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	Centro Universitario de Formación de la Policía Nacional, O.A.	05006594

NIVEL	DENOMINACIÓN CORTA
Máster	Ciberdelincuencia en el Ámbito de la Función Policial

DENOMINACIÓN ESPECÍFICA
Máster Universitario en Ciberdelincuencia en el Ámbito de la Función Policial por la Universidad de Salamanca

NIVEL MECES
3

RAMA DE CONOCIMIENTO	CAMPO DE ESTUDIO	CONJUNTO
Ingeniería y Arquitectura	Ingeniería informática y de sistemas	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
María Angélica González Arrieta	Directora del Máster Universitario

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		686443690

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 17 de junio de 2025
	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 Ciberdelincuencia en el Ámbito de la Función Policial por la Universidad de Salamanca	No		Ver Apartado 1: Anexo 1.

RAMA
Ingeniería y Arquitectura
CAMPO DE ESTUDIO
Ingeniería informática y de sistemas
AGENCIA EVALUADORA
Agencia para la Calidad del Sistema Universitario de Castilla y León
LISTADO DE ESPECIALIDADES
No existen datos
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		9
CRÉDITOS OPTATIVOS	**CRÉDITOS OBLIGATORIOS**	**CRÉDITOS TRABAJO FIN GRADO/ MÁSTER**
0	45	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**
05006594	Centro Universitario de Formación de la Policía Nacional, O.A.	Si	No

1.4-1.9.2 Centro Universitario de Formación de la Policía Nacional, O.A.

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**
No	No	Sí
PLAZAS POR MODALIDAD		
		35
NÚMERO TOTAL DE PLAZAS	**NÚMERO DE PLAZAS DE NUEVO INGRESO PARA PRIMER CURSO**	

35	35	
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. Objetivos formativos

1.3.1.a) Principales objetivos formativos del título

Los objetivos del plan formativo correspondiente al título y cuyo logro, en su caso, se verificará mediante la adquisición de los resultados de formación y del aprendizaje, son los siguientes:

- Dotar al estudiantado de los conocimientos teórico-prácticos que de modo específico rigen la labor directiva de la actividad de la Ciberdelincuencia en el ámbito policial.
- Garantizar una formación necesaria y homogénea en ciberinteligencia, ciberseguridad y ciberdelincuencia en la actividad policial.
- Desarrollar competencias relacionadas con la gestión documental y tratamiento de evidencias (preferentemente digitales) en el ámbito de la ciberinteligencia, ciberseguridad y ciberdelincuencia en la actividad policial.
- Fomentar habilidades de prevención, reacción e investigación en el ámbito de la ciberinteligencia, ciberseguridad y ciberdelincuencia en la actividad policial.
- Potenciar la capacidad de análisis y afrontamiento e intervención de situaciones que supongan riesgos o amenazas digitales en el ámbito de la ciberseguridad, ciberinteligencia y ciberdelincuencia en el ámbito policial.
- Favorecer la adquisición y consolidación, por parte de los profesionales policiales, de competencias de procedimientos metodológicos especializados relacionados con la ciberdelincuencia y la investigación policial.

ESTRUCTURAS CURRICULARES ESPECÍFICAS Y ESTRATEGIAS METODOLÓGICAS DE INNOVACIÓN DOCENTE

1.14 PERFILES FUNDAMENTALES DE EGRESO Y PROFESIONES REGULADAS

PERFILES DE EGRESO		
Ver al final del Apartado: Justificación (1.10)		
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
C01 - Describir las amenazas y vulnerabilidades en ciberseguridad y su impacto en infraestructuras críticas, con especial atención al ámbito policial. TIPO: Conocimientos o contenidos
C02 - Explicar las distintas legislaciones y mecanismos de prevención y respuesta en ciberseguridad, ciberdelincuencia y ciberinteligencia, aplicados a la función policial. TIPO: Conocimientos o contenidos
C03 - Distinguir, describir y explicar los fundamentos y aplicaciones del cifrado simétrico, asimétrico y los principales protocolos criptográficos. TIPO: Conocimientos o contenidos
C04 - Describir de forma detallada la Psicología del ciberdelincuente y manipulación digital en delitos como fraude, extorsión y desinformación. TIPO: Conocimientos o contenidos
C05 - Aplicar el tratamiento y custodia de evidencias digitales, asegurando su validez en investigaciones y procesos judiciales. TIPO: Conocimientos o contenidos
C06 - Aplicar análisis forense digital y trazabilidad en ciberdelincuencia, aplicando metodologías avanzadas en investigaciones policiales. TIPO: Conocimientos o contenidos

C07 - Analizar los protocolos de prevención, respuesta y recuperación ante ciberamenazas, aplicados a la protección de infraestructuras y la ciberdefensa institucional. TIPO: Conocimientos o contenidos
C08 - Aplicar los fundamentos de estadística aplicada a la ciberseguridad y la detección de patrones en datos masivo. TIPO: Conocimientos o contenidos
C09 - Definir la Inteligencia Artificial aplicada a la ciberseguridad y el cibercrimen, con uso en detección de amenazas y apoyo a investigaciones. TIPO: Conocimientos o contenidos
C10 - Detallar los modelos avanzados de aprendizaje profundo y su aplicación en la identificación de patrones de ciberdelincuencia. TIPO: Conocimientos o contenidos
H01-HC01 - Identificar y evaluar situaciones que requieran intervención operativa ante ciberamenazas en el ámbito policial. TIPO: Habilidades o destrezas
H02-HC02 - Identificar elementos clave para auditorías y evaluación de la seguridad en sistemas de información. TIPO: Habilidades o destrezas
H03-HC03 - Identificar y analizar fuentes de información relevantes para la seguridad y la actuación policial en ciberamenazas. TIPO: Habilidades o destrezas
H04-HC04 - Analizar e identificar infracciones y patrones de ciberdelincuencia y ciberataques en el marco de la legislación penal y administrativa. TIPO: Habilidades o destrezas
H05-HP01 - Utilizar aplicaciones informáticas para analizar y extraer conclusiones en ciberseguridad, ciberamenazas y ciberdelincuencia. TIPO: Habilidades o destrezas
H06-HP02 - Gestionar documentación clave en la prevención, reacción e investigación de la ciberdelincuencia. TIPO: Habilidades o destrezas
H07-HP03 - Redactar y presentar informes sobre incidentes cibernéticos y su impacto normativo en contextos policiales, judiciales y académicos. TIPO: Habilidades o destrezas
H08-HP04 - Diseñar, desarrollar o asesorar en protocolos de actuación para la prevención, reacción e investigación de ciberdelitos. TIPO: Habilidades o destrezas
H09-HP05 - Elaborar protocolos de seguridad sobre arquitectura, diseño seguro, infraestructura y gestión de riesgos en entornos cibernéticos. TIPO: Habilidades o destrezas
H10-HP06 - Aplicar herramientas de inteligencia artificial en la prevención e investigación de ciberdelitos. TIPO: Habilidades o destrezas
H11-HP07 - Aplicar métodos y técnicas en la investigación de la cibercriminalidad. TIPO: Habilidades o destrezas
K01 - Fomentar la colaboración plena con organismos españoles y extranjeros, públicos y privados, en cuestiones relacionadas con aspectos cibernéticos. TIPO: Competencias
K02 - Elaborar exposiciones de conclusiones de diferentes análisis y estudios, así como presentarlas en distintos ámbitos, como análisis situacionales, de riesgos, inteligencia o estratégicos. TIPO: Competencias
K03 - Garantizar el tratamiento adecuado de las evidencias informáticas, especialmente en el ámbito de la ciberseguridad y ciberdelincuencia. TIPO: Competencias
K04 - Diseñar acciones formativas, asesoramiento y protocolos orientados a minimizar los riesgos y consecuencias de incidentes cibernéticos. TIPO: Competencias
K05 - Analizar continuamente la situación sociopolítica en el ámbito competencial de la Policía Nacional en materia de ciberinteligencia, ciberseguridad y ciberdelincuencia, con el fin de detectar cambios presentes o futuros y fomentar el aprendizaje autorregulado y autónomo. TIPO: Competencias
K06 - Promover la formación en ciberinteligencia, ciberseguridad y ciberdelincuencia dentro de la Policía Nacional mediante los medios disponibles. TIPO: Competencias
K07 - Detectar la evolución de amenazas dirigidas a personas físicas y/o jurídicas vulnerables, infraestructuras críticas y servicios esenciales, así como la generación de nuevas amenazas, para adaptar las estrategias de actuación policial de manera efectiva. TIPO: Competencias
K08 - Gestionar incidentes y coordinar la respuesta ante amenazas en entornos digitales, aplicando estrategias de ciberseguridad y ciberdelincuencia en el ámbito de las ciencias policiales para la protección de infraestructuras críticas y la seguridad pública. TIPO: Competencias
K09 - Aplicar tecnologías avanzadas en ciberseguridad y análisis de amenazas digitales, utilizando herramientas forenses, inteligencia artificial y metodologías especializadas en el ámbito de la ciberdelincuencia y la investigación policial. 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) Perfil de ingreso recomendado

Este Máster Universitario está dirigido al funcionariado de la Policía Nacional que desempeñe funciones de mando y/o coordinación en el ámbito de la Ciberdelincuencia, tanto a nivel central como territorial. ~~No obstante, de manera excepcional, se podrá invitar a personas ajenas a la Policía Nacional a cursar el Máster Universitario, siempre que ocupen un puesto en las Administraciones Públicas relacionado con la función policial.~~

Los aspirantes, aparte de los conocimientos informáticos adquiridos en el proceso selectivo de ingreso a la Policía Nacional, la propia titulación (grado o titulación del mismo nivel) de áreas de conocimiento relacionadas con la ingeniería informática de acceso a un máster universitario, proceden de los campos de trabajo de las ciberamenazas, seguridad TIC, ciberseguridad, ciberinteligencia y ciberdelincuencia en los que, en principio, desarrollan o han desarrollado sus funciones con la consiguiente experiencia profesional adquirida y que ahora con esta titulación se trata de dar un paso en la especialización en las materias con capacidades para dirigir servicios policiales y equipos de trabajo, creando una unidad de acción en lo que a formación y actualización se refiere que repercuta en los más de 70.000 funcionarios que directa o indirectamente dependan de los egresados.

Para el correcto desempeño y aprovechamiento de la docencia, el estudiante deberá disponer de equipo informático con conexión a internet y equipamiento estándar para seguir una videoconferencia. Los estudiantes deben disponer para ello de un equipamiento informático básico con los siguientes requerimientos mínimos de software: Sistema operativo Windows 10 o superior, macOS 11 o superior, o una distribución moderna de Linux; un navegador actualizado: Google Chrome, Mozilla Firefox, Microsoft Edge o Safari (última versión estable); Hardware: PC, portátil, tablet o móvil con procesador moderno (Intel i3/Ryzen 3 o superior), 4 GB de RAM como mínimo, y conexión estable a Internet y tener altavoces o auriculares y micrófono. También deberá disponer de una cámara independiente (no integrada en el equipo informático, bien cámara web, o bien Tablet o smartphone con cámara).

3.1.b) Requisitos de acceso

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.c) Procedimiento y criterios de admisión

Los funcionarios/as policiales interesados realizarán la correspondiente solicitud en el procedimiento que se determine en la correspondiente convocatoria pública intraorganizacional, a la que acompañarán aquellos documentos que acrediten la condición y méritos solicitados según las bases que se establezcan en la misma.

La admisión de los miembros de la Policía Nacional, en la Dirección General de la Policía, se realizará atendiendo a quienes obtengan la mayor puntuación sobre 100, de los siguientes criterios específicos de admisión que obedecerán a la siguiente ponderación:

Desarrollar en la actualidad, o de modo inminente, puesto de trabajo que implique la actividad profesional en el ámbito de la ciberdelincuencia a nivel central en alguna de las unidades siguientes: -Unidad Central de Ciberdelincuencia de la Comisaría General de Policía Judicial. -Unidad Central de Apoyo Tecnológico o Jefatura de Sistemas Especiales de la División de Operaciones y Transformaciones digitales. -Unidad Informática Comunicaciones, de la Subdirección General de Logística e Innovación. -Unidad especializada en Ciberdelincuencia de la Comisaría General de Información.	40%
Desarrollar en la actualidad puesto de trabajo que implique la actividad profesional en el ámbito de la ciberdelincuencia a nivel central en alguna de las unidades diferentes a las anteriores en: - Comisaría General de Policía Judicial. - División de Operaciones y Transformaciones digitales. - Subdirección General de Logística e Innovación. - Comisaría General de Información.	20%
Desarrollar en la actualidad puesto de trabajo que implique la actividad profesional en el ámbito de la ciberdelincuencia a nivel territorial en alguna de las unidades de Policía Judicial o de Información.	15%
Haber desarrollado en el pasado o estar en disposición de desarrollar puesto de trabajo que implique la actividad profesional en el ámbito de la ciberdelincuencia a nivel central en alguna de las unidades siguientes: -Unidad Central de Ciberdelincuencia de la Comisaría General de Policía Judicial. -Unidad Central de Apoyo Tecnológico o Jefatura de Sistemas Especiales de la División de Operaciones y Transformaciones digitales. -Unidad Informática Comunicaciones, de la Subdirección General de Logística e Innovación. -Unidad especializada en Ciberdelincuencia de la Comisaría General de Información.	13%
Haber desarrollado en el pasado puesto de trabajo que implique la actividad profesional en el ámbito de la ciberdelincuencia a nivel central en alguna de las unidades diferentes a las referidas en el apartado anterior en: - Comisaría General de Policía Judicial. - División de Operaciones y Transformaciones digitales. - Subdirección General de Logística e Innovación. - Comisaría General de Información.	6%
Desarrollar la actividad profesional en destinos nacionales de la Policía Nacional.	5%
Desarrollar la actividad profesional en Policía Nacional fuera del territorio nacional.	1%

3.2 CRITERIOS PARA EL RECONOCIMIENTO Y TRANSFERENCIAS DE CRÉDITOS

Reconocimiento de Créditos cursados en centros de formación profesional de grado superior	
MÍNIMO	**MÁXIMO**
0	0
Adjuntar Convenio	
Reconocimiento de Créditos Cursados en Títulos Propios	
MÍNIMO	**MÁXIMO**
0	0
Adjuntar Título Propio	
Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional	
MÍNIMO	**MÁXIMO**
0	0
DESCRIPCIÓN	
No procede.	
3.3 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.		
NIVEL 1: Fundamentos de ciberdelincuencia y legislación		
4.1.1 Datos Básicos del Nivel 1		
ECTS NIVEL1	12	
NIVEL 2: Fundamentos de ciberdelincuencia y legislación		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	12	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
12		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Ciberinteligencia y ciberdelincuencia en el ámbito Policial		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
3		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**

ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Criptografía aplicada y seguridad de la información		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
3		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Psicología del ciberdelincuente y sociología digital		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
3		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Legislación nacional e internacional en ciberdelincuencia		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
3		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
C03 - Distinguir, describir y explicar los fundamentos y aplicaciones del cifrado simétrico, asimétrico y los principales protocolos criptográficos. TIPO: Conocimientos o contenidos		
C04 - Describir de forma detallada la Psicología del ciberdelincuente y manipulación digital en delitos como fraude, extorsión y desinformación. TIPO: Conocimientos o contenidos		
C05 - Aplicar el tratamiento y custodia de evidencias digitales, asegurando su validez en investigaciones y procesos judiciales. TIPO: Conocimientos o contenidos		
H01-HC01 - Identificar y evaluar situaciones que requieran intervención operativa ante ciberamenazas en el ámbito policial. TIPO: Habilidades o destrezas		
H03-HC03 - Identificar y analizar fuentes de información relevantes para la seguridad y la actuación policial en ciberamenazas. TIPO: Habilidades o destrezas		
H04-HC04 - Analizar e identificar infracciones y patrones de ciberdelincuencia y ciberataques en el marco de la legislación penal y administrativa. TIPO: Habilidades o destrezas		

H05-HP01 - Utilizar aplicaciones informáticas para analizar y extraer conclusiones en ciberseguridad, ciberamenazas y ciberdelincuencia. TIPO: Habilidades o destrezas
H07-HP03 - Redactar y presentar informes sobre incidentes cibernéticos y su impacto normativo en contextos policiales, judiciales y académicos. TIPO: Habilidades o destrezas
H09-HP05 - Elaborar protocolos de seguridad sobre arquitectura, diseño seguro, infraestructura y gestión de riesgos en entornos cibernéticos. TIPO: Habilidades o destrezas
H10-HP06 - Aplicar herramientas de inteligencia artificial en la prevención e investigación de ciberdelitos. TIPO: Habilidades o destrezas
H11-HP07 - Aplicar métodos y técnicas en la investigación de la cibercriminalidad. TIPO: Habilidades o destrezas
K01 - Fomentar la colaboración plena con organismos españoles y extranjeros, públicos y privados, en cuestiones relacionadas con aspectos cibernéticos. TIPO: Competencias
K02 - Elaborar exposiciones de conclusiones de diferentes análisis y estudios, así como presentarlas en distintos ámbitos, como análisis situacionales, de riesgos, inteligencia o estratégicos. TIPO: Competencias
K03 - Garantizar el tratamiento adecuado de las evidencias informáticas, especialmente en el ámbito de la ciberseguridad y ciberdelincuencia. TIPO: Competencias
K04 - Diseñar acciones formativas, asesoramiento y protocolos orientados a minimizar los riesgos y consecuencias de incidentes cibernéticos. TIPO: Competencias
K05 - Analizar continuamente la situación sociopolítica en el ámbito competencial de la Policía Nacional en materia de ciberinteligencia, ciberseguridad y ciberdelincuencia, con el fin de detectar cambios presentes o futuros y fomentar el aprendizaje autorregulado y autónomo. TIPO: Competencias
K06 - Promover la formación en ciberinteligencia, ciberseguridad y ciberdelincuencia dentro de la Policía Nacional mediante los medios disponibles. TIPO: Competencias
K08 - Gestionar incidentes y coordinar la respuesta ante amenazas en entornos digitales, aplicando estrategias de ciberseguridad y ciberdelincuencia en el ámbito de las ciencias policiales para la protección de infraestructuras críticas y la seguridad pública. TIPO: Competencias
C01 - Describir las amenazas y vulnerabilidades en ciberseguridad y su impacto en infraestructuras críticas, con especial atención al ámbito policial. TIPO: Conocimientos o contenidos
C02 - Explicar las distintas legislaciones y mecanismos de prevención y respuesta en ciberseguridad, ciberdelincuencia y ciberinteligencia, aplicados a la función policial. TIPO: Conocimientos o contenidos

NIVEL 1: Técnicas de investigación y análisis		
4.1.1 Datos Básicos del Nivel 1		
ECTS NIVEL1	9	
NIVEL 2: Técnicas de investigación y análisis		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	9	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
9		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Recopilación y análisis de Información en fuentes abiertas		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**

3		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Inteligencia estratégica en ciberseguridad		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
3		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Análisis forense digital y preservación de la cadena de custodia		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
3		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
C05 - Aplicar el tratamiento y custodia de evidencias digitales, asegurando su validez en investigaciones y procesos judiciales. TIPO: Conocimientos o contenidos		
C06 - Aplicar análisis forense digital y trazabilidad en ciberdelincuencia, aplicando metodologías avanzadas en investigaciones policiales. TIPO: Conocimientos o contenidos		
C07 - Analizar los protocolos de prevención, respuesta y recuperación ante ciberamenazas, aplicados a la protección de infraestructuras y la ciberdefensa institucional. TIPO: Conocimientos o contenidos		
H01-HC01 - Identificar y evaluar situaciones que requieran intervención operativa ante ciberamenazas en el ámbito policial. TIPO: Habilidades o destrezas		
H02-HC02 - Identificar elementos clave para auditorías y evaluación de la seguridad en sistemas de información. TIPO: Habilidades o destrezas		
H03-HC03 - Identificar y analizar fuentes de información relevantes para la seguridad y la actuación policial en ciberamenazas. TIPO: Habilidades o destrezas		
H06-HP02 - Gestionar documentación clave en la prevención, reacción e investigación de la ciberdelincuencia. TIPO: Habilidades o destrezas		
H08-HP04 - Diseñar, desarrollar o asesorar en protocolos de actuación para la prevención, reacción e investigación de ciberdelitos. TIPO: Habilidades o destrezas		
H10-HP06 - Aplicar herramientas de inteligencia artificial en la prevención e investigación de ciberdelitos. TIPO: Habilidades o destrezas		
H11-HP07 - Aplicar métodos y técnicas en la investigación de la cibercriminalidad. TIPO: Habilidades o destrezas		

K01 - Fomentar la colaboración plena con organismos españoles y extranjeros, públicos y privados, en cuestiones relacionadas con aspectos cibernéticos. TIPO: Competencias
K02 - Elaborar exposiciones de conclusiones de diferentes análisis y estudios, así como presentarlas en distintos ámbitos, como análisis situacionales, de riesgos, inteligencia o estratégicos. TIPO: Competencias
K03 - Garantizar el tratamiento adecuado de las evidencias informáticas, especialmente en el ámbito de la ciberseguridad y ciberdelincuencia. TIPO: Competencias
K05 - Analizar continuamente la situación sociopolítica en el ámbito competencial de la Policía Nacional en materia de ciberinteligencia, ciberseguridad y ciberdelincuencia, con el fin de detectar cambios presentes o futuros y fomentar el aprendizaje autorregulado y autónomo. TIPO: Competencias
K06 - Promover la formación en ciberinteligencia, ciberseguridad y ciberdelincuencia dentro de la Policía Nacional mediante los medios disponibles. TIPO: Competencias
K07 - Detectar la evolución de amenazas dirigidas a personas físicas y/o jurídicas vulnerables, infraestructuras críticas y servicios esenciales, así como la generación de nuevas amenazas, para adaptar las estrategias de actuación policial de manera efectiva. TIPO: Competencias
K08 - Gestionar incidentes y coordinar la respuesta ante amenazas en entornos digitales, aplicando estrategias de ciberseguridad y ciberdelincuencia en el ámbito de las ciencias policiales para la protección de infraestructuras críticas y la seguridad pública. TIPO: Competencias
K09 - Aplicar tecnologías avanzadas en ciberseguridad y análisis de amenazas digitales, utilizando herramientas forenses, inteligencia artificial y metodologías especializadas en el ámbito de la ciberdelincuencia y la investigación policial. TIPO: Competencias
C01 - Describir las amenazas y vulnerabilidades en ciberseguridad y su impacto en infraestructuras críticas, con especial atención al ámbito policial. TIPO: Conocimientos o contenidos

NIVEL 1: Ciberataques y gestión de incidentes de seguridad		
4.1.1 Datos Básicos del Nivel 1		
ECTS NIVEL1	9	
NIVEL 2: Ciberataques y seguridad ofensiva		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	9	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
9		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Ciberataques y gestión de incidentes de seguridad		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
3		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Criptoactivos, blockchain y fraudes cibernéticos		

4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
3		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Hacking ético y auditorías de seguridad		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
3		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
C03 - Distinguir, describir y explicar los fundamentos y aplicaciones del cifrado simétrico, asimétrico y los principales protocolos criptográficos. TIPO: Conocimientos o contenidos		
C07 - Analizar los protocolos de prevención, respuesta y recuperación ante ciberamenazas, aplicados a la protección de infraestructuras y la ciberdefensa institucional. TIPO: Conocimientos o contenidos		
H01-HC01 - Identificar y evaluar situaciones que requieran intervención operativa ante ciberamenazas en el ámbito policial. TIPO: Habilidades o destrezas		
H02-HC02 - Identificar elementos clave para auditorías y evaluación de la seguridad en sistemas de información. TIPO: Habilidades o destrezas		
H04-HC04 - Analizar e identificar infracciones y patrones de ciberdelincuencia y ciberataques en el marco de la legislación penal y administrativa. TIPO: Habilidades o destrezas		
H08-HP04 - Diseñar, desarrollar o asesorar en protocolos de actuación para la prevención, reacción e investigación de ciberdelitos. TIPO: Habilidades o destrezas		
H09-HP05 - Elaborar protocolos de seguridad sobre arquitectura, diseño seguro, infraestructura y gestión de riesgos en entornos cibernéticos. TIPO: Habilidades o destrezas		
H11-HP07 - Aplicar métodos y técnicas en la investigación de la cibercriminalidad. TIPO: Habilidades o destrezas		
K03 - Garantizar el tratamiento adecuado de las evidencias informáticas, especialmente en el ámbito de la ciberseguridad y ciberdelincuencia. TIPO: Competencias		
K04 - Diseñar acciones formativas, asesoramiento y protocolos orientados a minimizar los riesgos y consecuencias de incidentes cibernéticos. TIPO: Competencias		
K07 - Detectar la evolución de amenazas dirigidas a personas físicas y/o jurídicas vulnerables, infraestructuras críticas y servicios esenciales, así como la generación de nuevas amenazas, para adaptar las estrategias de actuación policial de manera efectiva. TIPO: Competencias		
K08 - Gestionar incidentes y coordinar la respuesta ante amenazas en entornos digitales, aplicando estrategias de ciberseguridad y ciberdelincuencia en el ámbito de las ciencias policiales para la protección de infraestructuras críticas y la seguridad pública. TIPO: Competencias		

K09 - Aplicar tecnologías avanzadas en ciberseguridad y análisis de amenazas digitales, utilizando herramientas forenses, inteligencia artificial y metodologías especializadas en el ámbito de la ciberdelincuencia y la investigación policial. TIPO: Competencias		
C01 - Describir las amenazas y vulnerabilidades en ciberseguridad y su impacto en infraestructuras críticas, con especial atención al ámbito policial. TIPO: Conocimientos o contenidos		
NIVEL 1: Inteligencia Artificial		
4.1.1 Datos Básicos del Nivel 1		
ECTS NIVEL1	9	
NIVEL 2: Inteligencia Artificial		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	9	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	9	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Aprendizaje estadístico y análisis de datos		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	3	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Fundamentos de inteligencia artificial y aprendizaje automático		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	3	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Modelos avanzados de inteligencia artificial en ciberdelincuencia		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	3	Semestral
DESPLIEGUE TEMPORAL		

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

4.1.1.2 RESULTADOS DE APRENDIZAJE
C08 - Aplicar los fundamentos de estadística aplicada a la ciberseguridad y la detección de patrones en datos masivo. TIPO: Conocimientos o contenidos
C09 - Definir la Inteligencia Artificial aplicada a la ciberseguridad y el cibercrimen, con uso en detección de amenazas y apoyo a investigaciones. TIPO: Conocimientos o contenidos
C10 - Detallar los modelos avanzados de aprendizaje profundo y su aplicación en la identificación de patrones de ciberdelincuencia. TIPO: Conocimientos o contenidos
H05-HP01 - Utilizar aplicaciones informáticas para analizar y extraer conclusiones en ciberseguridad, ciberamenazas y ciberdelincuencia. TIPO: Habilidades o destrezas
H07-HP03 - Redactar y presentar informes sobre incidentes cibernéticos y su impacto normativo en contextos policiales, judiciales y académicos. TIPO: Habilidades o destrezas
H10-HP06 - Aplicar herramientas de inteligencia artificial en la prevención e investigación de ciberdelitos. TIPO: Habilidades o destrezas
H11-HP07 - Aplicar métodos y técnicas en la investigación de la cibercriminalidad. TIPO: Habilidades o destrezas
K06 - Promover la formación en ciberinteligencia, ciberseguridad y ciberdelincuencia dentro de la Policía Nacional mediante los medios disponibles. TIPO: Competencias
K07 - Detectar la evolución de amenazas dirigidas a personas físicas y/o jurídicas vulnerables, infraestructuras críticas y servicios esenciales, así como la generación de nuevas amenazas, para adaptar las estrategias de actuación policial de manera efectiva. TIPO: Competencias
K09 - Aplicar tecnologías avanzadas en ciberseguridad y análisis de amenazas digitales, utilizando herramientas forenses, inteligencia artificial y metodologías especializadas en el ámbito de la ciberdelincuencia y la investigación policial. TIPO: Competencias

NIVEL 1: Metodología de investigación y aplicaciones prácticas	
4.1.1 Datos Básicos del Nivel 1	
ECTS NIVEL1	6

NIVEL 2: Metodología de investigación y aplicaciones prácticas	
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**

NIVEL 3: Metodología de investigación en ciberdelincuencia		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	3	Semestral
DESPLIEGUE TEMPORAL		

ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3

	3	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Estudio de casos reales en ciberdelincuencia y ciberseguridad		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	3	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
C05 - Aplicar el tratamiento y custodia de evidencias digitales, asegurando su validez en investigaciones y procesos judiciales. TIPO: Conocimientos o contenidos		
C06 - Aplicar análisis forense digital y trazabilidad en ciberdelincuencia, aplicando metodologías avanzadas en investigaciones policiales. TIPO: Conocimientos o contenidos		
H01-HC01 - Identificar y evaluar situaciones que requieran intervención operativa ante ciberamenazas en el ámbito policial. TIPO: Habilidades o destrezas		
H02-HC02 - Identificar elementos clave para auditorías y evaluación de la seguridad en sistemas de información. TIPO: Habilidades o destrezas		
H03-HC03 - Identificar y analizar fuentes de información relevantes para la seguridad y la actuación policial en ciberamenazas. TIPO: Habilidades o destrezas		
H04-HC04 - Analizar e identificar infracciones y patrones de ciberdelincuencia y ciberataques en el marco de la legislación penal y administrativa. TIPO: Habilidades o destrezas		
H05-HP01 - Utilizar aplicaciones informáticas para analizar y extraer conclusiones en ciberseguridad, ciberamenazas y ciberdelincuencia. TIPO: Habilidades o destrezas		
H06-HP02 - Gestionar documentación clave en la prevención, reacción e investigación de la ciberdelincuencia. TIPO: Habilidades o destrezas		
H07-HP03 - Redactar y presentar informes sobre incidentes cibernéticos y su impacto normativo en contextos policiales, judiciales y académicos. TIPO: Habilidades o destrezas		
H08-HP04 - Diseñar, desarrollar o asesorar en protocolos de actuación para la prevención, reacción e investigación de ciberdelitos. TIPO: Habilidades o destrezas		
H09-HP05 - Elaborar protocolos de seguridad sobre arquitectura, diseño seguro, infraestructura y gestión de riesgos en entornos cibernéticos. TIPO: Habilidades o destrezas		
H11-HP07 - Aplicar métodos y técnicas en la investigación de la cibercriminalidad. TIPO: Habilidades o destrezas		
K01 - Fomentar la colaboración plena con organismos españoles y extranjeros, públicos y privados, en cuestiones relacionadas con aspectos cibernéticos. TIPO: Competencias		
K02 - Elaborar exposiciones de conclusiones de diferentes análisis y estudios, así como presentarlas en distintos ámbitos, como análisis situacionales, de riesgos, inteligencia o estratégicos. TIPO: Competencias		
K05 - Analizar continuamente la situación sociopolítica en el ámbito competencial de la Policía Nacional en materia de ciberinteligencia, ciberseguridad y ciberdelincuencia, con el fin de detectar cambios presentes o futuros y fomentar el aprendizaje autorregulado y autónomo. TIPO: Competencias		
K06 - Promover la formación en ciberinteligencia, ciberseguridad y ciberdelincuencia dentro de la Policía Nacional mediante los medios disponibles. TIPO: Competencias		

C01 - Describir las amenazas y vulnerabilidades en ciberseguridad y su impacto en infraestructuras críticas, con especial atención al ámbito policial. TIPO: Conocimientos o contenidos		
NIVEL 1: Prácticas profesionales		
4.1.1 Datos Básicos del Nivel 1		
ECTS NIVEL1	9	
NIVEL 2: Prácticas profesionales		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Prácticas Externas	
ECTS NIVEL 2	9	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	9	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Prácticas académicas externas		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Prácticas Externas	9	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	9	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
C03 - Distinguir, describir y explicar los fundamentos y aplicaciones del cifrado simétrico, asimétrico y los principales protocolos criptográficos. TIPO: Conocimientos o contenidos		
C04 - Describir de forma detallada la Psicología del ciberdelincuente y manipulación digital en delitos como fraude, extorsión y desinformación. TIPO: Conocimientos o contenidos		
C05 - Aplicar el tratamiento y custodia de evidencias digitales, asegurando su validez en investigaciones y procesos judiciales. TIPO: Conocimientos o contenidos		
C06 - Aplicar análisis forense digital y trazabilidad en ciberdelincuencia, aplicando metodologías avanzadas en investigaciones policiales. TIPO: Conocimientos o contenidos		
C07 - Analizar los protocolos de prevención, respuesta y recuperación ante ciberamenazas, aplicados a la protección de infraestructuras y la ciberdefensa institucional. TIPO: Conocimientos o contenidos		
C08 - Aplicar los fundamentos de estadística aplicada a la ciberseguridad y la detección de patrones en datos masivo. TIPO: Conocimientos o contenidos		
C09 - Definir la Inteligencia Artificial aplicada a la ciberseguridad y el cibercrimen, con uso en detección de amenazas y apoyo a investigaciones. TIPO: Conocimientos o contenidos		
C10 - Detallar los modelos avanzados de aprendizaje profundo y su aplicación en la identificación de patrones de ciberdelincuencia. TIPO: Conocimientos o contenidos		
H01-HC01 - Identificar y evaluar situaciones que requieran intervención operativa ante ciberamenazas en el ámbito policial. TIPO: Habilidades o destrezas		
H02-HC02 - Identificar elementos clave para auditorías y evaluación de la seguridad en sistemas de información. TIPO: Habilidades o destrezas		

H03-HC03 - Identificar y analizar fuentes de información relevantes para la seguridad y la actuación policial en ciberamenazas. TIPO: Habilidades o destrezas
H04-HC04 - Analizar e identificar infracciones y patrones de ciberdelincuencia y ciberataques en el marco de la legislación penal y administrativa. TIPO: Habilidades o destrezas
H05-HP01 - Utilizar aplicaciones informáticas para analizar y extraer conclusiones en ciberseguridad, ciberamenazas y ciberdelincuencia. TIPO: Habilidades o destrezas
H06-HP02 - Gestionar documentación clave en la prevención, reacción e investigación de la ciberdelincuencia. TIPO: Habilidades o destrezas
H07-HP03 - Redactar y presentar informes sobre incidentes cibernéticos y su impacto normativo en contextos policiales, judiciales y académicos. TIPO: Habilidades o destrezas
H08-HP04 - Diseñar, desarrollar o asesorar en protocolos de actuación para la prevención, reacción e investigación de ciberdelitos. TIPO: Habilidades o destrezas
H09-HP05 - Elaborar protocolos de seguridad sobre arquitectura, diseño seguro, infraestructura y gestión de riesgos en entornos cibernéticos. TIPO: Habilidades o destrezas
H10-HP06 - Aplicar herramientas de inteligencia artificial en la prevención e investigación de ciberdelitos. TIPO: Habilidades o destrezas
H11-HP07 - Aplicar métodos y técnicas en la investigación de la cibercriminalidad. TIPO: Habilidades o destrezas
K01 - Fomentar la colaboración plena con organismos españoles y extranjeros, públicos y privados, en cuestiones relacionadas con aspectos cibernéticos. TIPO: Competencias
K02 - Elaborar exposiciones de conclusiones de diferentes análisis y estudios, así como presentarlas en distintos ámbitos, como análisis situacionales, de riesgos, inteligencia o estratégicos. TIPO: Competencias
K03 - Garantizar el tratamiento adecuado de las evidencias informáticas, especialmente en el ámbito de la ciberseguridad y ciberdelincuencia. TIPO: Competencias
K04 - Diseñar acciones formativas, asesoramiento y protocolos orientados a minimizar los riesgos y consecuencias de incidentes cibernéticos. TIPO: Competencias
K05 - Analizar continuamente la situación sociopolítica en el ámbito competencial de la Policía Nacional en materia de ciberinteligencia, ciberseguridad y ciberdelincuencia, con el fin de detectar cambios presentes o futuros y fomentar el aprendizaje autorregulado y autónomo. TIPO: Competencias
K06 - Promover la formación en ciberinteligencia, ciberseguridad y ciberdelincuencia dentro de la Policía Nacional mediante los medios disponibles. TIPO: Competencias
K07 - Detectar la evolución de amenazas dirigidas a personas físicas y/o jurídicas vulnerables, infraestructuras críticas y servicios esenciales, así como la generación de nuevas amenazas, para adaptar las estrategias de actuación policial de manera efectiva. TIPO: Competencias
K08 - Gestionar incidentes y coordinar la respuesta ante amenazas en entornos digitales, aplicando estrategias de ciberseguridad y ciberdelincuencia en el ámbito de las ciencias policiales para la protección de infraestructuras críticas y la seguridad pública. TIPO: Competencias
K09 - Aplicar tecnologías avanzadas en ciberseguridad y análisis de amenazas digitales, utilizando herramientas forenses, inteligencia artificial y metodologías especializadas en el ámbito de la ciberdelincuencia y la investigación policial. TIPO: Competencias
C01 - Describir las amenazas y vulnerabilidades en ciberseguridad y su impacto en infraestructuras críticas, con especial atención al ámbito policial. TIPO: Conocimientos o contenidos
C02 - Explicar las distintas legislaciones y mecanismos de prevención y respuesta en ciberseguridad, ciberdelincuencia y ciberinteligencia, aplicados a la función policial. TIPO: Conocimientos o contenidos

NIVEL 1: Trabajo fin de máster	
4.1.1 Datos Básicos del Nivel 1	
ECTS NIVEL1	6
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**

NIVEL 3: Trabajo fin de máster		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Trabajo Fin de Grado / Máster	6	Semestral

DESPLIEGUE TEMPORAL		
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**

4.1.1.2 RESULTADOS DE APRENDIZAJE
C03 - Distinguir, describir y explicar los fundamentos y aplicaciones del cifrado simétrico, asimétrico y los principales protocolos criptográficos. TIPO: Conocimientos o contenidos
C04 - Describir de forma detallada la Psicología del ciberdelincuente y manipulación digital en delitos como fraude, extorsión y desinformación. TIPO: Conocimientos o contenidos
C08 - Aplicar los fundamentos de estadística aplicada a la ciberseguridad y la detección de patrones en datos masivo. TIPO: Conocimientos o contenidos
C09 - Definir la Inteligencia Artificial aplicada a la ciberseguridad y el cibercrimen, con uso en detección de amenazas y apoyo a investigaciones. TIPO: Conocimientos o contenidos
C10 - Detallar los modelos avanzados de aprendizaje profundo y su aplicación en la identificación de patrones de ciberdelincuencia. TIPO: Conocimientos o contenidos
H08-HP04 - Diseñar, desarrollar o asesorar en protocolos de actuación para la prevención, reacción e investigación de ciberdelitos. TIPO: Habilidades o destrezas
H09-HP05 - Elaborar protocolos de seguridad sobre arquitectura, diseño seguro, infraestructura y gestión de riesgos en entornos cibernéticos. TIPO: Habilidades o destrezas
H10-HP06 - Aplicar herramientas de inteligencia artificial en la prevención e investigación de ciberdelitos. TIPO: Habilidades o destrezas
K02 - Elaborar exposiciones de conclusiones de diferentes análisis y estudios, así como presentarlas en distintos ámbitos, como análisis situacionales, de riesgos, inteligencia o estratégicos. TIPO: Competencias
K04 - Diseñar acciones formativas, asesoramiento y protocolos orientados a minimizar los riesgos y consecuencias de incidentes cibernéticos. TIPO: Competencias
K06 - Promover la formación en ciberinteligencia, ciberseguridad y ciberdelincuencia dentro de la Policía Nacional mediante los medios disponibles. TIPO: Competencias
4.2 ACTIVIDADES Y METODOLOGÍAS DOCENTES
ACTIVIDADES FORMATIVAS

4.2. Actividades y metodologías docentes

A tenor de la naturaleza de la titulación y de sus destinatarios, la modalidad de impartición será virtual. La misma sería en modo síncrono con independencia de que las clases quedasen grabadas, con lo cual, en sentido estricto, habría una conjugación de ambas modalidades, si bien, la predominante sería la síncrona.

Las actividades formativas dentro de la titulación comprenderán la siguiente tipología:

- **Clases teóricas:** Actividad formativa virtual síncrona que consiste en la exposición de contenidos fundamentales del texto base por parte del profesorado. Se desarrolla en las correspondientes sesiones de cada materia. Se prioriza la transmisión de conocimientos por parte del profesor, exigiendo al alumnado la preparación previa o el estudio posterior de los contenidos relacionados con la clase.
- **Lectura y preparación del material y recursos complementarios:** Actividad formativa no presencial que consiste en que los estudiantes lean y preparen los contenidos del texto base y, en su caso, los recursos complementarios (documentación) de cada materia que estarán disponibles en la plataforma Studium.
- **Clases prácticas:** a través de resolución de problemas, de casos y situaciones vinculadas a la práctica profesional.
- **Actividades formativas on-line**: que consiste en el planteamiento, desarrollo y resolución de casos prácticos o de otra actividad sobre las materias del programa. Se realizarán los planteamientos de las prácticas en la plataforma virtual de forma asincrónica y se revisarán en sesiones síncronas con los estudiantes.
- **Foros**: Actividad formativa virtual que consiste en el planteamiento de temas para su debate por los estudiantes. Los debates estarán moderados por el profesorado y se referirán a aspectos de interés relacionados con cada materia. Se desarrollarán en la plataforma virtual de forma asíncrona.
- **Elaboración de informes, proyectos o trabajos**: individuales o en grupo. Exposición de informes, proyectos o trabajos: individuales o en grupo. Se desarrollarán de forma virtual síncrona en el aula.
- **Tutorías:** Actividad formativa virtual a través de la que se realiza el seguimiento y asesoramiento de los estudiantes relacionado con el desarrollo de cada materia por parte de un tutor o tutora. Se realizarán sesiones virtuales síncronas para estas actividades de tutorización.
- **Tareas en entornos profesionales:** de manera que el alumno/a de forma autónoma aplicará los resultados de formación y del aprendizaje alcanzados en su formación en escenarios reales en el que aplicar las funciones y operatividad policial.

- **Tutorías específicas:** Tutorías asociadas a la realización de las prácticas profesionales. La finalidad es la llevar a cabo un seguimiento de las funciones realizadas por el estudiante. Se desarrollarán de manera presencial con el tutor/a profesional designado de la unidad policial correspondiente.
- **Elaboración memoria en centro de trabajo de prácticas:** esta incluirá, como mínimo, un análisis de la organización del centro, las actividades realizadas y repercusión de sus aportaciones y conclusiones vinculados con los resultados de formación y del aprendizaje.

- **Elaboración del TFM**: Actividad formativa que consiste en la realización del trabajo personal y autónomo obligatorio del fin del Máster, de acuerdo con la normativa específica al efecto. El trabajo se realizará bajo la dirección académica de un profesor o profesora del Máster.
- **Tutorías específicas TFM:** Tutorías asociadas a la realización del TFM. El objeto de estas tutorías es el de realizar un adecuado planteamiento del TFM y un seguimiento de los avances del trabajo individual y autónomo del estudiante. En ellas se orientará y tutelará al estudiante para el correcto desarrollo de su trabajo. Estas podrán desarrollarse en modalidad virtual y, si así se acordase, de manera individual o grupal, siendo en este último caso los aspectos genéricos a abordar los relacionados con la estructura, formalidad... del Trabajo. Aplicable solo en la materia TFM.
- **Presentación y defensa:** exposición y defensa de forma virtual ~~de forma presencial, con independencia de situaciones excepcionales que por su justificación se autorice motivadamente a que se realice de forma virtual~~ ante un tribunal de conclusiones resultantes de un trabajo de investigación original.

METODOLOGÍAS DOCENTES

4.2. Actividades y metodologías docentes

A tenor de la naturaleza de la titulación y de sus destinatarios, la modalidad de impartición será virtual. La misma sería en modo síncrono con independencia de que las clases quedasen grabadas, con lo cual, en sentido estricto, habría una conjugación de ambas modalidades, si bien, la predominante sería la síncrona.

Las actividades formativas dentro de la titulación comprenderán la siguiente tipología:

- **Clases teóricas:** Actividad formativa virtual síncrona que consiste en la exposición de contenidos fundamentales del texto base por parte del profesorado. Se desarrolla en las correspondientes sesiones de cada materia. Se prioriza la transmisión de conocimientos por parte del profesor, exigiendo al alumnado la preparación previa o el estudio posterior de los contenidos relacionados con la clase.
- **Lectura y preparación del material y recursos complementarios:** Actividad formativa no presencial que consiste en que los estudiantes lean y preparen los contenidos del texto base y, en su caso, los recursos complementarios (documentación) de cada materia que estarán disponibles en la plataforma Studium.
- **Clases prácticas:** a través de resolución de problemas, de casos y situaciones vinculadas a la práctica profesional.
- **Actividades formativas on-line**: que consiste en el planteamiento, desarrollo y resolución de casos prácticos o de otra actividad sobre las materias del programa. Se realizarán los planteamientos de las prácticas en la plataforma virtual de forma asincrónica y se revisarán en sesiones síncronas con los estudiantes.
- **Foros**: Actividad formativa virtual que consiste en el planteamiento de temas para su debate por los estudiantes. Los debates estarán moderados por el profesorado y se referirán a aspectos de interés relacionados con cada materia. Se desarrollarán en la plataforma virtual de forma asíncrona.
- **Elaboración de informes, proyectos o trabajos**: individuales o en grupo. Exposición de informes, proyectos o trabajos: individuales o en grupo. Se desarrollarán de forma virtual síncrona en el aula.
- **Tutorías:** Actividad formativa virtual a través de la que se realiza el seguimiento y asesoramiento de los estudiantes relacionado con el desarrollo de cada materia por parte de un tutor o tutora. Se realizarán sesiones virtuales síncronas para estas actividades de tutorización.
- **Tareas en entornos profesionales:** de manera que el alumno/a de forma autónoma aplicará los resultados de formación y del aprendizaje alcanzados en su formación en escenarios reales en el que aplicar las funciones y operatividad policial.
    - **Tutorías específicas:** Tutorías asociadas a la realización de las prácticas profesionales. La finalidad es la llevar a cabo un seguimiento de las funciones realizadas por el estudiante. Se desarrollarán de manera presencial con el tutor/a profesional designado de la unidad policial correspondiente.
    - **Elaboración memoria en centro de trabajo de prácticas:** esta incluirá, como mínimo, un análisis de la organización del centro, las actividades realizadas y repercusión de sus aportaciones y conclusiones vinculados con los resultados de formación y del aprendizaje.
- **Elaboración del TFM**: Actividad formativa que consiste en la realización del trabajo personal y autónomo obligatorio del fin del Máster, de acuerdo con la normativa específica al efecto. El trabajo se realizará bajo la dirección académica de un profesor o profesora del Máster.
- **Tutorías específicas TFM:** Tutorías asociadas a la realización del TFM. El objeto de estas tutorías es el de realizar un adecuado planteamiento del TFM y un seguimiento de los avances del trabajo individual y autónomo del estudiante. En ellas se orientará y tutelará al estudiante para el correcto desarrollo de su trabajo. Estas podrán desarrollarse en modalidad virtual y, si así se acordase, de manera individual o grupal, siendo en este último caso los aspectos genéricos a abordar los relacionados con la estructura, formalidad... del Trabajo. Aplicable solo en la materia TFM.

- **Presentación y defensa:** exposición y defensa de forma virtual ~~de forma presencial, con independencia de situaciones excepcionales que por su justificación se autorice motivadamente a que se realice de forma virtual~~ ante un tribunal de conclusiones resultantes de un trabajo de investigación original.

4.3 SISTEMAS DE EVALUACIÓN

Los criterios e instrumentos de evaluación concretos para cada asignatura, así como la repercusión que tendrán en las calificaciones finales, se fijarán por materias en la presente memoria. El estudiantado tendrá a su disposición en la Guía Académica los sistemas de evaluación de cada una de las asignaturas que componen el plan de estudios antes de comenzar el curso académico, previa revisión por la Comisión Académica de la Titulación. Para las asignaturas de los Módulos I al V, el sistema de evaluación propuesto es la evaluación continua y sumativa, utilizando instrumentos de cada uno de los bloques que se describen a continuación. La combinación de medios y pruebas, así como su peso en la evaluación global, las deberá ajustar el profesorado de cada asignatura. Los instrumentos, modos y rangos de evaluación son:

- Participación individual (entre 0 y 10 % de la calificación final):
- Participación activa en el aula virtual y/o foros. Valoración mediante control de participación.
- Participación en tutorías individuales virtuales. Valoración mediante control de participación.
- Pruebas de autoevaluación individuales virtuales. Valoración mediante rúbrica, salvo que sean pruebas tipo test o cuestionarios.
- ~~Trabajos individuales o grupales (entre 40 y 60% de la calificación final):~~

- ~~Evaluación de trabajos consistentes, individuales o en grupo, entre otros, en resolución de casos prácticos, elaboración de informes, (individuales o grupales), aplicando los conocimientos adquiridos en las diferentes materias. Valoración mediante rúbrica.~~

- ~~Exposición de trabajos o proyectos individual o de grupo en aula virtual. Valoración mediante control de asistencia y/o participación.~~

- Trabajos individuales (hasta 40 % de la calificación final):
  - Evaluación de trabajos individuales~~,~~ consistentes, entre otros, en resolución de casos prácticos, elaboración de informes, aplicando los conocimientos adquiridos en las diferentes materias. Valoración mediante rúbrica.
  - Exposición de trabajos o proyectos individuales en aula virtual. Valoración mediante rúbrica.

- Trabajos grupales (hasta 30 % de la calificación final):
  - Evaluación de trabajos grupales consistentes, entre otros, en resolución de casos prácticos, elaboración de informes, aplicando los conocimientos adquiridos en las diferentes materias. Valoración mediante rúbrica.
  - Exposición de trabajos o proyectos grupales en aula virtual. Valoración mediante rúbrica.

- Pruebas escritas u orales individuales (entre 40 y 60% de la calificación final):
- Pruebas escritas u orales en plataforma virtual. Valoración objetiva de la prueba de acuerdo a la naturaleza de la misma (examen de desarrollo, examen tipo test, exposición oral, etc).
- Pruebas sobre supuestos prácticos en plataforma virtual. Valoración mediante rúbrica.
- Pruebas escritas u orales finales presenciales. Valoración objetiva de la prueba de acuerdo con la naturaleza de la misma (examen de desarrollo, de preguntas cortas o de concepto, tipo test, exposición oral, sobre supuestos prácticos, etc).
- Pruebas finales sobre supuestos prácticos presenciales en aula. Valoración mediante rúbrica.

Para la asignatura del Módulo VI (Prácticas Académicas Externas), los instrumentos a utilizar en el sistema de evaluación son:

- Evaluación de la memoria elaborada acerca de las actividades llevadas a cabo con ocasión de la actividad desarrollada en el centro de Trabajo (hasta un 30% de la calificación final).

- Valoración por parte del tutor académico, teniendo en cuenta los comentarios del tutor externo y valorando la memoria presentada, la capacidad de organización y el grado de madurez alcanzado durante todo el proceso de seguimiento del estudiante durante el desarrollo de las prácticas (hasta un 70% de la calificación final).

La evaluación de las Prácticas Académicas Externas (Módulo VI), se realizará siguiendo lo establecido en el correspondiente Reglamento académico de las Prácticas Académicas Externas de la Universidad de Salamanca a expensas de que en los plazos establecidos legalmente se regule el Reglamento de Prácticas Académicas Externas de la titulación por el propio centro adscrito (Centro Universitario de Formación de la Policía Nacional) en consonancia con el mencionado Reglamento de la Universidad de Salamanca.

Para la asignatura del Módulo VII (Trabajo Fin de Máster), los instrumentos a utilizar en el sistema de evaluación son:

- Evaluación de las fases del Trabajo de Fin de Máster por parte del director/a del mismo. Se considerarán aspectos tales como el interés de la investigación, la elaboración de informes, así como la metodología indicada por el director/a del Trabajo Fin de Máster. Asimismo, se valorará el interés manifestado y su grado de implicación y compromiso (hasta un ~~70%~~ 40% de la calificación final).

- Defensa y evaluación del Trabajo de Fin de Máster ante el tribunal con experiencia en la disciplina en que se ha desarrollado. La composición del tribunal será la contemplada en la correspondiente guía docente, de acuerdo con la normativa vigente (hasta un ~~30%~~ 60% de la calificación final).

En cuanto al procedimiento de defensa del TFM, estos se defenderán en un acto público de manera virtual ante un Tribunal de Evaluación, cuya composición respetará lo establecido en la normativa que la regula de la Universidad de Salamanca vigente (tres miembros actualmente), lo que se desarrollará en el Reglamento para los Trabajos Fin de Máster del CUFPN y en la propia Guía académica de la asignatura, garantizándose la identificación de la persona a la que se evalúe, la publicidad del acto, y la calidad del mismo.

La publicidad del acto de defensa se garantizará mediante el anuncio de la defensa en la plataforma virtual oficial de la propia universidad (Studium) con la facilitación de un enlace con la finalidad de que cualquier persona que lo desee pueda conectarse. Además, se contará con un curso propio en la plataforma Studium donde se publicará toda la documentación relativa a los procesos de asignación de propuestas, asignación de tutores, normativa, plazos, fechas clave y tribunales. Asimismo, este curso contendrá espacios para el alojamiento de los propios TFM y otra documentación complementaria de interés para el alumnado.

Para la defensa del TFM (virtual) se requerirá al estudiante que muestre su documento de identificación ante el tribunal, y seguidamente el alumnado dispondrá de un tiempo de exposición al que seguirá un turno de preguntas y debate con el tribunal. Con el objetivo de garantizar la defensa del TFM en acto público, se permitirá el acceso a la misma por parte de todos los usuarios interesados a las sesiones de defensa, de manera que el enlace de conexión a la sala de defensa de Trabajos Fin de Máster se encontrará a disposición de toda aquella persona interesada.

Asimismo, las fechas de defensa de los Trabajos Fin de Máster se harán públicas a través de los instrumentos y mecanismos oficiales.

El órgano encargado de velar por el procedimiento de defensa del TFM será una Comisión Académica para los Trabajos Fin de Máster, respetando y cumpliendo con lo establecido en el Reglamento para los Trabajos Fin de Máster de la Universidad de Salamanca vigente así, como en segunda instancia, la propia Comisión Académica de la Facultad, según el Reglamento de Evaluación de la propia Universidad de Salamanca.

De igual modo, esta Comisión Académica ~~del Máster~~ para los Trabajos Fin de Máster establecerá un protocolo público de evaluación acorde a lo dispuesto en el Real Decreto 822/2021, de 28 de septiembre que incluya escalas descriptivas de calificación en forma de rúbrica donde se fijarán las dimensiones básicas de valoración del TFM (corrección de aspectos formales, coherencia en la estructura, rigor y profundidad de contenidos, adecuada presentación y defensa oral, entre otros) 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.~~

La identidad del estudiante se garantizará a través del uso de sistemas de identificación personal en la plataforma Studium. ~~mediante el control directo en las actividades presenciales (laboratorios y prácticas) y mediante el sistema de detección de plagio Turnitin.~~

4.4 ESTRUCTURAS CURRICULARES ESPECÍFICAS

5. PERSONAL ACADÉMICO Y DE APOYO A LA DOCENCIA

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

6. RECURSOS MATERIALES E INFRAESTRUCTURALES, PRÁCTICAS Y SERVICIOS

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

7. CALENDARIO DE IMPLANTACIÓN

7.1 CRONOGRAMA DE IMPLANTACIÓN	
CURSO DE INICIO	2025
Ver Apartado 7: Anexo 1.	
7.2 PROCEDIMIENTO DE ADAPTACIÓN	
No 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 título es el de la web institucional del Máster (véase **https://www.usal.es/masteres**) que contará con la siguiente información:

1. Descripción del título (centro, modalidad, idioma, plazas de nuevo ingreso ofertadas).
2. Objetivos formativos y Resultados de aprendizaje.
3. Perfil de ingreso.
4. Acceso, preinscripción, admisión y matrícula.
5. Criterios de admisión.
6. Apoyo y orientación.
7. Reconocimiento y transferencia de créditos.
8. Plan de estudios.
9. Guía académica (guías docentes de todas las asignaturas).
10. Perfil del currículum vitae del profesorado.
11. Salidas académicas y profesionales.
12. Indicadores de calidad e informes externos (información sobre la evaluación de la actividad docente del profesorado, resultados académicos y de encuestas, incluidas las de inserción laboral, informes externos de evaluación del título.
13. Becas, ayudas al estudio y a la movilidad.
14. Coste.
15. Normativa.
16. Contacto.
17. Folleto divulgativo.

Las necesidades de información de los estudiantes se atenderán también a través de la web de la Facultad de Ciencias 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**
Directora del Máster Universitario	María Angélica	González	Arrieta
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Facultad de Ciencias. Pza de los Caídos s/n	37008	Salamanca	Salamanca
EMAIL	**FAX**		
angelica@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	686443690		

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	923294502		

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.pdf

HASH SHA1 :D8BC1D3A360D218DBAAE26FA937017CA840D29B6

Código CSV :929973446526367864587134

Ver Fichero: 1. Justificación.pdf

Apartado 4: Anexo 1

Nombre :4. Planificación de las enseñanzas.pdf

HASH SHA1 :F929A558545AAA2D7710B3950FC10B28B4D3A519

Código CSV :92997388525923458980 5202

Ver Fichero: 4. Planificación de las enseñanzas.pdf

Apartado 5: Anexo 1

Nombre :5. Perfil básico del profesorado.pdf

HASH SHA1 :55A105B5F897737F18E81C7887907A7DF353D0B9

Código CSV :92997420468659099878588 2

Ver Fichero: 5. Perfil básico del profesorado.pdf

Apartado 5: Anexo 2

Nombre :5.2 Otros recursos humanos.pdf

HASH SHA1 :5B2653C28B1858C4C2407459167049BFD8B6EB2C

Código CSV :92997459466023787043191 5

Ver Fichero: 5.2 Otros recursos humanos.pdf

Apartado 6: Anexo 1

Nombre :6. Recursos materiales.pdf

HASH SHA1 :D91DCC62379C645F83DC7AEC568E487ECDF38A78

Código CSV :92997294888713471000589O

Ver Fichero: 6. Recursos materiales.pdf

Apartado 7: Anexo 1

Nombre :7.1. Cronograma.pdf

HASH SHA1 :3E8C8F779433A036F3CAB3B88AD298DF350F91DC

Código CSV :865233749757805996065521

Ver Fichero: 7.1. Cronograma.pdf

Apartado Personas asociadas a la solicitud: Anexo 1

Nombre : Delegacion competencias Rector RUCT.pdf

HASH SHA1 :6A7918DF4A3FFA0431B73E0CCB718F3C133BCBFC

Código CSV :865246831994948116832838

Ver Fichero: Delegacion competencias Rector RUCT.pdf

Apartado Informe previo de la Comunidad Autónoma: Anexo 1

Nombre : Informe viabilidad.pdf

HASH SHA1 :E5FC26FDA4D516F543C3B8E2249B7640140BA168

Código CSV :872193613198694001064761

Ver Fichero: Informe viabilidad.pdf