así como otros factores relacionados con el proceso penal. TIPO: Conocimientos o contenidos
K9. E2 - Elaborar informes criminológicos relacionados con el ciberdelito, en los que se seleccione los conocimientos específicos y las cualidades más idóneos y en los que se identifiquen los factores que favorecen la criminalidad y se defina y reconstruya el modus operandi o la actuación posterior. TIPO: Competencias

NIVEL 2: Trabajo fin de Máster		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Trabajo Fin de Grado / Máster	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
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**
NO CONSTAN ELEMENTOS DE NIVEL 3		
4.1.1.2 RESULTADOS DE APRENDIZAJE		
H7. E1 - Ante casos específicos de ciberdelincuencia, elaborar, exponer y defender una solución jurídicamente fundamentada y adecuada al caso, de la que se deriven actuaciones concretas ante el delito. TIPO: Habilidades o destrezas		
H8. E1 - Argumentar los derechos, garantías y principios que deben primar en atención al tipo delictivo concreto, así como las autoridades competentes para la práctica de diferentes funciones TIPO: Habilidades o destrezas		

K10. E2 - Determinar, tras su evaluación, el tratamiento individualizado de las víctimas de un cibercrimen, así como planes de prevención para hacer frente a los riesgos derivados de este tipo de criminalidad en diferentes sectores de la población. TIPO: Competencias
H9. E2 - Ante casos específicos de cibercriminalidad, elaborar, exponer y defender informes criminológicos jurídicamente fundamentados adecuados al caso y en relación con las exigencias procedimentales. TIPO: Habilidades o destrezas
H10. E2 - Desarrollar estrategias de prevención e intervención ante ciberataques u otro tipo de ciberdelitos, razonando y argumentando la propuesta con un enfoque interdisciplinar y teniendo en cuenta las particularidades de las víctimas para que la propuesta responda a las necesidades de éstas. TIPO: Habilidades o destrezas
K8. E1 - Realizar análisis críticos, auditorías y asesoramiento jurídico ante ciberamenazas, ciberataques u otro tipo de riesgos detectados. TIPO: Competencias
C3 - Identificar de forma exhaustiva el funcionamiento de los diferentes tipos de cibercrimen; modus operandi, autoría, víctimas, tecnología empleada. TIPO: Conocimientos o contenidos
C6 - Discriminar, por un lado, las particularidades de las personas víctimas de las actividades ilícitas que llevan a cabo los criminales utilizando tecnologías de la información y las comunicaciones; y, por otro, las necesidades de intervención que se derivan tras estos delitos. TIPO: Conocimientos o contenidos
C7 - Contrastar la jurisprudencia estatal y supranacional en materia de ciberdelincuencia e investigación tecnológica TIPO: Conocimientos o contenidos
H5 - Aplicar con dominio la normativa nacional e internacional que regula la ciberdelincuencia, así como su persecución, investigación y represión en casos concretos. TIPO: Habilidades o destrezas
H6 - Concluir las cuestiones jurídicas más relevantes implicadas en un conjunto complejo de hechos relacionados con casos de cibercriminalidad. TIPO: Habilidades o destrezas
K3 - Analizar pormenorizadamente cada ciberdelito, incluyendo perfiles diferenciados de víctimas y agresores en el uso de la tecnología cibernética. TIPO: Competencias
K5 - En casos de cibercriminalidad, redactar textos legales para los diferentes momentos procesales y desde el punto de vistas de diferentes profesiones implicadas, y que estos textos sean comprensibles tanto para un público especialista como para un público profano. TIPO: Competencias
K4 - Aplicar el ordenamiento jurídico español y la normativa internacional, con todas las garantías, ante riesgos, amenazas y ciberdelitos concretos. TIPO: Competencias
C8. E1 - Seleccionar conocimientos jurídicos especializados de los diferentes tipos de ciberdelincuencia para poder asesorar a los profesionales que intervienen en el proceso penal, así como a otras instituciones públicas o privadas. TIPO: Conocimientos o contenidos
C9. E2 - Comparar conocimientos específicos para elaborar estudios e informes criminológicos en el ámbito de la ciberdelincuencia y profundizar en las teorías criminológicas que explican el delito en el ciberespacio, así como otros factores relacionados con el proceso penal. TIPO: Conocimientos o contenidos
K7. E1 - Seleccionar los conocimientos específicos y cualidades más idóneos necesarios para garantizar y salvaguardar los derechos y principios jurídicos que favorezcan la intervención eficaz de diferentes autoridades en casos de ciberdelincuencia nacional e internacional. TIPO: Competencias
K9. E2 - Elaborar informes criminológicos relacionados con el ciberdelito, en los que se seleccione los conocimientos específicos y las cualidades más idóneos y en los que se identifiquen los factores que favorecen la criminalidad y se defina y reconstruya el modus operandi o la actuación posterior. TIPO: Competencias
NO CONSTAN ELEMENTOS DE NIVEL 2

4.2 ACTIVIDADES Y METODOLOGÍAS DOCENTES

ACTIVIDADES FORMATIVAS

4.2. Actividades y metodologías docentes

Las actividades y metodologías docentes que se adoptarán en la presente titulación serán delimitadas por el profesorado de la asignatura en las fichas académicas con carácter previo al comienzo del curso, siempre favoreciendo y respetando el cumplimiento de los objetivos, competencias, conocimientos y habilidades recogidas en la presente memoria.

El proceso de aprendizaje de este título tiene su fundamento en las actividades formativas, cuyo objetivo es promover la participación y la implicación activa del estudiante. Dichas actividades, además, garantizarán que el aprendizaje del estudiante sea, a la vez, guiado y autónomo, y le permita adquirir todas las competencias, conocimientos y destrezas propuestas de la manera más completa y coherente posible.

Para ello, el diseño del proceso de aprendizaje se basa en la planificación de actividades teóricas y prácticas presenciales como eje central del máster, que se complementarán con actividades individuales, tanto dirigidas como autónomas, del estudiante. Las actividades formativas que se ajustan a las materias propuestas son las siguientes:

- Clases teóricas: exposición, explicación y análisis crítico de contenidos fundamentales por parte del profesorado. Serán sesiones de obligatoria asistencia, en las que fomentará la reflexión crítica del alumnado, así como su participación.
- Clases prácticas: planteamiento, desarrollo y resolución de problemas y de casos prácticos. Serán sesiones de obligatoria asistencia
- Debates: presentación y defensa de posturas contrarias sobre temas tratados, ya sean previamente preparados o improvisados en el transcurso de la clase. También son de obligatoria asistencia.
- Seminarios: se profundizará en diferentes aspectos que rodean a la ciberdelincuencia con expertos en la materia. En algunos de ellos se requerirá la lectura previa de textos científicos y la entrega de una actividad posterior. En todo caso, se incentivará la participación del alumnado, así como la eventual práctica de debates o la resolución de problemas.
- Elaboración de trabajos: aplicando los contenidos teóricos a casos prácticos más elaborados. Pueden ser individuales o grupales. En el caso de los trabajos individuales se perseguirá trabajar la capacidad individual de análisis, reflexión y síntesis. Por otro lado, en el caso de los grupales se fomentará que los alumnos colaboren y desarrollen habilidades de comunicación, liderazgo y gestión de conflictos.
- Tutorías: se pondrá a disposición de los estudiantes la solicitud de tutorías para el seguimiento y asesoramiento individual en relación con el desarrollo de cada asignatura. Se utilizarán, asimismo, para profundizar en temas de interés e incluso para el seguimiento de actividades grupales.
- Talleres y exposiciones: se profundizará en tipologías delictivas y otros aspectos relativos al proceso penal a través de talleres didácticos con expertos y, eventualmente, se complementarán con exposiciones del alumnado.
- Trabajo de fin de Máster: el profesorado del Máster ofrecerá diferentes líneas de investigación generales y específicas relacionadas con la asignatura que imparte. Las líneas de investigación serán seleccionadas por el alumnado y asignadas al mismo antes de que finalice el primer semestre, para que puedan realizar un trabajo de investigación tutorizado a lo largo de todo el segundo semestre. Será fundamental el trabajo continuado, completo y exhaustivo que garantice que el alumnado ha conseguido el objetivo perseguido con este trabajo. Se priorizará el trabajo autónomo tutorizado, auxiliado por el profesorado que le orientará para la práctica de una investigación adecuada al nivel de posgrado. Asimismo, se prevé la organización de seminarios, talleres y exposiciones (como se ha indicado anteriormente) que garanticen que los y las alumnas cuenten con herramientas específicas para realizar investigaciones criminológicas o jurídicas en materia de cibercriminalidad.

METODOLOGÍAS DOCENTES

4.2. Actividades y metodologías docentes

Las actividades y metodologías docentes que se adoptarán en la presente titulación serán delimitadas por el profesorado de la asignatura en las fichas académicas con carácter previo al comienzo del curso, siempre favoreciendo y respetando el cumplimiento de los objetivos, competencias, conocimientos y habilidades recogidas en la presente memoria.

El proceso de aprendizaje de este título tiene su fundamento en las actividades formativas, cuyo objetivo es promover la participación y la implicación activa del estudiante. Dichas actividades, además, garantizarán que el aprendizaje del estudiante sea, a la vez, guiado y autónomo, y le permita adquirir todas las competencias, conocimientos y destrezas propuestas de la manera más completa y coherente posible.

Para ello, el diseño del proceso de aprendizaje se basa en la planificación de actividades teóricas y prácticas presenciales como eje central del máster, que se complementarán con actividades individuales, tanto dirigidas como autónomas, del estudiante. Las actividades formativas que se ajustan a las materias propuestas son las siguientes:

- Clases teóricas: exposición, explicación y análisis crítico de contenidos fundamentales por parte del profesorado. Serán sesiones de obligatoria asistencia, en las que fomentará la reflexión crítica del alumnado, así como su participación.
- Clases prácticas: planteamiento, desarrollo y resolución de problemas y de casos prácticos. Serán sesiones de obligatoria asistencia
- Debates: presentación y defensa de posturas contrarias sobre temas tratados, ya sean previamente preparados o improvisados en el transcurso de la clase. También son de obligatoria asistencia.
- Seminarios: se profundizará en diferentes aspectos que rodean a la ciberdelincuencia con expertos en la materia. En algunos de ellos se requerirá la lectura previa de textos científicos y la entrega de una actividad posterior. En todo caso, se incentivará la participación del alumnado, así como la eventual práctica de debates o la resolución de problemas.
- Elaboración de trabajos: aplicando los contenidos teóricos a casos prácticos más elaborados. Pueden ser individuales o grupales. En el caso de los trabajos individuales se perseguirá trabajar la capacidad individual de análisis, reflexión y síntesis. Por otro lado, en el caso de los grupales se fomentará que los alumnos colaboren y desarrollen habilidades de comunicación, liderazgo y gestión de conflictos.
- Tutorías: se pondrá a disposición de los estudiantes la solicitud de tutorías para el seguimiento y asesoramiento individual en relación con el desarrollo de cada asignatura. Se utilizarán, asimismo, para profundizar en temas de interés e incluso para el seguimiento de actividades grupales.
- Talleres y exposiciones: se profundizará en tipologías delictivas y otros aspectos relativos al proceso penal a través de talleres didácticos con expertos y, eventualmente, se complementarán con exposiciones del alumnado.
- Trabajo de fin de Máster: el profesorado del Máster ofrecerá diferentes líneas de investigación generales y específicas relacionadas con la asignatura que imparte. Las líneas de investigación serán seleccionadas por el alumnado y asignadas al mismo antes de que finalice el primer semestre, para que puedan realizar un trabajo de investigación tutorizado a lo largo de todo el segundo semestre. Será fundamental el trabajo continuado, completo y exhaustivo que garantice que el alumnado ha conseguido el objetivo perseguido con este trabajo. Se priorizará el trabajo autónomo tutorizado, auxiliado por el profesorado que le orientará para la práctica de una investigación adecuada al nivel de posgrado. Asimismo, se prevé la organización de seminarios, talleres y exposiciones (como se ha indicado anteriormente) que garanticen que los y las alumnas cuenten con herramientas específicas para realizar investigaciones criminológicas o jurídicas en materia de cibercriminalidad.

4.3 SISTEMAS DE EVALUACIÓN

4.3. Sistemas de evaluación

Los criterios e instrumentos de evaluación, así como la repercusión que tendrán en las calificaciones finales, se fijarán por asignaturas, cumpliendo los criterios que aquí se recogen. Los estudiantes tendrán a su disposición en la Guía Académica los sistemas de evaluación específicos de cada una de las asignaturas que componen el plan de estudios antes de comenzar el curso académico, previa revisión por parte de la Comisión Académica del título.

Para la evaluación de las asignaturas será importante delimitar por el profesorado los porcentajes exactos. Para efectuar la evaluación, el profesorado elegirá algunas de las herramientas que mejor se adapten al cumplimiento de los objetivos y que fomenten la adquisición de las competencias de esta titulación.

Respecto a la **evaluación continua**, el porcentaje oscilará entre el **30-60%**, que se podrá ajustar y dividir en los siguientes métodos de evaluación:

1. Participación en clase
2. Entrega de trabajos individuales o grupales: realización de casos, problemas o ejercicios prácticos en el aula, ya sea a través de las TIC, utilizando medidas en el medio *offline* o el aula invertida
3. Exposición de trabajos y/o presentaciones, resultado de trabajos de investigación. También podrá consistir en la realización de debates, simulaciones, role-playing, estudios de caso
4. Prácticas en las aulas de informática
5. Participación en seminarios o congresos relativos a la materia en cuestión
6. Prácticas de campo y/o asistencia externa a instituciones especializadas: juzgados, audiencias, comisarías de policía, asociaciones, prisiones, etc.

Por otro lado, el porcentaje restante, entre el **40-70%,** corresponderá a una **prueba de evaluación final**, que podrá consistir en:

- Examen final**:** tipo test, de desarrollo, de preguntas cortas, teórico, práctico, etc.
- Entrega de trabajo de investigación final y/o exposición con debate crítico con el profesorado y resto de alumnado.

Con carácter general, se apostará por la evaluación tanto teórica como práctica, estableciendo evaluación continua y evaluación final, la cual conocerá el alumnado antes del inicio de cada curso académico. Asimismo, en cualquier asignatura, la combinación de medios y pruebas, así como su peso en la evaluación global, la deberá ajustar el profesor.

La evaluación del Trabajo Fin de Máster se realizará siguiendo el Reglamento de Trabajos Fin de Máster de la Universidad de Salamanca. La Comisión Académica del Máster establecerá un protocolo público de evaluación acorde a lo dispuesto en el Real Decreto 822/2021 que incluirá escalas descriptivas de calificación en forma de rúbrica, donde se fijen las dimensiones básicas de valoración del TFM que se consideren necesarias para mostrar de forma integrada la comprensión de los contenidos y la adquisición de las competencias definitorias del Máster. El TFM será expuesto y defendido en acto público ante un tribunal nombrado a tal efecto, integrado por tres miembros del profesorado del Máster que evaluará de forma individual la adquisición de los resultados del proceso de formación y aprendizaje por parte de cada estudiante.

La Comisión de Calidad del Título tendrá funciones primordialmente de evaluación y seguimiento del Título siguiendo las líneas generales marcadas por el Sistema de Garantía de Calidad de la USAL. Se responsabilizará, entre otras funciones de:

1. Recopilar datos y evidencias sobre el desarrollo del programa formativo (objetivos, planificación y desarrollo de la enseñanza y aprendizaje, admisión y orientación a los estudiantes, personal académico y de apoyo, recursos y servicios, y resultados)
2. Analizar y valorar los datos y evidencias recopiladas
3. Proponer, a partir de lo anterior, planes de mejora para el programa
4. Realizar un seguimiento de los planes de mejora propuestos, así como de las acciones que se deriven de la respuesta a sugerencias, reclamaciones o quejas recibidas de cualquier miembro de la comunidad universitaria implicada (estudiantes, PDI, PTGAS, egresados, empleadores)
5. Gestionar el #Archivo Documental del Título#, donde archivará toda la documentación relacionada con la implantación, desarrollo y seguimiento del Título (actas, informes, propuestas, datos, indicadores, quejas, sugerencias, planes de mejora, etc.), y que servirá a los responsables académicos para garantizar su calidad y promover mejoras en el desarrollo del plan de estudios.

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	
7.2 Procedimiento de adaptación No proNo procede.	
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://qualitas.usal.es/docs/SGIC_Grados%20y%20MU_CG20150326_con%20anexo2016.pdf
8.2 INFORMACIÓN PÚBLICA	

8.2. Medios para la información pública

El medio principal de información pública del plan de estudios es la web institucional del Máster Universitario (**https://www.usal.es/masteres**). Ésta contará con la información que la Agencia para la Calidad del Sistema de Castilla y León, ACSUCyl, requiere actualmente para superar con éxito los procesos de renovación de acreditación de los títulos y que puede consultarse en ACSUCyL 2021, II. Manual de evaluación (**https://www.acsucyl.es/web/jcyl/binarios/448/438/ACSUCYL_RenovacionAcreditacion_II.ManualEvaluacion_Ed2021.pdf?blobheader=application%2Fpdf%3Bcharset%3DUTF-8&blobnocache=true**): Descripción del título (centro, modalidad, idioma, plazas de nuevo ingreso ofertadas, salidas profesionales, etc.), Objetivos (Objetivos formativos y Resultados del proceso de formación y de aprendizaje), Acceso y admisión de estudiantes (Perfil de ingreso, Acceso, preinscripción y matrícula, Criterios de admisión, Apoyo y orientación, Reconocimiento y Transferencia de créditos), Planificación de las enseñanzas (plan de estudios general, guías docentes), Calendario de implantación, Sistema de garantía de calidad (Informes externos de evaluación del título, Información sobre evaluaciones de la actividad docente del profesorado), Resultados (Académicos, y de encuestas, incluidas las de inserción laboral), Normativa.

La Universidad de Salamanca cuenta con un sitio web específico para garantizar la publicidad, información sobre la preinscripción, matrícula, acceso, comunicación del calendario académico, etc. La web institucional de máster es: **https://www.usal.es/masteres**. De igual modo, la Facultad de Derecho cuenta con un sitio web oficial: **https://derecho.usal.es**.

Las necesidades de información de los estudiantes se atenderán también a través de la web de la Facultad de Derecho (**https://derecho.usal.es/**), de la de los Departamentos de Derecho Administrativo, Financiero y Procesal además de Derecho Público General (https://derechoafp.usal.es/ y https://derechopublicogeneral.usal.es/) y del correo electrónico, ya que cada estudiante contará con una cuenta personal y que será básica para interactuar a través del Campus Virtual Studium.

8.3 ANEXOS
Ver Apartado 8: Anexo 1.

PERSONAS ASOCIADAS A LA SOLICITUD

RESPONSABLE DEL TÍTULO			
CARGO	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
Director del Máster	Federico	Bueno	de Mata
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Facultad de Derecho. Campus Miguel de Unamuno, s/n	37007	Salamanca	Salamanca
EMAIL	**FAX**		
febuma@usal.es			
REPRESENTANTE LEGAL			

CARGO	NOMBRE	PRIMER APELLIDO	SEGUNDO APELLIDO
Delegada del Rector para Estudios de Postgrado y Formación Permanente	María Teresa	Escribano	Bailón
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Hospedería Fonseca, Fonseca, nº 2, 1ª planta	37002	Salamanca	Salamanca
EMAIL	**FAX**		
delegadapostgrado@usal.es			

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
Director Académico de Postgrado	Javier	Peña	González
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Patio de Escuelas 1, 2ª planta	37008	Salamanca	Salamanca
EMAIL	**FAX**		
dir.postgrado@usal.es			

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 6

Nombre :1. Justificación, alegaciones y perfil de egreso.pdf

HASH SHA1 :A261113A6DB755BF5BFCD55CD191A21CF27A6B19

Código CSV :833276293432012197621089

Ver Fichero: 1. Justificación, alegaciones y perfil de egreso.pdf

Apartado 4: Anexo 1

Nombre :4. Planificación de las enseñanzas.pdf

HASH SHA1 :A5F6D8AA5A44175783245973BDD34C93DD36B8A4

Código CSV :833679599768170298072769

Ver Fichero: 4. Planificación de las enseñanzas.pdf

Apartado 5: Anexo 1

Nombre :5.1. Personal académico y de apoyo a la docencia.pdf

HASH SHA1 :95218FBD8C82B5FEE3F6970873027C192F162B79

Código CSV :833297718287030957966426

Ver Fichero: 5.1. Personal académico y de apoyo a la docencia.pdf

Apartado 5: Anexo 2

Nombre :5.2 Otros recursos de apoyo a la docencia.pdf

HASH SHA1 :A676AA577C36C65A9BE49E6F0ABC34294110ECD2

Código CSV :795943068932834598714903

Ver Fichero: 5.2 Otros recursos de apoyo a la docencia.pdf

Apartado 6: Anexo 1

Nombre :6. Recursos para el aprendizaje.pdf

HASH SHA1 :4A59A125F918BC54E79A0BAA8682CEED956DBA0C

Código CSV :833298114658984524548254

Ver Fichero: 6. Recursos para el aprendizaje.pdf

Apartado 7: Anexo 1

Nombre :7.1 Cronograma de implantación.pdf

HASH SHA1 :1B4AFDBA598CB826573E642FA7217720A7472E7F

Código CSV :795945199503796537167276

Ver Fichero: 7.1 Cronograma de implantación.pdf

Apartado Personas asociadas a la solicitud: Anexo 1

Nombre : Delegacion competencias Rector RUCT.pdf

HASH SHA1 :67EE0C805B0D582D48DBB6C3345C66EB561FA900

Código CSV :797365265422474411987889

Ver Fichero: Delegacion competencias Rector RUCT.pdf

Apartado Informe previo de la Comunidad Autónoma: Anexo 1

Nombre : Inf Viabilidad - MU Cibercriminalidad8GPQF9KPBCWRBR0CSLLATT.pdf

HASH SHA1 :089CB1B3D253F11D9A6DE670641CC1C933866DA1

Código CSV :801198913225835442104280

Ver Fichero: Inf Viabilidad - MU Cibercriminalidad8GPQF9KPBCWRBR0CSLLATT.pdf