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
Universitat Politècnica de València	Escuela Técnica Superior de Ingeniería Informática	46035653

NIVEL	DENOMINACIÓN CORTA
Máster	Ciberseguridad y Ciberinteligencia

DENOMINACIÓN ESPECÍFICA
Máster Universitario en Ciberseguridad y Ciberinteligencia por la Universitat Politècnica de València

NIVEL MECES
3|3

RAMA DE CONOCIMIENTO	CONJUNTO
Ingeniería y Arquitectura	No

HABILITA PARA EL EJERCICIO DE PROFESIONES REGULADAS	NORMA HABILITACIÓN
No	

SOLICITANTE

NOMBRE Y APELLIDOS	CARGO
SARA BLANC CLAVERO	Directora del Área de Estudios y Ordenación de Títulos
Tipo Documento	**Número Documento**
NIF	22559928X

REPRESENTANTE LEGAL

NOMBRE Y APELLIDOS	CARGO
FRANCISCO MIGUEL BAENA AROCA	Jefe del Servicio de Procesos Electrónicos y Transparencia
Tipo Documento	**Número Documento**
NIF	52748140D

RESPONSABLE DEL TÍTULO

NOMBRE Y APELLIDOS	CARGO
Silvia María Terrasa Barrena	Directora de la Escuela Técnica Superior de Informática
Tipo Documento	**Número Documento**
NIF	25407751L

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
Camino de Vera, s/n	46022	Valencia	963877101
E-MAIL	**PROVINCIA**		**FAX**
veca@upv.es	Valencia/València		963877101

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: Valencia/València, AM 31 de marzo de 2022
	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 y Ciberinteligencia por la Universitat Politècnica de València	No		Ver Apartado 1: Anexo 1.

LISTADO DE ESPECIALIDADES
No existen datos

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

NO HABILITA O ESTÁ VINCULADO CON PROFESIÓN REGULADA ALGUNA

AGENCIA EVALUADORA
Agencia Nacional de Evaluación de la Calidad y Acreditación

UNIVERSIDAD SOLICITANTE
Universitat Politècnica de València

LISTADO DE UNIVERSIDADES	
CÓDIGO	UNIVERSIDAD
027	Universitat Politècnica de València

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
90	0	0
CRÉDITOS OPTATIVOS	**CRÉDITOS OBLIGATORIOS**	**CRÉDITOS TRABAJO FIN GRADO/ MÁSTER**
12	60	18

LISTADO DE ESPECIALIDADES	
ESPECIALIDAD	CRÉDITOS OPTATIVOS
No existen datos	

1.3. Universitat Politècnica de València

1.3.1. CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS	
CÓDIGO	CENTRO
46035653	Escuela Técnica Superior de Ingeniería Informática

1.3.2. Escuela Técnica Superior de Ingeniería Informática

1.3.2.1. Datos asociados al centro

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

PLAZAS DE NUEVO INGRESO OFERTADAS	
PRIMER AÑO IMPLANTACIÓN	SEGUNDO AÑO IMPLANTACIÓN
50	50

	TIEMPO COMPLETO	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	40.1	60.0
RESTO DE AÑOS	40.1	60.0
	TIEMPO PARCIAL	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	18.0	40.0
RESTO DE AÑOS	18.0	40.0
NORMAS DE PERMANENCIA		
http://www.upv.es/orgpeg/normativa/progreso_y_permanencia.pdf		
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

2. JUSTIFICACIÓN, ADECUACIÓN DE LA PROPUESTA Y PROCEDIMIENTOS

Ver Apartado 2: Anexo 1.

3. COMPETENCIAS

3.1 COMPETENCIAS BÁSICAS Y GENERALES
BÁSICAS
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
GENERALES
CG6 - Fomentar el espíritu crítico y emprendedor, el compromiso ético, y desarrollar hábitos de excelencia y calidad en el ejercicio profesional.
CG7 - Emitir juicios en función de criterios, normas externas o de reflexiones personales, en los ámbitos de la ciberseguridad y la ciberinteligencia.
CG8 - Dirigir y coordinar equipos de trabajo para el desarrollo, implantación y mantenimiento de proyectos en los ámbitos de la ciberseguridad y la ciberinteligencia.
3.2 COMPETENCIAS TRANSVERSALES
CT-01 - Comprensión e integración.
CT-02 - Aplicación y pensamiento práctico.
CT-03 - Análisis y resolución de problemas
CT-04 - Innovación, creatividad y emprendimiento.
CT-05 - Diseño y proyecto.
CT-06 - Trabajo en equipo y liderazgo.
CT-07 - Responsabilidad ética, medioambiental y profesional.
CT-08 - Comunicación efectiva.
CT-09 - Pensamiento crítico.
CT-10 - Conocimiento de problemas contemporáneos.
CT-11 - Aprendizaje permanente.
CT-12 - Planificación y gestión del tiempo.
CT-13 - Instrumental específica.
3.3 COMPETENCIAS ESPECÍFICAS
CE01 - Conocer los conceptos y principios de la seguridad informática tanto a nivel defensivo como ofensivo.
CE02 - Gestionar adecuada y eficientemente incidentes de ciberseguridad.
CE03 - Evaluar estándares criptográficos y aplicar los adecuados según las necesidades de las organizaciones.
CE04 - Diseñar mecanismos de privacidad y anonimización de la información.
CE05 - Diseñar y desarrollar software seguro, aplicando buenas prácticas y técnicas adecuadas para la depuración, prueba, verificación y validación de las soluciones desarrolladas.
CE06 - Adaptar las metodologías y estándares de seguridad atendiendo a las plataformas de ejecución disponible.
CE07 - Adoptar técnicas y mecanismos para mejorar la seguridad tanto en sistemas informáticos a como en los servicios desplegados.

CE08 - Analizar y descubrir vulnerabilidades en sistemas reales.
CE09 - Explotar las vulnerabilidades de los sistemas con la finalidad de valorar las capacidades reales de los atacantes.
CE10 - Analizar y diseñar arquitecturas de comunicaciones seguras, en entornos de internet de las cosas.
CE11 - Caracterizar y evaluar mecanismos de seguridad y privacidad por diseño en entornos de internet de las cosas.
CE12 - Aplicar técnicas para la generación de ciberinteligencia, en base a diversas fuentes de información.
CE13 - Detectar anomalías mediante técnicas de análisis masivo de datos e inteligencia artificial.
CE14 - Aplicar estrategias y técnicas para la obtención y preservación de evidencias en incidentes informáticos.
CE15 - Analizar y caracterizar malware con el objetivo de elevar las capacidades de defensa frente a amenazas futuras.
CE16 - Mejorar la gestión de incidentes de ciberseguridad mediante el uso de técnicas y herramientas de ciberconciencia situacional.
CE17 - Aplicar técnicas de ciberinteligencia para la protección de sistemas industriales e infraestructuras críticas.
CE18 - Considerar las normas legales aplicables en el ámbito de la ciberseguridad.
CE19 - Aplicar la deontología profesional, la responsabilidad social y la ética en la resolución de problemas vinculados a la ciberseguridad.
CE20 - Complementar las competencias técnicas con otras transversales abordando aspectos de gestión, certificación profesional, soluciones tecnológicas, desarrollo profesional y tendencias de futuro.
CE21 - Realizar actividades correspondientes a la práctica profesional bajo la supervisión de tutores académicos y profesionales asignados.
TFM - Realización, presentación y defensa, una vez obtenidos todos los créditos del plan de estudios, de un ejercicio original realizado individualmente ante un tribunal universitario, consistente en un proyecto integral de ciberseguridad y/o ciberinteligencia de naturaleza profesional en el que se sinteticen las competencias adquiridas en las enseñanzas.

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

Este máster va dirigido a titulados universitarios que quieran especializarse en el ámbito de la seguridad de los sistemas de información y comunicaciones.

Perfil de acceso

Podrán acceder al Máster, como grados de referencia, los Graduados y Graduadas en Ingeniería Informática y en Ingeniería de Tecnologías y Servicios de Telecomunicación.

También se permitirá el acceso al Máster a los titulados en Ingeniería Telemática, Matemática Computacional y afines si acreditan competencias cercanas a los grados de referencia.

Asímismo, se permitirá el acceso al Máster a quienes estén en posesión del título de Licenciado o Licenciada en Informática, Ingeniero o Ingeniera en Informática, Ingeniero o Ingeniera de Telecomunicaciones, o de cualquier especialidad de Ingeniería Técnica en Informática e Ingeniería Técnica en Telecomunicaciones.

Admisión y criterios de valoración de méritos

Podrán solicitar el ingreso en este máster aquellos candidatos que cumplan con las condiciones que establece el artículo 18 del Real Decreto 822/2021, de 28 de septiembre, por el que se establece la organización de las enseñanzas universitarias y del procedimiento de aseguramiento de su calidad:

1. La posesión de un título universitario oficial de Graduada o Graduado español o equivalente es condición para acceder a un Máster Universitario, o en su caso disponer de otro título de Máster Universitario, o títulos del mismo nivel que el título español de Grado o Máster expedidos por universidades e instituciones de educación superior de un país del EEES que en dicho país permita el acceso a los estudios de Máster.

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

La Comisión Académica del Máster será el órgano encargado de regular la admisión de estudiantes al Máster. El acceso al Máster se regirá por la normativa de la Universitat Politècnica de València para títulos con límite de plazas y será conforme con los criterios generales de selección que la universidad establece.

A esas normas y criterios generales se añaden los criterios de baremo para el caso en que el número de preinscritos supere la oferta de plazas actual.

Los criterios que se valorarán para establecer una lista priorizada de candidatos serán:

- Expediente académico:

La valoración del expediente se expresará en una puntuación en escala de 0 a 10 y se obtendrá de la calificación media del expediente del Grado con el que el solicitante accede al Máster, de conformidad con lo indicado en 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. A efectos de la obtención de la calificación media citada, no se contabilizan los créditos reconocidos sin calificación.

La calificación media de cada expediente se normalizará de acuerdo a las condiciones que regule la UPV, última aprobada en Consejo de Gobierno del 29 de mayo de 2014. El objetivo de la normalización de la calificación media del expediente no es otro que el de asegurar el principio de equidad estableciendo condiciones de comparabilidad de los méritos de los solicitantes.

- Afinidad del perfil del candidato, estudios universitarios previos, con el contenido del máster:

La afinidad del perfil se expresará en una puntuación en escala de 0 a 10 según el coeficiente de adecuación.

Se dará prioridad a aquellos titulados en los grados de referencia o que hayan cursado algún grado en el que hayan podido adquirir unas competencias cercanas a las de los grados de referencia, cuyo coeficiente de adecuación será de 10. Tendrá también el mismo coeficiente de adecuación la Licenciatura en Informática. El resto de grados afines a los grados de referencia, el coeficiente de adecuación será de 8. Para los títulos, en cualquier especialidad, de Ingeniería Técnica en Informática e Ingeniería Técnica en Telecomunicaciones, el coeficiente de adecuación será de 6.

- Currículum vitae (experiencia profesional e investigadora, otros cursos recibidos y otros méritos relacionados con el contenido del máster):

Se valorará el curriculum vitae del solicitante, especialmente en aquellos aspectos que tengan que ver con la experiencia laboral en el ámbito del Máster, la formación continua y el conocimiento de idiomas extranjeros. Los criterios de valoración serán propuestos por la Comisión Académica del Máster y aprobados por la Comisión Académica del Consejo de Gobierno. La valoración se expresará con una puntuación en escala de 0 a 10.

Se recomienda considerar en la valoración final los tres criterios reseñados. Los pesos correspondientes a cada criterio serán:

a) Expediente: 40%

b) Titulación: 50%

c) Currículum vitae: 10%

El procedimiento, criterios y ponderación de la valoración de méritos referidos se harán públicos al inicio del plazo de preinscripción establecido por la ERT.

Todas las solicitudes recibidas serán ordenadas de acuerdo con la puntuación ponderada obtenida. Serán admitidos tantos solicitantes como plazas se oferten, por estricto orden de prelación. En caso de que se produzcan renuncias, y siempre que existan solicitudes en lista de espera, se cubrirán las vacantes hasta completar la oferta de plazas o hasta agotar la lista de espera, siguiendo el orden de prelación anteriormente establecido.

Requisito lingüístico, aprobado por la Comisión Académica del Máster el 30 de abril de 2021

Se utilizará el castellano como lengua vehicular para el proceso formativo de la titulación.

Los alumnos extranjeros que provengan de países en los que el español no sea idioma oficial deberán acreditar el nivel de español a través de títulos oficiales, acreditativos del grado de competencia y dominio del idioma español. En concreto será necesario el diploma que acredite el nivel B2 de Español DELE o certificados de nivel equivalente reconocidos por la Asociación de Centros de Lenguas en la Enseñanza Superior (ACLES) del idioma español.

El Director/a Académico/a del Máster podrá solicitar una entrevista personal para comprobar el nivel de español.

Composición de la Comisión Académica del Título

La Comisión Académica del Máster es el órgano encargado de regular la admisión de estudiantes al máster. La Comisión Académica, tal y como establece la Normativa de Régimen Académico y Evaluación del Alumnado de la UPV en su artículo 4, está compuesta por los siguientes miembros:

- El Director o Directora o Decano o Decana de la Estructura Responsable de Título, que ostentará la presidencia.
- Un Subdirector o Subdirectora o Vicedecano o Vicedecana con competencias en materia académica, que ejercerá la secretaría.
- El Director Académico o la Directora Académica del Título.
- Cuatro profesores y profesoras que, preferentemente, impartan docencia en el título, de diferentes departamentos con docencia en el mismo y que dispongan de, al menos, un tramo docente valorado positivamente. Cuando el número de departamentos implicados en la docencia del título sea superior a cuatro o cuando la Comisión Académica de Título lo sea de variostítulos, el número de profesorado podrá ampliarse hasta un máximo de seis.
- Dos estudiantes.
- El Jefe o la Jefa de los Servicios Administrativos de la Estructura Responsable de Título.
- El Técnico o la Técnica de Gestión Académica.

Admisión para el caso de estudiantes discapacitados

En el caso de estudiantes con necesidades educativas específicas derivadas de la discapacidad, se establecerán los servicios de apoyo y asesoramiento adecuados para evaluar las necesidades de adaptaciones curriculares, itinerario o estudios alternativos a través del apoyo de la fundación CEDAT de la UPV (**http://www.upv.es/entidades/CAD/**). Esta fundación ofrece información y asesoramiento a los miembros de la comunidad universitaria con discapacidad, así como acompañamiento y apoyo en el aula. Presta ayudas técnicas para el estudio a aquellos alumnos que, por sus necesidades educativas especiales, así lo requieren. Promueve y gestiona acciones de formación y empleo para este colectivo dentro y fuera de los campus de la UPV, y presta diferentes servicios desde su Centro Especial de Empleo. Asimismo, realiza proyectos de eliminación de barreras arquitectónicas y urbanísticas, Planes Integrales de Accesibilidad, auditorías en materia de accesibilidad, revisión de proyectos y asesoramiento y diseño de modelos ideales.

4.3 APOYO A ESTUDIANTES

El Plan Integral de Acompañamiento al Estudiante (PIAE+) (**https://piae.blogs.upv.es/**) es un proyecto institucional inmerso en el currículum de todos los cursos de grado, máster y doctorado. Se dirige a todos los estudiantes desde su matriculación en cualquier curso hasta la finalización de sus estu-

dios. Tiene como objetivo favorecer el desarrollo integral en el ámbito académico, personal y social, mediante acciones de orientación, guía y apoyo sistemático. El PIAE+ es un recurso pedagógico ejecutado en coordinación por centros, equipos directivos, profesorado, estudiantes y servicios de la UPV para mejorar los niveles de rendimiento académico, evitar el abandono y estimular la adquisición de las competencias transversales.

El PIAE+ es un plan concebido para escuchar a los estudiantes y ofrecerles apoyo personalizado y acompañamiento a lo largo de toda su trayectoria universitaria. Para los estudios de máster abarca las siguientes acciones en diferentes momentos clave:

- Al iniciar el primer curso, Jornadas de Acogida donde se recibe a los estudiantes, se les presenta la UPV y se les permite interactuar con los distintos servicios que les pueden prestar apoyo durante su recorrido académico.
- De forma planificada durante el desarrollo de los estudios, el PIAE+ proporciona un programa de sesiones informativas y/o formativas, coordinadas con la red de servicios de la UPV. Se planifican de acuerdo con las necesidades detectadas por la dirección del máster en cada etapa del mismo. Algunos ejemplos son: igualdad, deportes, voluntariado, emprendimiento, prácticas en empresa, intercambio internacional, empleo, doctorado, entre otros.
- De forma continua, en cualquier curso, proporciona recursos de apoyo pedagógico específicos para cada máster. Esta acción está dirigida desde el Instituto de Ciencias de la Educación (ICE) con la finalidad de impulsar el rendimiento académico; reforzar valores; estimular el emprendimiento, la innovación y la transferencia, y dotar a los estudiantes de competencias y destrezas suficientes para perfilar un itinerario profesional acorde a sus gustos y preferencias y, también, a las demandas de la sociedad actual.

El Plan Integral de Acompañamiento al Estudiante (PIAE+) reafirma a los estudiantes como objetivo esencial de la UPV, y vela por su formación integral, el desarrollo de su máximo potencial, la excelencia y su incorporación al mercado laboral.

Sistemas de atención presencial y no presencial

La UPV entiende la calidad en la atención a los usuarios como un elemento esencial de la calidad de Sistemas de apoyo y orientación de estudiantes en los servicios que presta, especialmente los orientados al estudiantado. En esta línea en 2014 comenzó el Proyecto QAU! (Qualitat en l¿Atenció als Usuaris). En el marco de este Proyecto y bajo el paraguas de la plataforma UPV [contacT] se ha desarrollado e implantado herramientas que permiten de una manera ágil y eficaz la atención no presencial, así como, si la presencialidad es necesaria, herramientas que proporcionan orden y control en la atención.

A continuación, se expone una breve reseña de estas herramientas y el objeto de cada una de ellas:

- **poli[Consulta].** Herramienta para la gestión telemática de consultas, dudas o aclaraciones. Se encuentra implementada en la totalidad de Escuelas y Facultades de la UPV, así como en la práctica totalidad de las Unidades de gestión. Es accesible tanto desde la página principal de la Web UPV como desde la propia Web de cada Escuela y Facultad o Unidad de gestión. Además, se ha incorporado en las Apps de Alumnado y MiUPV para hacerla más accesible e inmediata. Incluye la utilidad que permite al usuario valorar en el momento la respuesta recibida.

- **poli[SQF].** Herramienta para la gestión telemática de comunicaciones tipo sugerencias, quejas y felicitaciones. Se encuentra implementada en la totalidad de los títulos de grado y máster oficial, en la práctica totalidad de las Unidades de gestión y en los órganos de gobierno unipersonales. Es accesible tanto desde la página principal de la Web UPV como desde la propia Web de cada título oficial, Unidad de gestión u órgano de gobierno unipersonal. Además, se ha incorporado en las Apps de Alumnado y MiUPV. También incluye la utilidad que permite al usuario valorar en el momento la respuesta recibida.
- **Mistral.** Herramienta para la gestión telemática de incidencias relativas a la actividad docente (tanto a nivel de asignatura como de profesorado) al objeto de poder emprender acciones que permitan la resolución de estas. A diferencia de una comunicación SQF, en Mistral es la Delegación de Alumnos de la Escuela o Facultad o la Central de la UPV quien tramita la incidencia, siendo la única que tiene acceso a los datos sobre la identidad del estudiante que ha interpuesto la incidencia. Es accesible desde la Intranet del estudiante.
- **Gregal.** Herramienta para la gestión telemática de incidencias, consultas o solicitudes de carácter informático (tanto Hardware como de Software). Es accesible desde la Intranet de cualquier miembro de la comunidad universitaria. También incluye la utilidad que permite al usuario valorar en el momento la respuesta recibida.
- **poli[Cita].** Herramienta para la solicitud telemática de atención en persona con cita previa (atención presencial o vía la herramienta on-line Teams de Microsoft). Se encuentra implementada en la totalidad de las Escuelas y Facultades de la UPV así como en aquellas Unidades de gestión que por la tipología de servicios que prestan así lo requieren. Es accesible desde la Web de cada Escuela y Facultad o Unidad de gestión que corresponda. Además, se ha incorporado en las Apps de Alumnado y MiUPV. Las citas contemplan tres modalidades de atención: presenciales necesariamente, no presenciales, y elegibles, en las que el usuario decide el modo de atención.
- **Tutoría bajo demanda.** Herramienta para la solicitud telemática de atención en persona a través de cita previa con el profesorado (atención presencial o vía la herramienta on-line Teams de Microsoft). Es accesible desde la Intranet del estudiante y la página Web de cada asignatura-profesor/a.

Paralelamente a las anteriores herramientas, existen en las Webs de todas las Escuelas y Facultades, sus títulos oficiales y Unidades de gestión de la UPV el apartado ¿Contacto¿, en el que se especifican los medios tradicionales: teléfono o teléfonos de contacto y correo institucional de la entidad correspondiente. También el WhatsApp centralizado +34 620 04 00 50.

Apoyo Técnico a la docencia en laboratorios no presenciales del máster Universitario en Ciberseguridad y Ciberinteligencia

La universidad cuenta entre otros recursos tecnológicos para la docencia, con los laboratorios virtuales Polilabs (https://polilabs.upv.es/uds/page/login), que es el servicio de la UPV que permite conectar desde cualquier dispositivo (Windows, Linux, MacOS, IOS y Android) a un escritorio o aplicación virtual. Entre los escritorios virtuales disponibles, se encuentran los ofrecidos por el Departamento de Sistemas Informáticos y Computación (DSIC-LINUX y DSIC-WINDOWS), los ofrecidos por la ETSINF (ETSINF LINUX y ETSINF WINDOWS), así como los escritorios Aula Gráfica 1 y Aula Gráfica 2, que incluyen las herramientas y soporte necesario para el trabajo de los alumnos en las asignaturas del máster. Por ejemplo, los escritorios virtuales DSIC-LINUX y DSIC-WINDOWS son equivalentes a las instalaciones Linux y Windows de los laboratorios docentes del DSIC. El servicio de acceso remoto se presta a todo el personal del DSIC y al alumnado de las asignaturas cuyas prácticas están asignadas a los laboratorios docentes del DSIC, así como al alumnado de otras asignaturas que hayan sido expresamente autorizadas por parte de la dirección del departamento previa solicitud del profesorado.

Asimismo, en otros casos los alumnos pueden acceder a trabajar tanto con software online (bien alojado en los servidores de UPV, bien en plataformas de terceros) vía navegador, como descargando programas para utilizarlos en sus propios ordenadores en modo remoto.

En ambos casos, además de contar con manuales multimedia, se realizan sesiones introductorias en las que el profesor ayuda al alumnado a utilizar o instalar las aplicaciones necesarias, incluso si tiene problemas de conectividad, puesto que el software descargado lo puede utilizar en modo offline.

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	13,5

Adjuntar Título Propio

Ver Apartado 4: Anexo 2.

Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional	
MÍNIMO	**MÁXIMO**
0	13,5

Los criterios para el reconocimiento y transferencia de créditos vienen regulados y establecidos en la Normativa para el Reconocimiento y Transferencia de Créditos en Títulos Oficiales de Grado y Máster de la Universitat Politècnica de València. Dicha normativa es accesible en el siguiente enlace:

NORMATIVA PARA EL RECONOCIMIENTO Y TRANSFERENCIA DE CRÉDITOS EN TÍTULOS OFICIALES DE GRADO Y MÁSTER DE LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA, aprobada por el Consejo de Gobierno de 23 de diciembre de 2021: **http://www.upv.es/orgpeg/normativa/reconocimiento_creditos.pdf**

4.6 COMPLEMENTOS FORMATIVOS

No procede.

5. PLANIFICACIÓN DE LAS ENSEÑANZAS

5.1 DESCRIPCIÓN DEL PLAN DE ESTUDIOS
Ver Apartado 5: Anexo 1.
5.2 ACTIVIDADES FORMATIVAS
Práctica Laboratorio
Teoría Aula
Teoría Seminario
Tutorización
Actividades de Trabajo Autónomo
5.3 METODOLOGÍAS DOCENTES
Seminarios
Tutorías individuales
Aprendizaje autónomo
Clase magistral
Trabajo en grupo
Aprendizaje basado en problemas.
Estudio de casos
Aprendizaje basado en proyectos.
Resolución de ejercicios y problemas.
Laboratorio
Supervisión
Actividades de evaluación
Trabajos prácticos
Estudio práctico
Actividades complementarias
Trabajos teóricos
Otras metodologías: Docencia inversa
5.4 SISTEMAS DE EVALUACIÓN
Examen oral
Prueba escrita de respuesta abierta
Pruebas objetivas (tipo test)
Trabajo académico
Portafolio
Proyecto
Caso
Observación
Coevaluación
Memoria escrita
Defensa pública del trabajo con tribunal
5.5 NIVEL 1: Módulo Materias Comunes
5.5.1 Datos Básicos del Nivel 1
NIVEL 2: Materia Seguridad de los Sistemas de Información
5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria

ECTS NIVEL 2	12	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
12		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		

5.5.1.2 RESULTADOS DE APRENDIZAJE

5.5.1.3 CONTENIDOS

La materia introduce el marco general de la ciberseguridad, partiendo de la caracterización de las vulnerabilidades, las amenazas y los incidentes de ciberseguridad; se introducen los principios de la gestión de ciberincidentes y del análisis de riesgos, con lo que el alumno obtiene una visión completa del ciclo de vida de la ciberseguridad y se le capacita para definir un plan de ciberseguridad para una organización, incluyendo el análisis de riesgos y la veneración de planes de contigencia.

Para trabajar las competencias CE1 y CE2, se partirá del análisis de incidentes de seguridad en sistemas informáticos reales para identificar las vulnerabilidades existentes en los mismos, los riesgos que éstas comportan y las tendencias actuales en materia de ciberataque. Para ello se valorarán las fuentes abiertas que ofrecen información relativa a las vulnerabilidades de los sistemas de información y a su explotación. Una vez definidos y estudiados los conceptos básicos como vulnerabilidad o incidente de seguridad, se abordará cómo gestionar de forma adecuada y eficientemente incidentes de ciberseguridad en todas las fases del ciclo de vida del incidente, incluyendo las Amenazas Permanentes Avanzadas.

Para trabajar las competencias CE3 y CE4, se abordará la evaluación de estándares criptográficos para el cifrado, el mantenimiento de la integridad de los datos, así como para la autenticación de los participantes en una comunicación. La evaluación considerará las técnicas de criptoanálisis aplicables en cada caso (análisis diferencial para el cifrado por bloques, resolución del problema del logaritmo discreto o la factorización de enteros en sistemas de cifrado de clave asimétrica¿). También se abordará las técnicas criptográficas y de criptoanálisis basadas en computación cuántica.

En la materia se estudiarán técnicas para preservar la confidencialidad, integridad, disponibilidad y no repudio de la información, así como los protocolos de autenticación para el acceso a los datos. También se abordará la seguridad y privacidad en los sistemas de información, estudiando la configuración de mecanismos de seguridad, el diseño e interpretación de consultas, el desarrollo de algoritmos de análisis de información y la integración de técnicas de privacidad, anonimización y trazabilidad de datos.

5.5.1.4 OBSERVACIONES

La evaluación de las materias deberá asegurar la adquisición de las competencias específicas y generales. Se potenciará la evaluación de los conocimientos a través de la participación activa del estudiante, la evaluación de trabajos académicos, casos prácticos, proyectos y prácticas de laboratorio, realizados de manera individual o en grupo. Como criterio general las asignaturas se ajustarán al siguiente esquema de evaluación:

Los porcentajes mínimo y máximo que pueden sumar las siguientes pruebas son 0% y 40%

1. Examen oral

2. Prueba escrita de respuesta abierta

3. Pruebas objetivas de tipo test

Los porcentajes mínimo y máximo que pueden sumar las siguientes pruebas son 40% y 80%

1. Trabajo académico

2. Proyecto

3. Caso

Los porcentajes mínimo y máximo que pueden sumar las siguientes pruebas son 10% y 20%

1. Portafolio

2. Observación

3. Coevaluación

Así vemos que, los porcentajes arriba señalados aseguran que, ninguna asignatura evaluará los contenidos teóricos impartido en TA por encima de un 40%. Que las actividades prácticas realizadas en teoría de seminario y laboratorio de prácticas se valorarán, al menos con un 40%. Y que todas las asignaturas realizarán un seguimiento individual del alumnado mediante con un peso no inferior al 10%.

Se seguirá la metodología docente definida por el National Institute of Standars and Technology, recogida en el documento "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework". Esta metodología está reconocida a nivel internacional como un estándar de facto para la formación y la elaboración de currículo en el campo de la ciberseguridad.

Los objetivos de la metodología serían, entre otros:

- Identificar requisitos de cualificación y entrenamiento para desarrollar los conocimientos, competencias y habilidades fundamentales en el ámbito de la ciberseguridad.
- Clasificar y hacer seguimiento de las capacidades del personal técnico dedicado a la ciberseguridad, en base a sus conocimientos, competencias y habilidades.
- Identificar los roles de trabajo más relevantes y definir carreras profesionales en base a sus conocimientos, competencias y habilidades.

Las guías docentes de las asignaturas que conforman la materia detallarán las metodologías docentes y sistemas de evaluación que se utilizarán durante el curso, con los pesos exactos para cada acto de evaluación. Antes del comienzo del curso académico, la Comisión Académica del Máster aprobará el contenido de las guías docentes.

5.5.1.5 COMPETENCIAS
5.5.1.5.1 BÁSICAS Y GENERALES
CG6 - Fomentar el espíritu crítico y emprendedor, el compromiso ético, y desarrollar hábitos de excelencia y calidad en el ejercicio profesional.
CG7 - Emitir juicios en función de criterios, normas externas o de reflexiones personales, en los ámbitos de la ciberseguridad y la ciberinteligencia.
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
CT-02 - Aplicación y pensamiento práctico.
CT-03 - Análisis y resolución de problemas
CT-08 - Comunicación efectiva.
CT-11 - Aprendizaje permanente.
CT-13 - Instrumental específica.
5.5.1.5.3 ESPECÍFICAS
CE01 - Conocer los conceptos y principios de la seguridad informática tanto a nivel defensivo como ofensivo.
CE02 - Gestionar adecuada y eficientemente incidentes de ciberseguridad.
CE03 - Evaluar estándares criptográficos y aplicar los adecuados según las necesidades de las organizaciones.
CE04 - Diseñar mecanismos de privacidad y anonimización de la información.

5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Práctica Laboratorio	30	25
Teoría Aula	30	25
Teoría Seminario	60	75
Actividades de Trabajo Autónomo	210	0
5.5.1.7 METODOLOGÍAS DOCENTES		
Seminarios		
Tutorías individuales		
Aprendizaje autónomo		
Clase magistral		
Trabajo en grupo		
Aprendizaje basado en problemas.		
Estudio de casos		
Aprendizaje basado en proyectos.		
Resolución de ejercicios y problemas.		
Laboratorio		
Supervisión		
Actividades de evaluación		
Trabajos prácticos		
Estudio práctico		
Actividades complementarias		
Otras metodologías: Docencia inversa		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Examen oral	0.0	40.0
Prueba escrita de respuesta abierta	0.0	40.0
Pruebas objetivas (tipo test)	0.0	40.0
Trabajo académico	0.0	80.0
Portafolio	0.0	20.0
Proyecto	0.0	80.0
Caso	0.0	80.0
Observación	0.0	20.0
Coevaluación	0.0	20.0
NIVEL 2: Materia Ciberseguridad		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	21	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
10,5	10,5	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**

ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

5.5.1.3 CONTENIDOS

La materia incluye tres aspectos básicos de las modernas técnicas de ciberseguridad, de forma aplicada hacia el ¿saber hacer¿, como son el desarrollo seguro de software y hardware, las técnicas de penetración para poner a prueba y mejorar los sistemas propios, y la protección de los sistemas posiblemente más sensibles en la vida cotidiana de los ciudadanos en los próximos años como son los sistemas IoT.

Para trabajar las competencias CE5, CE6 y CE7, se abordará los principios y buenas prácticas para el desarrollo seguro de código, incluyendo la programación defensiva, así como técnicas adecuadas para la depuración, verificación, validación, evaluación y mitigación de riesgos en las soluciones desarrolladas. Se estudiará cómo adaptar y/o aplicar las metodologías y estándares necesarios para garantizar la seguridad de las soluciones independientemente de las características de cada tipo de aplicación (hardware, web, móvil, servicio en la nube, etc.) y/o plataforma de ejecución disponible.

Del mismo modo, se expondrán las técnicas para mejorar la seguridad en sistemas informáticos a todos los niveles, con objeto de aplicar los mecanismos y buenas prácticas de seguridad para el despliegue operacional de servicios, incluyendo en su caso la gestión segura y trazabilidad del acceso.

Para trabajar las competencias CE8 y CE9, se parte de pruebas de penetración o "pentesting" que son auditorías de seguridad realizadas siguiendo estrategias de ataque similares a las empleadas por los atacantes. Se estudia la seguridad desde el punto de vista del atacante, aprendiendo a identificar los potenciales vectores de ataque, buscar en repositorios de vulnerabilidades, herramientas de escaneado y enumeración, así como los tipos de fallos más comunes en cada sistema. El estudiante adquirirá las habilidades para integrarse en un ¿red team¿. Para poder valorar correctamente el peligro que representan las vulnerabilidades es necesario conocer las capacidades ofensivas de los atacantes. El riesgo de un fallo no depende del tipo de fallo sino de lo que un atacante es capaz de hacer con él. Se estudian las principales técnicas de desarrollo de ¿exploits¿. El alumno será capaz de desarrollar varios tipos de exploits: shell reverso, inyección de comandos, etc.

Las competencias CE10 y CE11 se trabajan a través de una de las aplicaciones más críticas de la ciberseguridad es la protección de sistemas IoT (Internet de las cosas). En la materia se introducirá el concepto de ¿Seguridad de las cosas¿ como aglutinador de las comunicaciones seguras en Internet, incluyendo los mecanismos y protocolos para la implementación de arquitecturas de comunicaciones seguras, así como el modelado y diseño de arquitecturas de seguridad y privacidad, en entornos de IoT.

En la materia se definirán los principios de seguridad, privacidad y confianza, considerando los principales riesgos, vulnerabilidades y ataques a los diferentes componentes que integran los despliegues en el marco de Internet de las Cosas. Se definirán los mecanismos de protección en los dispositivos embebidos, la infraestructura de comunicaciones en todos los niveles incluidas las inalámbricas, la interoperabilidad, el almacenamiento y el tratamiento de la información. Se tendrá en cuenta la regulación y normativa, así como los diferentes estándares existentes. Adicionalmente se describirá y considerará la reducida capacidad de los dispositivos y componentes de Internet de las cosas, para particularizar las soluciones de ciberseguridad a las limitaciones inherentes de este tipo de entornos.

5.5.1.4 OBSERVACIONES

La evaluación de las materias deberá asegurar la adquisición de las competencias específicas y generales. Se potenciará la evaluación de los conocimientos a través de la participación activa del estudiante, la evaluación de trabajos académicos, casos prácticos, proyectos y prácticas de laboratorio, realizados de manera individual o en grupo. Como criterio general las asignaturas se ajustarán al siguiente esquema de evaluación:

Los porcentajes mínimo y máximo que pueden sumar las siguientes pruebas son 0% y 40%

1. Examen oral

2. Prueba escrita de respuesta abierta

3. Pruebas objetivas de tipo test

Los porcentajes mínimo y máximo que pueden sumar las siguientes pruebas son 40% y 80%

1. Trabajo académico

2. Proyecto

3. Caso

Los porcentajes mínimo y máximo que pueden sumar las siguientes pruebas son 10% y 20%

1. Portafolio

2. Observación

3. Coevaluación

Así vemos que, los porcentajes arriba señalados aseguran que, ninguna asignatura evaluará los contenidos teóricos impartido en TA por encima de un 40%. Que las actividades prácticas realizadas en teoría de seminario y laboratorio de prácticas se valorarán, al menos con un 40%. Y que todas las asignaturas realizarán un seguimiento individual del alumnado mediante con un peso no inferior al 10%.

Se seguirá la metodología docente definida por el National Institute of Standars and Technology, recogida en el documento "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework". Esta metodología está reconocida a nivel internacional como un estándar de facto para la formación y la elaboración de currículo en el campo de la ciberseguridad.

Los objetivos de la metodología serían, entre otros:

- Identificar requisitos de cualificación y entrenamiento para desarrollar los conocimientos, competencias y habilidades fundamentales en el ámbito de la ciberseguridad.
- Clasificar y hacer seguimiento de las capacidades del personal técnico dedicado a la ciberseguridad, en base a sus conocimientos, competencias y habilidades.
- Identificar los roles de trabajo más relevantes y definir carreras profesionales en base a sus conocimientos, competencias y habilidades.

Las guías docentes de las asignaturas que conforman la materia detallarán las metodologías docentes y sistemas de evaluación que se utilizarán durante el curso, con los pesos exactos para cada acto de evaluación. Antes del comienzo del curso académico, la Comisión Académica del Máster aprobará el contenido de las guías docentes.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG6 - Fomentar el espíritu crítico y emprendedor, el compromiso ético, y desarrollar hábitos de excelencia y calidad en el ejercicio profesional.

CG8 - Dirigir y coordinar equipos de trabajo para el desarrollo, implantación y mantenimiento de proyectos en los ámbitos de la ciberseguridad y la ciberinteligencia.

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

CT-01 - Comprensión e integración.

CT-04 - Innovación, creatividad y emprendimiento.

CT-05 - Diseño y proyecto.

CT-06 - Trabajo en equipo y liderazgo.

CT-07 - Responsabilidad ética, medioambiental y profesional.

CT-10 - Conocimiento de problemas contemporáneos.

CT-12 - Planificación y gestión del tiempo.

5.5.1.5.3 ESPECÍFICAS

CE05 - Diseñar y desarrollar software seguro, aplicando buenas prácticas y técnicas adecuadas para la depuración, prueba, verificación y validación de las soluciones desarrolladas.

CE06 - Adaptar las metodologías y estándares de seguridad atendiendo a las plataformas de ejecución disponible.		
CE07 - Adoptar técnicas y mecanismos para mejorar la seguridad tanto en sistemas informáticos a como en los servicios desplegados.		
CE08 - Analizar y descubrir vulnerabilidades en sistemas reales.		
CE09 - Explotar las vulnerabilidades de los sistemas con la finalidad de valorar las capacidades reales de los atacantes.		
CE10 - Analizar y diseñar arquitecturas de comunicaciones seguras, en entornos de internet de las cosas.		
CE11 - Caracterizar y evaluar mecanismos de seguridad y privacidad por diseño en entornos de internet de las cosas.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Práctica Laboratorio	60	25
Teoría Aula	60	75
Teoría Seminario	90	50
Actividades de Trabajo Autónomo	367.5	0
5.5.1.7 METODOLOGÍAS DOCENTES		
Seminarios		
Tutorías individuales		
Aprendizaje autónomo		
Clase magistral		
Trabajo en grupo		
Aprendizaje basado en problemas.		
Estudio de casos		
Aprendizaje basado en proyectos.		
Resolución de ejercicios y problemas.		
Laboratorio		
Supervisión		
Actividades de evaluación		
Trabajos prácticos		
Estudio práctico		
Actividades complementarias		
Otras metodologías: Docencia inversa		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Examen oral	0.0	40.0
Prueba escrita de respuesta abierta	0.0	40.0
Pruebas objetivas (tipo test)	0.0	40.0
Trabajo académico	0.0	80.0
Portafolio	0.0	20.0
Proyecto	0.0	80.0
Caso	0.0	80.0
Observación	0.0	20.0
Coevaluación	0.0	20.0
NIVEL 2: Materia Ciberinteligencia		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	

ECTS NIVEL 2	18	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	18	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		

5.5.1.2 RESULTADOS DE APRENDIZAJE

5.5.1.3 CONTENIDOS

La materia aborda visión más actual dentro de la ciberseguridad, que podría denominarse ciberseguridad proactiva o ciberinteligencia. También denominada inteligencia de amenazas, la ciberinteligencia se basa en el conocimiento previo de la amenaza antes de que suceda el incidente de ciberseguridad. Este conocimiento previo permite una mejor gestión del incidente, una mejor contención del mismo y la limitación en los daños que pueda producir.

Para trabajar las competencias CE12 y CE13, la materia incluye el análisis de las distintas fuentes de información para la generación de ciberinteligencia. Para ello se describirán las técnicas de ciberinteligencia basadas en fuentes humanas (HUMINT), en fuentes abiertas (OSINT), en la monitorización de los sistemas (SIGINT) y en el análisis de artefactos (TECHINT). También se abordarán técnicas para el análisis masivo de datos, junto con distintas aproximaciones al ¿Machine Learning¿ para la generación de ciberinteligencia, permitiendo la detección de anomalías y firmas de ataques en los sistemas, así como la identificación de contenidos o eventos falsos o maliciosos, aplicando estas técnicas a la generación de ciberinteligencia HUMINT, OSINT y SIGINT.

Para trabajar las competencias CE14 y CE15, en la materia se cubrirán todos los aspectos técnicos del peritaje informático: estrategias para extraer la información relevante (tanto del sistema en caliente como de medios de almacenamiento permanente); herramientas de recopilación de indicios y evidencias; mantenimiento de la cadena de custodia; análisis y clasificación de pruebas; generación de informes y comunicación efectiva con las fuerzas y cuerpos de seguridad y agentes judiciales.

Adicionalmente se abordará el análisis concreto de muestras de malware. En muchas ocasiones, los ataques tienen éxito porque el malware ha sido capaz de burlar los sistemas de defensa. Es necesario analizar y caracterizar el funcionamiento de este para mejorar o desarrollar nuevos sistemas de defensa contra posteriores ataques. Por otra parte, el conocimiento detallado del modus operandi del malware es necesario para elaborar ciberinteligencia. Para ello, se aprenderá a hacer análisis estático (ingeniería inversa) y análisis dinámico en entornos controlados; también se estudiarán las principales técnicas anti-análisis usadas por los atacantes.

Para trabajar las CE16 y CE17, en la materia se introducirá el concepto y las aplicaciones de ciberconciencia situacional como herramientas avanzadas fundamentales para mejorar el proceso de toma de decisiones en la gestión de incidentes de cibeseguridad. Se hará especial hincapié en la fusión de ciberinteligencia de distintas fuentes y en las técnicas de visualización.

Se introducirá también el concepto de conciencia situacional híbrida, aplicable en aquellos sistemas en que los ciberincidentes tienen efectos sobre el mundo físico, como es el caso de los sistemas industriales y las infraestructuras críticas. Para ello se identificarán las vulnerabilidades específicas de los sistemas ciber-físicos en entornos industriales y en infraestructuras críticas. Por último, se aplicarán herramientas de ciberconciencia situacional en la protección de estos sistemas.

5.5.1.4 OBSERVACIONES

La evaluación de las materias deberá asegurar la adquisición de las competencias específicas y generales. Se potenciará la evaluación de los conocimientos a través de la participación activa del estudiante, la evaluación de trabajos académicos, casos prácticos, proyectos y prácticas de laboratorio, realizados de manera individual o en grupo. Como criterio general las asignaturas se ajustarán al siguiente esquema de evaluación:

Los porcentajes mínimo y máximo que pueden sumar las siguientes pruebas son 0% y 40%

1. Examen oral

2. Prueba escrita de respuesta abierta

3. Pruebas objetivas de tipo test

Los porcentajes mínimo y máximo que pueden sumar las siguientes pruebas son 40% y 80%

1. Trabajo académico

2. Proyecto

3. Caso

Los porcentajes mínimo y máximo que pueden sumar las siguientes pruebas son 10% y 20%

1. Portafolio

2. Observación

3. Coevaluación

Así vemos que, los porcentajes arriba señalados aseguran que, ninguna asignatura evaluará los contenidos teóricos impartido en TA por encima de un 40%. Que las actividades prácticas realizadas en teoría de seminario y laboratorio de prácticas se valorarán, al menos con un 40%. Y que todas las asignaturas realizarán un seguimiento individual del alumnado mediante con un peso no inferior al 10%.

Se seguirá la metodología docente definida por el National Institute of Standars and Technology, recogida en el documento "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework". Esta metodología está reconocida a nivel internacional como un estándar de facto para la formación y la elaboración de currículo en el campo de la ciberseguridad.

Los objetivos de la metodología serían, entre otros:

- Identificar requisitos de cualificación y entrenamiento para desarrollar los conocimientos, competencias y habilidades fundamentales en el ámbito de la ciberseguridad.
- Clasificar y hacer seguimiento de las capacidades del personal técnico dedicado a la ciberseguridad, en base a sus conocimientos, competencias y habilidades.
- Identificar los roles de trabajo más relevantes y definir carreras profesionales en base a sus conocimientos, competencias y habilidades.

Las guías docentes de las asignaturas que conforman la materia detallarán las metodologías docentes y sistemas de evaluación que se utilizarán durante el curso, con los pesos exactos para cada acto de evaluación. Antes del comienzo del curso académico, la Comisión Académica del Máster aprobará el contenido de las guías docentes.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG7 - Emitir juicios en función de criterios, normas externas o de reflexiones personales, en los ámbitos de la ciberseguridad y la ciberinteligencia.

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
CT-02 - Aplicación y pensamiento práctico.
CT-03 - Análisis y resolución de problemas
CT-05 - Diseño y proyecto.
CT-08 - Comunicación efectiva.
CT-09 - Pensamiento crítico.
CT-10 - Conocimiento de problemas contemporáneos.
CT-11 - Aprendizaje permanente.
CT-13 - Instrumental específica.
5.5.1.5.3 ESPECÍFICAS
CE12 - Aplicar técnicas para la generación de ciberinteligencia, en base a diversas fuentes de información.
CE13 - Detectar anomalías mediante técnicas de análisis masivo de datos e inteligencia artificial.
CE14 - Aplicar estrategias y técnicas para la obtención y preservación de evidencias en incidentes informáticos.
CE15 - Analizar y caracterizar malware con el objetivo de elevar las capacidades de defensa frente a amenazas futuras.
CE16 - Mejorar la gestión de incidentes de ciberseguridad mediante el uso de técnicas y herramientas de ciberconciencia situacional.
CE17 - Aplicar técnicas de ciberinteligencia para la protección de sistemas industriales e infraestructuras críticas.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Práctica Laboratorio	45	50
Teoría Aula	45	50
Teoría Seminario	90	50
Actividades de Trabajo Autónomo	315	0

5.5.1.7 METODOLOGÍAS DOCENTES
Seminarios
Tutorías individuales
Aprendizaje autónomo
Clase magistral
Trabajo en grupo
Aprendizaje basado en problemas.
Estudio de casos
Aprendizaje basado en proyectos.
Resolución de ejercicios y problemas.
Laboratorio
Supervisión
Actividades de evaluación

Trabajos prácticos		
Estudio práctico		
Actividades complementarias		
Otras metodologías: Docencia inversa		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Examen oral	0.0	40.0
Prueba escrita de respuesta abierta	0.0	40.0
Pruebas objetivas (tipo test)	0.0	40.0
Trabajo académico	0.0	80.0
Portafolio	0.0	20.0
Proyecto	0.0	80.0
Caso	0.0	80.0
Observación	0.0	20.0
Coevaluación	0.0	20.0
NIVEL 2: Materia Aspectos Legales y Profesionales		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	9	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
7,5	1,5	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
5.5.1.3 CONTENIDOS		

La materia aborda aspectos más allá de lo estrictamente tecnológico, necesarios desde el punto de vista ético y legal. Partiendo de los principios básicos éticos y deontológicos de la aplicación de las técnicas de ciberseguridad y ciberinteligencia, se introduce la normativa legal fundamental en el ámbito de la ciberseguridad. La propia naturaleza del ciberespacio, muchas veces comparado con un espacio nuevo, vacío, susceptible de ser colonizado al margen de las normas, requiere la adecuada reglamentación, y lo que es más importante, la aplicación de principios éticos y deontológicos.

Para trabajar las competencias CE18 y CE19, en la materia se abordan aspectos de la ciberseguridad vinculados al marco legal de la misma, en particular en lo que respecta a privacidad e identificación, como en lo relativo a infraestructuras críticas y medidas conducentes a elevar el nivel de la ciberseguridad (entre otras, directiva NIS, Esquema Nacional de Seguridad). Se considerarán los aspectos de interés para la presentación de un dictamen pericial ante los tribunales de justicia (destacando la Ley de Enjuiciamiento Civil y normativa UNE).

Asimismo, se revisarán los planteamientos deontológicos más relevantes desde el esquema clásico de las cinco dimensiones de la sociedad de la información (derechos y obligaciones de la información, derechos y obligaciones de propiedad, responsabilidad formal y control, calidad del sistema y calidad de vida), adaptándolas y focalizándolas al campo de la ciberseguridad.

Por último, mediante seminarios impartidos por profesionales de la ciberseguridad, todos ellos especialistas de primer nivel en sus materias, se pretende transmitir a los alumnos ¿la realidad del día al día¿ en un campo tan nuevo como trascendente.

Además, se complementarán las competencias técnicas del alumno con otras transversales abordando aspectos de gestión, certificación profesional, soluciones tecnológicas, desarrollo profesional y tendencias de futuro.

5.5.1.4 OBSERVACIONES

La evaluación de las materias deberá asegurar la adquisición de las competencias específicas y generales. Se potenciará la evaluación de los conocimientos a través de la participación activa del estudiante, la evaluación de trabajos académicos, casos prácticos, proyectos y prácticas de laboratorio, realizados de manera individual o en grupo. Como criterio general las asignaturas se ajustarán al siguiente esquema de evaluación:

Los porcentajes mínimo y máximo que pueden sumar las siguientes pruebas son 0% y 40%

1. Examen oral

2. Prueba escrita de respuesta abierta

3. Pruebas objetivas de tipo test

Los porcentajes mínimo y máximo que pueden sumar las siguientes pruebas son 40% y 80%

1. Trabajo académico

2. Proyecto

3. Caso

Los porcentajes mínimo y máximo que pueden sumar las siguientes pruebas son 10% y 20%

1. Portafolio

2. Observación

3. Coevaluación

Así vemos que, los porcentajes arriba señalados aseguran que, ninguna asignatura evaluará los contenidos teóricos impartido en TA por encima de un 40%. Que las actividades prácticas realizadas en teoría de seminario y laboratorio de prácticas se valorarán, al menos con un 40%. Y que todas las asignaturas realizarán un seguimiento individual del alumnado mediante con un peso no inferior al 10%.

Se seguirá la metodología docente definida por el National Institute of Standars and Technology, recogida en el documento "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework". Esta metodología está reconocida a nivel internacional como un estándar de facto para la formación y la elaboración de currículo en el campo de la ciberseguridad.

Los objetivos de la metodología serían, entre otros:

- Identificar requisitos de cualificación y entrenamiento para desarrollar los conocimientos, competencias y habilidades fundamentales en el ámbito de la ciberseguridad.
- Clasificar y hacer seguimiento de las capacidades del personal técnico dedicado a la ciberseguridad, en base a sus conocimientos, competencias y habilidades.
- Identificar los roles de trabajo más relevantes y definir carreras profesionales en base a sus conocimientos, competencias y habilidades.

Las guías docentes de las asignaturas que conforman la materia detallarán las metodologías docentes y sistemas de evaluación que se utilizarán durante el curso, con los pesos exactos para cada acto de evaluación. Antes del comienzo del curso académico, la Comisión Académica del Máster aprobará el contenido de las guías docentes.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG6 - Fomentar el espíritu crítico y emprendedor, el compromiso ético, y desarrollar hábitos de excelencia y calidad en el ejercicio profesional.

CG7 - Emitir juicios en función de criterios, normas externas o de reflexiones personales, en los ámbitos de la ciberseguridad y la ciberinteligencia.

CG8 - Dirigir y coordinar equipos de trabajo para el desarrollo, implantación y mantenimiento de proyectos en los ámbitos de la ciberseguridad y la ciberinteligencia.

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
CT-06 - Trabajo en equipo y liderazgo.
CT-07 - Responsabilidad ética, medioambiental y profesional.
CT-09 - Pensamiento crítico.
CT-10 - Conocimiento de problemas contemporáneos.
CT-11 - Aprendizaje permanente.
5.5.1.5.3 ESPECÍFICAS
CE18 - Considerar las normas legales aplicables en el ámbito de la ciberseguridad.
CE19 - Aplicar la deontología profesional, la responsabilidad social y la ética en la resolución de problemas vinculados a la ciberseguridad.
CE20 - Complementar las competencias técnicas con otras transversales abordando aspectos de gestión, certificación profesional, soluciones tecnológicas, desarrollo profesional y tendencias de futuro.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Práctica Laboratorio	15	100
Teoría Aula	30	25
Teoría Seminario	45	50
Actividades de Trabajo Autónomo	157.5	0

5.5.1.7 METODOLOGÍAS DOCENTES
Seminarios
Tutorías individuales
Aprendizaje autónomo
Clase magistral
Trabajo en grupo
Aprendizaje basado en problemas.
Estudio de casos
Aprendizaje basado en proyectos.
Resolución de ejercicios y problemas.
Laboratorio
Supervisión
Actividades de evaluación
Trabajos prácticos
Estudio práctico
Actividades complementarias
Otras metodologías: Docencia inversa

5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Examen oral	0.0	40.0
Prueba escrita de respuesta abierta	0.0	40.0
Pruebas objetivas (tipo test)	0.0	40.0
Trabajo académico	0.0	80.0
Portafolio	0.0	20.0
Proyecto	0.0	80.0
Caso	0.0	80.0
Observación	0.0	20.0
Coevaluación	0.0	20.0

5.5 NIVEL 1: Modulo Desarrollo Profesional		
5.5.1 Datos Básicos del Nivel 1		
NIVEL 2: Materia Desarrollo Profesional		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
ECTS NIVEL 2	12	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
		12
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
5.5.1.3 CONTENIDOS		

El estudiantado tendrá la posibilidad de obtener los créditos correspondientes a esta materia o, bien con prácticas en empresas, o bien en su totalidad o complementar con créditos en alguna de las asignaturas que se propondrán para esta materia. La oferta de asignaturas podrá contemplar, entre otras:

- *Trabajo de especialización profesional*: En esta asignatura el estudiante podrá llevar a cabo trabajos en temas específicos en el ámbito de la Ciberseguridad y Ciberinteligencia que le permitirán especializarse en aspectos y tecnologías concretas.

- *Soft skills*: Esta asignatura permitirá al estudiante profundizar en el desarrollo de aptitudes y habilidades de carácter interpersonal o sociales. Se abordarán principalmente los siguientes aspectos: los distintos tipos de "soft skills", los tipos de inteligencia, los aspectos y claves para el desarrollo personal, la marca personal, la persona en el mundo laboral, el trabajo en equipo, liderazgo y motivación, comunicación.

- *Seminarios de especialización*: Esta asignatura tendrá como objetivo acercar la realidad de la profesión y profundizar en algunos temas específicos a los que no se ha dado cobertura en algunas asignaturas, se organizarán seminarios y charlas llevadas a cabo por expertos, empresas e instituciones. El estudiante podrá conocer, entre otros aspectos, modelos de negocio, soluciones tecnológicas, posibilidades de desarrollo profesional, líneas futuras, etc.

Es necesario realizar esta oferta complementaria ya que, en caso de alumnos o alumnas con contratos en empresas y que no puedan reconocer la totalidad de los 12 ETCS podrán completar el reconocimiento con prácticas adicionales y/o créditos ofertados.En cualquier caso, el tipo de oferta garantiza que el alumnado adquiere la CE21. La oferta de prácticas es interesante y motivadora para que el alumnado elija esa vía. Sólo en el caso de un alumno o alumna que ya esté trabajando en el sector y no pueda convalidar los 12 ETCS, se complementa su formación con la oferta arriba explicada.

5.5.1.4 OBSERVACIONES

La evaluación de las materias deberá asegurar la adquisición de las competencias específicas y generales. Se potenciará la evaluación de los conocimientos a través de la participación activa del estudiante, la evaluación de trabajos académicos, casos prácticos, proyectos y prácticas de laboratorio, realizados de manera individual o en grupo. Como criterio general las asignaturas se ajustarán al siguiente esquema de evaluación:

Los porcentajes mínimo y máximo que pueden sumar las siguientes pruebas son 0% y 40%

1. Examen oral

2. Prueba escrita de respuesta abierta

3. Pruebas objetivas de tipo test

Los porcentajes mínimo y máximo que pueden sumar las siguientes pruebas son 40% y 80%

1. Trabajo académico

2. Proyecto

3. Caso

Los porcentajes mínimo y máximo que pueden sumar las siguientes pruebas son 10% y 20%

1. Portafolio

2. Observación

3. Coevaluación

Así vemos que, los porcentajes arriba señalados aseguran que, ninguna asignatura evaluará los contenidos teóricos impartido en TA por encima de un 40%. Que las actividades prácticas realizadas en teoría de seminario y laboratorio de prácticas se valorarán, al menos con un 40%. Y que todas las asignaturas realizarán un seguimiento individual del alumnado mediante con un peso no inferior al 10%.

Se seguirá la metodología docente definida por el National Institute of Standars and Technology, recogida en el documento "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework". Esta metodología está reconocida a nivel internacional como un estándar de facto para la formación y la elaboración de currículo en el campo de la ciberseguridad.

Los objetivos de la metodología serían, entre otros:

- Identificar requisitos de cualificación y entrenamiento para desarrollar los conocimientos, competencias y habilidades fundamentales en el ámbito de la ciberseguridad.
- Clasificar y hacer seguimiento de las capacidades del personal técnico dedicado a la ciberseguridad, en base a sus conocimientos, competencias y habilidades.
- Identificar los roles de trabajo más relevantes y definir carreras profesionales en base a sus conocimientos, competencias y habilidades.

Las guías docentes de las asignaturas que conforman la materia detallarán las metodologías docentes y sistemas de evaluación que se utilizarán durante el curso, con los pesos exactos para cada acto de evaluación. Antes del comienzo del curso académico, la Comisión Académica del Máster aprobará el contenido de las guías docentes.

Los 12 créditos de la materia podrán ser convalidables por prácticas en empresa o experiencia profesional, tal como indica la normativa de reconocimiento y transferencia de créditos de la UPV.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG6 - Fomentar el espíritu crítico y emprendedor, el compromiso ético, y desarrollar hábitos de excelencia y calidad en el ejercicio profesional.

CG7 - Emitir juicios en función de criterios, normas externas o de reflexiones personales, en los ámbitos de la ciberseguridad y la ciberinteligencia.

CG8 - Dirigir y coordinar equipos de trabajo para el desarrollo, implantación y mantenimiento de proyectos en los ámbitos de la ciberseguridad y la ciberinteligencia.

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
CT-01 - Comprensión e integración.
CT-04 - Innovación, creatividad y emprendimiento.
CT-05 - Diseño y proyecto.
CT-07 - Responsabilidad ética, medioambiental y profesional.
CT-08 - Comunicación efectiva.
CT-09 - Pensamiento crítico.
CT-10 - Conocimiento de problemas contemporáneos.
CT-11 - Aprendizaje permanente.
CT-12 - Planificación y gestión del tiempo.
5.5.1.5.3 ESPECÍFICAS
CE21 - Realizar actividades correspondientes a la práctica profesional bajo la supervisión de tutores académicos y profesionales asignados.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Teoría Seminario	120	50
Actividades de Trabajo Autónomo	210	0

5.5.1.7 METODOLOGÍAS DOCENTES
Seminarios
Tutorías individuales
Aprendizaje autónomo
Clase magistral
Trabajo en grupo
Aprendizaje basado en problemas.
Estudio de casos
Aprendizaje basado en proyectos.
Resolución de ejercicios y problemas.
Laboratorio
Supervisión
Actividades de evaluación
Trabajos prácticos
Estudio práctico
Actividades complementarias

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA

Examen oral	0.0	40.0
Prueba escrita de respuesta abierta	0.0	40.0
Pruebas objetivas (tipo test)	0.0	40.0
Trabajo académico	0.0	80.0
Portafolio	0.0	20.0
Proyecto	0.0	80.0
Caso	0.0	80.0
Observación	0.0	20.0
Coevaluación	0.0	20.0

5.5 NIVEL 1: Módulo Trabajo Fin de Máster

5.5.1 Datos Básicos del Nivel 1

NIVEL 2: Materia Trabajo Fin de Máster

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Trabajo Fin de Grado / Máster
ECTS NIVEL 2	18

DESPLIEGUE TEMPORAL: Semestral

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

LENGUAS EN LAS QUE SE IMPARTE

CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

LISTADO DE ESPECIALIDADES

No existen datos

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

5.5.1.3 CONTENIDOS

El Trabajo de Fin de Máster comprende la realización, presentación y defensa pública y con tribunal, una vez obtenidos todos los créditos del plan de estudios, de un ejercicio original realizado individualmente ante un tribunal universitario, consistente en un proyecto integral de Ciberseguridad y/o Ciberinteligencia de naturaleza profesional en el que se sinteticen las competencias adquiridas en las enseñanzas. Se fomentará la realización del Trabajo Fin de Máster en empresas o instituciones externas en alguno de los dominios de aplicación de la ciberseguridad y ciberinteligencia desarrollados en el plan de estudios. El Trabajo de Fin de Máster será dirigido por al menos un profesor con docencia en la titulación, que planificará las actividades necesarias para realizar la tutorización y el seguimiento del trabajo.

5.5.1.4 OBSERVACIONES

Para la presentación del Trabajo Final de Máster es requisito haber superado la totalidad de créditos obligatorios del módulo de *Materias comunes* (60.0 ECTS) y los créditos de la materia *Desarrollo profesional* (12.0 ECTS).

5.5.1.5 COMPETENCIAS
5.5.1.5.1 BÁSICAS Y GENERALES
CG6 - Fomentar el espíritu crítico y emprendedor, el compromiso ético, y desarrollar hábitos de excelencia y calidad en el ejercicio profesional.
CG7 - Emitir juicios en función de criterios, normas externas o de reflexiones personales, en los ámbitos de la ciberseguridad y la ciberinteligencia.
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
No existen datos
5.5.1.5.3 ESPECÍFICAS
TFM - Realización, presentación y defensa, una vez obtenidos todos los créditos del plan de estudios, de un ejercicio original realizado individualmente ante un tribunal universitario, consistente en un proyecto integral de ciberseguridad y/o ciberinteligencia de naturaleza profesional en el que se sinteticen las competencias adquiridas en las enseñanzas.

5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Teoría Seminario	20	50
Tutorización	10	50
Actividades de Trabajo Autónomo	420	0

5.5.1.7 METODOLOGÍAS DOCENTES
Tutorías individuales
Aprendizaje autónomo
Trabajos prácticos
Estudio práctico
Trabajos teóricos

5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Memoria escrita	50.0	50.0
Defensa pública del trabajo con tribunal	50.0	50.0

6. PERSONAL ACADÉMICO

6.1 PROFESORADO Y OTROS RECURSOS HUMANOS				
Universidad	**Categoría**	**Total %**	**Doctores %**	**Horas %**
Universitat Politècnica de València	Profesor Asociado (incluye profesor asociado de C.C.: de Salud)	5.9	100	1,4
Universitat Politècnica de València	Profesor Contratado Doctor	11.8	100	5,6
Universitat Politècnica de València	Profesor Titular de Escuela Universitaria	11.8	100	15,3
Universitat Politècnica de València	Catedrático de Universidad	17.7	100	29,2
Universitat Politècnica de València	Profesor Titular de Universidad	52.8	100	48,5

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 %
75	10	90

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

Anualmente, una vez finalizado el curso anterior, el Servicio de Evaluación, Planificación y Calidad (SEPQ) elabora y difunde, a través del Área de Rendimiento Académico y Evaluación Curricular, los siguientes estudios e informes para que pueda valorarse el progreso y resultados del aprendizaje de los alumnos y plantearse las acciones pertinentes:

- Estudio de resultados académicos por titulación, con evoluciones.
- Estudio de graduados por titulación: tiempo medio de estudios, tasa de eficiencia de graduados, con evoluciones.
- Estudio de flujos por titulación: ingresos, egresos, cambios desde y hacia otras titulaciones y abandonos.

A demanda de las Estructuras Responsables de la Titulación (ERTs), el SEPQ también elabora y proporciona estudios e informes relacionados con las asignaturas.

Competencias Transversales UPV

La UPV se ha planteado el estudio y COMPARACIÓN de distintos referentes (RD861/MECES, normas CIN, referentes internacionales REFLEX, ABET, EUR-ACE, NAAB) para SIMPLIFICAR la definición de las competencias e IMPLANTAR los necesarios procesos sistemáticos de evaluación. Resultado de este análisis surgen las COMPETENCIAS TRANSVERSALES.

Las Competencias Transversales (CT-UPV) pretenden sintetizar el perfil competencial que adquieren los alumnos de la UPV garantizando además cubrir el marco de referencia de algunas titulaciones con regulaciones o recomendaciones específicas.

El documento de definición de las CT-UPV contempla una relación de 13 conceptos que se definen a su vez en términos de competencias y que se despliegan en resultados de aprendizaje para los niveles de grado y máster.

A partir de estas referencias se identificarán y desarrollarán herramientas de apoyo para facilitar el proceso de enseñanza-aprendizaje a los equipos de profesores, tanto indicando las actividades formativas más coherentes para coadyuvar a la adquisición de cada CT-UPV como los sistemas de evaluación e instrumentos concretos que puedan utilizarse, favoreciendo también el trabajo colaborativo y difusión de buenas prácticas entre todo el profesorado de la UPV.

CT1	**Comprensión e integración**	Demostrar la comprensión e integración del conocimiento tanto de la propia especialización como en otros contextos más amplios
CT2	**Aplicación pensamiento práctico**	Aplicar los conocimientos a la práctica, atendiendo a la información disponible, y estableciendo el proceso a seguir para alcanzar los objetivos con eficacia y eficiencia
CT3	**Análisis y resolución de problemas**	Analizar y resolver problemas de forma efectiva, identificando y definiendo los elementos significativos que lo constituyen
CT4	**Innovación, creatividad y emprendimiento**	Innovar para responder satisfactoriamente y de forma original a las necesidades y demandas personales, organizativas y sociales con una actitud emprendedora
CT5	**Diseño y proyecto**	Diseñar, dirigir y evaluar una idea de manera eficaz hasta concretarla en un proyecto
CT6	**Trabajo en equipo y liderazgo**	Trabajar y liderar equipos de forma efectiva para la consecución de objetivos comunes, contribuyendo al desarrollo personal y profesional de los mismos
CT7	**Responsabilidad ética, medioambiental y profesional**	Actuar con responsabilidad ética, medioambiental y profesional ante uno mismo y los demás
CT8	**Comunicación efectiva**	Comunicarse de manera efectiva, tanto de forma oral como escrita, utilizando adecuadamente los recursos necesarios y adaptándose a las características de la situación y de la audiencia
CT9	**Pensamiento crítico**	Desarrollar un pensamiento crítico interesándose por los fundamentos en los que se asientan las ideas, acciones y juicios, tanto propios como ajenos
CT10	**Conocimiento de los problemas contemporáneos**	Identificar e interpretar los problemas contemporáneos en su campo de especialización, así como en otros campos del conocimiento
CT11	**Aprendizaje permanente**	Utilizar el aprendizaje de manera estratégica, autónoma y flexible, a lo largo de toda la vida, en función del objetivo perseguido
CT12	**Planificación y gestión del tiempo**	Planificar adecuadamente el tiempo disponible y programar las actividades necesarias para alcanzar los objetivos, tanto académico-profesionales como personales
CT13	**Instrumental específica**	Capacidad para utilizar las técnicas, las habilidades y las herramientas actualizadas necesarias para la práctica de la profesión

Entre las ventajas de la implementación de las CT-UPV destacaríamos las siguientes:

- Clarificar y ordenar conceptos tanto a los estudiantes, como al profesorado y a los empleadores.
- Homogeneizar las competencias que se adquieren en nuestros títulos.
- Permitir la comparabilidad de los diferentes títulos de la UPV.
- Simplificar el proceso de evaluación y proporcionar herramientas adaptadas.
- Proporcionar valor añadido y diferenciador a nuestros alumnos. Todo ello con un doble objetivo:
- Por una parte conseguir una evaluación individualizada de progreso y acreditación de la adquisición final de competencias de cada alumno.
- Proporcionar datos agregados para la gestión y mejora del título por parte de las estructuras responsables de los títulos (centros, departamentos, institutos..).

Matrices de asociación

Para asegurar una adecuada definición de las competencias respetando los referentes correspondientes a cada titulación se elaboran una serie de matrices de asociación

- Cruce de competencias RD861 con CT-UPV (común para todos los títulos)
- Cruce resto de competencias (generales y específicas) definidas con CT-UPV
  - Cruce de competencias ABET/EUR-ACE/otros referentes con CT-UPV (común para todos los títulos en función del ámbito de acreditación internacional posible)

Métodos a utilizar para evaluar la adquisición de competencias Se han definido en la UPV dos aproximaciones complementarias:

- Evaluación de adquisición durante el proceso formativo (a través de materias/asignaturas del plan de estudios). El principio que asume la UPV para la evaluación de las competencias es utilizar las CT-UPV realizando el seguimiento del progreso de los estudiantes a través de materias/asignaturas seleccionadas y que denominaremos ¿puntos de control¿. La base de selección de las materias/asignaturas en los que se fundamenta el seguimiento son identificadas y coordinadas por las Estructuras Responsables del Título (ERTs) siguiendo también posibles niveles de adquisición o dominio y criterios de temporalidad en plan de estudios, y siempre asegurando que se evalúan el 100% de las CT-UPV/competencias.
- Evaluación al finalizar los estudios (ligado al TFM).

El procedimiento plantea recoger información a través de 2 cuestionarios:

- Cuestionario 1: Cuestionario a los alumnos

Los alumnos cumplimentan este cuestionario cuando han de presentar su TFG/TFM. El alumno valora el nivel que considera que ha adquirido en cada una de las CT-UPV (valora obligatoriamente cada una de 1 a 5) y hay un campo libre en el que puede plantear comentarios. La recogida de información no es anónima aunque explícitamente se le indica que su valoración no tendrá efectos académicos.

- Cuestionario 2: Cuestionario para los tribunales/comisiones de evaluación de TFG/TFM.

Cada comisión evalúa para cada proyecto cada una de las CT-UPV, aunque pueden indicar en algún caso que no tienen elementos de juicio para valorar alguna de ellas. Por último existe también un campo de observaciones.

9. SISTEMA DE GARANTÍA DE CALIDAD

ENLACE	http://www.upv.es/entidades/ACA/info/734272normalc.html

10. CALENDARIO DE IMPLANTACIÓN

10.1 CRONOGRAMA DE IMPLANTACIÓN	
CURSO DE INICIO	2020
Ver Apartado 10: Anexo 1.	
10.2 PROCEDIMIENTO DE ADAPTACIÓN	
No procede.	
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**
25407751L	Silvia María	Terrasa	Barrena
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Camino de Vera, s/n	46022	Valencia/València	Valencia
EMAIL	**MÓVIL**	**FAX**	**CARGO**

sterrasa@disca.upv.es	963875728	963875728	Directora de la Escuela Técnica Superior de Informática
11.2 REPRESENTANTE LEGAL			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
52748140D	FRANCISCO MIGUEL	BAENA	AROCA
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Camino de Vera, s/n	46022	Valencia/València	Valencia
EMAIL	**MÓVIL**	**FAX**	**CARGO**
veca@upv.es	963877101	963877101	Jefe del Servicio de Procesos Electrónicos y Transparencia
El Rector de la Universidad no es el Representante Legal			
Ver Apartado 11: Anexo 1.			
11.3 SOLICITANTE			
El responsable del título no es el solicitante			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
22559928X	SARA	BLANC	CLAVERO
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Camino de Vera, s/n	46022	Valencia/València	Valencia
EMAIL	**MÓVIL**	**FAX**	**CARGO**
aeot@upv.es	963879897	963877969	Directora del Área de Estudios y Ordenación de Títulos

Apartado 2: Anexo 1

Nombre : 2. Justificación.pdf

HASH SHA1 : 6A5187524AF0E7AD14FD16C0C6FCB3745702FF1A

Código CSV : 495774851780732313642837

Ver Fichero: 2. Justificación.pdf

Apartado 4: Anexo 1

Nombre : 4.1.pdf

HASH SHA1 : 9967B9E8677DAB748CF4CF8C059B1D221699FE77

Código CSV : 484190547473797329812330

Ver Fichero: 4.1.pdf

Apartado 5: Anexo 1

Nombre : 5.1_MUCC.pdf

HASH SHA1 : 4153A36B79D2ECB58B71014643C0B29CEA6671D2

Código CSV : 49578132593305777892331 1

Ver Fichero: 5.1_MUCC.pdf

Apartado 6: Anexo 1

Nombre : 6.1.Personal_MUCC.pdf

HASH SHA1 : FEABE563AAF37A17541FD5137FC376EF1A828C67

Código CSV : 49581130121197962292418 5

Ver Fichero: 6.1.Personal_MUCC.pdf

Apartado 6: Anexo 2

Nombre : 6.2 Otros Recursos Humanos MUCC_1Aleg.pdf

HASH SHA1 : 867BBDC8400B340A214D5B5A45173E1AA5FF01C0

Código CSV : 378671716406970564681822

Ver Fichero: 6.2 Otros Recursos Humanos MUCC_1Aleg.pdf

Apartado 7: Anexo 1

Nombre : 7. Recursos materiales y Servicios MUCC.pdf

HASH SHA1 : 966F7A5A6B8A6F062B54E9A5A8B3D539B0265DB4

Código CSV : 485159683633175656676831

Ver Fichero: 7. Recursos materiales y Servicios MUCC.pdf

Apartado 8: Anexo 1

Nombre : 8.1 Resultados previstos MUCC.pdf

HASH SHA1 : 5885A3A5C47CF46B4E3DA8E351C13A087D2297A4

Código CSV : 364594178115767440003296

Ver Fichero: 8.1 Resultados previstos MUCC.pdf

Apartado 10: Anexo 1

Nombre : 10. Cronograma de implantación MUCC.pdf

HASH SHA1 : 8CB0F089A4175E6E24B54AEE60B5573A7753DE76

Código CSV : 364594723819437581628342

Ver Fichero: 10. Cronograma de implantación MUCC.pdf

Apartado 11: Anexo 1

Nombre : 11.2 DELEGACIÓN ACCESO A SEDES ELECTRÓNICAS FRANCISCO MIGUEL BAENA AROCA.pdf

HASH SHA1 : CBCC0EFE97B8876B56C5F43BA55028450AD279F4

Código CSV : 484213059836528452318719

Ver Fichero: 11.2 DELEGACIÓN ACCESO A SEDES ELECTRÓNICAS FRANCISCO MIGUEL BAENA AROCA.pdf