D.ª REBECA DE JUAN DÍAZ, SECRETARIA GENERAL DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA,

C E R T I F I C A: Que en la reunión del Consejo de Gobierno, celebrada el día cinco de marzo de dos mil diecinueve fue adoptado, entre otros, el siguiente acuerdo:

05. Estudio y aprobación, si procede, de las propuestas del Vicerrectorado de Grado y Posgrado

05.08. El Consejo de Gobierno aprueba la creación del "Máster Universitario en Ciberseguridad", según anexo

Y para que conste a los efectos oportunos, se extiende la presente certificación haciendo constar que se emite con anterioridad a la aprobación del Acta y sin perjuicio de su ulterior aprobación en Madrid, a seis de marzo de dos mil diecinueve.

Juan Martínez Romo
Secretario Académico

UNED ETS de Ingeniería Informática

D. JUAN MARTÍNEZ ROMO, SECRETARIO ACADÉMICO DE LA ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA DE LA UNED

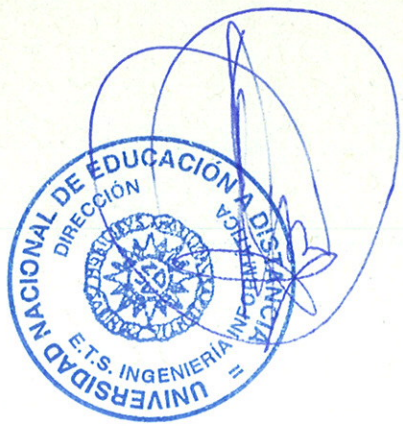
CERTIFICA: Que en la Junta de la Escuela Técnica Superior de Ingeniería Informática, celebrada el día cuatro de julio de dos mil dieciocho fue adoptado, entre otros, el siguiente acuerdo:

5. Debate y aprobación de nuevas Titulaciones.

Propuesta de nuevo Máster en Ciberseguridad.

Se aprueba.

Para que así conste, a los efectos oportunos, se extiende el presente certificado en Madrid a catorce de febrero de dos mil diecinueve.



C/ Juan del Rosal, 16
28040 MADRID
Tel. 91 398 7306

IMPRESO SOLICITUD PARA VERIFICACIÓN DE TÍTULOS OFICIALES

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

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

UNIVERSIDAD SOLICITANTE	CENTRO	CÓDIGO CENTRO
Universidad Nacional de Educación a Distancia	Escuela Técnica Superior de Ingeniería Informática	28050756
NIVEL	**DENOMINACIÓN CORTA**	
Máster	Ciberseguridad	
DENOMINACIÓN ESPECÍFICA		
Máster Universitario en Ciberseguridad por la Universidad Nacional de Educación a Distancia		
RAMA DE CONOCIMIENTO	**CONJUNTO**	
Ingeniería y Arquitectura	No	
HABILITA PARA EL EJERCICIO DE PROFESIONES REGULADAS	**NORMA HABILITACIÓN**	
No		
SOLICITANTE		
NOMBRE Y APELLIDOS	**CARGO**	
ROBERTO HERNÁNDEZ BERLINCHES	Catedrático de Universidad	
Tipo Documento	**Número Documento**	
NIF	05266644N	
REPRESENTANTE LEGAL		
NOMBRE Y APELLIDOS	**CARGO**	
RICARDO MAIRAL USON	Rector	
Tipo Documento	**Número Documento**	
NIF	18021524N	
RESPONSABLE DEL TÍTULO		
NOMBRE Y APELLIDOS	**CARGO**	
RAFAEL MARTINEZ TOMAS	Director de la ETSI Informática	
Tipo Documento	**Número Documento**	
NIF	05149707F	

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
C/Bravo Murillo, 38	28015	Madrid	913989632
E-MAIL	**PROVINCIA**		**FAX**
admin.masteresoficiales@adm.uned.es	Madrid		913989632

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

	En: Madrid, AM 25 de octubre de 2018
	Firma: Representante legal de la Universidad

1. DESCRIPCIÓN DEL TÍTULO

1.1. DATOS BÁSICOS

NIVEL	DENOMINACIÓN ESPECIFICA	CONJUNTO	CONVENIO	CONV. ADJUNTO
Máster	Máster Universitario en Ciberseguridad por la Universidad Nacional de Educación a Distancia	No		Ver Apartado 1: Anexo 1.

LISTADO DE ESPECIALIDADES
No existen datos

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

NO HABILITA O ESTÁ VINCULADO CON PROFESIÓN REGULADA ALGUNA

AGENCIA EVALUADORA
Agencia Nacional de Evaluación de la Calidad y Acreditación

UNIVERSIDAD SOLICITANTE
Universidad Nacional de Educación a Distancia

LISTADO DE UNIVERSIDADES	
CÓDIGO	UNIVERSIDAD
028	Universidad Nacional de Educación a Distancia

LISTADO DE UNIVERSIDADES EXTRANJERAS	
CÓDIGO	UNIVERSIDAD
No existen datos	

LISTADO DE INSTITUCIONES PARTICIPANTES
No existen datos

1.2. DISTRIBUCIÓN DE CRÉDITOS EN EL TÍTULO

CRÉDITOS TOTALES	CRÉDITOS DE COMPLEMENTOS FORMATIVOS	CRÉDITOS EN PRÁCTICAS EXTERNAS
60	0	0
CRÉDITOS OPTATIVOS	**CRÉDITOS OBLIGATORIOS**	**CRÉDITOS TRABAJO FIN GRADO/ MÁSTER**
18	30	12

LISTADO DE ESPECIALIDADES	
ESPECIALIDAD	CRÉDITOS OPTATIVOS
No existen datos	

1.3. Universidad Nacional de Educación a Distancia

1.3.1. CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS	
CÓDIGO	CENTRO
28050756	Escuela Técnica Superior de Ingeniería Informática

1.3.2. Escuela Técnica Superior de Ingeniería Informática

1.3.2.1. Datos asociados al centro

TIPOS DE ENSEÑANZA QUE SE IMPARTEN EN EL CENTRO		
PRESENCIAL	SEMIPRESENCIAL	A DISTANCIA
No	No	Sí
PLAZAS DE NUEVO INGRESO OFERTADAS		
PRIMER AÑO IMPLANTACIÓN	**SEGUNDO AÑO IMPLANTACIÓN**	
75	100	

	TIEMPO COMPLETO	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	60.0	60.0
RESTO DE AÑOS	6.0	60.0
	TIEMPO PARCIAL	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	6.0	48.0
RESTO DE AÑOS	6.0	60.0
NORMAS DE PERMANENCIA		
http://portal.uned.es/pls/portal/docs/PAGE/UNED_MAIN/LAUNIVERSIDAD/VICERRECTORADOS/SECRETARIA/NORMATIVA/ESTUDIANTES/NORMAS%20DE%20PERMANENCIA%20APROBADO%20CONSEJO%20GOBIERNO%206%20OCTUBRE%202015.PDF		
LENGUAS EN LAS 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	

2. JUSTIFICACIÓN, ADECUACIÓN DE LA PROPUESTA Y PROCEDIMIENTOS

Ver Apartado 2: Anexo 1.

3. COMPETENCIAS

3.1 COMPETENCIAS BÁSICAS Y GENERALES
BÁSICAS
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
GENERALES
CG1 - Analizar métodos y técnicas de ciberataques.
CG2 - Diseñar, poner en marcha y mantener un sistema de ciberseguridad.
CG3 - Conocer la normativa y la legislación en materia de ciberseguridad, sus implicaciones en el diseño y puesta en marcha de sistemas informáticos.
CG4 - Identificar, gestionar y desarrollar medidas y protocolos de seguridad en la operación y gestión de sistemas informáticos.
3.2 COMPETENCIAS TRANSVERSALES
CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.
CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).
3.3 COMPETENCIAS ESPECÍFICAS
CE1 - Utilizar mecanismos criptográficos avanzados de para garantizar los requisitos de seguridad en un sistema, así como el acceso y seguridad en las comunicaciones.
CE2 - Diseñar mecanismos de prevención de amenazas a la seguridad, así como de reconocer y resolver incidentes de seguridad en los sistemas críticos.
CE3 - Utilizar herramientas para monitorizar el tráfico de red y generar, explorar y manipular el tráfico en los sistemas de comunicación.
CE4 - Analizar e identificar vulnerabilidades ante posibles ataques en los sistemas de comunicaciones y los servicios asociados.
CE5 - Analizar e identificar técnicas de ocultación de ataques a sistemas de comunicaciones y aplicaciones.
CE6 - Conocer las tendencias actuales en técnicas de ciberataque y las experiencias en casos reales.
CE7 - Analizar sistemas para encontrar evidencias de ataques en los mismos y adoptar las medidas precisas para mantener la cadena de custodia de dichas evidencias.
CE8 - Conocer las técnicas y herramientas para la realización de un análisis forense con la preservación de pruebas digitales.
CE9 - Conocer las principales técnicas y herramientas de Inteligencia Artificial y sus aplicaciones en problemas de ciberseguridad.
CE10 - Comprender la importancia del Derecho como sistema regulador de las relaciones sociales.
CE11 - Conseguir la percepción del carácter unitario del ordenamiento jurídico y de la necesaria visión interdisciplinaria de los problemas jurídicos.

4. ACCESO Y ADMISIÓN DE ESTUDIANTES

4.1 SISTEMAS DE INFORMACIÓN PREVIO

Ver Apartado 4: Anexo 1.

4.2 REQUISITOS DE ACCESO Y CRITERIOS DE ADMISIÓN
ACCESO A LAS ENSEÑANZAS OFICIALES DE MÁSTER

1. Para acceder a las enseñanzas oficiales de Máster será necesario estar en posesión de un título universitario oficial español u otro expedido por una institución de educación superior perteneciente a otro Estado integrante del Espacio Europeo de Educación Superior que faculte en el mismo para el acceso a enseñanzas de Máster.

2. Así mismo, podrán acceder los titulados conforme a sistemas educativos ajenos al Espacio Europeo de Educación Superior sin necesidad de la homologación de sus títulos, previa comprobación por la Universidad de que aquellos acreditan un nivel de formación equivalente a los correspondientes títulos universitarios oficiales españoles y que facultan en el país expedidor del título para el acceso a enseñanzas de postgrado. El acceso por esta vía no implicará, en ningún caso, la homologación del título previo de que esté en posesión el interesado, ni su reconocimiento a otros efectos que el de cursar las enseñanzas de Máster.

REQUISITOS DE ACCESO

Teniendo en cuenta lo establecido en el Real Decreto 1393/2007, será requisito mínimo para matricularse en el Máster Universitario en Ciberseguridad por la Universidad Nacional de Educación a Distancia que el estudiante esté en posesión del Título de Licenciado y/o Graduado en Informática.

La Comisión de Coordinación del Máster (CCM) podría considerar también la admisión a titulados superiores de carreras afines, como Telecomunicaciones, Física, Matemáticas, o Química, y a Ingenieros Técnicos en Informática. Se valorarán también los conocimientos de informática adquiridos fuera de la carrera y en la práctica profesional.

Se recomienda que los estudiantes de nuestro máster tengan el nivel B1 (del Marco Común Europeo de Referencia para las Lenguas). De esa manera, los estudiantes deben ser capaces de leer textos en inglés. No se requiere ningún conocimiento de las otras habilidades lingüísticas (hablar, escribir y escuchar) en los mencionados idiomas.

CRITERIOS DE ADMISIÓN

El órgano encargado de la selección y admisión de los estudiantes a este Máster Universitario será la Comisión formada por el Coordinador del Título en la ETS de Informática, el Secretario del Máster y un profesor permanente del equipo docente del Máster, atendiendo a los criterios de valoración que se detallan a continuación:

1. Titulación de acceso (hasta 4 puntos).

Adecuación de la Titulación por la que se accede al máster en el área de Ingeniería.

2. Expediente académico (hasta 4 puntos).

3. Currículum Vitae (hasta 2 puntos). Se valorará la experiencia profesional, la formación complementaria y el conocimiento de idiomas.

En cada una de las fases de reparto de las plazas únicamente se considerarán las solicitudes de aquellos estudiantes que cumplan y hayan demostrado documentalmente los requisitos planteados y los méritos aludidos.

4.3 APOYO A ESTUDIANTES

La UNED ofrece los siguientes servicios a los estudiantes:

- **Orientación antes de matricularse.**

La UNED proporciona al alumno orientación durante el periodo de matrícula para que se ajuste al tiempo real del que dispone para el estudio y a su preparación previa para los requerimientos de las materias. Con esto se pretende que no abandone y que se adapte bien a la Universidad. Para ello cuenta tanto con información en la web como con orientaciones presenciales en su Centro Asociado.

- **Guías de apoyo.**

Para abordar con éxito los estudios en la UNED es necesario que el estudiante conozca su metodología específica y que desarrolle las competencias necesarias para estudiar a distancia de forma autónoma, y así, ser capaz de autorregular su proceso de aprendizaje.

Para ello, se han elaborado una serie de **guías de apoyo** inicial al entrenamiento de estas competencias:

- **Competencias necesarias para Estudiar a Distancia**.
- **Orientaciones para la Planificación del Estudio**.
- Técnicas de estudio.
- **Preparación de Exámenes en la UNED**.

- **Jornadas de Bienvenida y de Formación para nuevos estudiantes en los Centros Asociados.**

La UNED es consciente de la importancia que tiene para el estudiante nuevo, conocer su Universidad e integrarse en ella de la mejor forma posible. Asimismo, está especialmente preocupada por poner a su alcance todos los recursos posibles para que pueda desarrollar las competencias necesarias para ser un estudiante a distancia.

Por ello, le ofrece un Plan de Acogida para nuevos estudiantes. Este Plan tiene tres objetivos fundamentales:

- Brindarle la mejor información posible para que se integre de forma satisfactoria en la Universidad.
- Orientarle mejor en su decisión para que se matricule de aquello que más le convenga y se ajuste a sus deseos o necesidades.
- Proporcionarle toda una serie de cursos de formación, tanto presenciales como en-línea, sobre la metodología específica del estudio a distancia y las competencias que necesita para llevar a cabo un aprendizaje autónomo, regulado por él mismo.

En definitiva, se trata de que logre una buena adaptación al sistema de enseñanza-aprendizaje de la UNED para que culmine con éxito sus estudios.

- **Cursos 0. Cursos de nivelación.**

Los cursos 0 permiten actualizar los conocimientos de entrada a la titulación de los nuevos alumnos. Se ofertan asociados a una serie de contenidos presentes en diferentes titulaciones y materias impartidas. En la dirección electrónica **http://ocw.innova.uned.es/ocwuniversia**, se encuentra toda la información necesaria para la realización de estos cursos de nivelación.

- **Comunidad virtual de estudiantes nuevos.**

El estudiante nuevo formará parte de la "Comunidad virtual de estudiantes nuevos" de su Facultad/Escuela, en la que se le brindará información y orientación precisas sobre la UNED y su metodología, así como sugerencias para guiarle en tus primeros pasos.

- **aLF.**

aLF es una plataforma de e-Learning y colaboración que permite impartir y recibir formación, gestionar y compartir documentos, crear y participar en comunidades temáticas, así como realizar proyectos online.

aLF facilita hacer un buen uso de los recursos de que disponemos a través de Internet para paliar las dificultades que ofrece el modelo de enseñanza a distancia.

Para ello ponemos a su disposición las herramientas necesarias para que, tanto el equipo docente como el alumnado, encuentren la manera de compaginar el trabajo individual como el aprendizaje cooperativo.

Funcionalidades:

- Gestión de grupos de trabajo bajo demanda.
- Espacio de almacenamiento compartido.
- Organización de los contenidos.
- Planificación de actividades.
- Evaluación y autoevaluación.
- Servicio de notificaciones automáticas.
- Diseño de encuestas.
- Publicación planificada de noticias.
- Portal personal y público configurable por el usuario.

- **El Centro de Orientación, Información y Empleo de la UNED (COIE).**

El Centro de Orientación, Información y Empleo de la UNED (COIE) es un servicio especializado de información y orientación académica y profesional que ofrece al alumno todo el soporte que necesita tanto para su adaptación académica en la UNED como para su promoción profesional una vez terminados sus estudios.

La dirección **web** del COIE es:

http://portal.uned.es/portal/page?_pageid=93,569737&_dad=portal&_schema=PORTAL

¿Qué ofrece el COIE?:

- Orientación académica: formación en técnicas de estudio a distancia y ayuda en la toma de decisiones para la elección de la carrera.
- Orientación profesional: asesoramiento del itinerario profesional e información sobre las salidas profesionales de cada carrera.
- Información y autoconsulta:
  - Titulaciones.
  - Estudios de posgrado.
  - Cursos de formación.
  - Becas, ayudas y premios.
  - Estudios en el extranjero.
- Empleo:
  - Bolsa de empleo y prácticas: bolsa on-line de trabajo y prácticas para estudiantes y titulados de la UNED
  - Ofertas de empleo: ofertas de las empresas colaboradoras del COIE y las recogidas en los diferentes medios de comunicación.
  - Prácticas: podrá realizar prácticas en empresas siempre y cuando haya superado el 50% de los créditos de tu titulación.

- **Servicio de Secretaría Virtual.**

El servicio de Secretaría Virtual proporciona servicios de consulta y gestión académica a través de Internet de manera personalizada y segura desde cualquier ordenador con acceso a la red. Para utilizar el servicio, el estudiante deberá tener el identificador de usuario que se proporciona en la matrícula.

Los servicios que ofrece la Secretaría Virtual son los siguientes:

- Cuenta de correo electrónico de estudiante: El usuario podrá activar o desactivar la cuenta de correo electrónico que ofrece la UNED a sus estudiantes.
- Cambio de la clave de acceso a los servicios: Gestión de la clave de acceso a la Secretaría Virtual.
- Consulta de expediente académico del estudiante y consulta de calificaciones.
- Consulta del estado de su solicitud de beca.
- Consulta del estado de su solicitud de título.
- Consulta del estado de su solicitud de matrícula.

- **Tutoría Presencial en los Centros Asociados.**

La UNED es plenamente consciente de la importancia que la tutoría presencial tiene para sus estudiantes, por lo que los alumnos podrán resolver todas tus dudas y llevar a cabo actividades de aprendizaje durante las tutorías presenciales en su Centro Asociado más cercano, donde contará con tutores especializados.

En la actualidad, la tutoría presencial se ha reforzado gracias a sistemas avanzados de videoconferencia y pizarras digitales interactivas (aulas AVIP), que permiten ofrecer, al tiempo, la tutoría en directo a distintos Centros Asociados a la vez optimizando, así, los recursos disponibles, tanto de los Centros grandes como de los pequeños.

La plataforma AVIP pretende ser la clave del acceso a la educación para el siglo de Internet.

Los Centros Asociados facilitan, además, la formación de grupos de trabajo y estudio constituidos por estudiantes pertenecientes al mismo Centro.

- **Tutorías en línea.**

En el curso virtual el estudiante puede contar con el apoyo de su equipo docente y de un Tutor desde cualquier lugar y de forma flexible. Este tipo de tutoría no impide poder acceder a la tradicional Tutoría Presencial en los Centros Asociados; es decir, se puede libremente utilizar, una, otra o las dos opciones a la vez.

Como novedad, si el estudiante está matriculado en estudios con un número reducido de ellos, la UNED posibilita que la tutoría presencial se traslade al entorno virtual en lo que se denomina Tutoría Intercampus. A través de este medio el estudiante podrá ver y escuchar a sus profesores tutores y participar en las actividades que se desarrollen.

Muchas de las tutorías desarrolladas mediante tecnología AVIP están disponibles en línea para que se puedan visualizar en cualquier momento, con posterioridad a su celebración.

- **La Biblioteca.**

La Biblioteca de la UNED es un centro de recursos para el aprendizaje, la docencia, la investigación, la formación continua y las actividades relacionadas con el funcionamiento y la gestión de la Universidad en su conjunto. La Biblioteca se identifica plenamente en la consecución de los objetivos de la Universidad y en su proceso de adaptación al nuevo entorno de educación superior.

La estructura del servicio de Biblioteca la constituyen las Bibliotecas: Central, Psicología e IUED (Instituto Universitario de Educación a Distancia), Ingenierías, y la biblioteca del Instituto Universitario ¿Gutiérrez Mellado¿. Esta estructura descentralizada por campus está unificada en cuanto a su política bibliotecaria, dirección, procesos y procedimientos normalizados.

Los servicios que presta son:

- Información y atención al usuario.
- Consulta y acceso a la información en sala y en línea.
- Adquisición de documentos.
- Préstamo y obtención de documentos (a domicilio e interbiblitecario).
- Publicación científica en abierto: la Biblioteca gestiona el repositorio institucional e-SpacioUNED donde se conservan, organizan y difunden los contenidos digitales resultantes de la actividad científica y académica de la Universidad, de manera que puedan ser buscados, recuperados y reutilizados con más facilidad e incrementando notablemente su visibilidad e impacto.
- Reproducción de materiales: fotocopiadoras de autoservicio, equipos para consulta de microformas, descargas de documentos electrónicos, etc.

- **La Librería Virtual.**

La Librería Virtual es un servicio pionero que la UNED pone a disposición de sus estudiantes, con el fin de que éstos puedan adquirir los materiales básicos recomendados en las guías de las distintas titulaciones. Asimismo, facilita a cualquier usuario de internet la adquisición rápida y eficaz del fondo de la Editorial UNED, la mayor editorial universitaria española.

- **UNIDIS.**

El Centro de Atención a Universitarios con Discapacidad (UNIDIS) es un servicio dependiente del **Vicerrectorado de Estudiantes, Empleo y Cultura**, cuyo objetivo principal es que los estudiantes con discapacidad que deseen cursar estudios en esta Universidad, puedan gozar de las mismas oportunidades que el resto de estudiantes de la UNED.

Con este fin, UNIDIS coordina y desarrolla una serie de acciones de asesoramiento y apoyo a la comunidad universitaria que contribuyan a suprimir barreras para el acceso, la participación y el aprendizaje de los universitarios con discapacidad.

- **Representación de estudiantes.**

Los representantes de estudiantes desarrollan en la UNED una función de gran importancia para nuestra Universidad. Los Estatutos de la UNED y el Estatuto del Estudiante Universitario subrayan el carácter democrático de la función de representación y su valor en la vida universitaria. En el caso de la UNED, los órganos colegiados de nuestra Universidad en los que se toman las decisiones de gobierno cuentan con representación estudiantil. Los representantes desarrollan sus funciones en las Facultades y Escuelas, en los Departamentos, en los Centros Asociados y en otras muchas instancias en las que es necesario tener en cuenta las opiniones y sugerencias de los colectivos de estudiantes.

Desde el Vicerrectorado de Estudiantes, Empleo y Cultura, así como desde los Centros Asociados, se facilita esta labor de representación defendiendo sus intereses en las distintas instancias, apoyando sus actividades con recursos económicos y reconociendo su actividad desde el punto de vista académico. Nuestra comunidad universitaria está reforzando la participación de estudiantes en los procesos de decisión que, sin duda, redunda en beneficio de la vida universitaria tanto en las Facultades y Escuelas como en los Centros Asociados.

4.4 SISTEMA DE TRANSFERENCIA Y RECONOCIMIENTO DE CRÉDITOS

Reconocimiento de Créditos Cursados en Enseñanzas Superiores Oficiales no Universitarias

MÍNIMO	MÁXIMO
0	0

Reconocimiento de Créditos Cursados en Títulos Propios

MÍNIMO	MÁXIMO
0	0

Adjuntar Título Propio

Ver Apartado 4: Anexo 2.

Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional	
MÍNIMO	**MÁXIMO**
0	0

NORMAS Y CRITERIOS GENERALES DE RECONOCIMIENTO Y TRANSFERENCIA DE CRÉDITOS PARA LOS MASTER

PREÁMBULO

El Real Decreto 1393/2007, de 29 de octubre, por el que se establecía la ordenación de las enseñanzas universitarias oficiales indica en su artículo sexto que, al objeto de hacer efectiva la movilidad de estudiantes, dentro y fuera del territorio nacional, las universidades elaborarán y harán pública su normativa sobre el sistema de reconocimiento y transferencia de créditos, con sujeción a los criterios generales establecidos en el mismo; este precepto ha sido modificado por el Real Decreto 861/2010, de 2 de julio, que da una nueva redacción al citado precepto para, según reza su exposición de motivos, ¿introducir los ajustes necesarios a fin de garantizar una mayor fluidez y eficacia en los criterios y procedimientos establecidos¿.

Con la finalidad de adecuar la normativa interna de la UNED en el ámbito de los Másteres a estas modificaciones normativas y en cumplimiento de lo establecido en el párrafo 1º del artículo sexto del citado Real Decreto 861/2010, y con objeto de hacer efectiva la movilidad de estudiantes, tanto dentro del territorio nacional como fuera de él, procede la aprobación de las siguientes normas y criterios generales de reconocimiento y transferencia de créditos para los Másteres.

Capítulo I. Reconocimiento de créditos.

Artículo 1. Ámbito de aplicación.

Esta normativa será de aplicación a las enseñanzas universitarias oficiales de Posgrado reguladas por el Real Decreto 1393/2007, de 29 de octubre, modificado por el Real Decreto 861/2010, de 2 de julio, que se impartan en la UNED.

Artículo 2. Conceptos básicos.

1. Se entiende por reconocimiento de créditos la aceptación por la universidad de créditos que son computados para la obtención de un título oficial de Master y que no se han obtenido cursando las asignaturas incluidas en su plan de estudios.

2. Las unidades básicas de reconocimiento son los créditos, las competencias y los conocimientos derivados de las enseñanzas y actividades laborales y profesionales acreditados por el estudiante.
Artículo 3. Ámbito objetivo de reconocimiento.

3.1. Serán objeto de reconocimiento:
a) Enseñanzas universitarias oficiales, finalizadas o no, de Master o Doctorado. b) Enseñanzas universitarias no oficiales.
c) Experiencia laboral o profesional relacionada con las competencias inherentes al título.

3.2. También podrán ser reconocidos como créditos los estudios parciales de doctorado superados con arreglo a las distintas legislaciones anteriores, siempre que tengan un contenido afín al del Master, a juicio de la Comisión Coordinadora de éste.

Artículo 4. Órganos competentes

1. El órgano competente para el reconocimiento de créditos será la "Comisión de Coordinación del Título de Master" establecida en cada caso para cada título con arreglo a la normativa de la UNED en materia de organización y gestión académica de los Másteres que en cada momento esté vigente.

2. La Comisión delegada de Ordenación Académica de la UNED actuará como órgano de supervisión y de resolución de dudas que puedan plantearse en las Comisiones de coordinación del título de Master y establecerá los criterios generales de procedimiento y plazos.

Artículo 5. Criterio general para el reconocimiento de créditos.

1. El reconocimiento de créditos deberá realizarse teniendo en cuenta la adecuación entre las competencias y conocimientos asociados a las materias cursadas por el estudiante y los previstos en el plan de estudios.

2.- El reconocimiento de los créditos se realizara conforme al procedimiento descrito en el Anexo I.

Artículo 6. Reconocimientos entre estudios universitarios oficiales.

1. A los efectos de esta normativa, se entiende por reconocimiento la aceptación por la UNED de los créditos que, habiendo sido obtenidos en unas enseñanzas oficiales, en ésta u otra Universidad, son computados en otras enseñanzas distintas a efectos de la obtención de un título oficial de Máster Universitario.

2. No podrán ser objeto de reconocimiento los créditos correspondientes al trabajo fin de Máster necesario para obtener el correspondiente título.

Artículo 7. Reconocimientos de enseñanzas universitarias no oficiales y experiencia laboral.

1. Podrán ser objeto de reconocimiento los créditos cursados en otras enseñanzas universitarias conducentes a la obtención de otros títulos, a los que se refiere el artículo 34.1 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, siempre que el nivel de titulación exigido para ellas sea el mismo que para el Master.

2. La experiencia laboral y profesional acreditada podrá ser también reconocida en forma de créditos que computarán a efectos de la obtención del título oficial de Máster, siempre que dicha experiencia esté relacionada con las competencias inherentes a dicho título o periodo de formación.

3. El número de créditos que sean objeto de reconocimiento a partir de la experiencia profesional o laboral y de enseñanzas universitarias no oficiales no podrá ser superior, en su conjunto, al 15 por ciento del total de créditos que constituyen el plan de estudios. El reconocimiento de estos créditos no incorporará calificación de los mismos por lo que no computarán a efectos de baremación del expediente.

Los créditos procedentes de títulos propios podrán, excepcionalmente, ser objeto de reconocimiento en un porcentaje superior al señalado en el párrafo anterior o, en su caso, ser objeto de un reconocimiento en su totalidad siempre que el correspondiente título propio haya sido extinguido y sustituido por un título oficial.

A tal efecto, en la memoria de verificación del nuevo plan de estudios propuesto y presentado a verificación se hará constar tal circunstancia y se deberá acompañar a la misma, además de los dispuesto en el anexo I de este real decreto, el diseño curricular relativo al título propio, en el que conste: número de créditos, planificación de las enseñanzas, objetivos, competencias, criterios de evaluación, criterios de calificación y obtención de la nota media del expediente, proyecto final de Grado o de Máster, etc., a fin de que la Agencia de Evaluación de la Calidad y Acreditación (ANECA) o el órgano de evaluación que la Ley de las comunidades autónomas determinen, compruebe que el título que se presenta a verificación guarda la suficiente identidad con el título propio anterior y se pronuncie en relación con el reconocimiento de créditos propuesto por la universidad.
Capítulo II. Transferencia de créditos.

Art. 8- Definición.

1. Se entiende por transferencia la inclusión en el expediente del estudiante de la totalidad de los créditos obtenidos en enseñanzas oficiales cursadas con anterioridad, en la UNED o en otra Universidad, que no hayan conducido a la obtención de un título oficial.

Art. 9. Requisitos y Procedimiento para la transferencia de créditos

Los estudiantes que se incorporen a un nuevo título deberán indicar si han cursado otros estudios oficiales no finalizados, y en caso de no tratarse de estudios de la UNED, aportar los documentos requeridos. Para hacer efectiva la transferencia de créditos el estudiante deberá realizar traslado de expediente. Una vez presentados los documentos requeridos, se actuará de oficio, incorporando la información al expediente del estudiante pero sin que, en ningún caso, puedan ser tomados en consideración para terminar las enseñanzas de Master cursadas, aquellos créditos que no hayan sido reconocidos..

Art. 10. Documentos académicos

Todos los créditos obtenidos por el estudiante en enseñanzas oficiales cursados en cualquier Universidad, los transferidos, los reconocidos y los superados para la obtención del correspondiente título, serán incluidos en su expediente académico y reflejados en el Suplemento Europeo al Título, regulado en el Real Decreto 1044/2003 de 1 de agosto, por el que se establece el procedimiento para la expedición por las Universidades del Suplemento Europeo al Título.

ANEXO I

1. El procedimiento se inicia a petición del interesado una vez que aporte en la Facultad o Escuela correspondiente la documentación necesaria para su tramitación. Este último requisito no será necesario para los estudiantes de la UNED cuando su expediente se encuentre en la Universidad. La Facultad/Escuela podrá solicitar a los interesados

información complementaria al Certificado Académico, en caso de que lo considere necesario, para posibilitar el análisis de la adecuación entre las competencias y conocimientos asociados a las asignaturas cursadas y los previstos en el plan de estudios de la enseñanza de ingreso.

2. Una vez resueltos y comunicados los reconocimientos al estudiante, este deberá abonar el importe establecido en la Orden Ministerial, que anualmente fija los precios públicos por este concepto, para hacer efectivos estos derechos, incorporarlos a su expediente y poner fin al procedimiento.

3. No obstante, y de acuerdo a lo dispuesto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, modificada por la Ley 4/1999, de 13 de enero, si el estudiante no estuviera de acuerdo con la resolución de la Comisión de reconocimiento podrá presentar en el plazo de un mes recurso de alzada ante el Rector.

4. En virtud de las competencias conferidas en el artículo 4º de la normativa para reconocimientos, la Comisión delegada de Ordenación Académica podrá establecer anualmente plazos de solicitud de reconocimiento de créditos para cada Facultad o Escuela, con el objeto de ordenar el proceso, de acuerdo con los períodos de matrícula anual.

5. El plazo máximo para resolver el procedimiento es de 3 meses. El procedimiento permanecerá suspenso por el tiempo que medie entre la petición de documentación por parte de la universidad al interesado y su efectivo cumplimiento.

6. Se autoriza al Vicerrectorado de Investigación a realizar cuantas modificaciones sean necesarias en este procedimiento para su mejor adecuación a posibles cambios normativos.

4.6 COMPLEMENTOS FORMATIVOS

Los estudiantes provenientes de otras titulaciones diferentes de un título universitario oficial cuya denominación incluya la referencia expresa a la profesión de Ingeniero en Informática siguiendo las directrices de la resolución del 8 de junio de 2009, de la Secretaría General de Universidades, deberán cursar un conjunto de complementos formativos asimilables a las competencias básicas de un Grado en Ingeniería Informática establecidas en dicha resolución. Estos complementos serán tomados entre las materias troncales y obligatorias que se estimen necesarias del Grado en Ingeniería Informática y del Grado en Ingeniería en Tecnologías de la Información de la UNED. Para ello, la Comisión de Coordinación del Máster será la encargada para cada caso de establecer el conjunto de complementos formativos que deberán ser cursados por el estudiante.

Las asignaturas que se deberán cursar para complementar la formacion serán seleccionadas de las siguientes:

- Teoría de la Información y Criptografía Básica
- Seguridad
- Consultoría y Auditoría
- Redes de Computadores
- Sistemas Distribuidos
- Sistemas Operativos
- Programación y Estructuras de Datos Avanzadas
- Ética y Legislación

5. PLANIFICACIÓN DE LAS ENSEÑANZAS

5.1 DESCRIPCIÓN DEL PLAN DE ESTUDIOS
Ver Apartado 5: Anexo 1.
5.2 ACTIVIDADES FORMATIVAS
Estudios de contenidos
Tutorías
Actividades en la plataforma virtual
Trabajos/Prácticas
5.3 METODOLOGÍAS DOCENTES
Las diferentes asignaturas que integran este Máster se impartirán todas ellas conforme a la metodología no presencial que caracteriza a la UNED, en la cual prima el autoaprendizaje del estudiante, pero asistido por el profesor y articulado a través de diversos sistemas de comunicación docente-discente. Dentro de estos sistemas, cabe destacar que el Máster en Ciberseguridad se imparte con apoyo en una plataforma virtual interactiva de la UNED donde el estudiante encuentra tanto materiales didácticos básicos como materiales didácticos complementarios, informaciones, noticias, ejercicios y también permite la evaluación correspondiente a las diferentes materias.
5.4 SISTEMAS DE EVALUACIÓN
Examen presencial
Trabajos
Pruebas de evaluación continua
Preparación, presentación y defensa pública del TFM
5.5 SIN NIVEL 1
NIVEL 2: Criptografía Aplicada
5.5.1.1 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**

LENGUAS EN LAS 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	

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

Los resultados básicos más relevantes que se pretenden alcanzar con el estudio de esta asignatura son los siguientes:

- Comprender los fundamentos matemáticos que sustentan la criptología.
- Elegir entre los diversos algoritmos de criptografía existentes aquellos más adecuados a los escenarios de la ciberseguridad.
- Desarrollar la implementación de algoritmos criptográficos en entornos de programación real.

- Analizar un texto cifrado utilizando diversas técnicas de criptoanálisis con el fin de determinar cuál es el texto plano asociado.
- Comprender la criptología post-cuántica.
- Analizar el papel de la criptología en las diversas aplicaciones actuales.

5.5.1.3 CONTENIDOS

Los contenidos se organizarán de la siguiente manera, aunque se podrán modificar en un futuro en función de la evolución de la tecnología:

- Principios matemáticos de la criptografía
- Criptología para la ciberseguridad
- Criptoanálisis
- Criptología y computación cuántica
- Aplicaciones de la criptografía

5.5.1.4 OBSERVACIONES

Se recomienda que los interesados en cursar el Máster tengan un nivel de lectura en inglés suficiente como para entender contenidos técnicos en dicha lengua.

Gran parte de la bibliografía, así como los recursos proporcionados al estudiante en el curso virtual pueden estar únicamente en inglés, debido a la novedad de algunos de los contenidos propuestos para la asignatura.

Por otra parte, cada una de las actividades propuestas formativas en la asignatura constarán de una parte de trabajo individual, otra colectiva (si fuera el caso) y la utilización de la plataforma virtual, además de ser eminentemente prácticas. Todo ello de manera conjunta, por lo que la división de horas realizada en el apartado de actividades formativas es orientativa.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Analizar métodos y técnicas de ciberataques.

CG2 - Diseñar, poner en marcha y mantener un sistema de ciberseguridad.

CG4 - Identificar, gestionar y desarrollar medidas y protocolos de seguridad en la operación y gestión de sistemas informáticos.

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

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

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

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

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

5.5.1.5.2 TRANSVERSALES

CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.

CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).

5.5.1.5.3 ESPECÍFICAS

CE1 - Utilizar mecanismos criptográficos avanzados de para garantizar los requisitos de seguridad en un sistema, así como el acceso y seguridad en las comunicaciones.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Estudios de contenidos	60	0
Tutorías	15	0
Actividades en la plataforma virtual	15	0
Trabajos/Prácticas	60	0

5.5.1.7 METODOLOGÍAS DOCENTES

Las diferentes asignaturas que integran este Máster se impartirán todas ellas conforme a la metodología no presencial que caracteriza a la UNED, en la cual prima el autoaprendizaje del estudiante, pero asistido por el profesor y articulado a través de diversos sistemas de comunicación docente-discente. Dentro de estos sistemas, cabe destacar que el Máster en Ciberseguridad

se imparte con apoyo en una plataforma virtual interactiva de la UNED donde el estudiante encuentra tanto materiales didácticos básicos como materiales didácticos complementarios, informaciones, noticias, ejercicios y también permite la evaluación correspondiente a las diferentes materias.

5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Examen presencial	10.0	80.0
Trabajos	30.0	80.0
Pruebas de evaluación continua	0.0	30.0

NIVEL 2: Auditoría y Monitorización de la Seguridad		
5.5.1.1 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**
LENGUAS EN LAS 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	
NO CONSTAN ELEMENTOS DE NIVEL 3		

5.5.1.2 RESULTADOS DE APRENDIZAJE

Los resultados básicos más relevantes que se pretenden alcanzar con el estudio de esta asignatura son los siguientes:

- Describir las principales funciones de un centro de operaciones de seguridad.
- Diseñar un plan de monitorización y auditoria de una organización.
- Evaluar los diversos mecanismos de adquisición de datos y seleccionar los más adecuados al contexto.
- Analizar diversas fuentes de datos y evaluar los resultados en el contexto de la ciberseguridad.

5.5.1.3 CONTENIDOS

Los contenidos se organizarán de la siguiente manera, aunque se podrán modificar en un futuro en función de la evolución de la tecnología:

- Monitorización y auditoria de sistemas en red
- Metodologías para la monitorización de sistemas
- Gestión del Centro de Operaciones de Seguridad (SOC)
- Diseño de mecanismos para la adquisición de datos
- Análisis e interpretación de la información

5.5.1.4 OBSERVACIONES

Se recomienda que los interesados en cursar el Máster tengan un nivel de lectura en inglés suficiente como para entender contenidos técnicos en dicha lengua.

Gran parte de la bibliografía, así como los recursos proporcionados al estudiante en el curso virtual pueden estar únicamente en inglés, debido a la novedad de algunos de los contenidos propuestos para la asignatura.

Por otra parte, cada una de las actividades propuestas formativas en la asignatura constarán de una parte de trabajo individual, otra colectiva (si fuera el caso) y la utilización de la plataforma virtual, además de ser eminentemente prácticas. Todo ello de manera conjunta, por lo que la división de horas realizada en el apartado de actividades formativas es orientativa.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Analizar métodos y técnicas de ciberataques.

CG2 - Diseñar, poner en marcha y mantener un sistema de ciberseguridad.

CG4 - Identificar, gestionar y desarrollar medidas y protocolos de seguridad en la operación y gestión de sistemas informáticos.

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

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

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

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

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

5.5.1.5.2 TRANSVERSALES

CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.

CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).

5.5.1.5.3 ESPECÍFICAS

CE2 - Diseñar mecanismos de prevención de amenazas a la seguridad, así como de reconocer y resolver incidentes de seguridad en los sistemas críticos.

CE3 - Utilizar herramientas para monitorizar el tráfico de red y generar, explorar y manipular el tráfico en los sistemas de comunicación.

CE9 - Conocer las principales técnicas y herramientas de Inteligencia Artificial y sus aplicaciones en problemas de ciberseguridad.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Estudios de contenidos	60	0
Tutorías	15	0
Actividades en la plataforma virtual	15	0
Trabajos/Prácticas	60	0

5.5.1.7 METODOLOGÍAS DOCENTES

Las diferentes asignaturas que integran este Máster se impartirán todas ellas conforme a la metodología no presencial que caracteriza a la UNED, en la cual prima el autoaprendizaje del estudiante, pero asistido por el profesor y articulado a través de diversos sistemas de comunicación docente-discente. Dentro de estos sistemas, cabe destacar que el Máster en Ciberseguridad se imparte con apoyo en una plataforma virtual interactiva de la UNED donde el estudiante encuentra tanto materiales didácticos básicos como materiales didácticos complementarios, informaciones, noticias, ejercicios y también permite la evaluación correspondiente a las diferentes materias.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Examen presencial	10.0	80.0
Trabajos	30.0	80.0
Pruebas de evaluación continua	0.0	30.0

NIVEL 2: Análisis Forense

5.5.1.1 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**
LENGUAS EN LAS 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	

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

Los resultados básicos más relevantes que se pretenden alcanzar con el estudio de esta asignatura son los siguientes:

- Diseñar estrategias de recopilación de eventos para distintos elementos de un sistema y analizar los eventos observados en un ataque concreto para distinguir cuáles son de interés.
- Identificar las características de los distintos tipos de ataques sobre un sistema informático e identificar las fuentes más probables.
- Reunir las evidencias de un ataque sobre un sistema informático, garantizando la cadena de custodia necesaria.
- Justificar las medidas necesarias para mantener la cadena de custodia de las evidencias obtenidas de un sistema atacado.
- Describir la normativa legal y técnica de aplicación en el marco del análisis forense.

5.5.1.3 CONTENIDOS

Los contenidos se organizarán de la siguiente manera, aunque se podrán modificar en un futuro en función de la evolución de la tecnología:

- Introducción al Análisis Forense
- Normativa legal vigente
- Adquisición y gestión de evidencias
- Análisis forense de sistemas
- Respuesta ante incidentes
- Informe pericial

5.5.1.4 OBSERVACIONES

Se recomienda que los interesados en cursar el Máster tengan un nivel de lectura en inglés suficiente como para entender contenidos técnicos en dicha lengua.

Gran parte de la bibliografía, así como los recursos proporcionados al estudiante en el curso virtual pueden estar únicamente en inglés, debido a la novedad de algunos de los contenidos propuestos para la asignatura.

Por otra parte, cada una de las actividades propuestas formativas en la asignatura constarán de una parte de trabajo individual, otra colectiva (si fuera el caso) y la utilización de la plataforma virtual, además de ser eminentemente prácticas. Todo ello de manera conjunta, por lo que la división de horas realizada en el apartado de actividades formativas es orientativa.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Analizar métodos y técnicas de ciberataques.

CG3 - Conocer la normativa y la legislación en materia de ciberseguridad, sus implicaciones en el diseño y puesta en marcha de sistemas informáticos.

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

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
5.5.1.5.2 TRANSVERSALES
CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.
CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).
5.5.1.5.3 ESPECÍFICAS
CE5 - Analizar e identificar técnicas de ocultación de ataques a sistemas de comunicaciones y aplicaciones.
CE7 - Analizar sistemas para encontrar evidencias de ataques en los mismos y adoptar las medidas precisas para mantener la cadena de custodia de dichas evidencias.
CE8 - Conocer las técnicas y herramientas para la realización de un análisis forense con la preservación de pruebas digitales.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Estudios de contenidos	60	0
Tutorías	15	0
Actividades en la plataforma virtual	15	0
Trabajos/Prácticas	60	0

5.5.1.7 METODOLOGÍAS DOCENTES

Las diferentes asignaturas que integran este Máster se impartirán todas ellas conforme a la metodología no presencial que caracteriza a la UNED, en la cual prima el autoaprendizaje del estudiante, pero asistido por el profesor y articulado a través de diversos sistemas de comunicación docente-discente. Dentro de estos sistemas, cabe destacar que el Máster en Ciberseguridad se imparte con apoyo en una plataforma virtual interactiva de la UNED donde el estudiante encuentra tanto materiales didácticos básicos como materiales didácticos complementarios, informaciones, noticias, ejercicios y también permite la evaluación correspondiente a las diferentes materias.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Examen presencial	10.0	80.0
Trabajos	30.0	80.0
Pruebas de evaluación continua	0.0	30.0

NIVEL 2: Hacking Ético

5.5.1.1 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**

LENGUAS EN LAS 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	

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

Los resultados más relevantes que se pretenden alcanzar con el estudio de esta asignatura son los siguientes:

- Estudio y análisis de los sistemas de información para el aseguramiento de los mismos.
- Comprender y aplicar métodos y técnicas de hacking ético en sistemas y aplicaciones.
- Análisis de amenazas y vulnerabilidades de los sistemas de información.
- Diseño de técnicas y uso de herramientas para evitar la seguridad en los sistemas de información.

5.5.1.3 CONTENIDOS

Los contenidos se organizarán de la siguiente manera, aunque se podrán modificar en un futuro en función de la evolución de la tecnología:

- Introducción al Ethical Hacking.
- Footprinting, reconocimiento.
- Hacking de servidores y aplicaciones web.
- Ingeniería social.
- Evadirse de IDS, Firewalls y Honeypots.
- Hacking de plataformas móviles.

5.5.1.4 OBSERVACIONES

Se recomienda que los interesados en cursar el Máster tengan un nivel de lectura en inglés suficiente como para entender contenidos técnicos en dicha lengua.

Gran parte de la bibliografía, así como los recursos proporcionados al estudiante en el curso virtual pueden estar únicamente en inglés, debido a la novedad de algunos de los contenidos propuestos para la asignatura.

Por otra parte, cada una de las actividades propuestas formativas en la asignatura constarán de una parte de trabajo individual, otra colectiva (si fuera el caso) y la utilización de la plataforma virtual, además de ser eminentemente prácticas. Todo ello de manera conjunta, por lo que la división de horas realizada en el apartado de actividades formativas es orientativa.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Analizar métodos y técnicas de ciberataques.

CG3 - Conocer la normativa y la legislación en materia de ciberseguridad, sus implicaciones en el diseño y puesta en marcha de sistemas informáticos.

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

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

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

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

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

5.5.1.5.2 TRANSVERSALES

CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.

CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).		
5.5.1.5.3 ESPECÍFICAS		
CE4 - Analizar e identificar vulnerabilidades ante posibles ataques en los sistemas de comunicaciones y los servicios asociados.		
CE6 - Conocer las tendencias actuales en técnicas de ciberataque y las experiencias en casos reales.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Estudios de contenidos	60	0
Tutorías	15	0
Actividades en la plataforma virtual	15	0
Trabajos/Prácticas	60	0
5.5.1.7 METODOLOGÍAS DOCENTES		
Las diferentes asignaturas que integran este Máster se impartirán todas ellas conforme a la metodología no presencial que caracteriza a la UNED, en la cual prima el autoaprendizaje del estudiante, pero asistido por el profesor y articulado a través de diversos sistemas de comunicación docente-discente. Dentro de estos sistemas, cabe destacar que el Máster en Ciberseguridad se imparte con apoyo en una plataforma virtual interactiva de la UNED donde el estudiante encuentra tanto materiales didácticos básicos como materiales didácticos complementarios, informaciones, noticias, ejercicios y también permite la evaluación correspondiente a las diferentes materias.		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Examen presencial	10.0	80.0
Trabajos	30.0	80.0
Pruebas de evaluación continua	0.0	30.0
NIVEL 2: Ciberilícitos		
5.5.1.1 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**
LENGUAS EN LAS 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	
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
Los resultados más relevantes que se pretenden alcanzar con el estudio de esta asignatura son los siguientes:		

- conocer la regulación de la protección de datos en nuestro país, en especial en aquellos aspectos relacionados con los métodos, técnicas y procesos informáticos y las TIC;
- conocer las conductas que en el ámbito de la informática y de las TIC son consideradas ilícito civil o administrativo en relación con la protección de datos;
- conocer la evolución de los delitos informáticos (por el medio utilizado y por el objeto de protección) a los ciberdelitos;
- conocer las clasificaciones de los ciberdelitos en relación con el bien jurídico afectado y en relación con el medio delictivo: ciberdelitos puros, ciberdelitos réplica y ciberdelitos de contenido;
- conocer la regulación de los ciberdelitos puros;
- conocer las principales particularidades del medio informático en los ciberdelitos réplica y los ciberdelitos de contenido.

5.5.1.3 CONTENIDOS

Los contenidos se organizarán de la siguiente manera, aunque se podrán modificar en un futuro en función de la evolución legislativa:

I.- Ilícitos administrativos contra la protección de datos.

1. Surgimiento y necesidad de la protección de datos. 2. Regulación europea y española sobre protección de datos. 3. Principios jurídicos en la protección de datos y derechos de los titulares de los datos. 4. Internet, redes sociales, y protección de datos. 5. Ilícitos administrativos e instituciones dedicadas a la protección de datos.

II.- Ciberdelitos.

1. Introducción criminológica al fenómeno de la ciberdelincuencia. 2. La informática y las TIC como medios delictivos y como objetos de protección: de los delitos informáticos a los ciberdelitos. 3. Clasificación de los ciberdelitos en función del bien jurídico afectado y de su relación con del medio cibernetico. 4. Los ciberdelitos puros, regulación legal e interpretación jurisprudencial. 5. Nuevos medios para delitos clásicos: los ciberdelitos réplica y los ciberdelitos de contenido.

5.5.1.4 OBSERVACIONES

Se recomienda que los interesados en cursar el Máster tengan un nivel de lectura en inglés suficiente como para entender contenidos técnicos en dicha lengua.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG3 - Conocer la normativa y la legislación en materia de ciberseguridad, sus implicaciones en el diseño y puesta en marcha de sistemas informáticos.

CG4 - Identificar, gestionar y desarrollar medidas y protocolos de seguridad en la operación y gestión de sistemas informáticos.

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

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

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

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

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

5.5.1.5.2 TRANSVERSALES

CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.

CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).

5.5.1.5.3 ESPECÍFICAS

CE10 - Comprender la importancia del Derecho como sistema regulador de las relaciones sociales.

CE11 - Conseguir la percepción del carácter unitario del ordenamiento jurídico y de la necesaria visión interdisciplinaria de los problemas jurídicos.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Estudios de contenidos	100	0
Tutorías	15	0
Actividades en la plataforma virtual	15	0
Trabajos/Prácticas	20	0

5.5.1.7 METODOLOGÍAS DOCENTES
Las diferentes asignaturas que integran este Máster se impartirán todas ellas conforme a la metodología no presencial que caracteriza a la UNED, en la cual prima el autoaprendizaje del estudiante, pero asistido por el profesor y articulado a través de diversos sistemas de comunicación docente-discente. Dentro de estos sistemas, cabe destacar que el Máster en Ciberseguridad se imparte con apoyo en una plataforma virtual interactiva de la UNED donde el estudiante encuentra tanto materiales didácticos básicos como materiales didácticos complementarios, informaciones, noticias, ejercicios y también permite la evaluación correspondiente a las diferentes materias.

5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Examen presencial	10.0	80.0
Trabajos	30.0	80.0
Pruebas de evaluación continua	0.0	30.0

NIVEL 2: Análisis de Malware		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
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**

LENGUAS EN LAS 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	

LISTADO DE ESPECIALIDADES
No existen datos
NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

Los resultados más relevantes que se pretenden alcanzar con el estudio de esta asignatura son los siguientes:

- Comprender y aplicar métodos y técnicas de investigación de ciberataques a un sistema informático
- Analizar y detectar anomalías y firmas de ataques en los sistemas informáticos
- Analizar y detectar técnicas de ocultación de ataques a sistemas informáticas.
- Conocer las tendencias actuales en técnicas malware y las experiencias aprendidas en casos reales.
- Conocer y aplicar los mecanismos pertinentes para proteger los datos residentes en un sistema o en tránsito por una red.

5.5.1.3 CONTENIDOS

Los contenidos se organizarán de la siguiente manera, aunque se podrán modificar en un futuro en función de la evolución de la tecnología:

- Introducción al análisis de malware.
- Herramientas y métodos de análisis de malware.
- Metodología de análisis y sistemas de obtención de análisis de malware.
- Técnicas de ofuscación de malware.
- Amenazas Avanzadas Persistentes (APT).

- Detección, Confinamiento y Erradicación.

5.5.1.4 OBSERVACIONES

Se recomienda que los interesados en cursar el Máster tengan un nivel de lectura en inglés suficiente como para entender contenidos técnicos en dicha lengua.

Gran parte de la bibliografía, así como los recursos proporcionados al estudiante en el curso virtual pueden estar únicamente en inglés, debido a la novedad de algunos de los contenidos propuestos para la asignatura.

Por otra parte, cada una de las actividades propuestas formativas en la asignatura constarán de una parte de trabajo individual, otra colectiva (si fuera el caso) y la utilización de la plataforma virtual, además de ser eminentemente prácticas. Todo ello de manera conjunta, por lo que la división de horas realizada en el apartado de actividades formativas es orientativa.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Analizar métodos y técnicas de ciberataques.

CG4 - Identificar, gestionar y desarrollar medidas y protocolos de seguridad en la operación y gestión de sistemas informáticos.

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

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

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

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

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

5.5.1.5.2 TRANSVERSALES

CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.

CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).

5.5.1.5.3 ESPECÍFICAS

CE5 - Analizar e identificar técnicas de ocultación de ataques a sistemas de comunicaciones y aplicaciones.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Estudios de contenidos	60	0
Tutorías	15	0
Actividades en la plataforma virtual	15	0
Trabajos/Prácticas	60	0

5.5.1.7 METODOLOGÍAS DOCENTES

Las diferentes asignaturas que integran este Máster se impartirán todas ellas conforme a la metodología no presencial que caracteriza a la UNED, en la cual prima el autoaprendizaje del estudiante, pero asistido por el profesor y articulado a través de diversos sistemas de comunicación docente-discente. Dentro de estos sistemas, cabe destacar que el Máster en Ciberseguridad se imparte con apoyo en una plataforma virtual interactiva de la UNED donde el estudiante encuentra tanto materiales didácticos básicos como materiales didácticos complementarios, informaciones, noticias, ejercicios y también permite la evaluación correspondiente a las diferentes materias.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Examen presencial	10.0	80.0
Trabajos	30.0	80.0
Pruebas de evaluación continua	0.0	30.0

NIVEL 2: Seguridad en Infraestructuras Críticas

5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
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**
LENGUAS EN LAS 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	
LISTADO DE ESPECIALIDADES		
No existen datos		
NO CONSTAN ELEMENTOS DE NIVEL 3		

5.5.1.2 RESULTADOS DE APRENDIZAJE

Los resultados básicos más relevantes que se pretenden alcanzar con el estudio de esta asignatura son los siguientes:

- Ser capaz de describir términos como ICS, DCS, SCADA, red industrial, protocolos industriales, zonas, etc.
- Ser capaz de identificar el alcance de las recomendaciones de seguridad industrial más comunes y cómo se han alcanzado
- Identificar las topologías y esquemas de segmentación más comunes en las redes industriales y cómo se integran las redes inalámbricas y el acceso remoto
- Identificar las particularidades de rendimiento de las redes industriales, como el tratamiento de la latencia y el *jitter*
- Identificar las principales características de algunos de los protocolos más típicos de este entorno
- Entender las principales motivaciones y las posibles consecuencias de incidentes de seguridad en entornos industriales
- Identificar los objetivos de ataque más comunes, así como los métodos de ataque más comunes, entendiendo las principales vías de ataque
- Conocer las principales metodologías de evaluación de riesgos en el sector industrial
- Identificar las amenazas principales, así como las vulnerabilidades más típicas
- Ser capaz de hacer una clasificación general de los riesgos para un entorno industrial
- Conocer cómo segmentar redes para implantar controles de seguridad de redes, de host y de acceso
- Conocer a nivel básico la detección de anomalías y amenazas en redes industriales
- Identificar procedimientos para monitorizar zonas de seguridad en entornos industriales con éxito
- Conocer cómo hacer una gestión segura de la información obtenida, así como de los logs

5.5.1.3 CONTENIDOS

Los contenidos se organizarán de la siguiente manera, aunque se podrán modificar en un futuro en función de la evolución de la tecnología:

- Introducción a los problemas de seguridad en redes industriales
- Diseño, arquitectura de red y protocolos en redes industriales
- Principales problemas de seguridad en sistemas de control industrial
- Evaluaciones de vulnerabilidades y riesgos
- Introducción a las defensas básicas en redes industriales
- Monitorización de la seguridad en redes industriales

5.5.1.4 OBSERVACIONES

Se recomienda que los interesados en cursar el Máster tengan un nivel de lectura en inglés suficiente como para entender contenidos técnicos en dicha lengua.

La mayor parte de la bibliografía, así como de los recursos proporcionados al estudiante en el curso virtual, estarán escritos únicamente en inglés, debido a la actualidad de los contenidos propuestos para la asignatura.

Por otra parte, cada una de las actividades propuestas formativas en la asignatura constará de una parte de trabajo individual, otra colectiva (si fuera el caso) y la utilización de la plataforma virtual. Todo ello de manera conjunta, por lo que la división de horas realizada en el apartado de actividades formativas es orientativa.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Analizar métodos y técnicas de ciberataques.

CG2 - Diseñar, poner en marcha y mantener un sistema de ciberseguridad.

CG4 - Identificar, gestionar y desarrollar medidas y protocolos de seguridad en la operación y gestión de sistemas informáticos.

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

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

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

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

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

5.5.1.5.2 TRANSVERSALES

CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.

CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).

5.5.1.5.3 ESPECÍFICAS

CE4 - Analizar e identificar vulnerabilidades ante posibles ataques en los sistemas de comunicaciones y los servicios asociados.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Estudios de contenidos	60	0
Tutorías	15	0
Actividades en la plataforma virtual	15	0
Trabajos/Prácticas	60	0

5.5.1.7 METODOLOGÍAS DOCENTES

Las diferentes asignaturas que integran este Máster se impartirán todas ellas conforme a la metodología no presencial que caracteriza a la UNED, en la cual prima el autoaprendizaje del estudiante, pero asistido por el profesor y articulado a través de diversos sistemas de comunicación docente-discente. Dentro de estos sistemas, cabe destacar que el Máster en Ciberseguridad se imparte con apoyo en una plataforma virtual interactiva de la UNED donde el estudiante encuentra tanto materiales didácticos básicos como materiales didácticos complementarios, informaciones, noticias, ejercicios y también permite la evaluación correspondiente a las diferentes materias.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Examen presencial	10.0	80.0
Trabajos	30.0	80.0
Pruebas de evaluación continua	0.0	30.0

NIVEL 2: Gestión de Incidentes de Ciberseguridad

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Optativa
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**
LENGUAS EN LAS 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	
LISTADO DE ESPECIALIDADES		
No existen datos		
NO CONSTAN ELEMENTOS DE NIVEL 3		

5.5.1.2 RESULTADOS DE APRENDIZAJE

Los resultados más relevantes que se pretenden alcanzar con el estudio de esta asignatura son los siguientes:

- Organizar y mantener un esquema de riesgos
- Conocer la estructura de un ciberataque
- Tipificar los Ciberincidentes y clasificar su peligrosidad
- Clasificar los grupos o niveles de un ciberataque
- Conocer la metodología de notificación al CERT
- Conocer los elementos para diseñar un plan de respuesta de Ciberincidentes

5.5.1.3 CONTENIDOS

Los contenidos se organizarán de la siguiente manera, aunque se podrán modificar en un futuro en función de la evolución de la tecnología:

- Introducción a la tipología y estructura de los ciberataques
- Organismos de Alerta en ciberseguridad. Organización y Servicios
- Análisis de Riesgos: Activos, Agentes y Escenarios de riesgo (ER)
- Gestión, clasificación y notificación de Ciberincidentes

5.5.1.4 OBSERVACIONES

Se recomienda que los interesados en cursar el Máster tengan un nivel de lectura en inglés suficiente como para entender contenidos técnicos en dicha lengua.

Gran parte de la bibliografía, así como los recursos proporcionados al estudiante en el curso virtual pueden estar únicamente en inglés, debido a la novedad de algunos de los contenidos propuestos para la asignatura.

Por otra parte, cada una de las actividades propuestas formativas en la asignatura constarán de una parte de trabajo individual, otra colectiva (si fuera el caso) y la utilización de la plataforma virtual, además de ser eminentemente prácticas. Todo ello de manera conjunta, por lo que la división de horas realizada en el apartado de actividades formativas es orientativa.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Analizar métodos y técnicas de ciberataques.

CG3 - Conocer la normativa y la legislación en materia de ciberseguridad, sus implicaciones en el diseño y puesta en marcha de sistemas informáticos.

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

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

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
5.5.1.5.2 TRANSVERSALES
CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.
CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).
5.5.1.5.3 ESPECÍFICAS
CE6 - Conocer las tendencias actuales en técnicas de ciberataque y las experiencias en casos reales.

5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Estudios de contenidos	60	0
Tutorías	15	0
Actividades en la plataforma virtual	15	0
Trabajos/Prácticas	60	0

5.5.1.7 METODOLOGÍAS DOCENTES
Las diferentes asignaturas que integran este Máster se impartirán todas ellas conforme a la metodología no presencial que caracteriza a la UNED, en la cual prima el autoaprendizaje del estudiante, pero asistido por el profesor y articulado a través de diversos sistemas de comunicación docente-discente. Dentro de estos sistemas, cabe destacar que el Máster en Ciberseguridad se imparte con apoyo en una plataforma virtual interactiva de la UNED donde el estudiante encuentra tanto materiales didácticos básicos como materiales didácticos complementarios, informaciones, noticias, ejercicios y también permite la evaluación correspondiente a las diferentes materias.

5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Examen presencial	10.0	80.0
Trabajos	30.0	80.0
Pruebas de evaluación continua	0.0	30.0

NIVEL 2: Introducción al Aprendizaje Automático para Ciberseguridad		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
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**
LENGUAS EN LAS 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	

LISTADO DE ESPECIALIDADES
No existen datos
NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

Los resultados más relevantes que se pretenden alcanzar con el estudio de esta asignatura son los siguientes:

- Conocer y saber aplicar los algoritmos básicos de agrupamiento para analizar patrones en ataques y posibles vulnerabilidades de seguridad.
- Conocer y aplicar las técnicas de aprendizaje automático para clasificación de patrones y su aplicación en ciberseguridad.
- Utilizar modelos probabilísticos para clasificación y agrupamiento en problemas de ciberseguridad.
- Conocer las arquitecturas básicas de aprendizaje profundo para su aplicación en ciberseguridad.

5.5.1.3 CONTENIDOS

Los contenidos se organizarán de la siguiente manera, aunque se podrán modificar en un futuro en función de la evolución de la tecnología:

- La Inteligencia Artificial en ciberseguridad
- Algoritmos de agrupamiento
- Clasificación
- Modelos probabilísticos
- Arquitecturas de aprendizaje profundo (Deep Learning)

5.5.1.4 OBSERVACIONES

Se recomienda que los interesados en cursar el Máster tengan un nivel de lectura en inglés suficiente como para entender contenidos técnicos en dicha lengua.

Gran parte de la bibliografía, así como los recursos proporcionados al estudiante en el curso virtual pueden estar únicamente en inglés, debido a la novedad de algunos de los contenidos propuestos para la asignatura.

Por otra parte, cada una de las actividades propuestas formativas en la asignatura constarán de una parte de trabajo individual, otra colectiva (si fuera el caso) y la utilización de la plataforma virtual, además de ser eminentemente prácticas. Todo ello de manera conjunta, por lo que la división de horas realizada en el apartado de actividades formativas es orientativa.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Analizar métodos y técnicas de ciberataques.

CG2 - Diseñar, poner en marcha y mantener un sistema de ciberseguridad.

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

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

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

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

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

5.5.1.5.2 TRANSVERSALES

CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.

CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).

5.5.1.5.3 ESPECÍFICAS

CE9 - Conocer las principales técnicas y herramientas de Inteligencia Artificial y sus aplicaciones en problemas de ciberseguridad.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Estudios de contenidos	60	0
Tutorías	15	0
Actividades en la plataforma virtual	15	0
Trabajos/Prácticas	60	0

5.5.1.7 METODOLOGÍAS DOCENTES

Las diferentes asignaturas que integran este Máster se impartirán todas ellas conforme a la metodología no presencial que caracteriza a la UNED, en la cual prima el autoaprendizaje del estudiante, pero asistido por el profesor y articulado a través de diversos sistemas de comunicación docente-discente. Dentro de estos sistemas, cabe destacar que el Máster en Ciberseguridad se imparte con apoyo en una plataforma virtual interactiva de la UNED donde el estudiante encuentra tanto materiales didácticos básicos como materiales didácticos complementarios, informaciones, noticias, ejercicios y también permite la evaluación correspondiente a las diferentes materias.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Examen presencial	10.0	80.0
Trabajos	30.0	80.0
Pruebas de evaluación continua	0.0	30.0

NIVEL 2: Marco jurídico de la Defensa Nacional en el Ciberespacio

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Optativa
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**

LENGUAS EN LAS 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	

LISTADO DE ESPECIALIDADES

No existen datos

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

Los resultados más relevantes que se pretenden alcanzar con el estudio de esta asignatura son los siguientes:

- Conocer la regulación básica de la ciberseguridad dentro del marco normativo del sistema español de Seguridad Nacional.
- Conocer la específica regulación y organización de la ciberdefensa militar.
- Conocer las singularidades de la aplicación en el ciberespacio de los principios generales del Derecho internacional público.
- Conocer las diferentes posiciones mantenidas en torno a cómo se aplican en el ciberespacio las normas internacionales relativas al uso de la fuerza armada.
- Conocer los aspectos fundamentales que presenta la aplicación del Derecho Internacional de los Conflictos Armados a las operaciones conducidas en y a través del ciberespacio.

5.5.1.3 CONTENIDOS

Los contenidos se organizarán de la siguiente manera, aunque se podrán modificar en un futuro en función de la evolución doctrinal y normativa:

I. *La ciberseguridad dentro del Sistema de Seguridad Nacional: normativa, documentos estratégicos y organización.*

II. El componente militar de la ciberseguridad en España: el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.

III. Aplicación de los principios de soberanía, diligencia debida, jurisdicción y responsabilidad internacional en el ciberespacio.

IV. Ciberespionaje y Derecho internacional público.

V. El *¿ius ad bellum¿* en el ciberespacio. Uso de la fuerza armada en el ciberespacio: prohibición general y excepciones.

VI. El *¿ius in bello¿* en el ciberespacio: aplicación del Derecho Internacional de los Conflictos Armados a las operaciones conducidas en y a través del ciberespacio.

5.5.1.4 OBSERVACIONES

Se recomienda que los interesados en cursar el Máster tengan un nivel de lectura en inglés suficiente como para entender contenidos técnicos en dicha lengua.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG3 - Conocer la normativa y la legislación en materia de ciberseguridad, sus implicaciones en el diseño y puesta en marcha de sistemas informáticos.

CG4 - Identificar, gestionar y desarrollar medidas y protocolos de seguridad en la operación y gestión de sistemas informáticos.

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

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

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

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

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

5.5.1.5.2 TRANSVERSALES

CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.

CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).

5.5.1.5.3 ESPECÍFICAS

CE10 - Comprender la importancia del Derecho como sistema regulador de las relaciones sociales.

CE11 - Conseguir la percepción del carácter unitario del ordenamiento jurídico y de la necesaria visión interdisciplinaria de los problemas jurídicos.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Estudios de contenidos	60	0
Tutorías	15	0
Actividades en la plataforma virtual	15	0
Trabajos/Prácticas	60	0

5.5.1.7 METODOLOGÍAS DOCENTES

Las diferentes asignaturas que integran este Máster se impartirán todas ellas conforme a la metodología no presencial que caracteriza a la UNED, en la cual prima el autoaprendizaje del estudiante, pero asistido por el profesor y articulado a través de diversos sistemas de comunicación docente-discente. Dentro de estos sistemas, cabe destacar que el Máster en Ciberseguridad se imparte con apoyo en una plataforma virtual interactiva de la UNED donde el estudiante encuentra tanto materiales didácticos

básicos como materiales didácticos complementarios, informaciones, noticias, ejercicios y también permite la evaluación correspondiente a las diferentes materias.

5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Examen presencial	10.0	80.0
Trabajos	30.0	80.0
Pruebas de evaluación continua	0.0	30.0

NIVEL 2: Trabajo Fin de Máster (TFM)		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Trabajo Fin de Grado / Máster	
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**

LENGUAS EN LAS 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	

LISTADO DE ESPECIALIDADES
No existen datos
NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

El estudiante será capaz de:

- Evaluar los recursos materiales y personales para realizar una planificación realista del trabajo.
- Establecer las hipótesis de trabajo con claridad, argumentando su validez para alcanzar los objetivos del proyecto.
- Explicar la metodología de búsqueda de la información utilizada, demostrando que se han consultado las fuentes más relevantes del campo de estudio.
- Resolver problemas de investigación relacionados con la Ciberseguridad con iniciativa y creatividad.
- Integrar distintas tecnologías relacionadas con la Ciberseguridad.
- Explicar razonadamente las diferentes alternativas que se han considerado a la hora de establecer la forma de enfrentarse al problema de Ciberseguridad planteado inicialmente.
- Defender las soluciones de Ciberseguridad propuestas mediante argumentos lógicos y coherentes.
- Escoger las herramientas de Ciberseguridad software y hardware más adecuadas y utilizarlas correctamente.

5.5.1.3 CONTENIDOS

Su desarrollo, consistente en un proyecto integral de Ciberseguridad en el que se sinteticen las competencias adquiridas en las enseñanzas, y que debe involucrar la articulación de los conocimientos, habilidades y destrezas adquiridos a lo largo de su formación dentro del Máster. Debe tener también carácter formativo, abordar problemas propios del área de Ciberseguridad y en su caso servir de preparación para posteriores etapas de formación académica en estudios de doctorado.

El trabajo involucrará la realización de estudios, valoraciones e informes acerca de las tecnologías disponibles, innovaciones y alternativas. Finalmente, debe ser realizado con rigor profesional o en su caso científico y ser conforme a los principios éticos.

5.5.1.4 OBSERVACIONES

No existen requisitos previos, más allá de los propios del Máster, aunque es necesario dominar el inglés técnico (leer y escribir) para manejar con facilidad las fuentes bibliográficas de investigación.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Analizar métodos y técnicas de ciberataques.

CG2 - Diseñar, poner en marcha y mantener un sistema de ciberseguridad.

CG3 - Conocer la normativa y la legislación en materia de ciberseguridad, sus implicaciones en el diseño y puesta en marcha de sistemas informáticos.

CG4 - Identificar, gestionar y desarrollar medidas y protocolos de seguridad en la operación y gestión de sistemas informáticos.

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

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

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

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

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

5.5.1.5.2 TRANSVERSALES

CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.

CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).

5.5.1.5.3 ESPECÍFICAS

No existen datos

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Estudios de contenidos	70	0
Tutorías	30	0
Trabajos/Prácticas	200	0

5.5.1.7 METODOLOGÍAS DOCENTES

Las diferentes asignaturas que integran este Máster se impartirán todas ellas conforme a la metodología no presencial que caracteriza a la UNED, en la cual prima el autoaprendizaje del estudiante, pero asistido por el profesor y articulado a través de diversos sistemas de comunicación docente-discente. Dentro de estos sistemas, cabe destacar que el Máster en Ciberseguridad se imparte con apoyo en una plataforma virtual interactiva de la UNED donde el estudiante encuentra tanto materiales didácticos básicos como materiales didácticos complementarios, informaciones, noticias, ejercicios y también permite la evaluación correspondiente a las diferentes materias.

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Preparación, presentación y defensa pública del TFM	100.0	100.0

6. PERSONAL ACADÉMICO

6.1 PROFESORADO Y OTROS RECURSOS HUMANOS				
Universidad	**Categoría**	**Total %**	**Doctores %**	**Horas %**
Universidad Nacional de Educación a Distancia	Catedrático de Universidad	16	100	13,3
Universidad Nacional de Educación a Distancia	Profesor Titular de Universidad	47.3	100	50,3
Universidad Nacional de Educación a Distancia	Profesor Titular de Escuela Universitaria	5	0	1
Universidad Nacional de Educación a Distancia	Profesor colaborador Licenciado	10.7	50	12
Universidad Nacional de Educación a Distancia	Ayudante Doctor	21	100	23,4
PERSONAL ACADÉMICO				
Ver Apartado 6: Anexo 1.				
6.2 OTROS RECURSOS HUMANOS				
Ver Apartado 6: Anexo 2.				

7. RECURSOS MATERIALES Y SERVICIOS

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

8. RESULTADOS PREVISTOS

8.1 ESTIMACIÓN DE VALORES CUANTITATIVOS		
TASA DE GRADUACIÓN %	**TASA DE ABANDONO %**	**TASA DE EFICIENCIA %**
25	30	50
CODIGO	**TASA**	**VALOR %**
No existen datos		
Justificación de los Indicadores Propuestos:		
Ver Apartado 8: Anexo 1.		

8.2 PROCEDIMIENTO GENERAL PARA VALORAR EL PROCESO Y LOS RESULTADOS

8.2.-Procedimiento general para valorar el progreso y resultados de aprendizaje

El procedimiento para recogida y análisis de información sobre los resultados de aprendizaje y la utilización de esa información en la mejora del desarrollo del plan de estudios en el Máster se llevará a cabo en función de los procedimientos generales establecidos por la UNED.

La evaluación del progreso en el Máster se llevará a cabo sobre la base de las competencias generales y específicas del Máster. Para una especificación de las características del proceso de evaluación se recomienda acudir al apartado ¿Planificación de las enseñanzas¿, donde se detalla cada uno de los procedimientos.

En síntesis, el progreso y resultados de aprendizaje se evaluarán en función de tres elementos principales:

- Los procedimientos generales establecidos por la UNED.

- El sistema de evaluación específico de cada una de las materias que componen el Máster

- El desarrollo y evaluación del Trabajo Fin de Máster.

El progreso y resultados de aprendizaje de este Máster se evaluarán al igual que el resto de las enseñanzas oficiales de la UNED en función de los procedimientos habituales en la enseñanza a distancia.

La valoración del progreso de los estudiantes y los resultados de aprendizaje señalados para cada una de las asignaturas que componen el Máster, vinculados al desarrollo de las competencias genéricas y específicas finales del Máster, se valorarán a través de distintas vías, en función del tipo de resultado de aprendizaje (conocimientos, destrezas o actitudes), y de las actividades planteadas para su logro, de forma que dicha evaluación sea coherente con dichos resultados. De esta manera, los resultados de aprendizaje alcanzados podrán valorarse a través de:

- Distintas pruebas de autoevaluación, evaluación en línea, de corrección automática, evaluaciones presenciales, etc¿

- Protocolos de evaluación, o rúbricas, diseñados para estimar el logro de los distintos resultados de aprendizaje previstos, a partir de las actividades de aprendizaje planteadas en el plan de actividades de cada asignatura. Estos protocolos estarán a disposición de los estudiantes, así como de los responsables de la evaluación continua)

- Evaluación del desarrollo y la defensa presencial del Trabajo Fin de Máster.

- Asimismo, está previsto recoger la opinión de los estudiantes a través de encuesta en línea, acerca de su valoración sobre si este Máster les ha permitido obtener los resultados de aprendizaje previstos y desarrollar las competencias del título La aplicación de estos procedimientos de valoración en diversos momentos y sobre diferentes producciones de los estudiantes nos permiten evaluar el progreso en el desarrollo de los aprendizajes de este Máster y, finalmente, el resultado definitivo de los mismos

Estos criterios y procedimientos tienen como objetivo principal garantizar la calidad de la formación y los servicios que reciben los estudiantes, así como fomentar acciones continuas de revisión y mejora de los programas.

Habrá un seguimiento continuo del MÁSTER y una reunión trimestral de la Comisión Académica del Programa con objeto de evaluar y controlar el funcionamiento del Programa, y en su caso planificar cambios y desarrollarlos. Se estudiará el perfil formativo de los estudiantes, el proceso de inscripción, la marcha del MÁSTER en sus aspectos administrativos y docentes y los posibles desajustes que haya, sobre todo en su curso inicial.

La Comisión garantizará la difusión del Programa a través de la página web y de medios impresos, que faciliten a los estudiantes su trabajo y les permitan conocer de forma exacta los contenidos, competencia y Especialidades de su opción formativa. Habrá un foro virtual del Programa en donde los estudiantes y Profesores podrán comunicarse, plantear preguntas y resolver dificultades.

Autoinformes, encuestas y análisis de resultados académicos y matrículas darán a conocer las deficiencias y los puntos fuertes del MÁSTER. Las deficiencias encontradas y la posible manera de paliarlas se reflejarán en el informe que la Comisión de Académica del máster tiene que elevar cada año a la Junta de Facultad.

Los estudiantes serán atendidos de forma individual. Las materias elegidas se adecuarán al número de créditos requeridos y horas de estudio a emplear. Se ponderará asimismo el nivel de aprendizaje del alumno, el grado de consecución de los objetivos planteados y sus resultados académicos. El profesor elaborará, en caso necesario, materiales específicos para los alumnos con el fin de facilitarles el trabajo y el estudio.

Para la evaluación de la docencia se contará con la colaboración de los tres sectores implicados: profesores, estudiantes y personal de administración.

Los profesores implicados en el MÁSTER harán una evaluación de los resultados.

En el foro virtual del MÁSTER habrá a disposición de los alumnos, profesores y personal administrativo un cuestionario sobre el programa, desarrollo y resultados del MÁSTER, los materiales, los conocimientos impartidos, su adaptación a la metodología de la enseñanza a distancia, las exigencias de rendimiento, los profesores, la tutorización, la atención administrativa, etc.

La Comisión Académica trabajará con las encuestas y observaciones de los tres sectores implicados, proponiendo soluciones en coordinación con los órganos rectores de cada uno de los Departamentos que participan en este MÁSTER. Tendrá para ello una reunión anual, a la cual asistirá asimismo un representante de los Estudiantes.

Además de los procedimientos institucionales vigentes en la UNED y recogidos en los Estatutos y Reglamento de Estudiantes, este programa habilita como cauces para la recepción de sugerencias y reclamaciones los siguientes medios:

- Dirección postal de la Coordinación del MÁSTER

- Número de teléfono y horario de atención para la recepción de sugerencias y reclamaciones.

- Dirección electrónica para recibir sugerencias y reclamaciones.

- Foro virtual del MÁSTER.

- Estos procedimientos y medios se harán públicos en la página web del Postgrado y en la información entregada a los estudiantes tras su matriculación en el programa.

9. SISTEMA DE GARANTÍA DE CALIDAD

ENLACE	http://portal.uned.es/portal/page?_pageid=93,25884524&_dad=portal&_schema=PORTAL

10. CALENDARIO DE IMPLANTACIÓN

10.1 CRONOGRAMA DE IMPLANTACIÓN	
CURSO DE INICIO	2019
Ver Apartado 10: Anexo 1.	
10.2 PROCEDIMIENTO DE ADAPTACIÓN	
No ha lugar.	
10.3 ENSEÑANZAS QUE SE EXTINGUEN	
CÓDIGO	**ESTUDIO - CENTRO**

11. PERSONAS ASOCIADAS A LA SOLICITUD

11.1 RESPONSABLE DEL TÍTULO			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
05149707F	RAFAEL	MARTINEZ	TOMAS

DOMICILIO	CÓDIGO POSTAL	PROVINCIA	MUNICIPIO
ETSI Informática, UNED; C/ Juan del Rosal, 16	28040	Madrid	Madrid
EMAIL	**MÓVIL**	**FAX**	**CARGO**
director@informatica.uned.es	913987242	913989383	Director de la ETSI Informática
11.2 REPRESENTANTE LEGAL			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
18021524N	RICARDO	MAIRAL	USON
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
C/Bravo Murillo, 38	28015	Madrid	Madrid
EMAIL	**MÓVIL**	**FAX**	**CARGO**
admin.masteresoficiales@adm.uned.es	913989632	913989632	Rector
11.3 SOLICITANTE			
El responsable del título no es el solicitante			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
05266644N	ROBERTO	HERNÁNDEZ	BERLINCHES
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
ETSI Informática, UNED; C/ Juan del Rosal, 16	28040	Madrid	Madrid
EMAIL	**MÓVIL**	**FAX**	**CARGO**
roberto@scc.uned.es	915485090	913989383	Catedrático de Universidad

Apartado 2: Anexo 1

Nombre :justificación.pdf

HASH SHA1 :34B67D44D7F29668DE13267B20DC53556DBE7B6A

Código CSV :313696562009214998468124

Ver Fichero: justificación.pdf

Apartado 4: Anexo 1

Nombre :4.1 SISTEMAS DE INFORMACIÓN PREVIO.pdf

HASH SHA1 :D3252FE016BC6F909A07690DAECF1619A6AD9E0B

Código CSV :312225132855352530330081

Ver Fichero: 4.1 SISTEMAS DE INFORMACIÓN PREVIO.pdf

Apartado 5: Anexo 1

Nombre :plan_estudios_y_mec_coordinación_docente.pdf

HASH SHA1 :C30BF80598442C7183C75439E8D633B3220E8185

Código CSV :313151621326454927157929

Ver Fichero: plan_estudios_y_mec_coordinación_docente.pdf

Apartado 6: Anexo 1

Nombre :6 Personal docente de Ciberseguridad.pdf

HASH SHA1 :38AD3372F724C324CBB0EF5D26FB6FE7F6F0AB84

Código CSV :314004173393514452758188

Ver Fichero: 6 Personal docente de Ciberseguridad.pdf

Apartado 6: Anexo 2

Nombre :6.2 RRHH ESCUELA DE INFORMÁTICA.pdf

HASH SHA1 :BEBCA3547A3C783CB7C77CAE38B091B0A59384F4

Código CSV :312225742602345964531051

Ver Fichero: 6.2 RRHH ESCUELA DE INFORMÁTICA.pdf

Apartado 7: Anexo 1

Nombre :7. RECURSOS MATERIALES Y SERVICIOS INFORMÁTICA.pdf

HASH SHA1 :F715DBCAE238AC56117B6DECB1DECFAFB13BA092

Código CSV :312225609500219019386442

Ver Fichero: 7. RECURSOS MATERIALES Y SERVICIOS INFORMÁTICA.pdf

Apartado 8: Anexo 1

Nombre :8 Justificación de los indicadores.pdf

HASH SHA1 :3374844473AB858CFA9446C37594BF66D2F38661

Código CSV :313602678303316394371436

Ver Fichero: 8 Justificación de los indicadores.pdf

Apartado 10: Anexo 1

Nombre :calendario_implantación.pdf

HASH SHA1 :B2C519622DCEE1F36D0812EE4FBCF144AB868614

Código CSV :312186041820073164002829

Ver Fichero: calendario_implantación.pdf