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 Politécnica de Catalunya	Escuela Técnica Superior de Ingeniería de Telecomunicación	08032865

NIVEL	DENOMINACIÓN CORTA
Máster	Ciberseguridad / Master in Cybersecurity

DENOMINACIÓN ESPECÍFICA
Máster Universitario en Ciberseguridad / Master in Cybersecurity por la Universidad Politécnica de Catalunya

RAMA DE CONOCIMIENTO	CONJUNTO
Ingeniería y Arquitectura	No

HABILITA PARA EL EJERCICIO DE PROFESIONES REGULADAS	NORMA HABILITACIÓN
No	

SOLICITANTE	
NOMBRE Y APELLIDOS	CARGO
Santiago Gassó Domingo	Vicerrector de Política Académica
Tipo Documento	Número Documento
NIF	42994071X

REPRESENTANTE LEGAL	
NOMBRE Y APELLIDOS	CARGO
Francesc Torres Torres	Rector
Tipo Documento	Número Documento
NIF	41443276J

RESPONSABLE DEL TÍTULO	
NOMBRE Y APELLIDOS	CARGO
Josep Rafael Pegueroles Vallés	Director de l'Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona (ETSETB)
Tipo Documento	Número Documento
NIF	52600728G

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/ Jordi Girona, 31 - Edificio Rectorado	08034	Barcelona	934016832
E-MAIL	PROVINCIA		FAX
rector@upc.edu	Barcelona		934016201

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: Barcelona, AM 6 de mayo de 2019
	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 / Master in Cybersecurity por la Universidad Politécnica de Catalunya	No		Ver Apartado 1: Anexo 1.

LISTADO DE ESPECIALIDADES
No existen datos

RAMA	ISCED 1	ISCED 2
Ingeniería y Arquitectura	Ingeniería y profesiones afines	

NO HABILITA O ESTÁ VINCULADO CON PROFESIÓN REGULADA ALGUNA
AGENCIA EVALUADORA
Agència per a la Qualitat del Sistema Universitari de Catalunya
UNIVERSIDAD SOLICITANTE
Universidad Politécnica de Catalunya
LISTADO DE UNIVERSIDADES

CÓDIGO	UNIVERSIDAD
024	Universidad Politécnica de Catalunya

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
CRÉDITOS OPTATIVOS	**CRÉDITOS OBLIGATORIOS**	**CRÉDITOS TRABAJO FIN GRADO/ MÁSTER**
18	30	12

LISTADO DE ESPECIALIDADES	
ESPECIALIDAD	CRÉDITOS OPTATIVOS
No existen datos	

1.3. Universidad Politécnica de Catalunya

1.3.1. CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS	
CÓDIGO	CENTRO
08032865	Escuela Técnica Superior de Ingeniería de Telecomunicación

1.3.2. Escuela Técnica Superior de Ingeniería de Telecomunicación

1.3.2.1. Datos asociados al centro

TIPOS DE ENSEÑANZA QUE SE IMPARTEN EN EL CENTRO		
PRESENCIAL	SEMIPRESENCIAL	A DISTANCIA
Sí	No	No

PLAZAS DE NUEVO INGRESO OFERTADAS	
PRIMER AÑO IMPLANTACIÓN	SEGUNDO AÑO IMPLANTACIÓN

30	40	
	TIEMPO COMPLETO	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	36.0	60.0
RESTO DE AÑOS	36.0	60.0
	TIEMPO PARCIAL	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	18.0	30.0
RESTO DE AÑOS	18.0	30.0
NORMAS DE PERMANENCIA		
https://www.upc.edu/sga/es/normativas/NormativasAcademicas		
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
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 - Resolver problemas y mejorar procesos en cualquier ámbito social a partir de la aplicación de las TIC, integrando conocimientos de diversos ámbitos y aplicando ingeniería de alto nivel tecnológico.
CG2 - Identificar y aplicar nuevas técnicas procedentes del ámbito de la investigación a sistemas reales de ciberseguridad para adaptarlos a la continua evolución de las ciberamenazas.
CG3 - Proyectar, diseñar e implantar productos, procesos, servicios e instalaciones en ámbitos de la Ciberseguridad.
CG4 - Elaborar, planificar estratégicamente, dirigir, coordinar y gestionar técnica y económicamente proyectos en ámbitos de la Ciberseguridad, siguiendo criterios de calidad y medioambientales.
CG5 - Analizar y aplicar la legislación y normativa necesaria en el ámbito de la Seguridad de la Información.
3.2 COMPETENCIAS TRANSVERSALES
CT1 - Emprendimiento e innovación. Conocer y entender los mecanismos en que se basa la investigación científica, así como los mecanismos e instrumentos de transferencia de resultados entre los diferentes agentes socioeconómicos implicados en los procesos de I+D+i.
CT2 - Sostenibilidad y Compromiso Social. Conocer y comprender la complejidad de los fenómenos económicos y sociales típicos de la sociedad del bienestar; tener capacidad para relacionar el bienestar con la globalización y la sostenibilidad; lograr habilidades para utilizar de forma equilibrada y compatible la técnica, la tecnología, la economía y la sostenibilidad.
CT3 - Trabajo en equipo. Ser capaz de trabajar como miembro de un equipo interdisciplinar, ya sea como un miembro más o realizando tareas de dirección, con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos teniendo en cuenta los recursos disponibles.
CT4 - Uso solvente de los recursos de información. Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información en el ámbito de especialidad y valorar de forma crítica los resultados de dicha gestión.
CT5 - Tercera lengua. Conocer una tercera lengua, preferentemente el inglés, con un nivel adecuado oral y escrito y en consonancia con las necesidades que tendrán los titulados y tituladas.
3.3 COMPETENCIAS ESPECÍFICAS
CE1 - Diseñar aplicaciones de alto valor añadido basadas en las Tecnologías de la Información y las Comunicaciones (TIC), aplicadas al ámbito de la ciberseguridad.
CE2 - Identificar y seleccionar las herramientas más adecuadas para la detección y el análisis de ataques e incidentes de seguridad dependiendo de su naturaleza y el entorno donde se han producido.
CE3 - Identificar y analizar las leyes y regulaciones aplicables en materia de ciberseguridad y entender las implicaciones éticas que las técnicas de ciberdefensa pueden tener en la privacidad de los usuarios y como minimizarlas.
CE4 - Analizar desde un punto de vista matemático protocolos criptográficos de cifrado y gestión de claves según su robustez.
CE5 - Diseñar, implementar y operar protocolos de autenticación, autorización y auditoría de sistemas informacionales como bases de datos.
CE6 - Aplicar técnicas de monitorización y análisis del tráfico de red para la detección de ataques de ciberseguridad y la investigación de incidentes.

CE7 - Diseñar, desarrollar, detectar, analizar y eliminar código malicioso que sea capaz de infectar y ocultarse en un sistema operativo actual.
CE8 - Identificar y aplicar técnicas para mantener en todo momento la seguridad y privacidad de las aplicaciones distribuidas construidas sobre los protocolos de Internet.
CE9 - Elaborar un trabajo original a realizar individualmente y presentar y defender ante un tribunal universitario, consistente en un proyecto de ingeniería en el ámbito de la Ciberseguridad en el que se sinteticen las competencias adquiridas en las enseñanzas del Máster.

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

4.2.1- Acceso

De acuerdo con lo previsto en el artículo 16 del Real Decreto 1393/2007, de 29 de octubre, modificado por el Real Decreto 861/2010, de 2 de julio, y por el Real Decreto 43/2015, de 2 de febrero, respectivamente, así como lo establecido por la orden CIN/355/2009, de 9 de febrero, podrán acceder a estas enseñanzas oficiales de máster quienes reúnan los requisitos exigidos:

1- Estar en posesión de un título universitario oficial español que cumpla:

- Haber adquirido previamente las competencias de un grado que habilite para el ejercicio de la profesión de Ingeniero Técnico de Telecomunicación o Ingeniero Informático.
- Igualmente, podrán acceder a este Máster quienes estén en posesión de cualquier título de grado sin perjuicio de que en este caso se establezcan los complementos de formación previos que se estimen necesarios.

2- 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 del área de la Ingeniería de Telecomunicación o Informática.

3- Estar en posesión de un título oficial de sistemas educativos externos al Espacio Europeo de Educación Superior sin que sea necesaria su homologación. En este caso, la Comisión Académica del Máster comprobará que se acredita un nivel de formación equivalente a los títulos universitarios oficiales españoles correspondientes y que el título faculta en el país expedidor para el acceso a estudios de posgrado. Para este efecto, la Comisión Académica del Máster podrá solicitar la documentación que considere necesaria para llevar a término esta comprobación, incluso la homologación del título si no puede determinar con seguridad que el título extranjero acredita los requisitos de acceso establecidos por la legislación vigente para acceder a este máster.

El acceso por esta vía no implica, en ningún caso, la homologación del título previo que esté en posesión de la persona interesada, ni su reconocimiento a otros efectos que no sean el de cursar las enseñanzas del máster.

Si la legislación española de referencia se modifica en sentido diferente esta normativa se revisará acorde con los cambios.

Los apartados anteriores se entenderán, sin perjuicio de lo dispuesto en el artículo 17.2 y en la disposición adicional cuarta del Real Decreto 1393/2007, de 29 de octubre.

4.2.2- Admisión

El artículo 17 del Real Decreto 1393/2007, modificado por el Real Decreto 861/2010, de 2 de julio, y por el Real Decreto 43/2015, de 2 de febrero, respectivamente, regula la admisión a las enseñanzas de máster y establece que los estudiantes podrán ser admitidos conforme a los requisitos específicos y criterios de valoración que establezca la universidad.

De acuerdo con la normativa académica de másteres universitarios aprobada por el Consejo de Gobierno de la Universidad Politécnica de Cataluña, los estudiantes pueden acceder a cualquier máster universitario de la UPC, relacionado o no con su currículum universitario, previa admisión por parte de la comisión del centro responsable del máster, de conformidad con los requisitos de admisión específicos y los criterios de valoración de méritos establecidos.

Los requisitos específicos de admisión al máster son competencia de la comisión del centro responsable del máster y tienen el objetivo de asegurar la igualdad de oportunidades de acceso a la enseñanza para estudiantes calificados suficientemente. En todos los casos, los elementos que se consideren incluirán la ponderación de los expedientes académicos de los candidatos.

El proceso de selección se podrá completar con una prueba de ingreso y con la valoración de aspectos del currículum, como los méritos que tengan una relevancia o significación especiales en relación con el programa solicitado.

La comisión del centro responsable del máster hará públicos los requisitos específicos de admisión y los criterios de valoración de méritos y de selección de candidatos especificados antes del inicio del periodo general de preinscripción de los másteres universitarios a través de los medios que considere adecuados. En cualquier caso, estos medios tendrán que incluir siempre la publicación de esta información en el sitio web institucional de la UPC.

Asimismo, dicha comisión responsable resolverá las solicitudes de acceso de acuerdo con los criterios mencionados y publicará el listado de estudiantes admitidos.

4.2.3- Comisión del centro responsable del máster

La comisión del centro responsable del máster es la **Comisión Académica de Másteres**, que estará integrada por los directores de los centros o en quien deleguen, el coordinador del máster y un número de vocales de los departamentos universitarios que imparten docencia en el máster a determinar por la Comisión Académica de los centros.

Esta comisión es la encargada de todos los procedimientos de acceso, admisión, y reconocimiento de créditos y elección de los complementos formativos que requieren los estudiantes para su acceso al máster.

4.2.4- Requisitos específicos de admisión

Dado que el máster se imparte íntegramente en inglés, se requiere acreditar un nivel B2 de inglés o equivalente.

Respecto a la titulación de acceso, el máster propuesto está abierto a estudiantes con los perfiles de ingreso recomendados anteriormente definidos en el apartado 4.1 de esta memoria, y no se establecen otros requisitos tecnológicos específicos ni pruebas de acceso para estos estudiantes. No obstante, en caso necesario se propondrán complementos de formación para homogenizar el nivel de los candidatos en función de su perfil de ingreso.

4.2.5- Criterios de valoración de méritos y selección

De acuerdo con la normativa de la UPC para másteres universitarios, el proceso de admisión en el máster es responsabilidad de la comisión del centro responsable del máster (Comisión Académica de Másteres), que establecerá los criterios de selección, siempre respetando los principios de mérito e igualdad de oportunidades.

En caso de haber más candidaturas que plazas, las candidaturas se ordenarán según una valoración que tendrá en cuenta los siguientes criterios:

1. Correspondencia de las competencias de la titulación de acceso del estudiante con las competencias del presente máster

Las competencias del máster se enmarcan en las áreas básicas de la ingeniería de telecomunicación e informática.

Aquellos candidatos cuyos perfiles de acceso cubran todas las áreas de manera adecuada serán mejor valorados.

2. Expediente

De conformidad con el punto 4.5 del anexo I del 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, y el artículo 5.3 del Real Decreto 1125/2003, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y validez en todo el territorio nacional, la ponderación del expediente de las tituladas y titulados se calculará de acuerdo con el siguiente criterio:

- Suma de los créditos superados por el estudiante o la estudiante, multiplicados cada uno por el valor de la calificación que corresponda y dividido por el número de créditos superados. A efectos de la ponderación del expediente, no se contabilizan los créditos reconocidos sin calificación.

Escala ECTS	A	B	C	D	E
Escala cualitativa internacional	Excellent	Very good	Good	Satisfactory	Sufficient
España cualitativa	Matrícula de honor	Sobresaliente	Notable	Bien	Suficiente
España numérica		9,0-10	7,0-8,9	6,0-6,9	5,0-5,9
PUNTUACIÓN	4	3	2	1	1

3. CV: Currículum Vitae

Valoración de la experiencia laboral y de otros estudios adicionales que pueda tener el estudiante, en particular los conocimientos de idiomas.

Los criterios de admisión se ponderarán de la siguiente forma:

1. Correspondencia de las competencias de la titulación de acceso del estudiante con las competencias del presente máster: 25%
2. Expediente: 60%
3. CV Currículum Vitae: 15%

Ordenados los estudiantes que solicitan la admisión con arreglo a los criterios de valoración antedichos, serán admitidos tantos solicitantes como plazas se oferten, por estricto orden de prelación. En caso de que se produzcan renuncias, podrán optar a la admisión los solicitantes no seleccionados en primera instancia, otra vez de acuerdo a su orden de méritos.

De forma excepcional, la Comisión Académica del Máster podrá admitir a un número mayor de solicitantes de los previstos en el período considerado, por la especial calidad de los currículos de los solicitantes o por razones estratégicas para la Universidad, siempre en función de la disponibilidad de las capacidades necesarias para ofrecer una docencia de calidad.

4.2.6- Perfil de estudiantes que requieren complementos de formación

Todos aquellos estudiantes que accedan al máster con las siguientes titulaciones NO DEBERÁN cursar complementos de formación fuera de los 60 ECTS del máster:

- Estudiantes con el grado en Ciencias y Tecnologías de Telecomunicación.

- Estudiantes con un grado que habilite para el ejercicio de la profesión de Ingeniero Técnico de Telecomunicación:
  - Estudiantes con un grado en Ingeniería de Sistemas Audiovisuales.
  - Estudiantes con un grado en Ingeniería de Sistemas Electrónicos.
  - Estudiantes con un grado en Ingeniería de Sistemas de Telecomunicación.
  - Estudiantes con un grado en Ingeniería Telemática.
  - Estudiantes con el grado en Ingeniería Electrónica de Telecomunicación
- Estudiantes con el grado en Ingeniería Informática.
- Ingenieros de Telecomunicación.
- Ingenieros Informáticos.

Si se produce la petición de entrada de estudiantes con otras titulaciones, la Comisión Académica del Máster estudiará cada situación. En caso de permitir el acceso, es posible que el estudiante deba cursar complementos de formación fuera de los 60 ECTS del máster.

4.3 APOYO A ESTUDIANTES

4.3.1- Sistemas accesibles de apoyo y orientación de los estudiantes una vez matriculados

La titulación dispone de un plan de Acción Tutorial que se plantea en la titulación como un servicio de atención al estudiantado, mediante el cual el profesorado orienta, informa y asesora de forma personalizada.

La orientación que propicia la tutoría constituye un soporte al alumnado con un doble objetivo:

- Realizar un seguimiento en cuanto a la progresión académica.
- Asesorar respecto a la trayectoria curricular y los recursos académicos (métodos de estudio, recursos disponibles).

Los mecanismos de apoyo y orientación a los estudiantes ya matriculados son los siguientes:

A) Actuaciones institucionales en el marco del Plan de Acción Tutorial:

1. Elaborar un calendario de actuación en cuanto a la coordinación de tutorías.
2. Seleccionar a las tutoras y tutores.
3. Informar al alumnado al inicio del máster sobre la tutora o tutor correspondiente.
4. Convocar la primera reunión grupal de inicio del máster.
5. Evaluar el Plan de acción tutorial de la titulación.

B) Por su parte, las actuaciones del tutor son las siguientes:

1. Asesorar al alumnado en el diseño de la planificación de su itinerario académico personal.
2. Facilitar información sobre la estructura y funcionamiento de la titulación, así como la normativa académica que afecta a sus estudios, sobre la inserción laboral, las prácticas externas y las estancias en el extranjero.
3. Valorar las acciones realizadas en cuanto a satisfacción y resultados académicos de los tutorados.

Por otro lado, de acuerdo con la normativa de la Universidad, es responsabilidad de la Comisión Académica de Másteres el establecimiento del itinerario curricular y de los planes de matrícula personalizados en función del resultado del reconocimiento de créditos y en coordinación con los tutores.

También es responsabilidad de la Comisión Académica de Másteres el seguimiento e información de la entrada y los resultados académicos de los estudiantes; esta información resulta fundamental para la efectividad de la acción Tutorial.

Plan de Acción Tutorial

El Plan de Acción Tutorial actúa a diferentes niveles: (i) en la fase de información sobre el máster, (ii) en la fase de preinscripción, (iii) en la fase de matrícula, (iv) en la fase de inicio de curso y finalmente (v) en la fase de seguimiento.

En la fase de información sobre el programa, se dispone de una dirección de correo electrónico donde una persona de administración responde todas las dudas de los estudiantes. En caso de que la duda sea académica se deriva al subdirector o vicedecano responsable de los másteres de los centros la ETSETB/FIB.

En la fase de preinscripción, se asigna otra persona de administración experta en procedimientos administrativos porque las dudas principales son sobre documentación y cartas de aceptación para la solicitar visados y becas. En este punto se atienden mayoritariamente estudiantes extranjeros.

En la fase de matrícula, la comisión académica ya ha asignado un tutor académico. El tutor académico guiará al estudiante en dicha fase de matrícula.

En la fase de inicio de curso, y especialmente para aquellos estudiantes extranjeros, el tutor dará soporte sobre los servicios que ofrece la universidad para cuestiones como alojamiento, servicios de biblioteca, intranets, contacto con otros profesores, etc.

Finalmente, la fase de seguimiento consiste en monitorizar la progresión académica del estudiante, aconsejarle de las dificultades que puede encontrar en ciertas asignaturas y dar apoyo en cualquier tipo de problema que pueda tener.

Esta ayuda general de la universidad se complementará con las acciones específicas que se organicen desde el máster, en particular como ya se ha indicado con la asignación inicial de un tutor para cada estudiante desde antes de la matriculación y el mantenimiento del mismo durante el curso. También con la organización de una sesión de orientación para los nuevos estudiantes del máster, que tratará, no sólo de detalles organizativos y de funcionamiento del máster, sino también de otros temas prácticos de la vida universitaria.

Otros servicios de apoyo:

Por otro lado, destacar que la UPC tiene activo un Programa de Atención a las Discapacidades (PAD) que se presenta en la Sección 7 de esta memoria y un Plan Director de Igualdad de Oportunidades que contempla como uno de sus objetivos el elaborar los procedimientos y los modelos de adaptaciones curriculares, con la finalidad de objetivar las formas de organizar las actividades, de disponer los instrumentos, de seleccionar los contenidos y de implementar las metodologías más apropiadas para atender las diferencias individuales del estudiantado con necesidades especiales. En este sentido, los centros refuerzan su programa de tutoría y suavizan la normativa de permanencia dentro del plan de estudios para estudiantes con necesidades especiales.

Asimismo, la Universidad Politécnica de Cataluña proporciona a sus estudiantes una serie de servicios de apoyo como Campus Virtual, acceso Wi-Fi, distribución de software, servicios de actividades sociales, etc. Dicha información puede encontrarse en el siguiente enlace:

https://www.upc.edu/en/university-services

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

Reconocimiento de créditos

En aplicación del artículo 6 del Real Decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales, modificado por el Real Decreto 861/2010 y por el Real Decreto 43/2015 respectivamente, el Consejo de Gobierno de esta universidad ha aprobado la Normativa Académica de los estudios de Másteres Universitarios de la UPC. Esta normativa, de aplicación a los estudiantes que cursen enseñanzas oficiales conducentes a la obtención de un título de máster, es pública y requiere la aprobación de los Órganos de Gobierno de la universidad en caso de modificaciones.

En dicha normativa se regulan, de acuerdo a lo establecido en el artículo 6 antes mencionado, los criterios y mecanismos de reconocimiento de créditos obtenidos en unas enseñanzas oficiales, en la misma u otra universidad, que son computados a efectos de la obtención de un título oficial, así como el sistema de transferencia de créditos.

El trabajo de fin de máster, tal y como establece el Real Decreto 861/2010, no será reconocido en ningún caso, en consecuencia, el estudiante ha de matricular y superar estos créditos definidos en el plan de estudios.

También se definen unos criterios de aplicación general, los cuales se detallan a continuación:

- Los reconocimientos se harán siempre a partir de las asignaturas cursadas en los estudios de origen, nunca a partir de asignaturas convalidadas, adaptadas o reconocidas previamente.
- Cuando los estudios de procedencia son oficiales, los reconocimientos conservarán la calificación obtenida en los estudios de origen y computarán a efectos de baremación del expediente académico.
- No se podrán realizar reconocimientos en un programa de máster universitario de créditos cursados en unos estudios de grado o de primer ciclo, si éste pertenece a la anterior ordenación de estudios, ni de créditos obtenidos como asignaturas de libre elección cursadas en el marco de unos estudios de primer, segundo y primer y segundo ciclo.
- Con independencia del número de créditos que sean objeto de reconocimiento, para tener derecho a la expedición de un título de máster de la UPC se han de haber matriculado y superado un mínimo de créditos ECTS, en los que no se incluyen créditos reconocidos o convalidados de otras titulaciones de origen oficiales o propias, ni el reconocimiento por experiencia laboral o profesional acreditada. El mínimo de créditos a superar en el caso de másteres de 60 ECTS es del 70% de los créditos de la titulación, por lo que en este máster, el número máximo de créditos a reconocer es de 18 ECTS. Este mínimo de créditos no se ha de exigir cuanto los estudios de origen sean de la UPC y el expediente de origen esté cerrado por traslado.
- El reconocimiento de créditos tendrá los efectos económicos que fije anualmente el decreto por el que se establecen los precios para la prestación de servicios académicos en las universidades públicas catalanas, de aplicación en las enseñanzas conducentes a la obtención de un título oficial con validez en todo el territorio nacional.

En referencia al procedimiento para el reconocimiento de créditos, el estudiante deberá presentar su solicitud en el período establecido a tal efecto junto con la documentación acreditativa establecida en cada caso y de acuerdo al procedimiento establecido al respecto.

La Comisión Académica del Máster, por delegación del rector o rectora, resolverá las solicitudes de reconocimiento de los estudiantes. Asimismo, esta comisión definirá y hará públicos los mecanismos, calendario y procedimiento para que los reconocimientos se hagan efectivos en el expediente correspondiente (siempre de acuerdo a la normativa académica vigente aprobada por la UPC, de aplicación a los másteres universitarios).

Transferencia de créditos

La transferencia de créditos (créditos que no computan a efectos de obtención del título) implica que, en los documentos académicos oficiales acreditativos de las enseñanzas seguidas por cada estudiante, se incluirán la totalidad de los créditos obtenidos en enseñanzas oficiales cursadas con anterioridad, en la misma u otra universidad, que no hayan conducido a la obtención de un título oficial.

Todos los créditos obtenidos por el estudiante en enseñanzas oficiales cursadas en cualquier universidad, los reconocidos y los superados para la obtención del correspondiente título, así como los transferidos, serán incluidos en su expediente académico tal y como establezca la legislación y normativa vigente de aplicación al respecto.

La transferencia de créditos se realizará a petición del estudiante mediante solicitud dirigida a la unidad responsable de la gestión del máster, acompañado de toda la documentación oficial (certificación académica oficial, etc.) que acredite los créditos superados.

La resolución de la transferencia de créditos no requerirá la autorización expresa de la Comisión del centro responsable del máster (Comisión Académica). Una vez la unidad responsable de la gestión compruebe que la documentación aportada por el estudiante es correcta, se procederá a la inclusión en el expediente académico de los créditos transferidos.

En el caso de créditos obtenidos en titulaciones propias, no procederá la transferencia de créditos.

4.6 COMPLEMENTOS FORMATIVOS

Este máster no contempla complementos formativos para las titulaciones de ingreso recomendadas en el punto 4.1.2. - *Perfil recomendado de ingreso,* de la sección 4.1 de la memoria (Sistemas de información previo).

Como se ha comentado en la Sección 4.2 - *Requisitos de acceso y criterios de admisión*, se considera posible pero excepcional la entrada de estudiantes con otras titulaciones.

En estas situaciones excepcionales, la Comisión Académica del Máster podrá estudiar el caso y permitir su acceso con posibles complementos de formación fuera de los 60 ECTS del máster. En este caso, los complementos formativos que un estudiante haya de cursar serán de los Grados de los centros solicitantes y como máximo equivaldrán a 10 ECTS.

El número de créditos y las asignaturas a cursar variarán dependiendo de la titulación de ingreso, ya sea de grado o de la anterior ordenación de estudios, y de las competencias académicas previas del estudiante reflejadas en su expediente académico particular.

Estos complementos de formación, si bien consistirán en la superación de asignaturas de grado, tendrán, a efectos de precio público, la consideración de créditos de máster.

5. PLANIFICACIÓN DE LAS ENSEÑANZAS

5.1 DESCRIPCIÓN DEL PLAN DE ESTUDIOS
Ver Apartado 5: Anexo 1.
5.2 ACTIVIDADES FORMATIVAS
Exposición de contenidos teóricos mediante clases magistrales (presencial).
Exposición de contenidos con participación del estudiante (presencial).
Resolución de problemas, con participación del estudiante (presencial).
Sesiones prácticas de laboratorio individuales o en equipo (presencial).
Discusión en el aula de problemas o artículos, realizada por los alumnos y moderada por el profesor/a (presencial).
Elaboración de trabajos cooperativos (presencial).
Visitas a empresas por parte de los estudiantes, con la finalidad de adquirir conocimientos prácticos relacionados con la temática de la materia (presencial).
Asistencia a seminarios y conferencias relacionados con la temática de la materia (presencial).
Tutoría (presencial).
Preparación, ensayo y realización de actividades evaluables relacionadas con el TFM (presencial).
Estudio y preparación de los contenidos (no presencial).
Realización de ejercicios y trabajos teóricos o prácticos fuera del aula, individualmente o en grupo (no presencial).
Realización de proyectos propuestos por los profesores fuera del aula, individualmente o en grupo (no presencial).
Preparación y realización de actividades evaluables (no presencial).
5.3 METODOLOGÍAS DOCENTES
Clase magistral
Clase expositiva participativa
Práctica de laboratorio
Aprendizaje basado en problemas / proyectos
Trabajo autónomo
Trabajo cooperativo
Tutoría
5.4 SISTEMAS DE EVALUACIÓN
Examen parcial y/o final (prueba escrita de control de conocimientos)
Ejercicios puntuales a realizar en clase o en casa
Trabajos individuales, presentados por escrito u oralmente
Trabajos en grupo, presentados por escrito u oralmente
Prácticas de laboratorio
Presentación y defensa oral del TFM
5.5 NIVEL 1: Formación obligatoria
5.5.1 Datos Básicos del Nivel 1
NIVEL 2: Seguridad en Datos
5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	10
DESPLIEGUE TEMPORAL: Cuatrimestral	

ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
10		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**

ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NIVEL 3: Protección de Datos / Data Protection		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	5	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
5		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NIVEL 3: Autenticación y Autorización de Red / Network Authentication & Authorization		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	5	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
5		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No

GALLEGO	VALENCIANO	INGLÉS
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Comprender las técnicas criptográficas necesarias para proteger los datos durante el almacenamiento y la transmisión, a fin de garantizar su confidencialidad, integridad y autenticación.
- Conocer y comprender las amenazas y los riesgos de seguridad en bases de datos, con especial atención a la privacidad y propiedad intelectual.
- Conocer las técnicas para auditar vulnerabilidades / ataques en los protocolos de autenticación y acceso a sistemas de información.

5.5.1.3 CONTENIDOS

- Cifrado de clave simétrica. Cifradores en flujo y en bloque. Modos de operación. *Message authentication codes*. Funciones de Hash. Cifrado autenticado.
- Gestión e intercambio de claves. Criptografía de clave pública. Ataques de Hombre en el medio (*Man-in-the-middle attacks*). Firmas digitales. Esquemas de identificación. Certificados de clave pública. Criptografía basada en identidad.
- Definición de tareas computacionalmente fáciles y difíciles. Nociones de seguridad para el cifrado. Nociones de seguridad para las firmas. El modelo del oráculo. Reducciones y pruebas de seguridad.
- Pruebas de conocimiento cero y argumentos. Conocimiento cero no interactivo. Aplicaciones.
- Criptografía para muchos usuarios. Compartición de secretos. Descifrado umbral. Firmas umbral. Computación segura multiparte.
- Autenticación de uno o múltiples factores: algo que se (passwords), algo que tengo (tokens, keys), algo que soy (biometrics).
- Autenticación con claves secretas, claves públicas, la necesidad de hápax (parámetro de un solo uso o *nonce*), *password hashing*, *salted hashes*, control de acceso adecuado, y transmisión segura de credenciales.
- Protocolos de autenticación para acceso a la red o recursos: PAP, CHAP, EAP con sus métodos.
- *Authentication, Authorization and Accounting* (AAA): RADIUS, DIAMETER, *federated cross-layer authentication*, EDUROAM
- *Single Sign-On*, autenticación delegada (OAuth)

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Resolver problemas y mejorar procesos en cualquier ámbito social a partir de la aplicación de las TIC, integrando conocimientos de diversos ámbitos y aplicando ingeniería de alto nivel tecnológico.

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

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

CT4 - Uso solvente de los recursos de información. Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información en el ámbito de especialidad y valorar de forma crítica los resultados de dicha gestión.

5.5.1.5.3 ESPECÍFICAS

CE1 - Diseñar aplicaciones de alto valor añadido basadas en las Tecnologías de la Información y las Comunicaciones (TIC), aplicadas al ámbito de la ciberseguridad.

CE4 - Analizar desde un punto de vista matemático protocolos criptográficos de cifrado y gestión de claves según su robustez.

CE5 - Diseñar, implementar y operar protocolos de autenticación, autorización y auditoría de sistemas informacionales como bases de datos.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Exposición de contenidos teóricos mediante clases magistrales (presencial).	26	100
Exposición de contenidos con participación del estudiante (presencial).	13	100
Resolución de problemas, con participación del estudiante (presencial).	13	100
Sesiones prácticas de laboratorio individuales o en equipo (presencial).	26	100

Discusión en el aula de problemas o artículos, realizada por los alumnos y moderada por el profesor/a (presencial).	6	100
Estudio y preparación de los contenidos (no presencial).	65	0
Realización de proyectos propuestos por los profesores fuera del aula, individualmente o en grupo (no presencial).	76	0
Preparación y realización de actividades evaluables (no presencial).	25	0
5.5.1.7 METODOLOGÍAS DOCENTES		
Clase expositiva participativa		
Práctica de laboratorio		
Trabajo cooperativo		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Examen parcial y/o final (prueba escrita de control de conocimientos)	30.0	30.0
Ejercicios puntuales a realizar en clase o en casa	30.0	30.0
Trabajos en grupo, presentados por escrito u oralmente	15.0	15.0
Prácticas de laboratorio	25.0	25.0
NIVEL 2: Seguridad en Infraestructuras		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	10	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
10		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NIVEL 3: Monitorización y Análisis del Tráfico de Red (TMA) / Network Traffic Monitoring and Analysis (TMA)		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**

Obligatoria	5	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
5		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NIVEL 3: Seguridad de Red / Network Security		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	5	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
5		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Comprender los retos tecnológicos asociados a la monitorización de la seguridad y el análisis del tráfico de red y conocer las técnicas necesarias para abordarlos.
- Conocer y ser capaces de aplicar las técnicas y sistemas de seguridad existentes para la clasificación del tráfico y la detección de anomalías, ataques e intrusiones de red.
- Comprender las implicaciones éticas, sociales y legales asociadas con la monitorización y el análisis del tráfico de red y conocer los mecanismos y regulaciones vigentes en materia de protección de datos.
- Conocer y comprender las amenazas y los riesgos de seguridad contra la administración de redes, con especial atención a la propiedad intelectual.
- Conocer las técnicas para auditar vulnerabilidades / ataques tanto en redes como en hosts.
- Conocer las técnicas para prevenir o contrarrestar esas amenazas de seguridad.

5.5.1.3 CONTENIDOS

- Monitorización de red: Métodos y red. Monitorización a nivel de paquetes. Monitorización a nivel de flujos.
- Algoritmos y estructuras de datos: Sampling, Bloom filters, Sketches. Herramientas, repositorios e infraestructuras.

- Clasificación de tráfico. Métodos basados en los puertos. Inspección profunda de los paquetes (DPI). Métodos basados en aprendizaje automático.
- Monitorización de la seguridad. Detección de anomalías. Detección de intrusiones y ataques: DDoS, escaneos, etc. Detección de botnets y malware.
- Privacidad online y protección de datos. Privacidad e implicaciones éticas en la monitorización de red. Anonimización del tráfico. Reglamento General de Protección de Datos (GDPR). Tracking digital: mecanismos, implicaciones y defensas.
- Seguridad en capa de enlace (ARP Spoofing). Seguridad en capa de enlace (WEP / WPA). Seguridad en capa de red (IPSEC /VPN). Seguridad en capa de red (Firewall / NAT). Seguridad en capa de red (IDS Snort). Seguridad en capa de Transporte SSL (SSL Strip). Seguridad en capa de aplicación (SQL Injection Attack). Seguridad en capa de aplicación (XSS). Ingeniería Social (SET).

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG2 - Identificar y aplicar nuevas técnicas procedentes del ámbito de la investigación a sistemas reales de ciberseguridad para adaptarlos a la continua evolución de las ciberamenazas.

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 - Emprendimiento e innovación. Conocer y entender los mecanismos en que se basa la investigación científica, así como los mecanismos e instrumentos de transferencia de resultados entre los diferentes agentes socioeconómicos implicados en los procesos de I+D+i.

CT3 - Trabajo en equipo. Ser capaz de trabajar como miembro de un equipo interdisciplinar, ya sea como un miembro más o realizando tareas de dirección, con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos teniendo en cuenta los recursos disponibles.

CT4 - Uso solvente de los recursos de información. Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información en el ámbito de especialidad y valorar de forma crítica los resultados de dicha gestión.

CT5 - Tercera lengua. Conocer una tercera lengua, preferentemente el inglés, con un nivel adecuado oral y escrito y en consonancia con las necesidades que tendrán los titulados y tituladas.

5.5.1.5.3 ESPECÍFICAS

CE2 - Identificar y seleccionar las herramientas más adecuadas para la detección y el análisis de ataques e incidentes de seguridad dependiendo de su naturaleza y el entorno donde se han producido.

CE3 - Identificar y analizar las leyes y regulaciones aplicables en materia de ciberseguridad y entender las implicaciones éticas que las técnicas de ciberdefensa pueden tener en la privacidad de los usuarios y como minimizarlas.

CE6 - Aplicar técnicas de monitorización y análisis del tráfico de red para la detección de ataques de ciberseguridad y la investigación de incidentes.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Exposición de contenidos teóricos mediante clases magistrales (presencial).	20	100
Exposición de contenidos con participación del estudiante (presencial).	13	100
Resolución de problemas, con participación del estudiante (presencial).	8	100
Sesiones prácticas de laboratorio individuales o en equipo (presencial).	26	100

Discusión en el aula de problemas o artículos, realizada por los alumnos y moderada por el profesor/a (presencial).	6	100
Elaboración de trabajos cooperativos (presencial).	5	100
Estudio y preparación de los contenidos (no presencial).	65	0
Realización de ejercicios y trabajos teóricos o prácticos fuera del aula, individualmente o en grupo (no presencial).	80	0
Preparación y realización de actividades evaluables (no presencial).	27	0
5.5.1.7 METODOLOGÍAS DOCENTES		
Clase magistral		
Práctica de laboratorio		
Trabajo autónomo		
Trabajo cooperativo		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Examen parcial y/o final (prueba escrita de control de conocimientos)	30.0	30.0
Ejercicios puntuales a realizar en clase o en casa	30.0	30.0
Trabajos individuales, presentados por escrito u oralmente	10.0	10.0
Trabajos en grupo, presentados por escrito u oralmente	5.0	5.0
Prácticas de laboratorio	25.0	25.0
NIVEL 2: Seguridad en Software		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	10	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
10		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	

No	No	
NIVEL 3: Malware		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	5	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
5		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NIVEL 3: Seguridad en Software y Aplicaciones / Internet Applications and Security		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	5	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
5		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
5.5.1.2 RESULTADOS DE APRENDIZAJE		

- Capacidad para detectar, analizar, solucionar y prevenir un ataque con código malicioso en un ordenador.
- Capacidad para diseñar y desarrollar las etapas de intrusión, infección, ofuscación y payload que componen una infección típica por código malicioso en un ordenador.
- Entender la implementación de firewalls y antivirus.
- Capacidad para identificar soluciones y técnicas de seguridad y privacidad relacionadas con las aplicaciones en Internet.
- Capacidad de diseñar aplicaciones teniendo en cuenta desde el principio los conceptos de seguridad y privacidad ("security by design" y "privacy by design").

- Capacidad de entender las cuestiones de seguridad en entornos específicos como los relacionados con los contenidos multimedia y las aplicaciones de salud, y la capacidad de aplicarlos en nuevos entornos.
- Capacidad de entender la evolución de las técnicas de seguridad en aplicaciones en Internet.

5.5.1.3 CONTENIDOS

- Conceptos básicos y avanzados de sistemas operativos.
- Conceptos básicos y avanzados de ingeniería inversa de software.
- Categorización de códigos maliciosos.
- Técnicas de propagación de infecciones mediante códigos maliciosos.
- Técnicas de ofuscación de malware.
- Prevención de ataques.
- Ética del desarrollo de código malicioso.
- Seguridad en aplicaciones: amenazas y mecanismos.
- Seguridad en protocolos de nivel de aplicación: XML y seguridad. Cifrado, Firma, protocolos específicos de seguridad. SAML, OAuth, OpenID Connect, Aplicaciones de Internet y privacidad. XACML.
- Seguridad y privacidad en eHealth. Privacidad en eHealth: Identificación de usuario, Políticas de privacidad en registros médicos, Políticas de acceso. Técnicas: Anonimización y pseudoanonimización.
- Privacy by design. Metoología. Regulaciones: GDPR, ejemplos.
- Seguridad y privacidad en contenido multimedia. Cifrado común en ficheros multimedia de formato ISO. *DASH encryption and authentication*. W3C approach: *Encrypted Media Extensions* (EME) & *Media Source Extensions* (MSE). Lenguajes de permisos y contratos (ODRL, MPEG CEL, ...)
- Privacidad de usuario en servicios web y aplicaciones: Web tracking, Privacidad en aplicaciones y redes sociales (Google, Instagram, Facebook, Retroshare, ..)

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG3 - Proyectar, diseñar e implantar productos, procesos, servicios e instalaciones en ámbitos de la 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

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

CT4 - Uso solvente de los recursos de información. Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información en el ámbito de especialidad y valorar de forma crítica los resultados de dicha gestión.

5.5.1.5.3 ESPECÍFICAS

CE2 - Identificar y seleccionar las herramientas más adecuadas para la detección y el análisis de ataques e incidentes de seguridad dependiendo de su naturaleza y el entorno donde se han producido.

CE3 - Identificar y analizar las leyes y regulaciones aplicables en materia de ciberseguridad y entender las implicaciones éticas que las técnicas de ciberdefensa pueden tener en la privacidad de los usuarios y como minimizarlas.

CE7 - Diseñar, desarrollar, detectar, analizar y eliminar código malicioso que sea capaz de infectar y ocultarse en un sistema operativo actual.

CE8 - Identificar y aplicar técnicas para mantener en todo momento la seguridad y privacidad de las aplicaciones distribuidas construidas sobre los protocolos de Internet.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Exposición de contenidos teóricos mediante clases magistrales (presencial).	26	100
Exposición de contenidos con participación del estudiante (presencial).	9	100
Sesiones prácticas de laboratorio individuales o en equipo (presencial).	5	100
Discusión en el aula de problemas o artículos, realizada por los alumnos y moderada por el profesor/a (presencial).	5	100

Elaboración de trabajos cooperativos (presencial).	23	100
Tutoría (presencial).	10	100
Estudio y preparación de los contenidos (no presencial).	50	0
Realización de proyectos propuestos por los profesores fuera del aula, individualmente o en grupo (no presencial).	75	0
Preparación y realización de actividades evaluables (no presencial).	47	0

5.5.1.7 METODOLOGÍAS DOCENTES
Clase magistral
Clase expositiva participativa
Práctica de laboratorio
Trabajo cooperativo
Tutoría

5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Examen parcial y/o final (prueba escrita de control de conocimientos)	30.0	30.0
Ejercicios puntuales a realizar en clase o en casa	30.0	30.0
Trabajos en grupo, presentados por escrito u oralmente	30.0	30.0
Prácticas de laboratorio	10.0	10.0

5.5 NIVEL 1: Formación optativa
5.5.1 Datos Básicos del Nivel 1
NIVEL 2: Temas transversales de Ciberseguridad

5.5.1.1 Datos Básicos del Nivel 2	
CARÁCTER	Optativa
ECTS NIVEL 2	18
DESPLIEGUE TEMPORAL: Cuatrimestral	

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

LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	

No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NIVEL 3: Casos de Uso en Ciberseguridad / Cybersecurity UseCases		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Optativa	5	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	5	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NIVEL 3: Gestión de la Ciberseguridad / Cybersecurity Management		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Optativa	5	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	5	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

LISTADO DE ESPECIALIDADES
No existen datos

5.5.1.2 RESULTADOS DE APRENDIZAJE

Esta materia se compone de créditos optativos (a cursar por el alumno un mínimo de 3 y un máximo de 18 ECTS), donde se tratarán de manera transversal los ejes de obligatoriedad del máster (datos, infraestructura, software).

Los resultados del aprendizaje dependerán mucho de la asignatura del ámbito de aplicación transversal de la ciberseguridad (biomédico, big data, Votaciones electrónicas,...)

5.5.1.3 CONTENIDOS

Los resultados de aprendizaje anteriormente descritos, así como otros que pueden sobrevenir debido al avance de la tecnología, se estructurarán en contenidos de las asignaturas optativas preferentemente en bloques de 5 ECTS (aunque no se excluyen ofertas de 6 ECTS de otros planes de estudio) y seminarios de 3 ECTS, y se impartirán preferentemente en el cuatrimestre 2 de la titulación.

5.5.1.4 OBSERVACIONES

Tal y como se ha indicado anteriormente, las asignaturas optativas pueden variar a lo largo de la existencia del máster y, por tanto, ofrecen la posibilidad de actualizar los contenidos de la titulación.

En un primer diseño de los contenidos, se propone ofrecer 10 créditos optativos en el ámbito transversal y 26 en el ámbito avanzado. A modo de ejemplo, en esta materia se han descrito 2 asignaturas del ámbito transversal.

Destacar que, tal y como se ha indicado en el apartado 5.1 de esta memoria, para la superación de la formación optativa del máster el estudiante ha de superar obligatoriamente 3 ECTS de esta materia de "Temas transversales de Ciberseguridad".

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG2 - Identificar y aplicar nuevas técnicas procedentes del ámbito de la investigación a sistemas reales de ciberseguridad para adaptarlos a la continua evolución de las ciberamenazas.

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

CT3 - Trabajo en equipo. Ser capaz de trabajar como miembro de un equipo interdisciplinar, ya sea como un miembro más o realizando tareas de dirección, con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos teniendo en cuenta los recursos disponibles.

CT4 - Uso solvente de los recursos de información. Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información en el ámbito de especialidad y valorar de forma crítica los resultados de dicha gestión.

CT5 - Tercera lengua. Conocer una tercera lengua, preferentemente el inglés, con un nivel adecuado oral y escrito y en consonancia con las necesidades que tendrán los titulados y tituladas.

5.5.1.5.3 ESPECÍFICAS

CE2 - Identificar y seleccionar las herramientas más adecuadas para la detección y el análisis de ataques e incidentes de seguridad dependiendo de su naturaleza y el entorno donde se han producido.

CE3 - Identificar y analizar las leyes y regulaciones aplicables en materia de ciberseguridad y entender las implicaciones éticas que las técnicas de ciberdefensa pueden tener en la privacidad de los usuarios y como minimizarlas.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Exposición de contenidos teóricos mediante clases magistrales (presencial).	35	100

Exposición de contenidos con participación del estudiante (presencial).	15	100
Sesiones prácticas de laboratorio individuales o en equipo (presencial).	35	100
Discusión en el aula de problemas o artículos, realizada por los alumnos y moderada por el profesor/a (presencial).	10	100
Elaboración de trabajos cooperativos (presencial).	10	100
Visitas a empresas por parte de los estudiantes, con la finalidad de adquirir conocimientos prácticos relacionados con la temática de la materia (presencial).	5	100
Asistencia a seminarios y conferencias relacionados con la temática de la materia (presencial).	20	100
Tutoría (presencial).	5	100
Estudio y preparación de los contenidos (no presencial).	30	0
Realización de ejercicios y trabajos teóricos o prácticos fuera del aula, individualmente o en grupo (no presencial).	40	0
Realización de proyectos propuestos por los profesores fuera del aula, individualmente o en grupo (no presencial).	165	0
Preparación y realización de actividades evaluables (no presencial).	80	0
5.5.1.7 METODOLOGÍAS DOCENTES		
Clase magistral		
Clase expositiva participativa		
Práctica de laboratorio		
Trabajo autónomo		
Trabajo cooperativo		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Examen parcial y/o final (prueba escrita de control de conocimientos)	30.0	30.0
Ejercicios puntuales a realizar en clase o en casa	30.0	30.0
Trabajos individuales, presentados por escrito u oralmente	10.0	10.0
Trabajos en grupo, presentados por escrito u oralmente	5.0	5.0
Prácticas de laboratorio	25.0	25.0
NIVEL 2: Temas avanzados de Ciberseguridad		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
ECTS NIVEL 2	15	

DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	15	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NIVEL 3: Seguridad en Redes Fijas 5G / Securing 5G Fixed Network		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Optativa	5	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	5	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NIVEL 3: Seminario de Blockchain / Blockchain Seminar		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Optativa	3	Cuatrimestral
DESPLIEGUE TEMPORAL		

ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
	3	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NIVEL 3: Seguridad en IoT / IoT Security		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Optativa	5	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	5	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NIVEL 3: Criptografía Cuántica / Quantum Cryptography		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Optativa	5	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**

	5	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		

5.5.1.2 RESULTADOS DE APRENDIZAJE

Esta materia se compone de créditos optativos (a cursar por el alumno un máximo de 15), que suponen una profundización/intensificación en algunos de los ejes de obligatoriedad del máster (datos, infraestructura, software).

Los resultados del aprendizaje dependerán mucho del eje escogido, no todos los estudiantes que cursen esta materia tendrán todos los mismos resultados de aprendizaje. A modo de ejemplo algunos de ellos son:

- Seguridad, autenticación y autorización en redes de comunicaciones de nueva generación.
- Concepto de Distributed Ledger y diferentes tipos de cadenas de bloques.
- Concepto de Contrato Inteligente (Smart Contract).
- Conocimientos básicos de las redes de transporte que dan soporte a 5G, incluidas las capas óptica y de paquetes y de los segmentos metro y core.
- Conocimientos de cloud and fog computing.
- Conocimientos de planificación y de re-optimización de la red.
- Conocimientos de control de red basados en SDN y sus aplicaciones para seguridad.
- Conocimientos de monitorización, análisis y visualización de datos orientados a seguridad.
- Conocimientos sobre redes autónomas.
- Experiencia utilizando herramientas de emulación de red (mininet), de planificación de red (net2plan), control de red (ONOS), almacenamiento, análisis y visualización de datos (Grafana).
- Trabajo en curso sobre aspectos de seguridad en los organismos de estandarización.
- Ideas fundamentales de la criptografía cuántica.
- Protocolos y pruebas de seguridad para la distribución de claves cuánticas.
- Los fundamentos de la criptografía cuántica independiente del dispositivo.
- Tareas y protocolos criptográficos cuánticos modernos.

5.5.1.3 CONTENIDOS

Los resultados de aprendizaje anteriormente descritos, así como otros que pueden sobrevenir debido al avance de la tecnología, se estructurarán en contenidos de las asignaturas optativas preferentemente en bloques de 5 ECTS (aunque no se excluyen ofertas de 6 ECTS de otros planes de estudio) y seminarios de 3 ECTS, y se impartirán preferentemente en el cuatrimestre 2 de la titulación.

5.5.1.4 OBSERVACIONES

Tal y como se ha indicado anteriormente, las asignaturas optativas pueden variar a lo largo de la existencia del máster y, por tanto, ofrecen la posibilidad de actualizar los contenidos de la titulación.

En un primer diseño de los contenidos, se propone ofrecer 10 créditos optativos en el ámbito transversal y 26 en el ámbito avanzado. A modo de ejemplo, en esta materia se han descrito 4 asignaturas del ámbito avanzado.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG2 - Identificar y aplicar nuevas técnicas procedentes del ámbito de la investigación a sistemas reales de ciberseguridad para adaptarlos a la continua evolución de las ciberamenazas.

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
CT3 - Trabajo en equipo. Ser capaz de trabajar como miembro de un equipo interdisciplinar, ya sea como un miembro más o realizando tareas de dirección, con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos teniendo en cuenta los recursos disponibles.
CT4 - Uso solvente de los recursos de información. Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información en el ámbito de especialidad y valorar de forma crítica los resultados de dicha gestión.
CT5 - Tercera lengua. Conocer una tercera lengua, preferentemente el inglés, con un nivel adecuado oral y escrito y en consonancia con las necesidades que tendrán los titulados y tituladas.
5.5.1.5.3 ESPECÍFICAS
CE2 - Identificar y seleccionar las herramientas más adecuadas para la detección y el análisis de ataques e incidentes de seguridad dependiendo de su naturaleza y el entorno donde se han producido.
CE3 - Identificar y analizar las leyes y regulaciones aplicables en materia de ciberseguridad y entender las implicaciones éticas que las técnicas de ciberdefensa pueden tener en la privacidad de los usuarios y como minimizarlas.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Exposición de contenidos teóricos mediante clases magistrales (presencial).	39	100
Exposición de contenidos con participación del estudiante (presencial).	13	100
Sesiones prácticas de laboratorio individuales o en equipo (presencial).	39	100
Discusión en el aula de problemas o artículos, realizada por los alumnos y moderada por el profesor/a (presencial).	5	100
Elaboración de trabajos cooperativos (presencial).	10	100
Visitas a empresas por parte de los estudiantes, con la finalidad de adquirir conocimientos prácticos relacionados con la temática de la materia (presencial).	2	100
Asistencia a seminarios y conferencias relacionados con la temática de la materia (presencial).	4	100
Tutoría (presencial).	5	100
Estudio y preparación de los contenidos (no presencial).	54	0
Realización de ejercicios y trabajos teóricos o prácticos fuera del aula, individualmente o en grupo (no presencial).	54	0
Realización de proyectos propuestos por los profesores fuera del aula, individualmente o en grupo (no presencial).	75	0

Preparación y realización de actividades evaluables (no presencial).	75	0
5.5.1.7 METODOLOGÍAS DOCENTES		
Clase magistral		
Clase expositiva participativa		
Práctica de laboratorio		
Trabajo autónomo		
Trabajo cooperativo		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Examen parcial y/o final (prueba escrita de control de conocimientos)	30.0	30.0
Ejercicios puntuales a realizar en clase o en casa	30.0	30.0
Trabajos individuales, presentados por escrito u oralmente	10.0	10.0
Trabajos en grupo, presentados por escrito u oralmente	5.0	5.0
Prácticas de laboratorio	25.0	25.0
5.5 NIVEL 1: Trabajo de Fin de Máster		
5.5.1 Datos Básicos del Nivel 1		
NIVEL 2: Trabajo de Fin de Máster		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Trabajo Fin de Grado / Máster	
ECTS NIVEL 2	12	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	12	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NIVEL 3: Trabajo de Fin de Máster / Master's Thesis		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**

Trabajo Fin de Grado / Máster	12	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	12	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
No	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

5.5.1.2 RESULTADOS DE APRENDIZAJE

Con la superación de esta materia, el alumno demuestra que es capaz de elaborar, presentar y defender de manera individual un ejercicio original de carácter profesional en el ámbito de la Ciberseguridad como demostración y síntesis de las competencias adquiridas en las enseñanzas.

Utiliza conocimientos y habilidades estratégicas para la creación y gestión de proyectos con visión innovadora, aplica soluciones sistémicas a problemas complejos. Específicamente:

- Planifica y utiliza la información necesaria para un proyecto o trabajo académico a partir de una reflexión crítica sobre los recursos de información utilizados.
- Aplica las competencias adquiridas a la realización de una tarea de forma autónoma. Identifica la necesidad del aprendizaje continuo y desarrolla una estrategia propia para llevarlo a cabo.
- Identifica y modela sistemas complejos. Lleva a cabo análisis cualitativos y aproximaciones, estableciendo la incertidumbre de los resultados.
- Plantea hipótesis y métodos experimentales para validarlas.
- Identifica componentes principales y establece compromisos y prioridades.
- Diseña experimentos y medidas para verificar hipótesis o validar el funcionamiento de equipos, procesos, sistemas o servicios en el ámbito de la ciberseguridad.
- Selecciona los equipos o herramientas software adecuadas y lleva a cabo análisis avanzados con los datos.
- Conoce el concepto de ciclo de vida de un producto y lo aplica al desarrollo de productos y servicios de ciberseguridad, usando la normativa y legislación adecuadas.
- Puede llevar a cabo una presentación oral y responder a las preguntas del auditorio.
- Se comunica de manera clara y eficiente en presentaciones orales y escritas sobre ciberseguridad, adaptándose a la situación, al tipo de público y a los objetivos de la comunicación.

5.5.1.3 CONTENIDOS

La materia TFM no es susceptible de ser descrita a partir de conocimientos concretos, ya que su propia definición está abierta a cualquier ámbito que se enmarque dentro de la ciberseguridad.

Se define como un trabajo individual original de carácter profesional en el ámbito de la ciberseguridad, con predominio de la vertiente creativa y de diseño. En él se deben desarrollar las competencias de la titulación.

Normalmente se llevará a cabo dentro de un grupo de investigación, con posibilidad de hacerlo en una institución o en una empresa nacional o extranjera.

La evaluación del Trabajo de Fin de Máster se realizará a través de la presentación de una memoria escrita y defensa oral del trabajo ante un tribunal específico. La presentación de la memoria deberá ser autorizada por el tutor. En el tribunal podrán participar profesores del Máster y profesionales de las empresas en las que se realicen trabajos de fin de Máster, en la forma en que pudiera determinar la normativa académica.

Todos los aspectos relativos a plazos, procedimientos, miembros integrantes del tribunal, así como la forma y modo de desarrollo del mismo y su calificación, se efectuarán de acuerdo a la normativa vigente.

Los criterios de evaluación de los trabajos de fin de máster son los siguientes:

- La investigación/desarrollo llevado a cabo de acuerdo con la hipótesis/situación de partida.
- El documento presentado sobre el trabajo de investigación incluyendo el trabajo de revisión bibliográfica.
- Las conclusiones planteadas como resultado del trabajo.
- El informe de evaluación presentado por el tutor.
- La presentación y defensa del trabajo ante el tribunal.

5.5.1.4 OBSERVACIONES

Podrán ser profesores de la materia (tutores de TFM) aquellos profesores de la titulación, o cualquier profesor de los centros que acredite experiencia en el ámbito de la ciberseguridad.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG3 - Proyectar, diseñar e implantar productos, procesos, servicios e instalaciones en ámbitos de la Ciberseguridad.

CG4 - Elaborar, planificar estratégicamente, dirigir, coordinar y gestionar técnica y económicamente proyectos en ámbitos de la Ciberseguridad, siguiendo criterios de calidad y medioambientales.

CG5 - Analizar y aplicar la legislación y normativa necesaria en el ámbito de la Seguridad de la Información.

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

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

5.5.1.5.2 TRANSVERSALES

CT1 - Emprendimiento e innovación. Conocer y entender los mecanismos en que se basa la investigación científica, así como los mecanismos e instrumentos de transferencia de resultados entre los diferentes agentes socioeconómicos implicados en los procesos de I+D+i.

CT2 - Sostenibilidad y Compromiso Social. Conocer y comprender la complejidad de los fenómenos económicos y sociales típicos de la sociedad del bienestar; tener capacidad para relacionar el bienestar con la globalización y la sostenibilidad; lograr habilidades para utilizar de forma equilibrada y compatible la técnica, la tecnología, la economía y la sostenibilidad.

CT4 - Uso solvente de los recursos de información. Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información en el ámbito de especialidad y valorar de forma crítica los resultados de dicha gestión.

CT5 - Tercera lengua. Conocer una tercera lengua, preferentemente el inglés, con un nivel adecuado oral y escrito y en consonancia con las necesidades que tendrán los titulados y tituladas.

5.5.1.5.3 ESPECÍFICAS

CE9 - Elaborar un trabajo original a realizar individualmente y presentar y defender ante un tribunal universitario, consistente en un proyecto de ingeniería en el ámbito de la Ciberseguridad en el que se sinteticen las competencias adquiridas en las enseñanzas del Máster.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Tutoría (presencial).	40	100
Preparación, ensayo y realización de actividades evaluables relacionadas con el TFM (presencial).	10	100
Estudio y preparación de los contenidos (no presencial).	210	0
Realización de proyectos propuestos por los profesores fuera del aula, individualmente o en grupo (no presencial).	40	0

5.5.1.7 METODOLOGÍAS DOCENTES

Aprendizaje basado en problemas / proyectos

Trabajo autónomo

Tutoría

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Presentación y defensa oral del TFM	100.0	100.0

6. PERSONAL ACADÉMICO

6.1 PROFESORADO Y OTROS RECURSOS HUMANOS				
Universidad	**Categoría**	**Total %**	**Doctores %**	**Horas %**
Universidad Politécnica de Catalunya	Profesor Asociado (incluye profesor asociado de C.C.: de Salud)	15	50	20
Universidad Politécnica de Catalunya	Profesor Contratado Doctor	20	100	20
Universidad Politécnica de Catalunya	Profesor Titular de Universidad	40	100	40
Universidad Politécnica de Catalunya	Catedrático de Universidad	25	100	20

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 %
70	15	85

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

La evaluación del aprendizaje del alumnado se plantea de forma continua, es decir, no se acumulará en la etapa final y además servirá tanto para regular el ritmo de trabajo y del aprendizaje a lo largo del transcurso de la asignatura, materia o titulación (evaluación formativa), como para permitir al alumnado conocer su grado de adquisición de aprendizaje (evaluación sumativa) y también para darle la opción a reorientar su aprendizaje (evaluación formativa).

La evaluación formativa se ha diseñado de tal modo que permita informar al alumnado sobre su progreso o falta de él, además de ayudarlo, mediante la correspondiente retroalimentación por parte del profesorado, a alcanzar los objetivos de aprendizaje contemplados en la correspondiente asignatura o materia.

La evaluación sumativa se ha diseñado con el objetivo de calificar al alumno o alumna, para su correspondiente promoción y acreditación o certificación ante terceros. La calificación de cada alumno o alumna está basada en una cantidad suficiente de notas, las cuales, debidamente ponderadas, configuran su calificación final.

Para valorar el aprendizaje del estudiantado se han planificado suficientes y diversos tipos de actividades de evaluación a lo largo de la impartición de cada asignatura o materia. La programación de dichas actividades es un documento útil tanto para el alumnado como para el profesorado. Todas las actividades de evaluación son coherentes con los objetivos específicos y/o competencias programadas por el plan de estudios, en cada asignatura o materia. El conjunto de tareas y/o actividades que realiza el alumno o alumna configura su aprendizaje y le permite la obtención de la calificación final de cada asignatura o materia.

A cualquier producto elaborado por el alumnado y que ha de entregar al profesor, tanto si es calificado como si no lo es, se le denomina "entregable". Asimismo, se especifica tanto el formato en el que se ha de presentar así como el tiempo de dedicación que el profesorado estima que los estudiantes necesitan para la realización de dicho entregable.

La evaluación se basa en unos criterios de calidad, suficientemente fundamentados, transparentes y públicos para el alumno o alumna desde el inicio. Dichos criterios están acordes tanto con las actividades planificadas, metodologías aplicadas, como con los objetivos de aprendizaje previstos a alcanzar por el alumnado.

La frecuencia de las actividades de evaluación viene determinada por el desarrollo tanto de los objetivos específicos como de la competencia o competencias contempladas en dicha asignatura o materia.

Las actividades de evaluación pueden ser individuales y/o de grupo, en el aula o fuera de ella, además de multidisciplinares o no.

Cada actividad de evaluación estará acompañada de un rápido retorno del profesorado, para que así el alumno o alumna pueda reconducir, a tiempo, su proceso de aprendizaje. El tipo de retroalimentación será desde comentarios personales acompañando las correspondientes correcciones, ya sea en el mismo material entregado o a través del campus digital.

Normativa de aplicación

El Consejo de Gobierno de esta universidad aprueba para cada curso académico la normativa académica de los estudios de grado y máster de la UPC donde se regula, entre otros, el sistema de evaluación a aplicar en sus estudios.

A continuación, y tal y como se define en dicha normativa, se recogen las normas que regulan la evaluación de los estudiantes de esta universidad.

Sistema de evaluación de la UPC

En un modelo de aprendizaje basado en competencias, evaluar significa valorar el progreso del estudiante para alcanzar los objetivos propuestos. La evaluación debe englobar todas las competencias programadas en el plan de estudios y debe basarse en criterios bien fundamentados y suficientemente transparentes y públicos. Debe existir una relación coherente entre los objetivos formativos, las actividades planificadas y los criterios de evaluación.

La evaluación de los estudios de máster en la UPC se divide en dos niveles:
- Las asignaturas/materias obligatorias y optativas programadas en el plan de estudios. Las personas responsables de la propuesta de calificación son los coordinadores y coordinadoras de las asignaturas.
- Los bloques curriculares. Un bloque curricular es un conjunto de asignaturas con unos objetivos formativos comunes que se evalúan de forma global en un procedimiento que se denomina evaluación curricular. El centro docente es el responsable de la evaluación curricular.

Con carácter general, la evaluación de estos estudios se realiza sólo en el primer nivel, excepto que tengan definido uno o más bloques curriculares, en cuyo caso también le sería de aplicación el segundo nivel.

El TFM se programa en la fase final del plan de estudios y tiene carácter de síntesis de las capacidades adquiridas en el proceso formativo pero, debe estar orientado a la evaluación de la adquisición de las competencias propias asociadas al título.

1. Evaluación de las asignaturas

1.1. Definición

La evaluación de una asignatura consiste en determinar el grado de consecución de sus objetivos. Su superación significará haber alcanzado los objetivos establecidos como básicos e implicará obtener una calificación numérica mínima de 5,0.

Con el objetivo de velar por la máxima corrección del proceso de evaluación de los estudiantes, cada centro establecerá una normativa específica que regule los procesos vinculados a la realización de los actos de evaluación de las asignaturas, que deberá incluir y completar lo establecido en este apartado.

1.2. Derechos y obligaciones de los estudiantes en el proceso de evaluación

Los estudiantes tienen derecho a la evaluación de todas las asignaturas de las que se hayan matriculado.

De acuerdo con el artículo 93 de los Estatutos de la UPC, según el cual la Universidad debe velar para que los representantes de los estudiantes puedan ejercer con libertad su representación y para que sus obligaciones académicas puedan ser compatibles, si a un estudiante no le es posible hacer una prueba de evaluación por este motivo, el centro debe garantizar las medidas necesarias para que la pueda realizar o para que este hecho no perjudique el estudiante. En cualquier caso, el estudiante debe justificarlo documentalmente dentro del período lectivo correspondiente.

Para los estudiantes que no puedan hacer una prueba de evaluación por otros motivos diferentes al anteriormente expuesto, y que sean excepcionales y debidamente justificados a criterio del centro, se deberán garantizar las medidas necesarias para que la puedan realizar, siempre dentro del periodo lectivo correspondiente. Sin embargo, y en este caso, el centro docente únicamente está obligado a cambiar las fechas de los actos o pruebas de evaluación que son más significativos en la evaluación final de la asignatura.

Por otra parte, el estudiante que se matricule de asignaturas con algún tipo de incompatibilidad horaria no podrá reclamar, por ese motivo, la evaluación en fechas diferentes a las previstas.

Los estudiantes tienen derecho a obtener un justificante documental de asistencia a un acto de evaluación. El estudiante debe poder identificarse en cualquier momento durante la realización de un acto de evaluación.

Las acciones irregulares que puedan conducir a una variación significativa de la calificación de uno o más estudiantes constituirán una realización fraudulenta de un acto de evaluación. Esa acción conllevará la calificación descriptiva de suspenso y numérica de 0 del acto de evaluación y de la asignatura, sin perjuicio del proceso disciplinario que pueda derivarse como consecuencia de los actos realizados.

Si el estudiante considera incorrecta la decisión, podrá formular una queja mediante una instancia ante el director o directora o el decano o decana del centro docente y, si la respuesta no le satisface, podrá interponer un recurso ante el rector o rectora.

La reproducción total o parcial de los trabajos académicos o de investigación, o su utilización para cualquier otro fin, deberán tener la autorización explícita de los autores o autoras.

Corresponderá al director o directora o el decano o decana del centro docente resolver las alegaciones sobre los aspectos no incluidos en las normativas.

1.3. Criterios de evaluación y método de calificación de las asignaturas

El profesor o profesora responsable de cada asignatura elaborará, conjuntamente con el profesorado que la imparta, una propuesta de guía docente, que incluirá los criterios de evaluación, el método de calificación y la ponderación de las pruebas de evaluación. Corresponderá al órgano de gobierno del centro que tiene las competencias en la evaluación de los estudiantes aprobar las propuestas antes del inicio del curso, hacer la máxima difusión de las mismas utilizando los recursos que tenga a su alcance, velar por que se apliquen correctamente y hacer su interpretación en el supuesto de que surja alguna duda.

Para estimular el aprendizaje progresivo a un ritmo regular de los estudiantes, en la evaluación de las asignaturas se tendrán en cuenta los resultados obtenidos en los diferentes actos de evaluación realizados a lo largo del curso. En la evaluación continua, el método de calificación de cada una de las asignaturas se debe definir de manera que los resultados de todos los actos de evaluación se tomen en consideración en la calificación final, que se guarde una cierta proporcionalidad con los créditos asignados a las actividades académicas evaluables y que el resultado de ningún acto de evaluación no pueda determinar por sí solo la superación de la asignatura.

El plan docente de una asignatura también puede prever una prueba final de carácter global que sustituya la evaluación continua, de modo que la superación de ésta suponga la superación de la asignatura. Si el plan docente no incluye esta posibilidad, los estudiantes podrán solicitar a la dirección del centro hacer una prueba que determine la calificación de una asignatura. Si la respuesta es positiva y la asignatura incluye proyectos o trabajos prácticos, el centro deberá arbitrar las medidas adecuadas para incorporarlos a la evaluación.

Si la hay, la calificación de la prueba global final deberá sustituir, siempre que sea superior y que coincidan los aspectos evaluados, los resultados obtenidos en los actos de evaluación que se hayan llevado a cabo a lo largo del curso.

El sistema de evaluación de las asignaturas deberá prever procedimientos que permitan reconducir resultados poco satisfactorios obtenidos durante el curso.

En el método de calificación de una asignatura no se podrán establecer condiciones de nota mínima en ningún acto de evaluación para tener en cuenta los resultados del resto. Sin embargo, si entre las actividades programadas existen proyectos o trabajos prácticos, bien sean de laboratorio o de campo, la guía docente de la asignatura podrá prever que sea una condición necesaria para superar la asignatura su realización y la presentación de los informes asociados.

1.4. Resultados de la evaluación de las asignaturas

Al finalizar el periodo lectivo, el profesor o profesora responsable de la asignatura consignará las calificaciones descriptiva y numérica de los estudiantes matriculados en el informe de evaluación, lo firmará y lo entregará al centro, que, en su caso, lo elevará a definitivo.

Las calificaciones numéricas se darán en una escala de 0 a10 y con una resolución de 0,1, y las descriptivas se asignarán según la siguiente correspondencia:

0-4,9: suspenso

5,0-6,9: aprobado

7,0-8,9 notable

9,0-10: sobresaliente/matrícula de honor

La mención de matrícula de honor se podrá otorgar a los estudiantes que tengan una calificación igual o superior a 9,0. El número de matrículas de honor que se otorguen no podrá ser superior al 5 % de los estudiantes matriculados en una asignatura en el periodo académico correspondiente, excepto que el número total de estudiantes matriculados sea inferior a 20, en cuyo caso se podrá otorgar una sola matrícula de honor.

En el caso del TFM, el tribunal propondrá la mención de matrícula de honor. En el caso de las prácticas externas, el profesor tutor o profesora tutora será quien realice la propuesta. Con posterioridad a esta propuesta, el centro arbitrará la manera en que deberán adjudicarse las matrículas de honor definitivas, sin superar el 5% de los estudiantes matriculados y teniendo en cuenta, en todos los casos, criterios objetivos.

En el caso de que las matrículas de honor concedidas a estudiantes que hayan hecho una matrícula ordinaria lleguen al 5 %, no se otorgará ninguna otra matrícula de honor a los estudiantes que se acogieron a la convocatoria adicional del TFM o de las prácticas externas.

La calificación de no presentado, que significa que el estudiante no ha sido evaluado, se otorgará cuando no haya participado en ninguno de los actos de evaluación previstos para la asignatura, excepto en el caso de que la guía docente de la asignatura publicada especifique algo distinto.

En los estudios organizados en bloques curriculares, las calificaciones descriptivas de las asignaturas superadas que figuren en los informes de evaluación serán definitivas, mientras que las calificaciones descriptiva y numérica de suspenso podrán cambiar en evaluaciones posteriores de la asignatura o en la evaluación del bloque curricular al que pertenezcan. La superación de un bloque curricular implicará que las calificaciones descriptivas y numéricas de las asignaturas que lo compongan sean definitivas.

Los resultados de los actos de evaluación se darán a conocer a los estudiantes en un plazo breve, que fijará cada centro, ya que constituyen un elemento importante para la mejora de su proceso de aprendizaje, especialmente si la información se complementa con una acción de tutoría. Los resultados de las evaluaciones finales se entregarán en un plazo no superior a 15 días naturales desde que tuvo lugar la última prueba.

En el caso de asignaturas cursadas en un programa de movilidad, se conservará la nota obtenida en la universidad de destino adaptada al sistema de calificaciones del centro de origen. En caso de que en la certificación académica emitida por el centro de destino alguna de las asignaturas haya sido evaluada con matrícula de honor, ésta se podrá conservar y tendrá los efectos económicos regulados en el Presupuesto de la UPC.

1.5 Trabajo de fin de máster

El sistema de evaluación del trabajo de fin de máster incluye una defensa pública ante un tribunal nombrado al efecto por el centro que imparte los estudios.

El tribunal estará formado por un mínimo de tres miembros del personal docente e investigador (presidente o presidenta, vocal y secretario o secretaria). El centro responsable regulará si puede añadirse al tribunal un miembro externo, ya sea personal docente o investigador o una persona de reconocido prestigio.

Corresponderá al centro responsable establecer la normativa específica para regular y completar los procesos relacionados tanto con la configuración de los tribunales evaluadores como con la realización de los actos de evaluación de los trabajos de fin de máster.

1.6. Calendario de los actos de evaluación

Los actos de evaluación que se realicen durante el periodo de impartición de la docencia tendrán lugar dentro de los horarios lectivos de la asignatura, a menos que el centro lo regule de un modo distinto. Los actos de evaluación se realizarán siempre dentro del periodo lectivo, de acuerdo con el calendario académico de la UPC.

1.7. Acciones de tutoría y orientación académica a los estudiantes

Independientemente del proceso de revisión de las calificaciones y en el marco de las acciones de tutoría y orientación académica, el estudiante tendrá derecho a recibir del profesor o profesora de la asignatura valoraciones sobre el trabajo que haya hecho en cualquier actividad objeto de evaluación, que deberá incluir una explicación sobre la calificación otorgada, con una finalidad de orientación académica.

Esta acción tutorial deberá tener lugar durante el periodo lectivo en el que el estudiante curse la asignatura o, como máximo, durante el primer mes una vez iniciado el siguiente periodo, y a través del medio acordado por el profesor o profesora de la asignatura y el estudiante. Sin embargo, el estudiante tendrá derecho a solicitar que la acción tutorial tenga carácter presencial.

2. Evaluación curricular

2.1. Definición de bloque curricular y evaluación curricular

Un bloque curricular se define como un conjunto de asignaturas con unos objetivos formativos comunes que se evalúan de forma global en un procedimiento denominado *evaluación curricular*.

Los planes de estudios de máster podrán estructurarse en uno o más bloques curriculares, que serán definidos por el centro.

2.2. Derecho a la evaluación curricular

Los estudiantes deberán ser evaluados curricularmente cuando hayan sido evaluados de todas las asignaturas que compongan un bloque curricular.

2.3. Renuncia a la evaluación curricular

Sin perjuicio de lo que determina el artículo anterior y cuando sea procedente, en caso de que un estudiante no desee ser incluido en un proceso de evaluación curricular que permita la compensación porque, habiendo suspendido una o más asignaturas con una calificación igual o superior a 4, quiere elegir la opción de repetirlas en el siguiente periodo lectivo, deberá comunicar de forma expresa su renuncia a la evaluación curricular. Los centros docentes establecerán un periodo previo a la evaluación para la presentación de estas renuncias.

Con el mismo procedimiento, un estudiante podrá renunciar a todas las evaluaciones curriculares de un bloque. Esta renuncia comportará que las calificaciones descriptivas y numéricas de las asignaturas del bloque curricular ya superadas que figuren en los informes de evaluación pasen a ser definitivas.

2.4. Mecanismo para efectuar la evaluación curricular

Cada centro establecerá los mecanismos para efectuar la evaluación curricular a partir de los resultados obtenidos en las asignaturas que compongan cada bloque curricular. Dicha evaluación será realizada por una comisión específica.

Al inicio del curso académico, cada centro publicará el calendario de evaluaciones curriculares de los planes de estudios que imparta.

2.5. Resultados de la evaluación curricular

Los resultados de la evaluación curricular se darán a conocer a los estudiantes mediante el acta curricular.

En caso de que el estudiante haya superado el bloque curricular, este documento deberá incluir las calificaciones descriptiva y numérica definitivas de cada una de las asignaturas y la calificación numérica del bloque curricular, obtenida como media de la calificación de las asignaturas ponderada con el número de créditos de cada una.

Si el estudiante no ha superado el bloque curricular, se especificará "suspenso de calificación", sin nota numérica.

Un bloque curricular se supera cuando las calificaciones numéricas de las asignaturas que lo integran, que figuran en los informes de evaluación, son iguales o superiores a 5. En este caso, las calificaciones numéricas y descriptivas pasarán a definitivas sin cambios.

Por otra parte, el centro podrá establecer otras condiciones que permitan superar un bloque curricular, que podrán incluir la superación por compensación de asignaturas suspendidas con una calificación numérica no inferior a 4, siempre que la nota media ponderada del bloque sea igual o mayor que un valor establecido por el centro y que ha de ser, como mínimo, de 5. Así mismo, el centro podrá, en casos concretos y de forma justificada, considerar otras condiciones que permitan compensar calificaciones inferiores a 4.

3. Revisión de los resultados de la evaluación

El estudiante tiene derecho a la revisión de los diferentes resultados de los actos de evaluación. El resultado del proceso de revisión nunca puede suponer una calificación inferior a la obtenida previamente, excepto cuando se justifique que se trata de un error de transcripción.

3.1 Revisión en primera instancia de los actos de evaluación

La revisión de los actos de evaluación es una actividad formativa. El profesor o profesora deberá publicar, junto con las notas de la actividad evaluable, el horario, el lugar y la fecha de la revisión, que será presencial y accesible para los estudiantes (a excepción de asignaturas con docencia semipresencial, en cuyo caso el profesor o profesora podrá prever otro método). La revisión será incondicional para todos los estudiantes que hayan realizado la actividad evaluable.

3.2. Reclamaciones contra resoluciones de los profesores o profesoras responsables de las asignaturas

El estudiante deberá presentar una solicitud razonada de revisión al director o directora o el decano o decana del centro, en un plazo máximo de 7 días naturales desde la fecha de publicación de las calificaciones revisadas que sean objeto de reclamación.

El director o directora o el decano o decana del centro arbitrará el procedimiento específico que considere adecuado para resolver cada reclamación de forma imparcial, procedimiento que siempre deberá incluir la audiencia al profesor o profesora responsable de la calificación. Si ese procedimiento incluye el nombramiento de un tribunal, el profesor o profesora responsable de la calificación objeto de reclamación no podrá formar parte del mismo.

La resolución se emitirá en un plazo máximo de 15 días desde la fecha de interposición de la reclamación. En todo caso, los procedimientos que puedan establecerse deberán garantizar el derecho del estudiante a matricularse una vez haya sido resuelta la impugnación. Contra las resoluciones de los directores o directoras o decanos o decanas de centro podrá interponerse un recurso de alzada ante el rector o rectora, en el plazo de un mes desde el día siguiente a la notificación de la resolución.

3.3. Seguimiento de los resultados académicos de los estudiantes

Los centros docentes tienen que hacer un seguimiento de los resultados obtenidos por los estudiantes mediante, entre otros indicadores, el parámetro de resultados académicos, que está definido en la Normativa de permanencia. Los resultados de este seguimiento se traducirán en actuaciones orientadas a la mejora del proceso de aprendizaje de los estudiantes.

3.4. Ponderación de los expedientes y cálculo de la calificación final

De acuerdo con los puntos 4.4. y 4.5 del anexo I del Real Decreto 22/2015, de 23 de enero, por el que se establecen los requisitos de expedición del suplemento europeo al título que regula el Real Decreto 1393/2007, y el artículo 5.3 del Real Decreto 1125/2003, por el que se establece el sistema de créditos europeo y el sistema de calificaciones de las titulaciones universitarias de carácter oficial, la ponderación del expediente y el cálculo de la nota global de los titulados y tituladas deberán hacerse mediante el siguiente criterio: suma de los créditos superados por el estudiante, cada uno de ellos multiplicados por el valor de la calificación correspondiente (a partir de las valoraciones del rendimiento de las asignaturas superadas) y dividido por el número de créditos superados.

El resultado se expresará adicionalmente en la escala 0-4, según la tabla de equivalencias:

Suspenso: 0 puntos

Aprobado/apto: 1 punto

Notable: 2 puntos

Sobresaliente: 3 puntos

Matrícula de honor: 4 puntos

Reconocida o convalidada: puntos correspondientes en función de la calificación obtenida en los estudios cursados previamente. Computarán a efectos de la obtención del título y se tendrán en cuenta para el cálculo de la baremación del expediente.

Las materias o asignaturas transferidas no computarán a efectos de la obtención del título y en ningún caso se tendrán en cuenta a efectos de la baremación del expediente.

No incluirán ninguna nota y, por tanto, no se tendrán en cuenta a efectos de la ponderación del expediente:
- los reconocimientos por experiencia laboral y profesional,
- las asignaturas cursadas en enseñanzas universitarias no oficiales (títulos propios), excepto en el caso de que el título propio sea substituido por un título oficial; en ese caso, se conservará la calificación de origen.

9. SISTEMA DE GARANTÍA DE CALIDAD

ENLACE	https://telecos.upc.edu/ca/escola/sistema-de-qualitat/guia-del-pla-de-qualitat

10. CALENDARIO DE IMPLANTACIÓN

10.1 CRONOGRAMA DE IMPLANTACIÓN	
CURSO DE INICIO	2020

Ver Apartado 10: Anexo 1.
10.2 PROCEDIMIENTO DE ADAPTACIÓN
Dado que este máster es de nueva implantación, no procede la adaptación de estudiantes.
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**
52600728G	Josep Rafael	Pegueroles	Vallés
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
C/ Jordi Girona, 1-3 Edificio C3 (308) CAMPUS NORD	08034	Barcelona	Barcelona
EMAIL	**MÓVIL**	**FAX**	**CARGO**
josep.pegueroles@upc.edu	934016832	934016801	Director de l'Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona (ETSETB)
11.2 REPRESENTANTE LEGAL			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
41443276J	Francesc	Torres	Torres
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
C/ Jordi Girona, 31 - Edificio Rectorado	08034	Barcelona	Barcelona
EMAIL	**MÓVIL**	**FAX**	**CARGO**
rector@upc.edu	934016101	934016201	Rector
11.3 SOLICITANTE			
El responsable del título no es el solicitante			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
42994071X	Santiago	Gassó	Domingo
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
C/ Jordi Girona, 31 - Edificio Rectorado	08034	Barcelona	Barcelona
EMAIL	**MÓVIL**	**FAX**	**CARGO**
verifica.upc@upc.edu	934016113	934016201	Vicerrector de Política Académica

Apartado 2: Anexo 1

Nombre :UPC_MU Ciberseguridad_Apart_2_ETSETB_FIB_06052019.pdf

HASH SHA1 :A04B7313C604CDD42383DE0E9BE296203831125C

Código CSV :338953429227157475504195

Ver Fichero: UPC_MU Ciberseguridad_Apart_2_ETSETB_FIB_06052019.pdf

Apartado 4: Anexo 1

Nombre :UPC_MU Ciberseguridad_Apart_4_1_ETSETB_FIB_06052019.pdf

HASH SHA1 :C6E14ECB63C4B7B79CA74380195AFDE56A01A000

Código CSV :338953545759537774123342

Ver Fichero: UPC_MU Ciberseguridad_Apart_4_1_ETSETB_FIB_06052019.pdf

Apartado 5: Anexo 1

Nombre :UPC_MU Ciberseguridad_Apart_5_1_ETSETB_06052019.pdf

HASH SHA1 :2A7DF2CA4B6E4F9AA3DE1AF6DA661CB15B36FABA

Código CSV :338953668470426561352051

Ver Fichero: UPC_MU Ciberseguridad_Apart_5_1_ETSETB_06052019.pdf

Apartado 6: Anexo 1

Nombre :UPC_MU Ciberseguridad_Apart_6_1_ETSETB_06052019.pdf

HASH SHA1 :9BB279D4D8F872342580F5D6E13D9F0A7BE8EF1D

Código CSV :338953789169602116021224

Ver Fichero: UPC_MU Ciberseguridad_Apart_6_1_ETSETB_06052019.pdf

Apartado 6: Anexo 2

Nombre :UPC_MU Ciberseguridad_Apart_6_2_ETSETB_06052019.pdf

HASH SHA1 :14D0F897778DA288069AB35E07A13B8E1FCB3062

Código CSV :338953906869724367690159

Ver Fichero: UPC_MU Ciberseguridad_Apart_6_2_ETSETB_06052019.pdf

Apartado 7: Anexo 1

Nombre :UPC_MU Ciberseguridad_Apart_7_ETSETB_06052019.pdf

HASH SHA1 :CFEA8830CD8A58BFA74BD8EC674F954DE6FC8E2D

Código CSV :338965473178286772272557

Ver Fichero: UPC_MU Ciberseguridad_Apart_7_ETSETB_06052019.pdf

Apartado 8: Anexo 1

Nombre :UPC_MU Ciberseguridad_Apart_8_1_ETSETB_06052019.pdf

HASH SHA1 :4AB119392B329065B6EDAE45A3BAF20ADE97D596

Código CSV :338954138414235325565234

Ver Fichero: UPC_MU Ciberseguridad_Apart_8_1_ETSETB_06052019.pdf

Apartado 10: Anexo 1

Nombre :UPC_MU Ciberseguridad_Apart_10_ETSETB_06052019.pdf

HASH SHA1 :529A52A6251A4AF61ED4FB3D7BD50AEE4DF06D98

Código CSV :338954249247649583106912

Ver Fichero: UPC_MU Ciberseguridad_Apart_10_ETSETB_06052019.pdf