SECRETARÍA GENERAL

C/ Bravo Murillo, n.º 38. Madrid 28015
secgral@adm.uned.es

D.ª ELENA MACULAN, 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 diez de julio de dos mil veintiséis, fue adoptado, entre otros, el siguiente acuerdo:

06. Estudio y aprobación, si procede, de las propuestas del Vicerrectorado de Ordenación Académica

06.08 El Consejo de Gobierno aprueba la modificación del Máster Universitario en Ciberseguridad (pendiente de fin de tramitación), 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 trece de julio de dos mil veintiséis.

D. MIGUEL ROMERO HORTELANO, VICESECRETARIO GENERAL TÉCNICO DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA, Y SECRETARIO POR SUSTITUCIÓN DE LA COMISIÓN DE ORDENACIÓN ACADÉMICA, DELEGADA DEL CONSEJO DE GOBIERNO,

CERTIFICA: que, en la reunión de la Comisión de Ordenación Académica, delegada del Consejo de Gobierno, celebrada el 24 de junio de dos mil veintiséis, fue adoptado, entre otros, el siguiente acuerdo:

Asuntos del Vicerrectorado de Ordenación Académica

4.8 Elevar al Consejo de Gobierno, con informe favorable, la propuesta de modificación del Máster Universitario en Ciberseguridad (pendiente de fin de tramitación).

Y para que conste a los efectos oportunos, se extiende la presente certificación en Madrid, a 25 de junio de 2026.

Departamento de Sistemas de Comunicación y Control

INFORME SOLICITUD MODIFICA PARA EL MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

La coordinación del Máster Universitario en Ciberseguridad ha propuesto a sus profesores la presentación de un MODIFICA a ANECA para atender a los diversos eventos que han ido aconteciendo durante este tiempo, los cuales son resumidos a continuación:

1.- Dejar constancia de que se atendieron las consideraciones hechas desde los paneles de ANECA, durante el proceso Monitor en el curso 20/21 y la renovación de la acreditación durante el curso 24/25.

2.- Jubilación y cambios de profesores en algunas asignaturas.

Para ello, se planteó un texto para este MODIFICA, que fue aprobado en sesión extraordinaria en la Comisión de Coordinación del Máster celebrada el pasado 19/05/2026 y cuyos puntos fueron los siguientes:

a) Puesta en extinción de la asignatura: "Marco Jurídico de la Defensa Nacional en el Ciberespacio".

b) Modificación en las fichas de las asignaturas: "Criptografía Aplicada" y "Seguridad en Infraestructuras Críticas".

c) Propuesta de dos nuevas asignaturas optativas: "Lenguajes y Aplicaciones en Ciberseguridad" y "Seguridad de Servicios y Protocolos de Red".

d) Modificación del perfil de ingreso. Solo acceden como titulados afines los Ingenieros Técnicos en Informática.

El secretario del máster.

Calle Juan del Rosal, 16
28040, Madrid.
Tel: 91 398 8752
info@scc.uned.es

MODIFICACIÓN: Añadir en “Requisitos de Acceso”, pág. 6/43:

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, Ingeniero, Máster y/o Graduado en Informática.

También se admitirán los titulados en Ingeniería Técnica Informática o Diplomado en Ingeniería Informática a los cuales se les asignará dos asignaturas del Grado en Ingeniería Informática como complementos formativos.

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.

~~La Comisión de Coordinación del Máster (CCM) podría considerar también la admisión a titulados universitarios 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.

MODIFICACIÓN: Sustituir en “Plan de estudios”, pág. 52/92:

Plan de estudios

El objetivo principal del Máster es llevar a cabo la formación de estudiantes en el ámbito de la Ciberseguridad, tanto para fines de investigación como fines formativos para ejercer de forma profesional. El programa propuesto intentará cubrir los principales aspectos de la Ciberseguridad, haciendo hincapié en aspectos técnicos y de legislación, y desde diferentes puntos de vista dentro del área.

Para lograr este fin, se aplicará la metodología de educación a distancia propia de la UNED, con la inclusión de una gran variedad recursos multimedia educativos, tanto para los contenidos como las prácticas de evaluación. Se utilizarán los medios de los que dispone la institución para tal fin.

El objetivo principal del plan de estudios puede desglosarse en diferentes objetivos específicos:

- Utilizar mecanismos criptográficos avanzados para garantizar los requisitos de seguridad en un sistema, así como el acceso y seguridad en las comunicaciones.
- Diseñar mecanismos de prevención de amenazas a la seguridad, así como de reconocer y resolver incidentes de seguridad en los sistemas críticos.
- Utilizar herramientas para monitorizar el tráfico de red y generar, explorar y manipular el tráfico en los sistemas de comunicación.
- Analizar e identificar vulnerabilidades ante posibles ataques en los sistemas de comunicaciones y los servicios asociados.
- Analizar e identificar técnicas de ocultación de ataques a sistemas de comunicaciones y aplicaciones.
- Conocer las tendencias actuales en técnicas de ciberataque, los mecanismos de defensa mediante aprendizaje automático y especialmente dirigido a casos reales.
- Analizar sistemas para encontrar evidencias de ataques en los mismos y adoptar las medidas precisas para mantener la cadena de custodia de dichas evidencias.
- Conocer las técnicas y herramientas para la realización de un análisis forense con la preservación de pruebas digitales.
- Comprender la importancia del Derecho como sistema regulador de las relaciones sociales.
- Conseguir la percepción del carácter unitario del ordenamiento jurídico y de la necesaria visión interdisciplinaria de los problemas jurídicos.

Estructura general del plan de estudios

Para alcanzar estos objetivos se propone el siguiente plan de estudios distribuido en dos cuatrimestres y con un diseño equilibrado de créditos por semestres. Para alcanzar los objetivos anteriores se propone una estructura de Máster Universitario con 60 créditos impartidos en un solo curso académico. En la Tabla 1 se presenta la distribución de créditos según el carácter de las asignaturas que lo componen.

1

Tipo de materia/asignatura	Créditos
Obligatorias	36
Optativas	12
Trabajo Fin de Máster	12
TOTAL	60

Tabla 1: Distribución de créditos por tipo de asignatura

En la Tabla 2 se muestra para cada asignatura se indica el número de créditos y si es obligatoria u optativa. Se debe destacar que se pretende con la oferta de optatividad en cada materia (excepto el Trabajo Fin de Máster) que el estudiante pueda focalizar su interés profesional en temas específicos de Ciberseguridad, tales y como aspectos legales, profundización en la automatización de tareas, etc.

Materia/asignatura	Créditos ECTS	Tipo	Semestre
Criptografía Aplicada	6	Obligatoria	1
Auditoría y Monitorización de la Seguridad	6	Obligatoria	1
Análisis Forense	6	Obligatoria	1
Hacking Ético	6	Obligatoria	1
Ciberilícitos	6	Obligatoria	1
Seguridad en Infraestructuras Críticas	6	Obligatoria	2
Análisis de Malware	6	Optativa	2
Gestión de Incidentes de Ciberseguridad	6	Optativa	2
Introducción al Aprendizaje Automático para Ciberseguridad	6	Optativa	2
~~Marco jurídico de la Defensa Nacional en el Ciberespacio~~	~~6~~	~~Optativa~~	~~2~~
Trabajo Fin de Máster (TFM)	12	Obligatoria	2
Lenguajes y Aplicaciones en Ciberseguridad	6	Optativa	2

Seguridad de Servicios y Protocolos de Red	6	Optativa	2

Tabla 2: Asignaturas, créditos, su carácter obligatorio/optativo y semestre de impartición

Planificación semestral

En esta titulación todas las asignaturas tienen un carácter semestral. El plan de estudios del título está organizado en dos semestres. La planificación intenta garantizar una distribución uniforme de créditos por semestre, de forma que el estudiante deberá cursar 30 créditos en el primer semestre y otros 30 créditos en el segundo. Cada crédito supondrá un volumen total de trabajo del estudiante de 25 horas. La Tabla 3 recoge los semestres en los que se planifican las asignaturas del plan de estudios, de carácter anual.

Primer semestre	Segundo semestre
Criptografía Aplicada	Seguridad en Infraestructuras Críticas
Auditoría y Monitorización de la Seguridad	Optativa 1
Análisis Forense	Optativa 2
Hacking Ético	Trabajo Fin de Máster
Ciberilícitos	

Tabla 3: Planificación temporal del curso académico

En el segundo semestre el/la estudiante deberá elegir dos optativas ofertadas de las cinco posibles, además del Trabajo Fin de Máster y otra asignatura obligatoria.

MODIFICACIÓN: Añadir en “Complementos formativos”, pág. 11/43:

Los estudiantes provenientes ~~de otras titulaciones~~ de la titulación Ingeniería Técnica en Informática o Diplomado en Ingeniería Informática, que son diferentes del 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 ~~como pueden ser los Ingenieros Técnicos en Informática~~, tienen que cursar dos asignaturas 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 a cursar son las siguientes:

· Consultoría y Auditoría.
· Ética y Legislación.

MODIFICACIÓN: Sustituir en “Planificación de las enseñanzas”, pág. 13/92 – 32/92 en las asignaturas que proceda:

Fichas de las asignaturas a modificar

-Criptografía Aplicada.

NOMBRE DE LA ASIGNATURA	Criptografía Aplicada			
ECTS	6			
CARÁCTER	Obligatoria			
SEMESTRE	Semestre 1			
IDIOMA	CASTELLANO			
RESULTADOS DEL APRENDIZAJE	· 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.			
CONTENIDOS	· Principios matemáticos de la criptografía · Criptología para la ciberseguridad · Criptoanálisis · Criptología y computación cuántica · Aplicaciones de la criptografía			
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. Se fomentará el uso de software libre siempre y cuando sea posible para la realización de las actividades y las practicas propuestas.			
COMPETENCIAS	Ver sección de Resultados de Aprendizaje			
METODOLOGÍA DOCENTE	ESTO NO APARECE EN NUESTRA MEMORIA DE VERIFICACIÓN. POR TANTO, NO HABRÁ QUE RELLENARLO.			
	NOMBRE	N.º HORAS	% P	% IEP

ACTIVIDADES FORMATIVAS **N.º HORAS** **% P= % PRESENCIALIDAD** **% IEP= % INTERACCIÓN ESTUDIANTADO/PROFESORADO**	**AF1** Aprendizaje autónomo de los contenidos teóricos	60	0	0
	AF2 Aprendizaje autónomo mediante la realización de problemas	40	0	0
	AF3 Aprendizaje con apoyo docente síncrono			
	AF3.1 Participación y utilización de herramientas síncronas del entorno virtual de aprendizaje	0	0	100
	AF3.2 Asistencia a tutorías presenciales	0	100	0
	AF3.3 Asistencia a seminarios presenciales	0	100	0
	AF4 Aprendizaje con apoyo docente asíncrono	48	0	0
	AF5 Evaluación formativa			
	AF5.1 Prueba formativa síncrona		0	100
	AF5.2 Prueba formativa asíncrona	0	0	0
	AF5.3 Prueba formativa presencial	2	100	0
	AF6 Prácticas de laboratorio			
	AF6.1 Prácticas de laboratorio presenciales	0	100	0
	AF6.2 Prácticas de laboratorio no presenciales síncronas	0	0	100
	AF6.3 Prácticas de laboratorio no presenciales asíncronas	0	0	0
	AF7 Elaboración del TFG		1	8
SISTEMAS DE EVALUACIÓN **PONDERACIÓN [MÍN, MÁX]**	**NOMBRE**		**MIN**	**MÁX**
	SE1 Evaluación por prueba presencial		70	80
	SE2 Evaluación por prácticas de laboratorio		0	0
	SE3 Evaluación por pruebas de evaluación continua		0	0
	SE4 Evaluación por trabajos, seminarios e informe de tutores		20	30
	SE5 Presentación y defensa en acto público ante tribunal del TFG			

-Seguridad en Infraestructuras Críticas.

NOMBRE DE LA ASIGNATURA	**Criptografía Aplicada**
ECTS	6
CARÁCTER	Obligatoria
SEMESTRE	Semestre 2
IDIOMA	CASTELLANO
RESULTADOS DEL APRENDIZAJE	- 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.

CONTENIDOS	- Introducción al contexto de seguridad en redes industriales - Diseño, arquitectura y principales protocolos de redes industriales - Principales problemas de seguridad en sistemas de control industrial - ¿Cómo hacer evaluaciones de vulnerabilidades y riesgos? - Herramientas y procedimientos de defensa en ICS - Monitorización de la seguridad de los ICS - Estándares y regulaciones
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. Se fomentará el uso de software libre siempre y cuando sea posible para la realización de las actividades y las practicas propuestas.
COMPETENCIAS	Ver sección de Resultados de Aprendizaje
METODOLOGÍA DOCENTE	ESTO NO APARECE EN NUESTRA MEMORIA DE VERIFICACIÓN. POR TANTO, NO HABRÁ QUE RELLENARLO.

ACTIVIDADES FORMATIVAS

N.º HORAS

% P= % PRESENCIALIDAD

% IEP= % INTERACCIÓN ESTUDIANTADO/PROFESORADO

		N.º HORAS	% P	% IEP
AF1	Aprendizaje autónomo de los contenidos teóricos	80	0	0
AF2	Aprendizaje autónomo mediante la realización de problemas	30	0	0
AF3	Aprendizaje con apoyo docente síncrono			
	AF3.1 Participación y utilización de herramientas síncronas del entorno virtual de aprendizaje	0	0	100
	AF3.2 Asistencia a tutorías presenciales	0	100	0
	AF3.3 Asistencia a seminarios presenciales	0	100	0
AF4	Aprendizaje con apoyo docente asíncrono	38	0	0
AF5	Evaluación formativa			
	AF5.1 Prueba formativa síncrona		0	100
	AF5.2 Prueba formativa asíncrona	0	0	0
	AF5.3 Prueba formativa presencial	2	100	0
AF6	Prácticas de laboratorio			
	AF6.1 Prácticas de laboratorio presenciales	0	100	0
	AF6.2 Prácticas de laboratorio no presenciales síncronas	0	0	100
	AF6.3 Prácticas de laboratorio no presenciales asíncronas	0	0	0
AF7	Elaboración del TFG		1	8

SISTEMAS DE EVALUACIÓN

PONDERACIÓN [MÍN, MÁX]

	NOMBRE	MIN	MÁX
SE1	Evaluación por prueba presencial	40	70
SE2	Evaluación por prácticas de laboratorio	0	0
SE3	Evaluación por pruebas de evaluación continua	20	50
SE4	Evaluación por trabajos, seminarios e informe de tutores	10	50
SE5	Presentación y defensa en acto público ante tribunal del TFG		

Fichas de las nuevas asignaturas optativas

Lenguajes y Aplicaciones en Ciberseguridad

NOMBRE DE LA ASIGNATURA	**Lenguajes y Aplicaciones en Ciberseguridad**
ECTS	6

CARÁCTER	Optativa
SEMESTRE	Semestre 2
IDIOMA	CASTELLANO
RESULTADOS DEL APRENDIZAJE	- Identificar los principales tipos de ataques a sistemas y aplicaciones - Describir el ciclo de vida del desarrollo seguro de software (SSDLC) y su importancia en la prevención de vulnerabilidades. - Utilización de lenguajes de programación en contextos y tareas de ciberseguridad - Identificar vulnerabilidades comunes en aplicaciones - Relacionar vulnerabilidades con malas prácticas de desarrollo de software - Aplicación práctica de técnicas y herramientas
CONTENIDOS	- Introducción a la ciberseguridad y al desarrollo seguro - Vulnerabilidades de software más importantes - Lenguajes de programación en ciberseguridad - Aplicaciones prácticas de lenguajes en ciberseguridad - -
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. Se fomentará el uso de software libre siempre y cuando sea posible para la realización de las actividades y las practicas propuestas.
COMPETENCIAS	Ver sección de Resultados de Aprendizaje
METODOLOGÍA DOCENTE	ESTO NO APARECE EN NUESTRA MEMORIA DE VERIFICACIÓN. POR TANTO, NO HABRÁ QUE RELLENARLO.

ACTIVIDADES FORMATIVAS

N.º HORAS

% P= % PRESENCIALIDAD

% IEP= % INTERACCIÓN ESTUDIANTADO/PROFESORADO

NOMBRE		N.º HORAS	% P	% IEP
AF1	Aprendizaje autónomo de los contenidos teóricos	60	0	0
AF2	Aprendizaje autónomo mediante la realización de problemas		0	0
AF3	Aprendizaje con apoyo docente síncrono			
	AF3.1 Participación y utilización de herramientas síncronas del entorno virtual de aprendizaje		0	100
	AF3.2 Asistencia a tutorías presenciales	10	100	0
	AF3.3 Asistencia a seminarios presenciales		100	0
AF4	Aprendizaje con apoyo docente asíncrono	18	0	0
AF5	Evaluación formativa			
	AF5.1 Prueba formativa síncrona		0	100
	AF5.2 Prueba formativa asíncrona	30	0	0
	AF5.3 Prueba formativa presencial	2	100	0
AF6	Prácticas de laboratorio			
	AF6.1 Prácticas de laboratorio presenciales		100	0
	AF6.2 Prácticas de laboratorio no presenciales síncronas		0	100
	AF6.3 Prácticas de laboratorio no presenciales asíncronas	30	0	0
AF7	Elaboración del TFG		1	8

SISTEMAS DE EVALUACIÓN

PONDERACIÓN [MÍN, MÁX]

NOMBRE		MIN	MÁX
SE1	Evaluación por prueba presencial	50	80
SE2	Evaluación por prácticas de laboratorio	20	50
SE3	Evaluación por pruebas de evaluación continua	10	20
SE4	Evaluación por trabajos, seminarios e informe de tutores		
SE5	Presentación y defensa en acto público ante tribunal del TFG		

Seguridad de Servicios y Protocolos de Red.

NOMBRE DE LA ASIGNATURA	**Seguridad de Servicios y Protocolos de Red**
ECTS	6
CARÁCTER	Optativa
SEMESTRE	Semestre 2
IDIOMA	CASTELLANO
RESULTADOS DEL APRENDIZAJE	• Comprender los fundamentos de la seguridad en redes • Articular los principios y prácticas de la monitorización • Conocer las vulnerabilidades de los protocolos más universales • Seleccionar, configurar y desplegar mecanismos de defensa • Diseñar arquitecturas resilientes y seguras
CONTENIDOS	• Fundamentos de seguridad en redes • Protocolos seguros y cifrado de las comunicaciones • Protocolos de acceso y autenticación • Seguridad en protocolos y servicios de red • Segmentación y aislamiento de tráfico • Seguridad de las aplicaciones web • Protocolos seguros para la transferencia de archivos • Seguridad en redes inalámbricas • Seguridad de infraestructuras y servidores
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 ya que la documentación más actualizada no está traducida al castellano. Se fomentará el uso de software libre siempre y cuando sea posible para la realización de las actividades y las practicas propuestas.
COMPETENCIAS	Ver sección de Resultados de Aprendizaje
METODOLOGÍA DOCENTE	Esta asignatura se impartirá conforme a la metodología no presencial que caracteriza a la UNED, en la cual prima el autoaprendizaje del estudiante, asistido por el profesorado mediante diversos sistemas de comunicación docente-discente mayoritariamente asíncronos y por las tutorías que pueden ser presenciales, impartidas en los Centros Asociados, o semipresenciales permitiendo la conexión del alumnado a las sesiones con independencia de su localización geográfica. Además, la docencia se imparte con apoyo de una plataforma virtual interactiva en la que se combinan distintos recursos, medios impresos, audiovisuales y virtuales. Más en concreto, la plataforma virtual contendrá: contenidos y material complementario, foros de discusión, glosario de términos, tareas y enlaces de interés.

ACTIVIDADES FORMATIVAS

N.º HORAS

% P= % PRESENCIALIDAD

% IEP= % INTERACCIÓN ESTUDIANTADO/PROFESORADO

NOMBRE	N.º HORAS	% P	% IEP
AF1 Aprendizaje autónomo de los contenidos teóricos	80	0	0
AF2 Aprendizaje autónomo mediante la realización de problemas		0	0
AF3 Aprendizaje con apoyo docente síncrono			
AF3.1 Participación y utilización de herramientas síncronas del entorno virtual de aprendizaje		0	100
AF3.2 Asistencia a tutorías presenciales	13	100	0
AF3.3 Asistencia a seminarios presenciales		100	0
AF4 Aprendizaje con apoyo docente asíncrono	10	0	0
AF5 Evaluación formativa			
AF5.1 Prueba formativa síncrona		0	100
AF5.2 Prueba formativa asíncrona	5	0	0
AF5.3 Prueba formativa presencial	2	100	0
AF6 Prácticas de laboratorio			
AF6.1 Prácticas de laboratorio presenciales		100	0
AF6.2 Prácticas de laboratorio no presenciales síncronas		0	100
AF6.3 Prácticas de laboratorio no presenciales asíncronas	40	0	0
AF7 Elaboración del TFG		1	8

NOMBRE	MIN	MÁX
SE1 Evaluación por prueba presencial	60	80

SISTEMAS DE EVALUACIÓN **PONDERACIÓN [MÍN, MÁX]**	**SE2**	Evaluación por prácticas de laboratorio	20	40
	SE3	Evaluación por pruebas de evaluación continua	10	20
	SE4	Evaluación por trabajos, seminarios e informe de tutores		
	SE5	Presentación y defensa en acto público ante tribunal del TFG		