IMPRESO SOLICITUD PARA VERIFICACIÓN DE TITULOS 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 Oberta de Catalunya	Universitat Oberta de Catalunya (BARCELONA)	08070118
NIVEL	**DENOMINACIÓN ESPECÍFICA**	
Máster	Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones	
RAMA DE CONOCIMIENTO		
Ingeniería y Arquitectura		
CONJUNTO	**CONVENIO**	
Nacional	Master interuniversitario coordinado por la Universitat Oberta de Catalunya, y con la paticipación de la Universitat Autònoma de Barcelona y la Universitat Rovira i Virgili.	
UNIVERSIDADES PARTICIPANTES	**CENTRO**	**CÓDIGO CENTRO**
Universidad Autónoma de Barcelona	Escuela de Ingeniería (CERDANYOLA DEL VALLÈS)	08071123
Universidad Rovira i Virgili	Escuela Técnica Superior de Ingeniería (TARRAGONA)	43007373
HABILITA PARA EL EJERCICIO DE PROFESIONES REGULADAS	**NORMA HABILITACIÓN**	
No		
SOLICITANTE		
NOMBRE Y APELLIDOS	**CARGO**	
Pere Fabra Abat	Vicerector de Ordenación Académica y Profesorado	
Tipo Documento	**Número Documento**	
NIF		
REPRESENTANTE LEGAL		
NOMBRE Y APELLIDOS	**CARGO**	
Oscar Aguer Bayarri	Gerent de la Universitat Oberta de Catalunya	
Tipo Documento	**Número Documento**	
NIF		
RESPONSABLE DEL TÍTULO		
NOMBRE Y APELLIDOS	**CARGO**	
Pere Fabra Abat	Vicerector de Ordenación Académica y Profesorado	
Tipo Documento	**Número Documento**	
NIF		

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
Av. Tibidabo 39-41	08035	Barcelona	932532341
E-MAIL	**PROVINCIA**		**FAX**
v_academica@uoc.edu	Barcelona		934176495

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 2 de marzo de 2011
	Firma: Representante legal de la Universidad

1. DESCRIPCIÓN DEL TÍTULO

1.1. DATOS BÁSICOS

NIVEL	DENOMINACIÓN ESPECIFICA	CONJUNTO	CONVENIO	CONV. ADJUNTO
Máster	Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones	Nacional		Ver anexos. Apartado 1.

LISTADO DE ESPECIALIDADES
Seguridad en Redes y Sistemas
Seguridad en Servicios y Aplicaciones
Gestión y Auditoría de la Seguridad Informática
Investigación

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

HABILITA PARA PROF. REG.	PROFESIÓN REGULADA	RESOLUCIÓN
No		

NORMA	AGENCIA EVALUADORA	UNIVERSIDAD SOLICITANTE
	Agència per a la Qualitat del Sistema Universitari de Catalunya (AQU)	Universidad Oberta de Catalunya

LISTADO DE UNIVERSIDADES	
CÓDIGO	UNIVERSIDAD
054	Universidad Oberta de Catalunya
022	Universidad Autónoma de Barcelona
042	Universidad Rovira i Virgili

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 FORMACIÓN BÁSICA	CRÉDITOS EN PRÁCTICAS EXTERNAS
60		3
CRÉDITOS OPTATIVOS	**CRÉDITOS OBLIGATORIOS**	**CRÉDITOS TRABAJO FIN GRADO/MÁSTER**
30	18	9

LISTADO DE ESPECIALIDADES	
ESPECIALIDAD	CRÉDITOS OPTATIVOS
Seguridad en Redes y Sistemas	18.0
Seguridad en Servicios y Aplicaciones	18.0
Gestión y Auditoría de la Seguridad Informática	18.0
Investigación	18.0

1.3. Universidad Oberta de Catalunya

1.3.1. CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS	
CÓDIGO	**CENTRO**
08070118	Universitat Oberta de Catalunya (BARCELONA)

1.3.2. Universitat Oberta de Catalunya (BARCELONA)

1.3.2.1. Datos asociados al centro

TIPOS DE ENSEÑANZA QUE SE IMPARTEN EN EL CENTRO		
PRESENCIAL	**SEMIPRESENCIAL**	**VIRTUAL**
No	No	Si
PLAZAS DE NUEVO INGRESO OFERTADAS		
PRIMER AÑO IMPLANTACIÓN	**SEGUNDO AÑO IMPLANTACIÓN**	
250	250	
	TIEMPO COMPLETO	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	4.0	60.0
RESTO DE AÑOS	4.0	60.0
	TIEMPO PARCIAL	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	4.0	60.0
RESTO DE AÑOS	4.0	60.0
NORMAS DE PERMANENCIA		
http://cv.uoc.edu/UOC2000/b/docs/secretaria/main/normativa/normes/permanencia/index.html		
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

1.3. Universidad Autónoma de Barcelona

1.3.1. CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS	
CÓDIGO	**CENTRO**
08071123	Escuela de Ingeniería (CERDANYOLA DEL VALLÈS)

1.3.2. Escuela de Ingeniería (CERDANYOLA DEL VALLÈS)

1.3.2.1. Datos asociados al centro

TIPOS DE ENSEÑANZA QUE SE IMPARTEN EN EL CENTRO		
PRESENCIAL	**SEMIPRESENCIAL**	**VIRTUAL**
No	No	Si
PLAZAS DE NUEVO INGRESO OFERTADAS		
PRIMER AÑO IMPLANTACIÓN	**SEGUNDO AÑO IMPLANTACIÓN**	
250	250	

	TIEMPO COMPLETO	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	4.0	60.0
RESTO DE AÑOS	4.0	60.0
	TIEMPO PARCIAL	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	4.0	60.0
RESTO DE AÑOS	4.0	60.0
NORMAS DE PERMANENCIA		
http://cv.uoc.edu/UOC2000/b/docs/secretaria/main/normativa/normes/permanencia/index.html		
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

1.3. Universidad Rovira i Virgili

1.3.1. CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS	
CÓDIGO	**CENTRO**
43007373	Escuela Técnica Superior de Ingeniería (TARRAGONA)

1.3.2. Escuela Técnica Superior de Ingeniería (TARRAGONA)

1.3.2.1. Datos asociados al centro

TIPOS DE ENSEÑANZA QUE SE IMPARTEN EN EL CENTRO		
PRESENCIAL	**SEMIPRESENCIAL**	**VIRTUAL**
No	No	Si
PLAZAS DE NUEVO INGRESO OFERTADAS		
PRIMER AÑO IMPLANTACIÓN	**SEGUNDO AÑO IMPLANTACIÓN**	
250	250	
	TIEMPO COMPLETO	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	4.0	60.0
RESTO DE AÑOS	4.0	60.0
	TIEMPO PARCIAL	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	4.0	60.0
RESTO DE AÑOS	4.0	60.0
NORMAS DE PERMANENCIA		
http://cv.uoc.edu/UOC2000/b/docs/secretaria/main/normativa/normes/permanencia/index.html		

LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	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 anexos, apartado 2.

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
CG0 - Hablar bien en público
3.2 COMPETENCIAS TRANSVERSALES
CT1 - Capacidad de análisis y síntesis de la seguridad de un sistema.
CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.
CT3 - Capacidad de comunicación tanto a público especializado como no especializado de modo claro y sin ambigüedades.
CT4 - Capacidad de aprendizaje autónomo consultando información
CT5 - Capacidad para seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas en entornos nuevos
CT6 - Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática
CT7 - Uso del inglés como lengua vehicular en el ámbito tecnológico
3.3 COMPETENCIAS ESPECÍFICAS
CE8 - Capacidad para analizar las técnicas de explotación de vulnerabilidades de una red y los puntos débles de un sistema.
CE9 - Capacidad para identificar, evaluar y gestionar los principales riesgos de un dominio informático, tanto tecnológicos como procedentes de la ingeniería social
CE10 - Capacidad para usar técnicas y contramedidas básicas de seguridad para la prevención de ataques derivados de la ingeniería social
CE11 - Capacidad para realizar, presentar y defender ante un tribunal interuniversitario, un ejercicio original realizado individualmente consistente en un proyecto integral de Seguridad de las Tecnologías de la Información y de las Comunicaciones de naturaleza profesional o de investigación en el que se sinteticen las competencias adquiridas en las enseñanzas
CE12 - Capacidad para aplicar el marco jurídico que afecta a la gestión de la seguridad de sistemas informáticos, teniendo en cuenta la legislación relativa a la propiedad intelectual, el comercio electrónico, la firma electrónica y la protección de datos de carácter personal.
CE13 - Poseer y comprender conocimientos de las estructuras normalizadoras, evaluadoras, certificadoras, y las normas correspondientes que regulan los ámbitos de la seguridad.
CE14 - Poseer y comprender conocimientos de las arquitecturas más importantes de AAA (Authentication, Authorization, Accounting), así como sistemas de federación de identidades y de autenticación única (SSO-Single Sign On).
CE15 - Capacidad para identificar las vulnerabilidades de privacidad de los sistemas (especialmente en aplicaciones web) y capacidad para protegerlos
CE16 - Capacidad para comprender y saber usar herramientas para la administración y protección de redes cableadas e inalámbricas, y la gestión de alertas de seguridad. (Perfil de Seguridad en Redes y Sistemas)

CE17 - Capacidad para concebir, desplegar, organizar y gestionar redes de comunicaciones en contextos residenciales, empresariales o institucionales, responsabilizándose de la seguridad del sistema y la protección de los datos de los usuarios. (Perfil de Seguridad en Redes y Sistemas)
CE18 - Poseer y comprender conocimientos de las técnicas principales de seguridad en los sistemas operativos. (Perfil de Seguridad en Redes y Sistemas)
CE19 - Capacidad para configurar y administrar una base de datos a nivel físico y lógico, a fin de asegurar la integridad, disponibilidad y confidencialidad de la información almacenada. (Perfil de Seguridad en Redes y Sistemas)
CE20 - Capacidad para realizar una configuración experta de un servidor GNU/Linux o Windows. (Perfil de Seguridad en Redes y Sistemas)
CE21 - Capacidad para diseñar soluciones integrales apropiadas en escenarios complejos que combinen las técnicas y contramedidas conocidas para la prevención, detección y disuasión de ataques. (Perfil de Seguridad en Redes y Sistemas)
CE22 - Capacidad para aplicar metodologías y buenas prácticas de programación de código robusto, así como capacidad de modelar las amenazas de un sistema para evaluar la seguridad de las aplicaciones desarrolladas.(Perfil de Seguridad en Servicios y Aplicaciones)
CE23 - Capacidad para analizar, diseñar y desarrollar aplicaciones y servicios web seguros. (Perfil de Seguridad en Servicios y Aplicaciones)
CE24 - Poseer y comprender conocimientos de los sistemas que forman parte de una arquitectura de comercio electrónico, y capacidad para desplegar una. (Perfil de Seguridad en Servicios y Aplicaciones)
CE25 - Capacidad para comprender y analizar los sistemas de facturación electrónica, de pago y de micro-pago.(Perfil de Seguridad en Servicios y Aplicaciones)
CE26 - Comprender las técnicas de reconocimiento de las personas a través de características físicas: cara, huellas dactilares, orejas, iris, manos, forma de caminar, voz, etc. (Perfil de Seguridad en Servicios y Aplicaciones)
CE27 - Capacidad para diseñar aplicaciones reales con acceso biométrico. Conocer el software y hardware actual para desarrollar aplicaciones. (Perfil de Seguridad en Servicios y Aplicaciones)
CE28 - Capacidad para identificar y analizar los procesos críticos de una organización, así como el impacto que produciría la interrupción de estos procesos. (Perfil de Gestión y Auditoría de Seguridad)
CE29 - Capacidad para elaborar un plan de seguridad, teniendo en cuento todo el proceso de inventario y clasificación de activos, estudio de amenazas, análisis de riesgos y definición del plan de acción con el presupuesto asociado para la aprobación de la dirección. (Perfil de Gestión y Auditoría de Seguridad)
CE30 - Capacidad para desarrollar un Plan de Continuidad, conocer sus fases y el personal que debe implicarse en su desarrollo. Conocer las normas y estándares de referencia relacionados con la Continuidad de Negocio. (Perfil de Gestión y Auditoría de Seguridad)
CE31 - Capacidad para implantar un Sistema de Gestión de la Seguridad de la Información siguiendo las fases del ciclo de Deming. (Perfil de Gestión y Auditoría de Seguridad)
CE32 - Capacidad para gestionar la certificación de un sistema de gestión de la seguridad de la información, así como capacidad para comprender, interpretar y explicar las ventajas que aporta la certificación de estos sistemas. (Perfil de Gestión y Auditoría de Seguridad)
CE33 - Capacidad de elaborar e implementar un plan de auditoría. Uso de las herramientas habituales para realizar una auditoría técnica de seguridad. (Perfil de Gestión y Auditoría de Seguridad)
CE34 - Capacidad para realizar un análisis forense de cualquier sistema informático (PC, móviles, routers, etc.) y presentarlo en una sede judicial. (Perfil de Gestión y Auditoría de Seguridad)
CE35 - Capacidad para aplicar las consideraciones legales adquiridas para realizar la gestión de un incidente de seguridad. (Perfil de Gestión y Auditoría de Seguridad)
CE36 - Capacidad para planificar, administrar, dirigir y coordinar proyectos de investigación en el campo de las TIC. (Perfil de Investigación en Seguridad de las TIC)
CE37 - Capacidad para diseñar y llevar a cabo la investigación según las normas del conocimiento científico en el campo de las TIC. (Perfil de Investigación en Seguridad de las TIC)
CE38 - Capacidad para redactar documentación científica, y sintetizar y presentar los resultados de un proyecto de investigación. (Perfil de Investigación en Seguridad de las TIC)
CE39 - Capacidad para determinar las características relevantes de un sistema TIC para su modelado y simulación, así como capacidad para sintetizar y presentar los resultados. (Perfil de Investigación en Seguridad de las TIC)

CE40 - Comprender los fundamentos teóricos de la criptografía moderna y el funcionamiento de los protocolos criptográficos actualmente en uso. (Perfil de Investigación en Seguridad de las TIC)
CE41 - Capacidad para analizar los distintos sistemas criptográficos que se utilizan habitualmente y criticar su aplicabilidad, así como entender la no aplicabilidad de otros sistemas teóricamente interesantes. (Perfil de Investigación en Seguridad de las TIC)
CE42 - Capacidad para interpretar, analizar y explicar las diferencias conceptuales y su aplicabilidad entre los diversos esquemas propuestos para resolver un mismo problema criptográfico. (Perfil de Investigación en Seguridad de las TIC)
CE43 - Capacidad para comprender y utilizar las aplicaciones criptográficas existentes basadas en técnicas avanzadas. (Perfil de Investigación en Seguridad de las TIC)
CE44 - Poseer y comprender conocimientos de las diferencias conceptuales entre los diferentes dominios de marcado de la información digital (dominio temporal/espacial y transformado). Capacidad crítica para analizar la bondad de distintos sistemas de marcado. (Materias Optativas)
CE45 - Capacidad para integrar conocimientos de las aplicaciones existentes para las técnicas de marcado de la información.(Materias Optativas)
CE46 - Capacidad para la dirección de proyectos de investigación, desarrollo e innovación, en empresas y centros tecnológicos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación. (Materias optativas)
CE47 - Capacidad para la integración de tecnologías, aplicaciones, servicios y sistemas propios de la Ingeniería Informática, con carácter generalista, y en contextos más amplios y multidisciplinares. (Materias optativas)
CE48 - Capacidad para la planificación estratégica, elaboración, dirección, coordinación, y gestión técnica y económica en los ámbitos de la ingeniería informática relacionados, entre otros, con: sistemas, aplicaciones, servicios, redes, infraestructuras o instalaciones informáticas y centros o factorías de desarrollo de software, respetando el adecuado cumplimiento de los criterios de calidad y medioambientales y en entornos de trabajo multidisciplinares. (Materias optativas)

4. ACCESO Y ADMISIÓN DE ESTUDIANTES

4.1 SISTEMAS DE INFORMACIÓN PREVIO

Ver anexos. Apartado 3.

4.2 REQUISITOS DE ACCESO Y CRITERIOS DE ADMISIÓN

Las vías de acceso al Máster son las previstas en la normativa aplicable.
Las solicitudes de acceso y admisión serán gestionadas por los órganos administrativos de la UOC, que garantizarán el cumplimiento de las condiciones de acceso legalmente establecidas, así como de las condiciones de admisión.
El tutor podrá recomendar la realización de formación compensatoria a la vista del expediente académico y experiencia profesional del estudiante con el objetivo de aproximarle al perfil de ingreso recomendado.

Criterios de acceso

De acuerdo con lo establecido en el Real decreto 861/2010, del 2 de julio, que modifica el apartado 1 del artículo 16 del Real decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales, para poder acceder a las enseñanzas oficiales de Máster es necesario estar en posesión de un título universitario oficial español u otro expedido por una institución de educación superior perteneciente a otro Estado integrante del Espacio Europeo de Educación Superior que faculte en el mismo para el acceso a enseñanzas de Máster.
Además, en virtud de lo dispuesto en la disposición adicional cuarta del Real decreto 1393/2007, quienes estén en posesión del título oficial de Diplomado, Arquitecto Técnico, Ingeniero Técnico, Licenciado, Arquitecto o Ingeniero podrán acceder a estas enseñanzas oficiales de Máster.
Asimismo, podrán acceder los titulados conforme a sistemas educativos ajenos al EEES, sin necesidad de la homologación de sus títulos, previa comprobación por parte de la Comisión de Coordinación de que se acredita un nivel de formación equivalente a los correspondientes títulos oficiales españoles y que

facultan en el país expedidor del título para el acceso a enseñanzas de postgrado. El acceso por esta vía no implicará, en ningún caso, la homologación del título previo ni su reconocimiento a otros efectos que el de cursar las enseñanzas de Máster.

Criterios de admisión

Los criterios de admisión se establecen en función del perfil de ingreso (titulación académica y experiencia profesional previa) del estudiante. Pueden ser admitidas al Máster las personas que hayan cursado los siguientes estudios:

1. Titulados en Ingeniería Informática (Graduados, Ingenieros, Ingenieros Técnicos).
2. Titulados del área de Ingeniería y Arquitectura (Graduados, Ingenieros, Ingenieros Técnicos, Licenciados, Diplomados) en especialidades vinculadas a las tecnologías de la información y de las comunicaciones. Por ejemplo, Telecomunicaciones o Multimedia.
3. Titulados en el área de Ciencias, en las especialidades de Matemáticas, Física y Estadística (Graduados, Licenciados, Diplomados).
4. Otros titulados.

Los dos primeros grupos de titulados (Ingenieros informáticos e Ingenieros del área TIC) no necesitarán cursar ningún complemento de formación para iniciar el MISTIC, mientras que el tercer grupo (Titulados en el área de Ciencias) es probable que tenga que cursar créditos de formación compensatoria (como máximo 30 ECTS). Para los restantes titulados (cuarto grupo), siempre y cuando cumplan las condiciones de acceso legalmente previstas, su admisión al máster quedará supeditada al número de créditos de complementos de formación que debieran cursar.

La superación de estos complementos de formación, previstos para los grupos 3 y 4, será un requisito necesario para la consecución del título.

En el tercer grupo (titulados en el área de Ciencias, en las especialidades de Matemáticas, Física y Estadística), la identificación de los créditos necesarios a cursar como complementos de formación se realizará mediante una tutorización y evaluación personalizada de la formación y experiencia previa de cada estudiante, y será aprobada por la Comisión de Coordinación del máster. La composición de dicha Comisión viene detallada en el convenio de colaboración (véase anexo 1 – Convenio interuniversitario).

En el cuarto grupo (quienes estén en posesión de otros títulos), los candidatos serán evaluados por la Comisión de Coordinación del máster, la cual determinará su admisión en función de su formación previa y experiencia profesional. Para evaluar su admisión, la Comisión de Coordinación analizará las evidencias aportadas por el estudiante sobre sus competencias en el área (certificaciones en seguridad, minors académicos, etc.). En cualquier caso, la admisión de estos estudiantes estará supeditada al número de créditos de complementos de formación necesarios para alcanzar el perfil de entrada: sólo se admitirá a los estudiantes que puedan alcanzar el perfil de entrada con, como máximo, 60 ECTS de formación compensatoria.

El listado de complementos de formación se presenta en la tabla siguiente y está compuesto por asignaturas del Grado en Ingeniería Informática de la Universitat Oberta de Catalunya.

Complementos de formación **(0-60 ECTS entre las siguientes asignaturas de 6 cr cada una)**	
· Fundamentos de programación	· Prácticas de programación

· Diseño y programación orientada a objetos	· Lógica
· Álgebra	· Grafos y complejidad
· Fundamentos de computadores	· Redes y aplicaciones Internet
· Criptografía	· Estructura de computadores
· Sistemas operativos	· Administración de redes y sistemas operativos
· Uso de bases de datos	· Seguridad en redes de computadores
· Sistemas distribuidos	· Fundamentos de sistemas de información

En caso que se considere que el estudiante no puede alcanzar el perfil de ingreso al máster con una formación complementaria de 60 créditos, no se le admitirá en el programa.

Incorporación

Como se ha explicado anteriormente, una vez obtenido el acceso al máster, el estudiante recibirá su alta en el Campus Virtual, con un perfil específico de «incorporación» que facilita el acceso a la información relevante de acogida y orientación para los estudiantes de nuevo ingreso, y además con la asignación de un tutor o tutora de inicio, que le dará apoyo y orientaciones en el momento de formalizar su primera matrícula.

Estudiantes con discapacidad

El MISTIC utilizará el modelo educativo de la UOC. Éste se basa en la personalización y el acompañamiento permanente al estudiante, más allá de las limitaciones del tiempo y del espacio. Se trata, pues, de un modelo que consigue intrínsecamente elevadas cotas de igualdad de oportunidades en el acceso a la formación, al que se suman los esfuerzos necesarios para responder a las necesidades de los estudiantes con discapacidad.

Desde sus inicios, la UOC ha dedicado un importante esfuerzo a adaptar su tecnología para facilitar el acceso a la universidad de las personas con discapacidad. El propio sistema virtual permite la participación de personas con discapacidad auditiva o motriz de forma natural, ya que se basa en la escritura y en la conexión remota asíncrona. En este sentido, se han adaptado las interfaces del aula virtual con el fin de cumplir con la estandarización WAI AA del Consorcio W3C (www.w3c.org/WAI), que se recomienda para permitir una buena navegación por las interfaces web.

En cuanto a las acciones relacionadas directamente con el aprendizaje, se ha buscado aproximar sus contenidos docentes a todo el mundo, de manera que facilita la documentación de las asignaturas en formato PDF para permitir una lectura automática a partir de herramientas TTS (TextToSpeech). Actualmente, además, está en curso el proyecto de transformación de los contenidos de la UOC al formato DAISY (formato de libro hablado). Este formato permite a las personas con discapacidad visual trabajar con el contenido audio como si se tratara de un libro, pasar página o avanzar al siguiente capítulo con facilidad.

Igualmente dispone de un catálogo de servicios para atender las necesidades especiales en las acciones formativas desarrolladas presencialmente: encuentros presenciales y realización de exámenes. Se cuida la accesibilidad de todos los estudiantes, ofreciendo puntos de trabajo adaptados con lector de pantalla y línea braille según las necesidades.

Entre el colectivo de estudiantes con un grado de minusvalía superior al 33%, se aplicarán en los precios del máster las mismas exenciones y descuentos que se aplican en los programas del conjunto de universidades públicas catalanas.
Más concretamente, los servicios que ofrece la universidad coordinadora a los estudiantes del MISTIC con discapacidad son los siguientes:
- Acogida y seguimiento: Todos los estudiantes, desde el momento en que solicitan el acceso a la universidad, de manera previa a la matrícula, hasta su graduación, tienen a su disposición un tutor que se encargará de orientarlos y asesorarlos de manera personalizada. De esta manera los estudiantes con discapacidad pueden tener incluso antes de matricularse por primera vez información sobre el tipo de apoyo que para cada caso pueden obtener de la universidad.
- Materiales didácticos de las asignaturas: Los materiales didácticos tiene como objetivo permitir que el estudiante pueda estudiar sean cuales sean las circunstancias en las que deba hacerlo, independientemente del contexto en el que se encuentre (biblioteca, transporte público, domicilio, etc.), del dispositivo que esté utilizando (PC, móvil, etc.), o de las propias características personales del estudiante. Por este motivo se ha trabajado en diversos proyectos que han permitido avanzar en la creación de materiales en formato XML a partir del cual se generan versiones de un mismo contenido en múltiples formatos, como pueden ser materiales en papel, PDF, HTML, karaoke, libro hablado, libro electrónico. Cada uno de estos formatos está diseñado para ser utilizado en un determinado momento o situación, y se está trabajando para garantizar que este abanico de posibilidades se encuentra disponible para los materiales de todas las asignaturas. Por ejemplo, el libro hablado resulta muy interesante para responder a las necesidades de las personas con discapacidad visual, ya que el formato DAISY que utiliza les permite trabajar con el contenido en audio como si se tratará de un libro, pasando página o avanzando hasta el siguiente capítulo con facilidad. La versión HTML permite realizar búsquedas en el contenido del material y el formato PDF permite una lectura automática a partir de herramientas TTS (TextToSpeech). Se sigue investigando en como elaborar nuevos formatos que se adapten a las necesidades de los distintos estudiantes cada vez con una mayor precisión, con el objetivo de avanzar hacia una universidad cada vez más accesible e inclusiva.
- Plataforma de aprendizaje. Campus de la UOC: Desde sus inicios la UOC siempre ha dedicado un importante esfuerzo a adaptar su tecnología con el objetivo de facilitar el acceso de las personas con discapacidad a la universidad. Ya su propio sistema virtual permite la participación de personas con discapacidad auditiva o motriz de forma natural, al estar basado en la escritura y en la conexión remota asíncrona. Además, se han adaptado las distintas interfaces del campus virtual para cumplir con la estandarización WAI AA del consorcio w3c (www.w3c.org/WAI), recomendada para permitir una buena navegación por las interfaces web en el caso de personas con discapacidad visual.
- Actos presenciales: La UOC es una universidad a distancia donde toda la formación se desarrolla a través de las herramientas de comunicación y trabajo que proporciona el campus virtual. Sin embargo, semestralmente se desarrollan determinadas actividades presenciales. Algunas son voluntarias, como la asistencia al encuentro de inicio de semestre o al acto de graduación, y otras son obligatorias, como la realización de las pruebas finales de evaluación.
• Encuentro de inicio de semestre y Acto de graduación. Los estudiantes con discapacidad pueden dirigirse al servicio de la UOC responsable de la organización de estos actos para hacerles llegar sus necesidades. A demanda del estudiante, se buscarán los medios necesarios para que su asistencia sea lo

más fácil y satisfactoria posible. Toda solicitud es siempre aceptada. En la página web informativa de estos actos se haya toda la información sobre la posibilidad de realizar este tipo de peticiones, así como el enlace que facilita a los estudiantes realizar su solicitud. Los servicios que pueden solicitarse son, entre otros:
o Rampas y accesos adaptados
o Aparcamiento reservado
o Acompañamiento durante el acto
o Intérprete de lenguaje de signos
• Pruebas presenciales de evaluación: En la secretaria del campus los estudiantes encuentran información sobre el procedimiento a seguir para solicitar adaptaciones para la realización de las pruebas presenciales. Han de rellenar un formulario. El estudiante puede solicitar cualquier tipo de adaptación, que se concederá siempre que sea justificada documentalmente. Las adaptaciones más solicitadas en el caso de las pruebas presenciales de evaluación son las siguientes:
o Rampas y accesos adaptados o Programa Jaws
o Zoomtext o Enunciados en Braille
o Realizar las pruebas con ayuda de un PC
o Realización de pruebas orales
o Enunciados adaptados
o Más tiempo para realizar las pruebas

4.3 APOYO A ESTUDIANTES

La universidad coordinadora del máster, la UOC, cuenta con una infraestructura que permite un sistema personalizado de apoyo y orientación a los estudiantes. Los profesores, docentes colaboradores y tutores de la UOC, UAB y URV darán apoyo y orientación al estudiante al largo de todos sus estudios.
El estudiante, una vez matriculado, tiene acceso a las aulas virtuales de las asignaturas que cursa. La responsabilidad sobre las asignaturas del máster es lo que definimos con el rol de profesor responsable de asignatura (PRA). Cada PRA se responsabiliza de un grupo de asignaturas dentro de su área de conocimiento y es el responsable de garantizar la docencia que recibe el estudiante, por lo que está presente en todo el proceso de enseñanza/aprendizaje, desde la elaboración, supervisión y revisión de los materiales docentes hasta la selección, coordinación y supervisión de los colaboradores docentes, el diseño del plan docente, la planificación de todas las actividades del semestre y la evaluación de los procesos de aprendizaje de los estudiantes.
El docente colaborador, bajo la dirección y coordinación del profesor responsable de asignatura, es para el estudiante la figura que le orientará en el proceso de enseñanza-aprendizaje, y en su progreso académico. Es la guía y el referente académico del estudiante, al que estimula y evalúa durante el proceso de aprendizaje, y garantiza una formación personalizada.
Su papel se centra en lo siguiente:
- Ayudar al estudiante a identificar sus necesidades de aprendizaje.
- Motivarle para mantener y reforzar su constancia y esfuerzo.
- Ofrecerle una guía y orientación del proceso que debe seguir.
- Resolver sus dudas y orientar su estudio.
- Evaluar sus actividades y reconocer el grado de consecución de los objetivos de aprendizaje y del nivel de competencias asumidas, proponiendo, cuando sea necesario, las medidas para mejorarlas.
Además del docente colaborador, el tutor ofrece apoyo a los estudiantes durante el desarrollo del programa.
En función del progreso académico del estudiante durante el desarrollo del programa, la acción tutorial se focaliza en aspectos diferentes de la actividad del estudiante. Así, en un primer momento, al inicio de su formación, el tutor se encarga de acoger e integrar al estudiante en la comunidad universitaria y de asesorarle respecto de las características académicas y docentes del programa al que quiere acceder; le acompaña en su adaptación al entorno de aprendizaje; le presenta los diferentes perfiles e itinerarios del programa de formación, y le orienta en relación con la coherencia de los contenidos que tiene que alcanzar, remarcando su sentido global, asesorándole sobre especialidades académicas y profesionales más adecuadas en función de los conocimientos y la experiencia profesional previa. El tutor desarrolla estas funciones teniendo en cuenta las especiales características de cada estudiante con respecto a su lengua, país de origen, intereses y motivaciones, y de acuerdo con su situación personal.
En un segundo momento le ayuda a adquirir autonomía y estrategias de aprendizaje mediante el modelo y la metodología de aprendizaje virtual. Durante el desarrollo de la actividad le orienta en función de la elección de contenidos hasta la consecución de los objetivos propuestos dentro del programa. También participa en la definición y la valoración de los proyectos de aplicación que realicen los estudiantes promoviendo el pensamiento crítico en torno a la profesión.
El equipo de tutores es coordinado por el director del programa, que realiza un seguimiento continuado del mismo en las diferentes acciones. El plan de tutoría se ajusta a la singularidad de cada una de las titulaciones. Los tutores elaboran una propuesta de plan de tutoría -a partir de las especificidades de cada programa- que cuenta para su desarrollo con la aprobación del Director del Programa y la validación del equipo de Desarrollo de la Función Tutorial de la universidad coordinadora. Son los tutores los que tienen la función de llevar a cabo el plan de tutoría a lo largo del semestre, a través de las aulas de tutoría del Campus Virtual.
En paralelo, el Grupo de Desarrollo de la Función Tutorial apoya a los tutores facilitándoles las herramientas y las informaciones necesarias con el fin de que puedan dar una respuesta adecuada a las necesidades de los estudiantes, principalmente en aquellos aspectos más transversales y vinculados a los servicios y a las informaciones de la universidad coordinadora.
El Grupo de Desarrollo de la Función Tutorial recopila, de forma sistemática, la actividad del estudiante en relación con el seguimiento de la docencia y también las acciones que lleva a cabo el tutor para asesorarlo.
Al finalizar el semestre, el director del programa y el Grupo de Desarrollo de la Función Tutorial, valoran el funcionamiento y los resultados obtenidos (rendimiento y satisfacción) con el fin de poder introducir cambios, en el siguiente semestre, en el plan de tutoría del programa y de esta manera poder dar una mejor respuesta a las necesidades de los estudiantes.

El director del Programa y el Grupo de Desarrollo de la Función Tutorial celebran reuniones presenciales con los tutores con el fin de hacer seguimiento de su actividad y compartir las propuestas de acciones de mejora. Son los responsables de que se apliquen las mejoras propuestas y de hacer un seguimiento de sus resultados.
Conviene recordar que el Comité de Evaluación Externo del proceso de Evaluación institucional seguido por la universidad, bajo las directrices de AQU Catalunya, valoró muy adecuadamente el funcionamiento de la acogida definido por la universidad, teniendo en cuenta "el buen desarrollo del plan tutorial: su alto grado de formalización, su evolución, y valoración por los diferentes colectivos, motivo por el cual se valoran como muy adecuados los mecanismos de aseguramiento de calidad de la acogida".
Como mecanismo de apoyo a los estudiantes, también podemos mencionar otros servicios de los que puede beneficiarse el estudiante de la universidad una vez matriculado. Básicamente destacamos los servicios de biblioteca y recursos de la UOC, la UAB y la URV, así como los servicios de ayuda informática, atención de consultas y servicios territoriales de la universidad coordinadora.
Los estudiantes tienen a su disposición, desde el inicio del semestre, todo el material y documentación de referencia de cada una de las asignaturas de las que se ha matriculado.
Los estudiantes encuentran en los materiales y recursos didácticos los contenidos que contribuyen, juntamente con la realización de las actividades que han sido planificadas desde el inicio del semestre, a la obtención de los conocimientos, las competencias y las habilidades previstas en las asignaturas. Todos estos contenidos han sido elaborados por un equipo de profesores expertos en las diversas áreas de conocimiento y de la didáctica, y de acuerdo con los principios del modelo pedagógico de la UOC. Los materiales pueden presentarse en diferentes formatos: papel, web, vídeo, multimedia… en función de la metodología y del tipo de contenido que se plantee. Igualmente los estudiantes pueden disponer de otros recursos a través de la biblioteca virtual que ofrece los servicios de consulta, préstamo, servicio de documentos electrónicos servicio de información a medida. Además, ofrece formación a los usuarios para facilitar el uso de los servicios.
Del mismo modo, la UOC pone a disposición de los estudiantes el Servicio de Atención que aglutina el Servicio de atención de consultas y el Servicio de ayuda informática. El Servicio de atención a consultas es el responsable de resolver cualquier duda académica o administrativa. El Servicio de ayuda informática es el responsable de asesorar a los usuarios del campus virtual en relación a las posibles dudas o incidencias que puedan surgir en la utilización del campus virtual, los problemas de acceso a los materiales y el software facilitado por la universidad. El servicio de ayuda informática se efectúa de manera digital, pero se habilita un servició de consulta directo de manera que el estudiante también puede tener acceso a través de vía telefónica.
El acceso al servicio de atención de consultas es único para el estudiante -siempre accede desde la misma aplicación informática disponible desde el campus- y es atendido por un mismo equipo. Este será el responsable de buscar la respuesta a la consulta hecha y de facilitarla al estudiante.
Por último para contribuir a mejorar la atención personalizada y presencial a los estudiantes, la UOC dispone de diecisiete centros de apoyo y también de cuarenta y siete puntos de información. Estos centros además de puntos de información son centros de servicios académicos y administrativos que facilitan la recogida de sugerencias, demandas o necesidades. Por otro lado, a parte de la universidad coordinadora, el resto de universidades participantes en el máster (UAB y URV) también ofrecerán información y a través de los puntos de información de sus campus universitarios.

4.4 SISTEMA DE TRANSFERENCIA Y RECONOCIMIENTO DE CRÉDITOS

Reconocimiento de Créditos Cursados en Enseñanzas Superiores Oficiales no Universitarias

MÍNIMO	MÁXIMO
0	60

Reconocimiento de Créditos Cursados en Títulos Propios

MÍNIMO	MÁXIMO
0	60

Adjuntar Título Propio

Ver anexos. Apartado 4.

Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional

MÍNIMO	MÁXIMO
0	9

Reconocimiento de créditos
El MISTIC entiende por reconocimiento de créditos ECTS la aceptación por parte de la universidad coordinadora de los créditos obtenidos en enseñanzas universitarias de carácter oficial, ya sea en la UOC, UAB, URV o en otra universidad, para que computen en otros estudios a los efectos de obtener una titulación universitaria de carácter oficial.
Asimismo, y de acuerdo con el artículo 6 del RD 1393/2007, de 29 octubre, según redacción otorgada por el RD 861/2010, de 2 de julio, la experiencia laboral y profesional acreditada, así como los créditos obtenidos en enseñanzas universitarias conducentes a la obtención de títulos no oficiales, también podrán ser reconocidos en forma de créditos que computarán a efectos de la obtención del MISTIC, siempre que dicha experiencia o títulos estén relacionados con las competencias inherentes al Máster.
La unidad básica del reconocimiento será el crédito ECTS (sistema europeo de transferencia de créditos), regulado en el Real decreto 1125/2003, de 5 de septiembre, por el cual se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y con validez en todo el territorio nacional.
Los créditos ECTS serán susceptibles de ser incorporados al expediente académico del estudiante y serán reflejadas en el Suplemento Europeo al Título, en virtud de lo establecido en el artículo 6 del Real decreto 1393/2007, de 29 de octubre, por el cual se establece la ordenación de las enseñanzas universitarias oficiales.
Los estudios previos y la experiencia laboral y profesional aportados serán susceptibles de reconocimiento en función del programa de Máster de destino. Por tanto, el reconocimiento de créditos ECTS podrá ser diferente si los mismos estudios de origen se aportan a otro programa de Máster de destino.
Las asignaturas reconocidas, transferidas, convalidadas y adaptadas, en la medida que tienen la consideración de asignaturas superadas, también serán susceptibles de reconocimiento.
Los criterios en materia de reconocimiento de asignaturas de titulaciones oficiales que se han establecido, cuando los estudios de destino sean enseñanzas oficiales de Máster, son los siguientes:
1. Cuando los estudios aportados sean enseñanzas universitarias conducentes a la obtención del título oficial de Diplomado, Ingeniero Técnico, Arquitecto Técnico o de Graduado, no serán susceptibles de reconocimiento al no existir adecuación entre el nivel de competencia exigido en las enseñanzas aportadas y el previsto en el programa de Máster de destino.
2. Cuando los estudios aportados sean enseñanzas universitarias conducentes a la obtención del título de Licenciado, Ingeniero, Arquitecto, Máster Universitario o Doctorado, las asignaturas aportadas serán susceptibles de reconocimiento si, a criterio de la dirección de programa de Máster correspondiente, existe equivalencia o adecuación entre las competencias y los conocimientos asociados a las asignaturas cursadas en los estudios aportados y los previstos en el programa de Máster de destino.
Los estudiantes del máster de Seguridad Informática de la UOC (título propio) podrán obtener el reconocimiento de créditos académicos del plan de estudios del MISTIC, en función de las asignaturas o grupo de asignaturas superadas hasta el momento por el estudiante de acuerdo con la tabla de equivalencias que se detalla a continuación.

Máster Seguridad UOC	MISTIC

Asignatura	Cr	Tp	Materia	Cr	Tp
Explotación de vulnerabilidades	6	C	Vulnerabilidades de seguridad	6	C
Aspectos legales	6	C	Legislación y regulación	6	C
Seguridad en redes	6	P	Seguridad en redes	6	OE
Seguridad en sistemas operativos	6	P	Seguridad en sistemas operativos	6	OE
Seguridad en bases de datos	6	P	Seguridad en bases de datos	6	OE
Sistemas de gestión de la seguridad de la información	6	C	Sistemas de gestión de la seguridad	6	OE
Auditoría técnica y de certificación	6	P	Auditoría técnica	6	OE
Análisis forense y evidencia digital	6	P	Análisis forense	6	OE
Grupos de asignaturas (3 de 4)	**Cr**		**Especialidad**	**Cr**	
- Sistemas de gestión de la seguridad de la información - Planes de continuidad de negocio - Auditoria técnica y de certificación	18		Gestión y auditoria de la seguridad	18	

- Análisis forense y evidencia digital			
Grupos de asignaturas (3 de 5)	**Cr**	**Especialidad**	**Cr**
- Seguridad en redes - Seguridad en aplicaciones web - Seguridad en bases de datos - Seguridad en sistemas operativos - Programación segura	18	Seguridad en redes y sistemas	18

C": asignatura común "
OE": asignatura obligatoria de especialidad
"P": asignatura optativa
Los criterios para el reconocimiento de competencias a través de la experiencia profesional y laboral son las siguientes:
1. Cuando el estudiante aporte evidencias de experiencia profesional de un mínimo de un año en puestos de administración de redes y servicios, programación de aplicaciones seguras, o en consultoría de sistemas de gestión de la seguridad de la información, se le reconocerá la materia de Prácticas profesionalizadoras, de 3 ECTS.
2. Cuando el estudiante aporte evidencias de experiencia profesional de un mínimo de dos años en los puestos anteriores y además pueda demostrar que ha alcanzado las competencias asociadas a una de las materias del MISTIC, se le reconocerá dicha materia (a excepción del Trabajo fin de máster, que no es susceptible a reconocimientos).
Solamente se otorgaran créditos por el aprendizaje mostrado, no por la simple experiencia acumulada.
Para la evaluación del reconocimiento de la experiencia profesional se tendrán en cuenta todas aquellas evidencias que el estudiante pueda aportar, tanto para demostrar su actividad profesional (p.e. contratos de trabajo, certificado de vida laboral de la Tesorería General de la Seguridad Social, certificados de empresa donde conste la duración del contrato, las actividades realizadas y la duración de las mismas), como para demostrar las características y la calidad de las actividades desarrolladas (p.e. cartas de recomendación, evidencias de los resultados del trabajo –muestras, fotos, videos, ..-).

Transferencia de créditos

Las asignaturas transferidas se verán reflejadas en el expediente académico del estudiante y en el Suplemento Europeo al Título, en virtud de lo establecido en el artículo 6.3 del Real decreto 1393/2007, de 29 de octubre, por el cual se establece la ordenación de las enseñanzas universitarias oficiales.

Sistema de gestión del reconocimiento y transferencia de créditos

La evaluación de estudios previos (EEP) es el trámite que permite a los estudiantes valorar su bagaje universitario anterior y obtener el reconocimiento -o en su caso la transferencia- de los créditos cursados y superados en alguna titulación anterior, en la UOC, UAB, URV, o en cualquier otra universidad.
Las solicitudes de EEP son evaluadas y resueltas por la Comisión de Evaluación de Estudios Previos. La Comisión de Evaluación de Estudios Previos (EEP) es el órgano competente para emitir las resoluciones correspondientes a las solicitudes de evaluación de estudios previos realizadas por los estudiantes.
La Comisión de EEP está formada por un representante de cada universidad participante en el MISTIC, el director académico del mismo, y es presidida por el Vicerrector de Ordenación Académica y Profesorado de la UOC. Actúa como secretario/a de la Comisión de EEP el responsable de este trámite de la Secretaria Académica.
Las funciones específicas de la Comisión de EEP son las siguientes:
1. Evaluar la equivalencia o adecuación entre las competencias y los conocimientos asociados a las asignaturas cursadas en los estudios aportados y los previstos en el plan de estudio de la titulación de destino.
2. Emitir las resoluciones de EEP.
3. Resolver las alegaciones formuladas por los estudiantes a la resolución de la solicitud de evaluación de estudios previos emitida, valorando la correspondencia entre las asignaturas y competencias adquiridas en los estudios aportados y los previstos en el plan de estudio de destino.
4. Velar por el cumplimiento de los criterios de reconocimiento y transferencia de créditos aprobados por la universidad, y por el correcto desarrollo del proceso de EEP.
Los estudiantes pueden realizar un número ilimitado de solicitudes de EEP, incluso aportando los mismos estudios previos.
Las solicitudes de EEP son válidas si el estudiante introduce sus datos en el repositorio de estudios previos, abona la tasa asociada al trámite y envía la documentación requerida dentro de los plazos establecidos.
Para poder realizar una solicitud de EEP es necesario haber introducido previamente los datos de los estudios aportados en el repositorio de estudios previos. El repositorio es un reflejo del estudio previo aportado por el estudiante, donde se indican las asignaturas superadas, el tipo de asignatura (básica, obligatoria, optativa, troncal o de libre elección), los créditos, la calificación obtenida, el año de superación y si se trata de una asignatura semestral o anual.

Una vez introducidos los datos en el repositorio, el estudiante ya podrá realizar una solicitud de EEP en los plazos establecidos en el calendario académico de la UOC.
Realizada la solicitud de EEP, el estudiante dispone de un plazo máximo de 15 días naturales para aportar la documentación correspondiente y abonar la tasa asociada a dicho trámite. Emitida la resolución por parte de la Comisión de EEP, el estudiante recibe notificación de la misma a través de un correo electrónico a su buzón personal. Una vez notificada la resolución de EEP, si el estudiante no está de acuerdo, dispone de un plazo de 15 días naturales para alegar contra el resultado de la resolución de EEP.

4.6 COMPLEMENTOS FORMATIVOS

Pueden ser admitidas al Máster las personas que hayan cursado los siguientes estudios:
1. Titulados en Ingeniería Informática (Graduados, Ingenieros, Ingenieros Técnicos).
2. Titulados del área de Ingeniería y Arquitectura (Graduados, Ingenieros, Ingenieros Técnicos, Licenciados, Diplomados) en especialidades vinculadas a las tecnologías de la información y de las comunicaciones. Por ejemplo, Telecomunicaciones o Multimedia.
3. Titulados en el área de Ciencias, en las especialidades de Matemáticas, Física y Estadística (Graduados, Licenciados, Diplomados).
4. Otros titulados.
Los dos primeros grupos de titulados (Ingenieros informáticos e Ingenieros del área TIC) no necesitarán cursar ningún complemento de formación para iniciar el MISTIC, mientras que el tercer grupo (Titulados en el área de Ciencias) es probable que tenga que cursar créditos de formación compensatoria (como máximo 30 ECTS).
Para los restantes titulados (cuarto grupo), siempre y cuando cumplan las condiciones de acceso legalmente previstas, su admisión al máster quedará supeditada al número de créditos de complementos de formación que debieran cursar.
El listado de complementos de formación se presenta en la tabla siguiente y está compuesto por asignaturas del Grado en Ingeniería Informática de la Universitat Oberta de Catalunya.

Complementos de formación
(0-60 ECTS entre las siguientes asignaturas de 6 cr cada una)

· Fundamentos de programación	· Prácticas de programación
· Diseño y programación orientada a objetos	· Lógica
· Álgebra	· Grafos y complejidad
· Fundamentos de computadores	· Redes y aplicaciones Internet
· Criptografía	· Estructura de computadores
· Sistemas operativos	· Administración de redes y sistemas operativos
· Uso de bases de datos	· Seguridad en redes de computadores
· Sistemas distribuidos	· Fundamentos de sistemas de información

5. PLANIFICACIÓN DE LAS ENSEÑANZAS

5.1 DESCRIPCIÓN DEL PLAN DE ESTUDIOS

Ver anexos. Apartado 5.

5.2 ACTIVIDADES FORMATIVAS

1- PREGUNTAS TEÓRICAS
2- RESOLUCIÓN DE PROBLEMAS
3- PRÁCTICAS
4- ESTUDIO DE CASOS
5- BÚSQUEDA DE INFORMACIÓN
6- DEBATE
7- REDACCIÓN DE TEXTOS
8- PRESENTACIONES ORALES
9- INFORME DE APRENDIZAJE
10- LECTURA DE TEXTOS Y ARTÍCULOS
11- PROYECTO

12- REDACCIÓN DE INFORMES
13- REDACCIÓN ARTÍCULO CIENTÍFICO
0- LECTURA DE MATERIAL DIDÁCTICO
5.3 METODOLOGÍAS DOCENTES
1- Instrucción programada a través de materiales docentes
2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)
3- Participación en un debate (los alumnos contraponen dos o más opiniones expertas sobre un tema polémico y de interés, que sigue un plan controlado por el docente)
4- Aprendizaje basado en la resolución de problemas
5- Aprendizaje basado en el desarrollo de proyectos prácticos
6- Método basado en el estudio y análisis de casos reales
7- Aprendizaje basado en la búsqueda de información
8- Lectura de documentación científico-técnica muy especializada
9- Exposición pública por parte de los estudiantes
5.4 SISTEMAS DE EVALUACIÓN
1- Participación en foros y debates
2- Resolución de problemas
3- Desarrollo de proyectos prácticos y demostradores
4- Elaboración de informes
5- Exposiciones de trabajos
6- Realización de pruebas finales de evaluación que engloban todo el contenido de una materia
7- Redacción de artículos científicos
5.5 NIVEL 1: Módulo de formación obligatoria: Comunes
5.5.1 Datos Básicos del Módulo
NIVEL 2: Vulnerabilidades de seguridad

5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	OBLIGATORIA	
ECTS MATERIA	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No

ITALIANO	**OTRAS**	
No	No	
NIVEL 3: Vulnerabilidades de Seguridad		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
OBLIGATORIA	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
5.5.1.2 RESULTADOS DE APRENDIZAJE		
• Conocer las bases de la seguridad informática en diferentes ámbitos: vulnerabilidades y ataques en redes y sistemas, necesidades de seguridad en el desarrollo de aplicaciones, consideraciones legislativas de la seguridad. • Describir los requerimientos de seguridad de un sistema y la criticidad de cada uno de ellos.		
5.5.1.3 CONTENIDOS		
Esta materia hace un repaso a las amenazas, vulnerabilidades y ataques de seguridad en redes y sistemas. La materia incide en el aprendizaje de metodologías y herramientas para identificar y minimizar las vulnerabilidades desde una perspectiva práctica y aplicada. Se expondrá a los estudiantes a una variedad de ataques actualmente presentes: virus, troyanos, gusanos, rootkits, bootnets. Asimismo, se analizarán las técnicas utilizadas para llevar a cabo ataques basados en Ingeniería social y se estudiarán las contramedidas de seguridad que pueden ayudar a prevenirla.		
5.5.1.4 OBSERVACIONES		
5.5.1.5 COMPETENCIAS		
5.5.1.5.1 BÁSICAS Y GENERALES		
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 - Capacidad de análisis y síntesis de la seguridad de un sistema.
CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.
CT3 - Capacidad de comunicación tanto a público especializado como no especializado de modo claro y sin ambigüedades.
CT4 - Capacidad de aprendizaje autónomo consultando información
CT6 - Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática
CT7 - Uso del inglés como lengua vehicular en el ámbito tecnológico
5.5.1.5.3 ESPECÍFICAS
CE8 - Capacidad para analizar las técnicas de explotación de vulnerabilidades de una red y los puntos débles de un sistema.
CE9 - Capacidad para identificar, evaluar y gestionar los principales riesgos de un dominio informático, tanto tecnológicos como procedentes de la ingeniería social
CE10 - Capacidad para usar técnicas y contramedidas básicas de seguridad para la prevención de ataques derivados de la ingeniería social
CE21 - Capacidad para diseñar soluciones integrales apropiadas en escenarios complejos que combinen las técnicas y contramedidas conocidas para la prevención, detección y disuasión de ataques. (Perfil de Seguridad en Redes y Sistemas)

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
1- PREGUNTAS TEÓRICAS	10	0
2- RESOLUCIÓN DE PROBLEMAS	20	0
3- PRÁCTICAS	40	0
4- ESTUDIO DE CASOS	40	0
5- BÚSQUEDA DE INFORMACIÓN	10	0
6- DEBATE	10	0
0- LECTURA DE MATERIAL DIDÁCTICO	20	0

5.5.1.7 METODOLOGÍAS DOCENTES
1- Instrucción programada a través de materiales docentes
2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)
3- Participación en un debate (los alumnos contraponen dos o más opiniones expertas sobre un tema polémico y de interés, que sigue un plan controlado por el docente)
4- Aprendizaje basado en la resolución de problemas
5- Aprendizaje basado en el desarrollo de proyectos prácticos
6- Método basado en el estudio y análisis de casos reales
7- Aprendizaje basado en la búsqueda de información

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
1- Participación en foros y debates	10.0	30.0
2- Resolución de problemas	20.0	40.0
3- Desarrollo de proyectos prácticos y demostradores	20.0	50.0
4- Elaboración de informes	20.0	50.0
6- Realización de pruebas finales de evaluación que engloban todo el contenido de una materia	0.0	100.0

NIVEL 2: Legislación y Regulación

5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	OBLIGATORIA	
ECTS MATERIA	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NIVEL 3: Legislación y Regulación		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
OBLIGATORIA	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
5.5.1.2 RESULTADOS DE APRENDIZAJE		
- Conocer las bases de la seguridad informática en diferentes ámbitos: vulnerabilidades y ataques en redes y sistemas, necesidades de seguridad en el desarrollo de aplicaciones, consideraciones legislativas de la seguridad. Esta materia se focalizará en las consideraciones legislativas de la seguridad. - Conocer los fundamentos jurídicos sobre seguridad informática		

5.5.1.3 CONTENIDOS

En esta materia se describen los aspectos de la legislación nacional e internacional que están relacionados con la seguridad informática. Se introducen los fundamentos jurídicos, el derecho penal y los tipos de delitos existentes. Se hace un amplio análisis de las leyes LOPD, LSSICE, firma digital, y facturación electrónica.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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

CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.

CT7 - Uso del inglés como lengua vehicular en el ámbito tecnológico

5.5.1.5.3 ESPECÍFICAS

CE12 - Capacidad para aplicar el marco jurídico que afecta a la gestión de la seguridad de sistemas informáticos, teniendo en cuenta la legislación relativa a la propiedad intelectual, el comercio electrónico, la firma electrónica y la protección de datos de carácter personal.

CE13 - Poseer y comprender conocimientos de las estructuras normalizadoras, evaluadoras, certificadoras, y las normas correspondientes que regulan los ámbitos de la seguridad.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
0- LECTURA DE MATERIAL DIDÁCTICO	20	0
1- PREGUNTAS TEÓRICAS	20	0
2- RESOLUCIÓN DE PROBLEMAS	20	0
3- PRÁCTICAS	20	0
4- ESTUDIO DE CASOS	40	0
5- BÚSQUEDA DE INFORMACIÓN	10	0
6- DEBATE	20	0

5.5.1.7 METODOLOGÍAS DOCENTES

1- Instrucción programada a través de materiales docentes

2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)

3- Participación en un debate (los alumnos contraponen dos o más opiniones expertas sobre un tema polémico y de interés, que sigue un plan controlado por el docente)

5- Aprendizaje basado en el desarrollo de proyectos prácticos

6- Método basado en el estudio y análisis de casos reales

7- Aprendizaje basado en la búsqueda de información

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
1- Participación en foros y debates	10.0	40.0
3- Desarrollo de proyectos prácticos y demostradores	20.0	50.0

4- Elaboración de informes	20.0	50.0
6- Realización de pruebas finales de evaluación que engloban todo el contenido de una materia	0.0	100.0

NIVEL 2: Identidad Digital		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	OBLIGATORIA	
ECTS MATERIA	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NIVEL 3: Identidad Digital		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
OBLIGATORIA	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	

No	No

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Conocer las bases de la seguridad informática en diferentes ámbitos: vulnerabilidades y ataques en redes y sistemas, necesidades de seguridad en el desarrollo de aplicaciones, consideraciones legislativas de la seguridad.
- Conocer la importancia de la seguridad en Internet, en términos de sus implicaciones en diferentes sectores: comercio electrónico, banca electrónica, distribución de contenidos, redes sociales, publicidad, spam.

5.5.1.3 CONTENIDOS

Esta materia se focaliza en las técnicas de gestión de las identidades digitales y su protección frente a los riesgos de privacidad y a los ataques de falsificación de datos. Se introducen protocolos y herramientas de autentificación fuerte, sistemas de autorización, sistemas de “single sign-on” y servicios de federación. También se aprenden los conceptos y métodos para la creación de tecnologías y políticas que garanticen la protección de la privacidad al mismo tiempo que permitan que la sociedad pueda compartir información personal para propósitos específicos y acordados. Los métodos incluyen procesos relacionados con la identidad de los datos, la vinculación de los registros, generar perfiles a partir de los datos, fusión de datos, datos de anonimato, especificación y aplicación de políticas, y data mining preservando la privacidad.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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

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.

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 - Capacidad de análisis y síntesis de la seguridad de un sistema.

CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.

CT4 - Capacidad de aprendizaje autónomo consultando información

CT5 - Capacidad para seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas en entornos nuevos

CT6 - Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática

CT7 - Uso del inglés como lengua vehicular en el ámbito tecnológico

5.5.1.5.3 ESPECÍFICAS

CE14 - Poseer y comprender conocimientos de las arquitecturas más importantes de AAA (Authentication, Authorization, Accounting), así como sistemas de federación de identidades y de autenticación única (SSO-Single Sign On).

CE15 - Capacidad para identificar las vulnerabilidades de privacidad de los sistemas (especialmente en aplicaciones web) y capacidad para protegerlos

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD

0- LECTURA DE MATERIAL DIDÁCTICO	20	0
1- PREGUNTAS TEÓRICAS	10	0
2- RESOLUCIÓN DE PROBLEMAS	20	0
3- PRÁCTICAS	40	0
4- ESTUDIO DE CASOS	30	0
5- BÚSQUEDA DE INFORMACIÓN	20	0
6- DEBATE	10	0

5.5.1.7 METODOLOGÍAS DOCENTES

1- Instrucción programada a través de materiales docentes

2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)

3- Participación en un debate (los alumnos contraponen dos o más opiniones expertas sobre un tema polémico y de interés, que sigue un plan controlado por el docente)

4- Aprendizaje basado en la resolución de problemas

5- Aprendizaje basado en el desarrollo de proyectos prácticos

6- Método basado en el estudio y análisis de casos reales

7- Aprendizaje basado en la búsqueda de información

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
1- Participación en foros y debates	10.0	30.0
2- Resolución de problemas	20.0	40.0
3- Desarrollo de proyectos prácticos y demostradores	20.0	50.0
4- Elaboración de informes	20.0	50.0
6- Realización de pruebas finales de evaluación que engloban todo el contenido de una materia	0.0	100.0

5.5 NIVEL 1: Módulo de Especialidad 1: Seguridad en Redes y Sistemas

5.5.1 Datos Básicos del Módulo

NIVEL 2: Seguridad en Redes

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	OPTATIVA	
ECTS MATERIA	6	

DESPLIEGUE TEMPORAL: Semestral

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

LENGUAS EN LAS QUE SE IMPARTE

CASTELLANO	CATALÁN	EUSKERA
Si	Si	No

GALLEGO	VALENCIANO	INGLÉS
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
Seguridad en Redes y Sistemas		

NIVEL 3: Seguridad en Redes

5.5.1.1.1 Datos Básicos del Nivel 3

CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
OPTATIVA	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
Seguridad en Redes y Sistemas		

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Conocer las herramientas para analizar la seguridad de una red y saber elegir la más apropiada en cada situación.
- Evaluar y proteger un sistema informático frente a ataques de seguridad.
- Detectar de forma rápida y eficiente las incidencias de seguridad en los sistemas, así como analizar de forma rigurosa su origen y los rastros de infección.
- Conocer dónde buscar información puntualmente actualizada de las vulnerabilidades de seguridad que los sistemas presentan.
- Saber actualizar los conocimientos de seguridad en redes, sistemas operativos y bases de datos, forma rápida y constante.

5.5.1.3 CONTENIDOS

Esta materia se centra en el diseño y planificación de redes seguras. Se hace un repaso a las arquitecturas de cortafuegos y redes privadas virtuales, y se analiza la seguridad de los protocolos Internet (ARP, DNS, IPSec,..). Se presentan las vulnerabilidades de las redes inalámbricas y se analizan los sistemas y protocolos para proteger las comunicaciones en este entorno. Se estudian protocolos de redes PAN (Bluetooth, Zigbee), LAN (wifi), MAN (wimax, ad hoc) y WAN (celulares). Finalmente, en esta materia se trabaja cómo diseñar y verificar que un sistema de comunicación es seguro.

5.5.1.4 OBSERVACIONES

La asignatura de esta materia es de obligatorio seguimiento para los estudiantes que quieran obtener la especialidad Seguridad en Redes y Sistemas

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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

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.

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

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

5.5.1.5.2 TRANSVERSALES

CT1 - Capacidad de análisis y síntesis de la seguridad de un sistema.

CT3 - Capacidad de comunicación tanto a público especializado como no especializado de modo claro y sin ambigüedades.

CT4 - Capacidad de aprendizaje autónomo consultando información

CT5 - Capacidad para seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas en entornos nuevos

CT6 - Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática

CT7 - Uso del inglés como lengua vehicular en el ámbito tecnológico

5.5.1.5.3 ESPECÍFICAS

CE8 - Capacidad para analizar las técnicas de explotación de vulnerabilidades de una red y los puntos débles de un sistema.

CE16 - Capacidad para comprender y saber usar herramientas para la administración y protección de redes cableadas e inalámbricas, y la gestión de alertas de seguridad. (Perfil de Seguridad en Redes y Sistemas)

CE17 - Capacidad para concebir, desplegar, organizar y gestionar redes de comunicaciones en contextos residenciales, empresariales o institucionales, responsabilizándose de la seguridad del sistema y la protección de los datos de los usuarios. (Perfil de Seguridad en Redes y Sistemas)

CE21 - Capacidad para diseñar soluciones integrales apropiadas en escenarios complejos que combinen las técnicas y contramedidas conocidas para la prevención, detección y disuasión de ataques. (Perfil de Seguridad en Redes y Sistemas)

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
0- LECTURA DE MATERIAL DIDÁCTICO	20	0
1- PREGUNTAS TEÓRICAS	10	0
2- RESOLUCIÓN DE PROBLEMAS	20	0
3- PRÁCTICAS	40	0
4- ESTUDIO DE CASOS	20	0
5- BÚSQUEDA DE INFORMACIÓN	10	0
6- DEBATE	10	0
10- LECTURA DE TEXTOS Y ARTÍCULOS	20	0

5.5.1.7 METODOLOGÍAS DOCENTES

1- Instrucción programada a través de materiales docentes

2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)
3- Participación en un debate (los alumnos contraponen dos o más opiniones expertas sobre un tema polémico y de interés, que sigue un plan controlado por el docente)
4- Aprendizaje basado en la resolución de problemas
5- Aprendizaje basado en el desarrollo de proyectos prácticos
6- Método basado en el estudio y análisis de casos reales
7- Aprendizaje basado en la búsqueda de información
8- Lectura de documentación científico-técnica muy especializada

5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
1- Participación en foros y debates	10.0	30.0
2- Resolución de problemas	20.0	40.0
3- Desarrollo de proyectos prácticos y demostradores	30.0	60.0
4- Elaboración de informes	10.0	30.0

NIVEL 2: Seguridad en Sistemas Operativos		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	OPTATIVA	
ECTS MATERIA	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
Seguridad en Redes y Sistemas		

NIVEL 3: Seguridad en Sistemas Operativos		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
OPTATIVA	6	Semestral
DESPLIEGUE TEMPORAL		

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

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

LISTADO DE ESPECIALIDADES

Seguridad en Redes y Sistemas

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Conocer las herramientas para analizar la seguridad de una red y saber elegir la más apropiada en cada situación.
- Evaluar y proteger un sistema informático frente a ataques de seguridad.
- Conocer dónde buscar información puntualmente actualizada de las vulnerabilidades de seguridad que los sistemas presentan.
- Saber actualizar los conocimientos de seguridad en redes, sistemas operativos y bases de datos, forma rápida y constante.

5.5.1.3 CONTENIDOS

Esta materia se focaliza en el estudio de la seguridad en diferentes sistemas operativos. Se introducen los mecanismos de seguridad pasiva y activa, se presentan los modelos y políticas de seguridad empresarial, y se detalla cómo realizar configuraciones de servidores. En concreto, el alumno aprenderá a realizar configuraciones expertas en servidores GNU/Linux y Windows.

5.5.1.4 OBSERVACIONES

La asignatura de esta materia es de obligatorio seguimiento para los estudiantes que quieran obtener la especialidad Seguridad en Redes y Sistemas

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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

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.

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 - Capacidad de análisis y síntesis de la seguridad de un sistema.

CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.

CT4 - Capacidad de aprendizaje autónomo consultando información

CT5 - Capacidad para seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas en entornos nuevos
CT6 - Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática
CT7 - Uso del inglés como lengua vehicular en el ámbito tecnológico
5.5.1.5.3 ESPECÍFICAS
CE18 - Poseer y comprender conocimientos de las técnicas principales de seguridad en los sistemas operativos. (Perfil de Seguridad en Redes y Sistemas)
CE20 - Capacidad para realizar una configuración experta de un servidor GNU/Linux o Windows. (Perfil de Seguridad en Redes y Sistemas)
CE21 - Capacidad para diseñar soluciones integrales apropiadas en escenarios complejos que combinen las técnicas y contramedidas conocidas para la prevención, detección y disuasión de ataques. (Perfil de Seguridad en Redes y Sistemas)

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
0- LECTURA DE MATERIAL DIDÁCTICO	20	0
1- PREGUNTAS TEÓRICAS	10	0
2- RESOLUCIÓN DE PROBLEMAS	20	0
3- PRÁCTICAS	40	0
4- ESTUDIO DE CASOS	20	0
5- BÚSQUEDA DE INFORMACIÓN	10	0
6- DEBATE	10	0
10- LECTURA DE TEXTOS Y ARTÍCULOS	20	0

5.5.1.7 METODOLOGÍAS DOCENTES

1- Instrucción programada a través de materiales docentes
2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)
3- Participación en un debate (los alumnos contraponen dos o más opiniones expertas sobre un tema polémico y de interés, que sigue un plan controlado por el docente)
4- Aprendizaje basado en la resolución de problemas
5- Aprendizaje basado en el desarrollo de proyectos prácticos
6- Método basado en el estudio y análisis de casos reales
7- Aprendizaje basado en la búsqueda de información
8- Lectura de documentación científico-técnica muy especializada

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
1- Participación en foros y debates	10.0	30.0
2- Resolución de problemas	20.0	40.0
3- Desarrollo de proyectos prácticos y demostradores	30.0	60.0
4- Elaboración de informes	10.0	30.0

NIVEL 2: Seguridad en Bases de Datos

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	OPTATIVA	
ECTS MATERIA	6	
DESPLIEGUE TEMPORAL: Semestral		

ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
Seguridad en Redes y Sistemas		
NIVEL 3: Seguridad en Bases de Datos		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
OPTATIVA	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
Seguridad en Redes y Sistemas		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
- Conocer las herramientas para analizar la seguridad de una red y saber elegir la más apropiada en cada situación. - Evaluar y proteger un sistema informático frente a ataques de seguridad.		

- Detectar de forma rápida y eficiente las incidencias de seguridad en los sistemas, así como analizar de forma rigurosa su origen y los rastros de infección.
- Conocer dónde buscar información puntualmente actualizada de las vulnerabilidades de seguridad que los sistemas presentan.
- Saber actualizar los conocimientos de seguridad en redes, sistemas operativos y bases de datos, forma rápida y constante.

5.5.1.3 CONTENIDOS

Esta materia se focaliza en el estudio de las arquitecturas de bases de datos, sus vulnerabilidades, y los mecanismos de fortificación. Se introducen los mecanismos de seguridad pasiva y activa, se presentan los modelos y políticas de seguridad empresarial, y se detalla cómo realizar configuraciones.

5.5.1.4 OBSERVACIONES

La asignatura de esta materia es de obligatorio seguimiento para los estudiantes que quieran obtener la especialidad Seguridad en Redes y Sistemas

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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

5.5.1.5.2 TRANSVERSALES

CT1 - Capacidad de análisis y síntesis de la seguridad de un sistema.

CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.

CT6 - Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática

5.5.1.5.3 ESPECÍFICAS

CE19 - Capacidad para configurar y administrar una base de datos a nivel físico y lógico, a fin de asegurar la integridad, disponibilidad y confidencialidad de la información almacenada. (Perfil de Seguridad en Redes y Sistemas)

CE21 - Capacidad para diseñar soluciones integrales apropiadas en escenarios complejos que combinen las técnicas y contramedidas conocidas para la prevención, detección y disuasión de ataques. (Perfil de Seguridad en Redes y Sistemas)

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
0- LECTURA DE MATERIAL DIDÁCTICO	20	0
1- PREGUNTAS TEÓRICAS	10	0
2- RESOLUCIÓN DE PROBLEMAS	20	0
3- PRÁCTICAS	40	0
4- ESTUDIO DE CASOS	20	0
5- BÚSQUEDA DE INFORMACIÓN	10	0
6- DEBATE	10	0
10- LECTURA DE TEXTOS Y ARTÍCULOS	20	0

5.5.1.7 METODOLOGÍAS DOCENTES

1- Instrucción programada a través de materiales docentes

2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)

3- Participación en un debate (los alumnos contraponen dos o más opiniones expertas sobre un tema polémico y de interés, que sigue un plan controlado por el docente)

4- Aprendizaje basado en la resolución de problemas
5- Aprendizaje basado en el desarrollo de proyectos prácticos
6- Método basado en el estudio y análisis de casos reales
7- Aprendizaje basado en la búsqueda de información
8- Lectura de documentación científico-técnica muy especializada

5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
1- Participación en foros y debates	10.0	30.0
2- Resolución de problemas	20.0	40.0
3- Desarrollo de proyectos prácticos y demostradores	30.0	60.0
4- Elaboración de informes	10.0	30.0

5.5 NIVEL 1: Módulo de Especialidad 2: Seguridad en Servicios y Aplicaciones
5.5.1 Datos Básicos del Módulo
NIVEL 2: Programación de Código Seguro

5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	OPTATIVA	
ECTS MATERIA	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
Seguridad en Servicios y Aplicaciones		
NIVEL 3: Progrmación de Código Seguro		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
OPTATIVA	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**

6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

LISTADO DE ESPECIALIDADES

Seguridad en Servicios y Aplicaciones

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Conocer y poner en práctica las metodologías de programación de código seguro.
- Conocer las librerías de programación de servicios de seguridad en diferentes tecnologías y saber elegir la más adecuada en cada situación.

5.5.1.3 CONTENIDOS

Esta materia se focaliza en el ámbito de la programación de aplicaciones de seguridad. Por un lado, se describirán las técnicas de programación para evitar la presencia de vulnerabilidades durante el proceso de ejecución. Se incidirá en los riesgos más comunes (desbordamientos del buffer y la pila, inyección de código, cross site scripting, etc.), y los procesos de seguridad básicos: cómo gestionar la memoria, el formato y el encapsulado de datos, la certificación de los compiladores y sus métodos de verificación, y la gestión de los flujos de información. Se presentarán las metodologías y herramientas para identificar y eliminar los agujeros de seguridad, y se explicaran las directrices esenciales para crear software seguro: como diseñar software pensando en la seguridad desde el inicio del desarrollo e integrar sistemas de análisis y gestión del riesgo en todo el ciclo de vida del software.

5.5.1.4 OBSERVACIONES

La asignatura de esta materia es de obligatorio seguimiento para los estudiantes que quieran obtener la especialidad Seguridad en Servicios y Aplicaciones

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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

5.5.1.5.2 TRANSVERSALES

CT1 - Capacidad de análisis y síntesis de la seguridad de un sistema.

CT5 - Capacidad para seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas en entornos nuevos

5.5.1.5.3 ESPECÍFICAS

CE22 - Capacidad para aplicar metodologías y buenas prácticas de programación de código robusto, así como capacidad de modelar las amenazas de un sistema para evaluar la seguridad de las aplicaciones desarrolladas.(Perfil de Seguridad en Servicios y Aplicaciones)

CE23 - Capacidad para analizar, diseñar y desarrollar aplicaciones y servicios web seguros. (Perfil de Seguridad en Servicios y Aplicaciones)

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
0- LECTURA DE MATERIAL DIDÁCTICO	20	0

1- PREGUNTAS TEÓRICAS	10	0
2- RESOLUCIÓN DE PROBLEMAS	20	0
3- PRÁCTICAS	40	0
4- ESTUDIO DE CASOS	20	0
5- BÚSQUEDA DE INFORMACIÓN	10	0
6- DEBATE	10	0
10- LECTURA DE TEXTOS Y ARTÍCULOS	20	0

5.5.1.7 METODOLOGÍAS DOCENTES

1- Instrucción programada a través de materiales docentes

2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)

3- Participación en un debate (los alumnos contraponen dos o más opiniones expertas sobre un tema polémico y de interés, que sigue un plan controlado por el docente)

4- Aprendizaje basado en la resolución de problemas

5- Aprendizaje basado en el desarrollo de proyectos prácticos

6- Método basado en el estudio y análisis de casos reales

7- Aprendizaje basado en la búsqueda de información

8- Lectura de documentación científico-técnica muy especializada

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
1- Participación en foros y debates	10.0	30.0
2- Resolución de problemas	20.0	40.0
3- Desarrollo de proyectos prácticos y demostradores	30.0	60.0
4- Elaboración de informes	10.0	30.0

NIVEL 2: Comercio Electrónico

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	OPTATIVA	
ECTS MATERIA	6	

DESPLIEGUE TEMPORAL: Semestral

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

LENGUAS EN LAS QUE SE IMPARTE

CASTELLANO	CATALÁN	EUSKERA
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No

ITALIANO	OTRAS	
No	No	
LISTADO DE ESPECIALIDADES		
Seguridad en Servicios y Aplicaciones		
NIVEL 3: Comercio Electrónico		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
OPTATIVA	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
Seguridad en Servicios y Aplicaciones		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
- Demostrar comprensión por las plataformas de pago electrónico. - Ser capaz de diseñar e implementar un sistema de comercio electrónico		
5.5.1.3 CONTENIDOS		
Esta materia hace un repaso de los estándares de firma electrónica y las bases para la seguridad en el comercio electrónica. El contenido central de la materia es la facturación electrónica y las arquitecturas de comercio electrónico. Se analizará la seguridad de los protocolos de transacciones electrónicas y los sistemas de pago electrónico y móvil.		
5.5.1.4 OBSERVACIONES		
La asignatura de esta materia es de obligatorio seguimiento para los estudiantes que quieran obtener la especialidad Seguridad en Servicios y Aplicaciones		
5.5.1.5 COMPETENCIAS		
5.5.1.5.1 BÁSICAS Y GENERALES		
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 - Capacidad de análisis y síntesis de la seguridad de un sistema.
CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.
CT3 - Capacidad de comunicación tanto a público especializado como no especializado de modo claro y sin ambigüedades.
CT4 - Capacidad de aprendizaje autónomo consultando información
CT5 - Capacidad para seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas en entornos nuevos
CT6 - Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática
CT7 - Uso del inglés como lengua vehicular en el ámbito tecnológico
5.5.1.5.3 ESPECÍFICAS
CE24 - Poseer y comprender conocimientos de los sistemas que forman parte de una arquitectura de comercio electrónico, y capacidad para desplegar una. (Perfil de Seguridad en Servicios y Aplicaciones)
CE25 - Capacidad para comprender y analizar los sistemas de facturación electrónica, de pago y de micro-pago.(Perfil de Seguridad en Servicios y Aplicaciones)

5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
0- LECTURA DE MATERIAL DIDÁCTICO	20	0
1- PREGUNTAS TEÓRICAS	10	0
2- RESOLUCIÓN DE PROBLEMAS	20	0
3- PRÁCTICAS	40	0
4- ESTUDIO DE CASOS	20	0
5- BÚSQUEDA DE INFORMACIÓN	10	0
6- DEBATE	10	0
10- LECTURA DE TEXTOS Y ARTÍCULOS	20	0

5.5.1.7 METODOLOGÍAS DOCENTES
1- Instrucción programada a través de materiales docentes
2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)
3- Participación en un debate (los alumnos contraponen dos o más opiniones expertas sobre un tema polémico y de interés, que sigue un plan controlado por el docente)
4- Aprendizaje basado en la resolución de problemas
5- Aprendizaje basado en el desarrollo de proyectos prácticos
6- Método basado en el estudio y análisis de casos reales
7- Aprendizaje basado en la búsqueda de información
8- Lectura de documentación científico-técnica muy especializada

5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
1- Participación en foros y debates	10.0	30.0
2- Resolución de problemas	20.0	40.0
3- Desarrollo de proyectos prácticos y demostradores	30.0	60.0
4- Elaboración de informes	10.0	30.0

NIVEL 2: Biometría

5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	OPTATIVA	
ECTS MATERIA	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
Seguridad en Servicios y Aplicaciones		
NIVEL 3: Biometría		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
OPTATIVA	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		

Seguridad en Servicios y Aplicaciones
5.5.1.2 RESULTADOS DE APRENDIZAJE
- Manejar las técnicas de reconocimiento biométrico.
5.5.1.3 CONTENIDOS
En esta materia se presentan los métodos para reconocer las personas mediante técnicas biométricas así como el impacto que estos métodos suponen en nuestra sociedad. Se explican, entre otros, el reconocimiento de caras, de huellas, del iris, y de la voz. Se discute sobre las consideraciones de seguridad de estos sistemas.
5.5.1.4 OBSERVACIONES
La asignatura de esta materia es de obligatorio seguimiento para los estudiantes que quieran obtener la especialidad Seguridad en Servicios y Aplicaciones
5.5.1.5 COMPETENCIAS
5.5.1.5.1 BÁSICAS Y GENERALES
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
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.
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
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
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
5.5.1.5.2 TRANSVERSALES
CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.
CT4 - Capacidad de aprendizaje autónomo consultando información
CT6 - Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática
CT7 - Uso del inglés como lengua vehicular en el ámbito tecnológico
5.5.1.5.3 ESPECÍFICAS
CE26 - Comprender las técnicas de reconocimiento de las personas a través de características físicas: cara, huellas dactilares, orejas, iris, manos, forma de caminar, voz, etc. (Perfil de Seguridad en Servicios y Aplicaciones)
CE27 - Capacidad para diseñar aplicaciones reales con acceso biométrico. Conocer el software y hardware actual para desarrollar aplicaciones. (Perfil de Seguridad en Servicios y Aplicaciones)
5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
0- LECTURA DE MATERIAL DIDÁCTICO	20	0
1- PREGUNTAS TEÓRICAS	10	0
2- RESOLUCIÓN DE PROBLEMAS	20	0
3- PRÁCTICAS	30	0
4- ESTUDIO DE CASOS	20	0
5- BÚSQUEDA DE INFORMACIÓN	20	0
6- DEBATE	10	0
10- LECTURA DE TEXTOS Y ARTÍCULOS	20	0

5.5.1.7 METODOLOGÍAS DOCENTES
1- Instrucción programada a través de materiales docentes
2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)

3- Participación en un debate (los alumnos contraponen dos o más opiniones expertas sobre un tema polémico y de interés, que sigue un plan controlado por el docente)
4- Aprendizaje basado en la resolución de problemas
5- Aprendizaje basado en el desarrollo de proyectos prácticos
6- Método basado en el estudio y análisis de casos reales
7- Aprendizaje basado en la búsqueda de información
8- Lectura de documentación científico-técnica muy especializada

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
1- Participación en foros y debates	10.0	30.0
2- Resolución de problemas	20.0	40.0
3- Desarrollo de proyectos prácticos y demostradores	20.0	50.0
4- Elaboración de informes	20.0	50.0
6- Realización de pruebas finales de evaluación que engloban todo el contenido de una materia	0.0	100.0

5.5 NIVEL 1: Módulo de Esp. 3: Gestión y Auditoria de la Seguridad Informática

5.5.1 Datos Básicos del Módulo

NIVEL 2: Sistemas de Gestión de la Seguridad

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	OPTATIVA	
ECTS MATERIA	6	

DESPLIEGUE TEMPORAL: Semestral

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

LENGUAS EN LAS QUE SE IMPARTE

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

LISTADO DE ESPECIALIDADES

Gestión y Auditoría de la Seguridad Informática

NIVEL 3: Sistemas de Gestión de la Seguridad

5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
OPTATIVA	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

LISTADO DE ESPECIALIDADES

Gestión y Auditoría de la Seguridad Informática

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Evaluar con rigor los procesos de una organización para identificar los puntos críticos de seguridad.
- Saber elaborar un sistema de gestión de la seguridad de la información.
- Demostrar conocimiento de las fases de desarrollo de un Plan de Continuidad y las herramientas para llevarlo a cabo.

5.5.1.3 CONTENIDOS

El objetivo de esta materia es aprender a realizar la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI). Se introducen los principios y normativas de seguridad empresarial, se aprende a hacer un análisis de riesgos con las metodologías más usadas (MARGERIT, NIST,CRAMM, OCTAVE), se presentan las medidas de seguridad ISO, y se estudian las fases de implantación de un SGSI.

5.5.1.4 OBSERVACIONES

La asignatura de esta materia es de obligatorio seguimiento para los estudiantes que quieran obtener la especialidad Gestión y Auditoria de la Seguridad Informática

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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 - Capacidad de análisis y síntesis de la seguridad de un sistema.

CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.

CT3 - Capacidad de comunicación tanto a público especializado como no especializado de modo claro y sin ambigüedades.

CT4 - Capacidad de aprendizaje autónomo consultando información
CT6 - Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática
CT7 - Uso del inglés como lengua vehicular en el ámbito tecnológico
5.5.1.5.3 ESPECÍFICAS
CE28 - Capacidad para identificar y analizar los procesos críticos de una organización, así como el impacto que produciría la interrupción de estos procesos. (Perfil de Gestión y Auditoría de Seguridad)
CE29 - Capacidad para elaborar un plan de seguridad, teniendo en cuento todo el proceso de inventario y clasificación de activos, estudio de amenazas, análisis de riesgos y definición del plan de acción con el presupuesto asociado para la aprobación de la dirección. (Perfil de Gestión y Auditoría de Seguridad)
CE30 - Capacidad para desarrollar un Plan de Continuidad, conocer sus fases y el personal que debe implicarse en su desarrollo. Conocer las normas y estándares de referencia relacionados con la Continuidad de Negocio. (Perfil de Gestión y Auditoría de Seguridad)
CE31 - Capacidad para implantar un Sistema de Gestión de la Seguridad de la Información siguiendo las fases del ciclo de Deming. (Perfil de Gestión y Auditoría de Seguridad)

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
0- LECTURA DE MATERIAL DIDÁCTICO	20	0
1- PREGUNTAS TEÓRICAS	10	0
2- RESOLUCIÓN DE PROBLEMAS	20	0
3- PRÁCTICAS	40	0
4- ESTUDIO DE CASOS	20	0
5- BÚSQUEDA DE INFORMACIÓN	10	0
6- DEBATE	10	0
10- LECTURA DE TEXTOS Y ARTÍCULOS	20	0

5.5.1.7 METODOLOGÍAS DOCENTES

1- Instrucción programada a través de materiales docentes
2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)
3- Participación en un debate (los alumnos contraponen dos o más opiniones expertas sobre un tema polémico y de interés, que sigue un plan controlado por el docente)
4- Aprendizaje basado en la resolución de problemas
5- Aprendizaje basado en el desarrollo de proyectos prácticos
6- Método basado en el estudio y análisis de casos reales
7- Aprendizaje basado en la búsqueda de información
8- Lectura de documentación científico-técnica muy especializada

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
1- Participación en foros y debates	10.0	30.0
2- Resolución de problemas	30.0	50.0
3- Desarrollo de proyectos prácticos y demostradores	10.0	30.0
4- Elaboración de informes	20.0	50.0
6- Realización de pruebas finales de evaluación que engloban todo el contenido de una materia	0.0	100.0

NIVEL 2: Auditoría Técnica		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	OPTATIVA	
ECTS MATERIA	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
Gestión y Auditoría de la Seguridad Informática		
NIVEL 3: Auditoría Técnica		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
OPTATIVA	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	

No	No

LISTADO DE ESPECIALIDADES
Gestión y Auditoría de la Seguridad Informática
5.5.1.2 RESULTADOS DE APRENDIZAJE
- Desarrollar una auditoría técnica y de certificación.
5.5.1.3 CONTENIDOS
En esta materia se presentan los diferentes tipos de auditorías. La materia se centra en las auditorías técnicas y de certificación. Se explican los objetivos y las fases (documental/ presencial/documentación) de la auditoría, así como el proceso de certificación. Se presentan las metodologías de auditoría así como los herramientas apropiadas para llevarlas a cabo.
5.5.1.4 OBSERVACIONES
La asignatura de esta materia es de obligatorio seguimiento para los estudiantes que quieran obtener la especialidad Gestión y Auditoria de la Seguridad Informática.
5.5.1.5 COMPETENCIAS
5.5.1.5.1 BÁSICAS Y GENERALES
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 - Capacidad de análisis y síntesis de la seguridad de un sistema.
CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.
CT3 - Capacidad de comunicación tanto a público especializado como no especializado de modo claro y sin ambigüedades.
CT4 - Capacidad de aprendizaje autónomo consultando información
CT5 - Capacidad para seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas en entornos nuevos
CT6 - Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática
5.5.1.5.3 ESPECÍFICAS
CE32 - Capacidad para gestionar la certificación de un sistema de gestión de la seguridad de la información, así como capacidad para comprender, interpretar y explicar las ventajas que aporta la certificación de estos sistemas. (Perfil de Gestión y Auditoría de Seguridad)
CE33 - Capacidad de elaborar e implementar un plan de auditoría. Uso de las herramientas habituales para realizar una auditoría técnica de seguridad. (Perfil de Gestión y Auditoría de Seguridad)
CE35 - Capacidad para aplicar las consideraciones legales adquiridas para realizar la gestión de un incidente de seguridad. (Perfil de Gestión y Auditoría de Seguridad)
5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
0- LECTURA DE MATERIAL DIDÁCTICO	20	0
1- PREGUNTAS TEÓRICAS	20	0
2- RESOLUCIÓN DE PROBLEMAS	10	0
3- PRÁCTICAS	30	0
4- ESTUDIO DE CASOS	30	0
5- BÚSQUEDA DE INFORMACIÓN	10	0

6- DEBATE	10	0
10- LECTURA DE TEXTOS Y ARTÍCULOS	20	0

5.5.1.7 METODOLOGÍAS DOCENTES

1- Instrucción programada a través de materiales docentes

2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)

3- Participación en un debate (los alumnos contraponen dos o más opiniones expertas sobre un tema polémico y de interés, que sigue un plan controlado por el docente)

4- Aprendizaje basado en la resolución de problemas

5- Aprendizaje basado en el desarrollo de proyectos prácticos

6- Método basado en el estudio y análisis de casos reales

7- Aprendizaje basado en la búsqueda de información

8- Lectura de documentación científico-técnica muy especializada

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
1- Participación en foros y debates	10.0	30.0
2- Resolución de problemas	30.0	50.0
3- Desarrollo de proyectos prácticos y demostradores	10.0	30.0
4- Elaboración de informes	20.0	50.0
6- Realización de pruebas finales de evaluación que engloban todo el contenido de una materia	0.0	100.0

NIVEL 2: Análisis Forense

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	OPTATIVA	
ECTS MATERIA	6	

DESPLIEGUE TEMPORAL: Semestral

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

LENGUAS EN LAS QUE SE IMPARTE

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

LISTADO DE ESPECIALIDADES		
Gestión y Auditoría de la Seguridad Informática		
NIVEL 3: Análisis Forense		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
OPTATIVA	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
Gestión y Auditoría de la Seguridad Informática		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
- Realizar el informe de un análisis forense.		
5.5.1.3 CONTENIDOS		
Esta materia se focaliza en los aspectos técnicos que se deben llevar a cabo para realizar un análisis forense, y la documentación que se debe generar. Se presentan las técnicas de recuperación de información y la metodología de un análisis, es decir, adquisición de datos, análisis e investigación de datos, y documentación del proceso. Se describe el marco legal de los análisis forenses. Se aprenden a usar las herramientas propias de un análisis de este tipo.		
5.5.1.4 OBSERVACIONES		
La asignatura de esta materia es de obligatorio seguimiento para los estudiantes que quieran obtener la especialidad Gestión y Auditoria de la Seguridad Informática.		
5.5.1.5 COMPETENCIAS		
5.5.1.5.1 BÁSICAS Y GENERALES		
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		
5.5.1.5.2 TRANSVERSALES		
CT1 - Capacidad de análisis y síntesis de la seguridad de un sistema.		
CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.		

CT3 - Capacidad de comunicación tanto a público especializado como no especializado de modo claro y sin ambigüedades.
CT5 - Capacidad para seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas en entornos nuevos
CT6 - Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática
5.5.1.5.3 ESPECÍFICAS
CE34 - Capacidad para realizar un análisis forense de cualquier sistema informático (PC, móviles, routers, etc.) y presentarlo en una sede judicial. (Perfil de Gestión y Auditoría de Seguridad)
CE35 - Capacidad para aplicar las consideraciones legales adquiridas para realizar la gestión de un incidente de seguridad. (Perfil de Gestión y Auditoría de Seguridad)

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
0- LECTURA DE MATERIAL DIDÁCTICO	20	0
1- PREGUNTAS TEÓRICAS	10	0
2- RESOLUCIÓN DE PROBLEMAS	20	0
3- PRÁCTICAS	30	0
4- ESTUDIO DE CASOS	30	0
5- BÚSQUEDA DE INFORMACIÓN	10	0
6- DEBATE	10	0
10- LECTURA DE TEXTOS Y ARTÍCULOS	20	0

5.5.1.7 METODOLOGÍAS DOCENTES
1- Instrucción programada a través de materiales docentes
2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)
3- Participación en un debate (los alumnos contraponen dos o más opiniones expertas sobre un tema polémico y de interés, que sigue un plan controlado por el docente)
4- Aprendizaje basado en la resolución de problemas
5- Aprendizaje basado en el desarrollo de proyectos prácticos
6- Método basado en el estudio y análisis de casos reales
7- Aprendizaje basado en la búsqueda de información
8- Lectura de documentación científico-técnica muy especializada

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
1- Participación en foros y debates	10.0	30.0
2- Resolución de problemas	30.0	50.0
3- Desarrollo de proyectos prácticos y demostradores	10.0	30.0
4- Elaboración de informes	20.0	50.0

5.5 NIVEL 1: Módulo de Especialidad 4: Investigación

5.5.1 Datos Básicos del Módulo

NIVEL 2: Metodologías de Investigación

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	OPTATIVA	
ECTS MATERIA	6	

DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
Investigación		
NIVEL 3: Metodologías de Investigación		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
OPTATIVA	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
Investigación		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
- Conocer el proceso de investigación, así como sus técnicas y métodos asociados - Saber buscar información eficiente y eficazmente.		

- Saber analizar un conjunto de datos o información rigurosamente, tanto de forma cualitativa como cuantitativa.

5.5.1.3 CONTENIDOS

Esta materia se centra en presentar las fases de un proceso de investigación, y las metodologías para llevar a cabo un proyecto. Se hace una introducción al proceso de investigación (propósito y productos de la investigación, proceso de investigación, aspectos éticos, revisión de la literatura) y se presentan las metodologías de investigación (encuestas, diseño y creación, experimentos, estudio de casos, action research, prueba formal). Se definen las estrategias de investigación (entrevistas, observación, cuestionarios, documentos), se detallan las técnicas de análisis cuantitativo y cualitativo, y se describen los métodos de prueba formal.

5.5.1.4 OBSERVACIONES

La asignatura de esta materia es de obligatorio seguimiento para los estudiantes que quieran obtener la especialidad de Investigación.
Los estudiantes deberán disponer de un nivel suficiente de inglés (el nivel indicado en las condiciones de ingreso al Máster en el apartado 4.1), para poder leer y escribir documentación técnica y científica en este idioma.
Todo el profesorado y los docentes colaboradores que realicen docencia en las asignaturas de este módulo tendrán el título de doctor.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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

CT4 - Capacidad de aprendizaje autónomo consultando información

CT5 - Capacidad para seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas en entornos nuevos

CT7 - Uso del inglés como lengua vehicular en el ámbito tecnológico

5.5.1.5.3 ESPECÍFICAS

CE38 - Capacidad para redactar documentación científica, y sintetizar y presentar los resultados de un proyecto de investigación. (Perfil de Investigación en Seguridad de las TIC)

CE39 - Capacidad para determinar las características relevantes de un sistema TIC para su modelado y simulación, así como capacidad para sintetizar y presentar los resultados. (Perfil de Investigación en Seguridad de las TIC)

CE41 - Capacidad para analizar los distintos sistemas criptográficos que se utilizan habitualmente y criticar su aplicabilidad, así como entender la no aplicabilidad de otros sistemas teóricamente interesantes. (Perfil de Investigación en Seguridad de las TIC)

CE42 - Capacidad para interpretar, analizar y explicar las diferencias conceptuales y su aplicabilidad entre los diversos esquemas propuestos para resolver un mismo problema criptográfico. (Perfil de Investigación en Seguridad de las TIC)

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
0- LECTURA DE MATERIAL DIDÁCTICO	10	0
3- PRÁCTICAS	40	0
4- ESTUDIO DE CASOS	30	0
5- BÚSQUEDA DE INFORMACIÓN	40	0
7- REDACCIÓN DE TEXTOS	20	0
10- LECTURA DE TEXTOS Y ARTÍCULOS	10	0

5.5.1.7 METODOLOGÍAS DOCENTES

1- Instrucción programada a través de materiales docentes

2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)

5- Aprendizaje basado en el desarrollo de proyectos prácticos

6- Método basado en el estudio y análisis de casos reales		
7- Aprendizaje basado en la búsqueda de información		
8- Lectura de documentación científico-técnica muy especializada		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
1- Participación en foros y debates	10.0	30.0
2- Resolución de problemas	20.0	40.0
3- Desarrollo de proyectos prácticos y demostradores	0.0	30.0
4- Elaboración de informes	20.0	50.0
6- Realización de pruebas finales de evaluación que engloban todo el contenido de una materia	0.0	100.0
NIVEL 2: Técnicas de Investigación		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	OPTATIVA	
ECTS MATERIA	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
Investigación		
NIVEL 3: Técnicas de Investigación		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
OPTATIVA	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**

ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

LISTADO DE ESPECIALIDADES

Investigación

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Escribir de forma correcta y apropiada para el ámbito investigador.
- Elaborar documentos científico-técnicos de forma rigurosa: organizar, estructurar, sistematizar y argumentar la información.

5.5.1.3 CONTENIDOS

Esta materia se centra en presentar las fases de un proceso de investigación, y las técnicas para llevar a cabo un proyecto. Se introduce al estudiante en la redacción de textos científicos. Se presentan los características principales de las publicaciones científicas (proceso de peer review, categorías de publicaciones: revistas indexadas y no indexadas, factores de impacto, índices científicos y bibliométricos, congresos, workshops, ...). y la selección de publicaciones en una área. Se estudia cómo gestionar proyectos de investigación y se aprende a manejar herramientas de apoyo a la investigación: procesadores de textos científicos, gestores de bibliografía, editores de presentaciones, bases de datos (ISI WoK, Google Scholar, DBLP), herramientas de análisis cuantitativo y cualitativo, herramientas de gestión de proyectos. También se introducen nociones sobre la propiedad intelectual: patentes, propiedad intelectual, derechos de autor. Finalmente, se aprende a presentar los resultados de una investigación, en forma de informes, artículos o presentaciones orales.

5.5.1.4 OBSERVACIONES

La asignatura de esta materia es de obligatorio seguimiento para los estudiantes que quieran obtener la especialidad de Investigación.
Los estudiantes deberán disponer de un nivel suficiente de inglés (el nivel indicado en las condiciones de ingreso al Máster en el apartado 4.1), para poder leer y escribir documentación técnica y científica en este idioma.
Todo el profesorado y los docentes colaboradores que realicen docencia en las asignaturas de este módulo tendrán el título de doctor.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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

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

CG0 - Hablar bien en público

5.5.1.5.2 TRANSVERSALES

CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.

CT3 - Capacidad de comunicación tanto a público especializado como no especializado de modo claro y sin ambigüedades.

CT5 - Capacidad para seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas en entornos nuevos

CT7 - Uso del inglés como lengua vehicular en el ámbito tecnológico

5.5.1.5.3 ESPECÍFICAS

CE36 - Capacidad para planificar, administrar, dirigir y coordinar proyectos de investigación en el campo de las TIC. (Perfil de Investigación en Seguridad de las TIC)
CE37 - Capacidad para diseñar y llevar a cabo la investigación según las normas del conocimiento científico en el campo de las TIC. (Perfi de Investigación en Seguridad de las TIC)
CE38 - Capacidad para redactar documentación científica, y sintetizar y presentar los resultados de un proyecto de investigación. (Perfil de Investigación en Seguridad de las TIC)

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
0- LECTURA DE MATERIAL DIDÁCTICO	10	0
3- PRÁCTICAS	20	0
4- ESTUDIO DE CASOS	30	0
5- BÚSQUEDA DE INFORMACIÓN	20	0
7- REDACCIÓN DE TEXTOS	40	0
8- PRESENTACIONES ORALES	10	0
10- LECTURA DE TEXTOS Y ARTÍCULOS	20	0

5.5.1.7 METODOLOGÍAS DOCENTES

1- Instrucción programada a través de materiales docentes
2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)
5- Aprendizaje basado en el desarrollo de proyectos prácticos
6- Método basado en el estudio y análisis de casos reales
7- Aprendizaje basado en la búsqueda de información
8- Lectura de documentación científico-técnica muy especializada
9- Exposición pública por parte de los estudiantes

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
1- Participación en foros y debates	10.0	30.0
2- Resolución de problemas	20.0	40.0
3- Desarrollo de proyectos prácticos y demostradores	0.0	30.0
4- Elaboración de informes	20.0	50.0
6- Realización de pruebas finales de evaluación que engloban todo el contenido de una materia	0.0	100.0

NIVEL 2: Criptografía Avanzada

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	OPTATIVA	
ECTS MATERIA	6	

DESPLIEGUE TEMPORAL: Semestral

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

ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
Investigación		
NIVEL 3: Criptografía Avanzada		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
OPTATIVA	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
Investigación		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
Demostrar conocimientos teóricos sobre criptografía avanzada.		
5.5.1.3 CONTENIDOS		
La criptografía avanzada incluye aquellos aspectos sobre dicha técnica que por su especificidad, complejidad o por que abarcan o relacionan diversos tópicos, se escapan a los cursos de criptografía básicos. En esta materia se hace un recorrido por las bases matemáticas que soportan dichos esquemas avanzados, cuerpos finitos, curvas elípticas, Tate pairings, etc. y se especifican los más importantes esquemas criptográficos, así como sus aplicaciones (por ejemplo, las firmas de grupo o de anillo, signaturas ciegas, cifrado basado en identidad, criptografía cuántica y post-cuántica, etc.)		
5.5.1.4 OBSERVACIONES		
La asignatura de esta materia es de obligatorio seguimiento para los estudiantes que quieran obtener la especialidad de Investigación. Los estudiantes deberán disponer de un nivel suficiente de inglés (el nivel indicado en las condiciones de ingreso al Máster en el apartado 4.1), para poder leer y escribir documentación técnica y científica en este idioma.		

Todo el profesorado y los docentes colaboradores que realicen docencia en las asignaturas de este módulo tendrán el título de doctor.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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

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

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 - Capacidad de análisis y síntesis de la seguridad de un sistema.

CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.

CT4 - Capacidad de aprendizaje autónomo consultando información

CT5 - Capacidad para seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas en entornos nuevos

CT6 - Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática

CT7 - Uso del inglés como lengua vehicular en el ámbito tecnológico

5.5.1.5.3 ESPECÍFICAS

CE40 - Comprender los fundamentos teóricos de la criptografía moderna y el funcionamiento de los protocolos criptográficos actualmente en uso. (Perfil de Investigación en Seguridad de las TIC)

CE41 - Capacidad para analizar los distintos sistemas criptográficos que se utilizan habitualmente y criticar su aplicabilidad, así como entender la no aplicabilidad de otros sistemas teóricamente interesantes. (Perfil de Investigación en Seguridad de las TIC)

CE42 - Capacidad para interpretar, analizar y explicar las diferencias conceptuales y su aplicabilidad entre los diversos esquemas propuestos para resolver un mismo problema criptográfico. (Perfil de Investigación en Seguridad de las TIC)

CE43 - Capacidad para comprender y utilizar las aplicaciones criptográficas existentes basadas en técnicas avanzadas. (Perfil de Investigación en Seguridad de las TIC)

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
0- LECTURA DE MATERIAL DIDÁCTICO	20	0
1- PREGUNTAS TEÓRICAS	10	0
2- RESOLUCIÓN DE PROBLEMAS	20	0
3- PRÁCTICAS	20	0
4- ESTUDIO DE CASOS	20	0
5- BÚSQUEDA DE INFORMACIÓN	10	0
6- DEBATE	10	0
10- LECTURA DE TEXTOS Y ARTÍCULOS	40	0

5.5.1.7 METODOLOGÍAS DOCENTES

1- Instrucción programada a través de materiales docentes

2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)

3- Participación en un debate (los alumnos contraponen dos o más opiniones expertas sobre un tema polémico y de interés, que sigue un plan controlado por el docente)
4- Aprendizaje basado en la resolución de problemas
5- Aprendizaje basado en el desarrollo de proyectos prácticos
6- Método basado en el estudio y análisis de casos reales
7- Aprendizaje basado en la búsqueda de información
8- Lectura de documentación científico-técnica muy especializada

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
1- Participación en foros y debates	10.0	30.0
2- Resolución de problemas	20.0	40.0
3- Desarrollo de proyectos prácticos y demostradores	0.0	30.0
4- Elaboración de informes	20.0	50.0
6- Realización de pruebas finales de evaluación que engloban todo el contenido de una materia	0.0	100.0

5.5 NIVEL 1: Módulo de Optativas

5.5.1 Datos Básicos del Módulo

NIVEL 2: Técnicas de Marcado de la Información

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	OPTATIVA	
ECTS MATERIA	6	

DESPLIEGUE TEMPORAL: Semestral

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

LENGUAS EN LAS QUE SE IMPARTE

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

LISTADO DE ESPECIALIDADES

No existen datos

NIVEL 3: Técnicas de Marcado de la Información

5.5.1.1.1 Datos Básicos del Nivel 3

CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
OPTATIVA	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

LISTADO DE ESPECIALIDADES

No existen datos

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Demostrar conocimientos sobre la problemática de la esteganografía en diferentes soportes (audio, imagen, video).
- Comprender y evaluar las técnicas de marcado de la información.

5.5.1.3 CONTENIDOS

Dicha materia incluye todas aquellas técnicas que se utilizan para el marcado de la información digital. Se estudian los esquemas de marcas de agua más utilizados hasta el momento tanto en contenidos de imágenes como de audio. Por otro lado, se estudian también las distintas aplicaciones que tienen las técnicas de marcado, como pueden ser el rastreo de la información digital, la detección de copia o la detección de manipulación.

5.5.1.4 OBSERVACIONES

La oferta de materias optativas para cada estudiante, además de las materias propias de este módulo, incluye las materias de todos los módulos de especialidad que no formen parte de la propia especialidad del estudiante.
Los estudiantes deberán disponer de un nivel suficiente de inglés (el nivel indicado en las condiciones de ingreso al Máster en el apartado 4.1), para poder leer y escribir documentación técnica y científica en este idioma.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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.

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

5.5.1.5.2 TRANSVERSALES

CT1 - Capacidad de análisis y síntesis de la seguridad de un sistema.

CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.
CT4 - Capacidad de aprendizaje autónomo consultando información
CT5 - Capacidad para seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas en entornos nuevos
CT6 - Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática
CT7 - Uso del inglés como lengua vehicular en el ámbito tecnológico
5.5.1.5.3 ESPECÍFICAS
CE44 - Poseer y comprender conocimientos de las diferencias conceptuales entre los diferentes dominios de marcado de la información digital (dominio temporal/espacial y transformado). Capacidad crítica para analizar la bondad de distintos sistemas de marcado. (Materias Optativas)
CE45 - Capacidad para integrar conocimientos de las aplicaciones existentes para las técnicas de marcado de la información.(Materias Optativas)

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
0- LECTURA DE MATERIAL DIDÁCTICO	20	0
1- PREGUNTAS TEÓRICAS	10	0
2- RESOLUCIÓN DE PROBLEMAS	20	0
3- PRÁCTICAS	40	0
4- ESTUDIO DE CASOS	20	0
5- BÚSQUEDA DE INFORMACIÓN	10	0
6- DEBATE	10	0
10- LECTURA DE TEXTOS Y ARTÍCULOS	20	0

5.5.1.7 METODOLOGÍAS DOCENTES
1- Instrucción programada a través de materiales docentes
2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)
3- Participación en un debate (los alumnos contraponen dos o más opiniones expertas sobre un tema polémico y de interés, que sigue un plan controlado por el docente)
4- Aprendizaje basado en la resolución de problemas
5- Aprendizaje basado en el desarrollo de proyectos prácticos
6- Método basado en el estudio y análisis de casos reales
7- Aprendizaje basado en la búsqueda de información
8- Lectura de documentación científico-técnica muy especializada

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
1- Participación en foros y debates	10.0	30.0
2- Resolución de problemas	20.0	40.0
3- Desarrollo de proyectos prácticos y demostradores	20.0	50.0
4- Elaboración de informes	20.0	50.0
6- Realización de pruebas finales de evaluación que engloban todo el contenido de una materia	0.0	100.0

NIVEL 2: Dirección Estratégica de SI/TI

5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	OPTATIVA	
ECTS MATERIA	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NIVEL 3: Dirección Estratégica de SI/TI		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
OPTATIVA	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		

No existen datos

5.5.1.2 RESULTADOS DE APRENDIZAJE

Conocer el funcionamiento, la organización y la dirección estratégica de los diferentes departamentos que utilizan sistemas de información
Comprender la gestión estratégica de los sistemas y tecnologías de la información, desde la planificación hasta la implantación en el día a día.

5.5.1.3 CONTENIDOS

Dicha materia estudia los conceptos básicos de la estrategia de empresa y el papel que tienen los sistemas y tecnologías de la información (SI/TI) en la consecución de los objetivos de negocio. En particular se trabaja la planificación
estratégica de SI/TI, la organización estratégica de departamentos de SI/TI, y la dirección estratégica de SI/TI.

5.5.1.4 OBSERVACIONES

La oferta de materias optativas para cada estudiante, además de las materias propias de este módulo, incluye las materias de todos los módulos de especialidad que no formen parte de la propia especialidad del estudiante. Los estudiantes deberán disponer de un nivel suficiente de inglés (el nivel indicado en las condiciones de ingreso al Máster en el apartado 4.1), para poder leer y escribir documentación técnica y científica en este idioma.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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

CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.

CT3 - Capacidad de comunicación tanto a público especializado como no especializado de modo claro y sin ambigüedades.

CT4 - Capacidad de aprendizaje autónomo consultando información

CT7 - Uso del inglés como lengua vehicular en el ámbito tecnológico

5.5.1.5.3 ESPECÍFICAS

CE46 - Capacidad para la dirección de proyectos de investigación, desarrollo e innovación, en empresas y centros tecnológicos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación. (Materias optativas)

CE47 - Capacidad para la integración de tecnologías, aplicaciones, servicios y sistemas propios de la Ingeniería Informática, con carácter generalista, y en contextos más amplios y multidisciplinares. (Materias optativas)
CE48 - Capacidad para la planificación estratégica, elaboración, dirección, coordinación, y gestión técnica y económica en los ámbitos de la ingeniería informática relacionados, entre otros, con: sistemas, aplicaciones, servicios, redes, infraestructuras o instalaciones informáticas y centros o factorías de desarrollo de software, respetando el adecuado cumplimiento de los criterios de calidad y medioambientales y en entornos de trabajo multidisciplinares. (Materias optativas)

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
0- LECTURA DE MATERIAL DIDÁCTICO	30	0
5- BÚSQUEDA DE INFORMACIÓN	20	0
10- LECTURA DE TEXTOS Y ARTÍCULOS	10	0
6- DEBATE	5	0
4- ESTUDIO DE CASOS	50	0
8- PRESENTACIONES ORALES	5	0
12- REDACCIÓN DE INFORMES	30	0

5.5.1.7 METODOLOGÍAS DOCENTES

1- Instrucción programada a través de materiales docentes
2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)
3- Participación en un debate (los alumnos contraponen dos o más opiniones expertas sobre un tema polémico y de interés, que sigue un plan controlado por el docente)
4- Aprendizaje basado en la resolución de problemas
5- Aprendizaje basado en el desarrollo de proyectos prácticos
6- Método basado en el estudio y análisis de casos reales
7- Aprendizaje basado en la búsqueda de información
8- Lectura de documentación científico-técnica muy especializada

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
1- Participación en foros y debates	10.0	20.0
2- Resolución de problemas	20.0	30.0
3- Desarrollo de proyectos prácticos y demostradores	50.0	60.0
6- Realización de pruebas finales de evaluación que engloban todo el contenido de una materia	40.0	100.0

5.5 NIVEL 1: Módulo de Prácticas

5.5.1 Datos Básicos del Módulo

NIVEL 2: Prácticas

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	PRÁCTICAS EXTERNAS	
ECTS MATERIA	3	

DESPLIEGUE TEMPORAL: Semestral

ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
	3	

ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NIVEL 3: Prácticas		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
PRÁCTICAS EXTERNAS	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	3	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
5.5.1.2 RESULTADOS DE APRENDIZAJE		
- Demostrar los conocimientos técnicos, éticos y legislativos para ejercer la actividad profesional en el ámbito de la seguridad de la información. - Saber adaptarse de forma eficiente y eficaz a nuevos entornos de trabajo y herramientas no experimentadas con anterioridad - Conocer el funcionamiento, la organización y la dirección estratégica de los diferentes departamentos que utilizan sistemas de información		
5.5.1.3 CONTENIDOS		
Por sus características especiales, las prácticas profesionalizadoras no tienen asociadas contenidos específicos. El desarrollo de éstas se nutrirá de los contenidos ya vistos a lo largo de los estudios más la documentación ad hoc que se requiera en función del tipo de práctica o tarea a llevar a cabo.		
5.5.1.4 OBSERVACIONES		
Uno de los objetivos principales del MISTIC es formar a expertos en seguridad que sean capaces de gestionar, diseñar e implementar nuevas soluciones innovadoras que permitan proteger y reducir el riesgo sobre los activos empresariales. Los estudiantes del máster deben ser capaces de atender las demandas empresariales, y es por ello que es fundamental reforzar el vínculo del máster con el ámbito más práctico y profesional. Las prácticas del máster están programadas como un módulo obligatorio de las especialidades profesionalizadoras. Las prácticas podrán desarrollarse en alguna de las siguientes modalidades: - Prácticas vinculadas al entorno profesional		

- Prácticas con convenios

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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

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.

CG0 - Hablar bien en público

5.5.1.5.2 TRANSVERSALES

CT1 - Capacidad de análisis y síntesis de la seguridad de un sistema.

CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.

CT4 - Capacidad de aprendizaje autónomo consultando información

CT5 - Capacidad para seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas en entornos nuevos

CT6 - Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática

5.5.1.5.3 ESPECÍFICAS

Seleccione un valor

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
2- RESOLUCIÓN DE PROBLEMAS	5	0
3- PRÁCTICAS	25	0
4- ESTUDIO DE CASOS	5	0
5- BÚSQUEDA DE INFORMACIÓN	10	0
9- INFORME DE APRENDIZAJE	10	0
10- LECTURA DE TEXTOS Y ARTÍCULOS	10	0
12- REDACCIÓN DE INFORMES	10	0

5.5.1.7 METODOLOGÍAS DOCENTES

2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)

4- Aprendizaje basado en la resolución de problemas

6- Método basado en el estudio y análisis de casos reales

7- Aprendizaje basado en la búsqueda de información

8- Lectura de documentación científico-técnica muy especializada

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
1- Participación en foros y debates	0.0	20.0
2- Resolución de problemas	10.0	30.0
3- Desarrollo de proyectos prácticos y demostradores	30.0	50.0
4- Elaboración de informes	20.0	50.0
5- Exposiciones de trabajos	20.0	40.0

5.5 NIVEL 1: Módulo de Trabajo Fin de Máster		
5.5.1 Datos Básicos del Módulo		
NIVEL 2: Proyecto Especialidades Profesionalizadoras		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	TRABAJO FIN DE MÁSTER	
ECTS MATERIA	9	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	9	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NIVEL 3: Trabajo fin de Master Especialidades Profesionalizadoras		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
TRABAJO FIN DE MÁSTER	9	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	9	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Demostrar comprensión detallada en un ámbito especializado dentro de la seguridad de la información.
- Saber analizar diferentes alternativas y elegir la más adecuada, justificando su elección.
- Saber evaluar y discutir decisiones tomadas, ya sea por uno mismo o por otros.
- Elaborar y defender un documento que sintetice un trabajo original en el ámbito de la seguridad de la información.
- Saber transmitir de forma eficiente y eficaz las partes más importantes de un contenido voluminoso a diferentes audiencias.

5.5.1.3 CONTENIDOS

El objetivo de esta materia es la elaboración de un trabajo escrito y opcionalmente, un prototipo de software, en los que se pone en práctica y se profundiza en las competencias generales del máster y las transversales de la especialización cursada por el estudiante. Asimismo, durante la elaboración de dicho trabajo se intenta fomentar el desarrollo de competencias similares a las de la práctica profesional. Del mismo modo, resaltar que se hará especial énfasis en los aspectos relacionados con la planificación, seguimiento, búsqueda de información, habilidades comunicativas, su impacto en el mundo real, análisis económico, etc.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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.

CG0 - Hablar bien en público

5.5.1.5.2 TRANSVERSALES

CT1 - Capacidad de análisis y síntesis de la seguridad de un sistema.

CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.

CT3 - Capacidad de comunicación tanto a público especializado como no especializado de modo claro y sin ambigüedades.

CT4 - Capacidad de aprendizaje autónomo consultando información

CT5 - Capacidad para seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas en entornos nuevos

CT6 - Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática

CT7 - Uso del inglés como lengua vehicular en el ámbito tecnológico

5.5.1.5.3 ESPECÍFICAS

CE11 - Capacidad para realizar, presentar y defender ante un tribunal interuniversitario, un ejercicio original realizado individualmente consistente en un proyecto integral de Seguridad de las Tecnologías de la Información y de las Comunicaciones de naturaleza profesional o de investigación en el que se sinteticen las competencias adquiridas en las enseñanzas

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
2- RESOLUCIÓN DE PROBLEMAS	10	0
3- PRÁCTICAS	35	0
4- ESTUDIO DE CASOS	10	0
5- BÚSQUEDA DE INFORMACIÓN	10	0
8- PRESENTACIONES ORALES	10	0
10- LECTURA DE TEXTOS Y ARTÍCULOS	10	0
11- PROYECTO	80	0
12- REDACCIÓN DE INFORMES	50	0

5.5.1.7 METODOLOGÍAS DOCENTES		
2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)		
5- Aprendizaje basado en el desarrollo de proyectos prácticos		
7- Aprendizaje basado en la búsqueda de información		
8- Lectura de documentación científico-técnica muy especializada		
9- Exposición pública por parte de los estudiantes		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
4- Elaboración de informes	50.0	70.0
5- Exposiciones de trabajos	30.0	50.0
NIVEL 2: Proyecto Especialidad de Investigación		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	TRABAJO FIN DE MÁSTER	
ECTS MATERIA	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**
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NIVEL 3: Trabajo Fin de Máster Especialidad Investigación		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
TRABAJO FIN DE MÁSTER	12	Semestral
DESPLIEGUE TEMPORAL		
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
Si	Si	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

5.5.1.2 RESULTADOS DE APRENDIZAJE

- Demostrar comprensión detallada en un ámbito especializado dentro de la seguridad de la información.
- Saber analizar diferentes alternativas y elegir la más adecuada, justificando su elección.
- Saber evaluar y discutir decisiones tomadas, ya sea por uno mismo o por otros.
- Elaborar y defender un documento que sintetice un trabajo original en el ámbito de la seguridad de la información.
- Saber transmitir de forma eficiente y eficaz las partes más importantes de un contenido voluminoso a diferentes audiencias.
- Leer y escribir con corrección en inglés

5.5.1.3 CONTENIDOS

En esta materia se ponen en práctica y se profundizan las competencias del módulo de investigación del máster mediante la elaboración de un artículo científico. Además, destacar que en función de la temática del trabajo fin de máster, el estudiante profundizará sus conocimientos en las competencias relacionadas con dicha temática. Durante la elaboración del trabajo se fomentará el desarrollo de competencias para ser un buen investigador, y se sentarán las bases para realizar una tesis doctoral.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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.

CG0 - Hablar bien en público

5.5.1.5.2 TRANSVERSALES

CT1 - Capacidad de análisis y síntesis de la seguridad de un sistema.

CT2 - Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.

CT3 - Capacidad de comunicación tanto a público especializado como no especializado de modo claro y sin ambigüedades.

CT4 - Capacidad de aprendizaje autónomo consultando información

CT5 - Capacidad para seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas en entornos nuevos

CT6 - Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática

CT7 - Uso del inglés como lengua vehicular en el ámbito tecnológico

5.5.1.5.3 ESPECÍFICAS

CE11 - Capacidad para realizar, presentar y defender ante un tribunal interuniversitario, un ejercicio original realizado individualmente consistente en un proyecto integral de Seguridad de las Tecnologías de la Información y de las Comunicaciones de naturaleza profesional o de investigación en el que se sinteticen las competencias adquiridas en las enseñanzas

CE39 - Capacidad para determinar las características relevantes de un sistema TIC para su modelado y simulación, así como capacidad para sintetizar y presentar los resultados. (Perfil de Investigación en Seguridad de las TIC)

5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
2- RESOLUCIÓN DE PROBLEMAS	10	0
3- PRÁCTICAS	40	0
4- ESTUDIO DE CASOS	20	0
5- BÚSQUEDA DE INFORMACIÓN	40	0
8- PRESENTACIONES ORALES	10	0
10- LECTURA DE TEXTOS Y ARTÍCULOS	60	0
11- PROYECTO	60	0
13- REDACCIÓN ARTÍCULO CIENTÍFICO	60	0

5.5.1.7 METODOLOGÍAS DOCENTES
2- Participación en el foro del aula (los alumnos discuten libremente un tema. El docente coordina y guía la participación de los alumnos)
7- Aprendizaje basado en la búsqueda de información
8- Lectura de documentación científico-técnica muy especializada
9- Exposición pública por parte de los estudiantes

5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
4- Elaboración de informes	10.0	30.0
5- Exposiciones de trabajos	20.0	40.0
7- Redacción de artículos científicos	50.0	70.0

6. PERSONAL ACADÉMICO

6.1 PROFESORADO Y OTROS RECURSOS HUMANOS				
Universidad	**Categoría**	**Total %**	**Doctores %**	**Horas %**
Universidad Autónoma de Barcelona	Catedrático de Universidad	11.0	100.0	9.0
Universidad Autónoma de Barcelona	Profesor Titular	11.0	100.0	7.0
Universidad Autónoma de Barcelona	Profesor Agregado	11.0	100.0	15.0
Universidad Rovira i Virgili	Profesor Titular	11.0	10.0	7.0
Universidad Rovira i Virgili	Profesor Agregado	11.0	100.0	9.0
Universidad Oberta de Catalunya	Profesor Agregado	33.0	100.0	38.0
Universidad Oberta de Catalunya	Profesor Titular	11.0	0.0	15.0

PERSONAL ACADÉMICO

Ver anexos. Apartado 6.

6.2 OTROS RECURSOS HUMANOS

Ver anexos. Apartado 6.2

7. RECURSOS MATERIALES Y SERVICIOS

Justificación de que los medios materiales disponibles son adecuados: Ver anexos, apartado 7.

8. RESULTADOS PREVISTOS

8.1 ESTIMACIÓN DE VALORES CUANTITATIVOS	
TASA DE GRADUACIÓN %	**TASA DE ABANDONO %**
25	25
TASA DE EFICIENCIA %	
85	
TASA	**VALOR %**
Tasa de exito	90
Tasa de rendimiento	65
Tasa de satisfacción	80

8.2 PROCEDIMIENTO GENERAL PARA VALORAR EL PROCESO Y LOS RESULTADOS

8.2. Progreso y resultados de aprendizaje

Cada final de semestre se facilita con el máximo detalle los resultados a través de los sistemas de información de la UOC, cuyos indicadores quedan recogidos principalmente en su Datawarehouse, que es la fuente básica de información de los resultados de valoración de la docencia para el profesorado. La información se recoge a todos los niveles: programa, asignatura y aula y por tanto va dirigida a diferentes perfiles: director de estudios, director de programa y profesor responsable de asignatura.

Las principales fuentes de información que permiten la obtención de los datos son:

- La gestión académica
- El proceso de recogida de la satisfacción de los estudiantes

Los resultados de estos procesos se cargan semestralmente al Datawarehouse de la universidad, la validación de estos procesos y la idoneidad de los indicadores es una función coordinada por el equipo de evaluación y calidad, que periódicamente se reúne con los administradores de los estudios para asegurar el uso y garantía de los indicadores.

Estos resultados se valoran a nivel de asignatura por el profesor responsable de asignatura, que puede determinar la necesidad de mayor información detallada para conocer las causas de los resultados o analizar las actividades y pruebas de evaluación puesto que todas ellas están accesibles a través de las herramientas del profesor en formato digital.

El director del programa, en el marco de la Comisión de titulación valorará los resultados globales de la titulación, esta valoración incluye la comparación con la información de previsión de resultados. Las valoraciones hechas por la comisión y las posibles acciones de mejora a desarrollar deberán ser recogidas por el director del programa y validadas por su director de estudios.

Los principales resultados que se valoran en la Comisión de la titulación semestralmente corresponden a:

- rendimiento: valorando los ítems de seguimiento de la evaluación continuada, tasa de rendimiento y tasa de éxito
- continuidad: valorando abandono principalmente a partir de la rematricula o las anulaciones voluntarias de primer semestre
- satisfacción: valorando los ítems correspondientes a la acción docente, la planificación, los recursos de aprendizaje y el sistema de evaluación

A final de cada curso además de los resultados expresados, se recogen los correspondientes al balance académico de curso y que presenta el Vicerrector de Ordenación Académica y Profesorado a la Comisión académica y a la Comisión de programas:

- rendimiento: valorando los mismos ítems
- continuidad: valorando los mismos y además la tasa de abandono
- satisfacción: valorando los mismos y además la satisfacción con la UOC, el programa, su aplicabilidad y los servicios
- graduación: tasa de graduación y de eficiencia, en este caso se valora empezar a disponer de estos a partir del curso 2011/12

- inserción o mejora profesional: a partir de los estudios propios elaborados por la universidad cada 2 años y a partir de los resultados obtenidos por los estudios transversales realizados por las universidades catalanas con el apoyo de AQU.
Este conjunto de datos están disponibles para todos los tipos de asignatura, aunque también está previsto disponer de información adicional para los trabajos de final de grado y también de las prácticas. En estos casos es pertinente valorar las memorias y trabajos realizados para valorar la adquisición del conjunto de competencias previstas.

9. SISTEMA DE GARANTÍA DE CALIDAD

ENLACE	http://cv.uoc.edu/UOC/a/intrauoc/qualitat/AUDIT-UOC_CAT_v.1.1.0_20101105.pdf

10. CALENDARIO DE IMPLANTACIÓN

10.1 CRONOGRAMA DE IMPLANTACIÓN	
CURSO DE INICIO	2011
Ver anexos, apartado 10.	
10.2 PROCEDIMIENTO DE ADAPTACIÓN	
No procede la adaptación. Sin embargo, de acuerdo con el art.6(4) del RD 1393/2007, según redacción otorgada por el RD 861/2010, los estudiantes del Máster de Seguridad Informática de la UOC (título propio) podrán obtener el reconocimiento de créditos académicos del plan de estudios del MISTIC, en función de las asignaturas o grupo de asignaturas superadas hasta el momento por el estudiante, de acuerdo con la tabla de equivalencias que se detalla en el apartado 4.4 de esta memoria.	
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**
	Pere	Fabra	Abat
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Av. Tibidabo 39-41	08035	Barcelona	Barcelona
EMAIL	**MÓVIL**	**FAX**	**CARGO**
v_academica@uoc.edu		934176495	Vicerector de Ordenación Académica y Profesorado

11.2 REPRESENTANTE LEGAL			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
	Oscar	Aguer	Bayarri
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Av. Tibidabo 39-41	08035	Barcelona	Barcelona
EMAIL	**MÓVIL**	**FAX**	**CARGO**
v_academica@uoc.edu		934176495	Gerent de la Universitat Oberta de Catalunya

11.3 SOLICITANTE			
El responsable del título es también el solicitante			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
	Pere	Fabra	Abat
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Av. Tibidabo 39-41	08035	Barcelona	Barcelona
EMAIL	**MÓVIL**	**FAX**	**CARGO**
v_academica@uoc.edu		934176495	Vicerector de Ordenación Académica y Profesorado

ANEXOS : APARTADO 1

Nombre : Declaracion_Intenciones_MISTIC.pdf

HASH SHA1 : G9cd9bk9Rw5GxuG7GYseSxDgSZQ=

Código CSV : 45903592245246256613957

DECLARACIÓN DE INTENCIONES

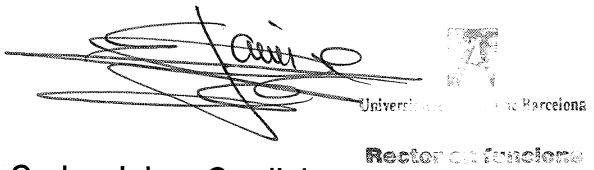
Ana Ripoll Aracil, Rectora Magnífica de la Universitat Autònoma de Barcelona (UAB), en virtud del nombramiento efectuado por el Decreto de la Generalitat de Catalunya 2/2009, de 7 de enero (DOGC 5295, de 13 de enero), como representante de esta institución en virtud de las competencias que prevé el artículo 75 de los Estatutos de la UAB, y en su nombre, el doctor Carles Jaime Cardiel, vicerrector de Proyectos Estratégicos y de Planificación, nombrado rector suplente según resolución de 9 de noviembre de 2010 (DOGC núm. 5759, de 19 de noviembre),

HAGO CONSTAR:

La voluntad de colaboración de la Universitat Autònoma de Barcelona en el desarrollo del proyecto formativo de creación de un Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC), presentado por la Universitat Oberta de Catalunya como universidad coordinadora, con la participación de las universidades Autònoma de Barcelona, Rovira i Virgili e Illes Balears, al amparo de lo establecido en la normativa aplicable a cada Universidad.

La Universitat Autònoma de Barcelona suscribe la presente Declaración de Intenciones, aprobada en su Consejo de Gobierno de 15 de julio de 2009, como garantía para que, en su momento y tras los trámites oportunos, se redacte y se apruebe un convenio específico de colaboración académica.

En Bellaterra (Cerdanyola del Vallès), a 24 de noviembre de 2010



Carles Jaime Cardiel
Rector suplente

UNIVERSITAT
ROVIRA I VIRGILI

DECLARACIÓN DE INTENCIONES DE COLABORACIÓN EN EL MÁSTER INTERUNIVERSITARIO EN SEGURIDAD DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES (MISTIC)

DECLARACIÓN DE INTENCIONES

Josep Manel Ricart, Vicerrector de Política Académica y de Investigación de la Universidad Rovira i Virgili, por delegación del Rector

HAGO CONSTAR:

La voluntad de colaboración interuniversitaria de la Universidad Rovira i Virgili en la solicitud de verificación del Máster oficial interuniversitario conducente al título conjunto de máster universitario en **Seguridad de las Tecnologias de la Información y de las Comunicaciones (MISTIC) para las universidades Oberta de Catalunya, Autònoma de Barcelona, Rovira i Virgili i Illes Balears**, presentada por la Universitat Oberta de Catalunya como universidad coordinadora.

La colaboración de la Universidad Rovira i Virgili en este máster se prevé que será aprobada por el Consejo de Gobierno de esta universidad en fecha 5 de noviembre de 2009

Tarragona, 15 de octubre de 2009

UNIVERSITAT
ROVIRA I VIRGILI

CPISR-1 C Jose Manuel
Ricart Pla
2009.10.15 08:10:51
+02'00'

Antonio González Senmartí, secretario general de la Universitat Rovira i Virgili,

CERTIFICO:

Que el convenio específico de colaboración interuniversitaria entre la Universitat Oberta de Catalunya, la Universitat Autònoma de Barcelona y la Universitat Rovira i Virgili para la realización conjunta del Master Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones, que será impartido a partir del curso académico 2011-2012, se encuentra en proceso de revisión por parte de los servicios académicos y jurídicos correspondientes a fin de poder proceder en el más breve plazo posible a su firma por parte de los representantes legales de las Universidades arriba mencionadas.

Y, para que así conste, firmo el presente certificado.

Tarragona, 18 de mayo de 2011

CPISR-1 C
Antonio Gonzalez
Senmartí
2011.05.18
21:19:07 +02'00'

UNIVERSITAT ROVIRA I VIRGILI
C/ de l'Escorxador, s/n
43003 Tarragona
Tel. +34 977 55 80 21
Fax +34 977 55 80 22
www.urv.cat

Antoni Gonzàlez Senmartí, secretari general de la Universitat Rovira i Virgili,

CERTIFICO:

Que el Consell de Govern de la Universitat Rovira i Virgili, en la seva sessió de data 24 de febrer de 2011, va aprovar la implantació, amb les modificacions que es puguin derivar del procés d'avaluació, i sempre que siguin verificats i autoritzats, dels màsters universitaris següents:

- Estudis Avançats en Administració i Gestió Públiques
- Relacions Euromediterrànies (interuniversitari, coordina URV)
- Enginyeria Ambiental i Producció Sostenible
- Enginyeria Química
- Noves Fronteres en Enginyeria Química i de Processos
- Seguretat de les Tecnologies de la Informació i de les Comunicacions (coordina UOC)

I, perquè consti, signo aquest certificat.

Tarragona, 14 de març de 2011

CPISR-1 C Antonio Gonzalez Senmartí
2011.03.20
23:18:05 +01'00'

D'acord amb l'art. 20.3 de la Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya, es fa constar que la present certificació s'expedeix amb anterioritat a l'acta del Consell de Govern.

Universitat Autònoma de Barcelona

Secretaria General

Isabel Pont Castejón, secretària general de la Universitat Autònoma de Barcelona,

CERTIFICO:

I. Que el Consell de Govern, en la sessió del dia 15 de juliol de 2009, acordà:

1. Aprovar la proposta de nous màsters universitaris 2010-2011, en els termes que consten al document que s'annexa.

2. Elevar la proposta al Consell Social per a la seva aprovació.

II. Que l'acta de la sessió en la qual es va prendre l'acord objecte d'aquesta certificació està pendent d'aprovació, la qual cosa es fa constar de conformitat amb el que estableix l'article 27.5 de la Llei 30/1992, de 26 de novembre, de *Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común,* modificada per la Llei 4/1999.

I, perquè en prengueu coneixement i tingui els efectes que corresponguin, signo aquest certificat.

Bellaterra (Cerdanyola del Vallès), 15 de juliol de 2009

Universitat Autònoma de Barcelona

Secretària general

Universitat Autònoma de Barcelona

Rectora

Vist i plau

La rectora

UAB
Universitat Autònoma de Barcelona

Llista de nous màsters universitaris 2010-2011

(Acord del Consell de Govern de 15 de juliol de 2009)

POP Màster	Coordinador POP/Màster	Inter.	Observacions
Art i Musicologia	**Jesús Hernández**		
Història, teoria i crítica del disseny (Escola EINA de Disseny i Art)	Oriol Pibernat	-	
Musicologia i educació musical	Jaume Ayats	UAB	Modificació de màster ja existent
Biociències	**Dolores Jaraquemada**		
Noves estratègies terapèutiques per malalties neurodegeneratives	Lydia Gimenez	-	
Estructura i funció de proteines	Xavier Daura	Sí	
Ciències	**Francesc Pi**		
Enginyeria Fotònica, Nanofotònica i Biofotònica/Photonics Engineering, Nanophotonics and Biophotonics	Jordi Mompart	EM-Sí	
Física dels sistemes biològics i radiofísica	Jordi Mompart		
Ciències de l'Educació	**Enric Roca**		
Recerca en didàctica de la història, de la geografia i de les ciències socials	Antoni Santisteban	-	
Recerca en motricitat, art i educació	Jaume Barrera	-	
Dret	**Carmen Tort Martorell**		
Criminologia i execució penal	Josep Cid Moliné	UAB	
Investigació en Dret	C. Tort Martorell	-	
Drets Socio-laborals	F.Pérez Amoros E.Rojo Torrecilla		
Advocacia i Procura	C. Tort Martorell	-	
Economia i Empresa	**Xavier Vilà**		
Anàlisi econòmica especialitzada/Specialized economic analysys	UPF/BSGE	Sí	
Enginyeria	**Ramon Vilanova**		
Logística i gestió de la cadena de subministrament/Logistics and supply chain management	Juan José Ramos	UAB	
Seguretat de les tecnologies de la informació i de les comunicacions	Jordi Herrera	Sí	
Estudis Europeus	**Francesc Morata**		
Polítiques públiques i desenvolupament internacional/Public policy and international development (UPF-UB-IBEI-Institute of Social Studies La Haia)	Laura Feliu	Sí	
Relacions internacionals (UPF-UAB-IBEI)	?	Sí	
Estudis Europeus avançats	Blanca Vilà Costa	EM-UAB	
Història	**Jesús Hernández**		
Arxivística i gestió de documents (Escola Superior d'Arxivística i Gestió de Documents)	Alfred Mauri	-	
Llengua i literatura	**Jesús Hernández**		
Recerca en estudis francòfons	Ricard Ripoll	EM	
Medicina i Salut	**Miquel Sabrià**		
Hematologia oncològica i trasplantament hemopoètic	Jordi Sierra	-	
Immunologia i retrovirologia de la vacuna del VIH	Bonaventura Clotet	UAB	

UOC
www.uoc.edu

LLORENÇ VALVERDE GARCIA, secretari del Consell de Govern de la UNIVERSITAT OBERTA DE CATALUNYA

CERTIFICO:

Que en el marc de la nova oferta de Màster universitari i Doctorat prevista pel curs 2011-12 de la Universitat Oberta de Catalunya, les memòries dels programes següents van ser aprovades pel Consell de Govern en les dates que s'indica:

Màster Universitari en Conflictologia, 19 de gener de 2011
Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions, 19 de gener de 2011
Màster Universitari en Direcció de les organitzacions a l'economia del coneixement, 22 de setembre de 2010

Barcelona, 24 de febrer de 2011

Av. Tibidabo, 39-43
08035 Barcelona - Spain

Tel. +34 932 532 300
Fax +34 934 176 495

ANEXOS : APARTADO 2

Nombre : P2_Memoria_MISTIC_F2.pdf

HASH SHA1 : 7JX+ezhKLha/iC2WgUWONu3DTws=

Código CSV : 4590360553155528290611 5

2. JUSTIFICACIÓN

2.1. Justificación del título propuesto, argumentando el interés académico, científico o profesional del mismo

Justificación del título

La demanda de ingenieros, informáticos o de telecomunicaciones, específicamente preparados para trabajar en el campo de la seguridad de las tecnologías de la información y de las comunicaciones es cada vez mayor. Por un lado, las transacciones electrónicas son cada vez más habituales y la legislación que hay a su alrededor es más exigente. Por el otro, las empresas son más conscientes de los riesgos de seguridad y la voluntad para invertir en sistemas de protección ha aumentado (ver más detalles sobre el mercado de la seguridad TIC en el apartado Estudios de mercado, pág. 10).

El crecimiento del mercado de la seguridad TIC en España también constituye una oportunidad para el desarrollo de proyectos técnicos en esta área que sean pioneros a nivel europeo y mundial. Ello implica la necesidad de promover la investigación y la innovación tecnológica, que deberá contribuir a generar empleo altamente cualificado y con capacidad para generar productos y servicios que a su vez generen puestos de trabajo.

Aunque la necesidad de profesionales formados en el ámbito de la seguridad de las tecnologías de la información y de las comunicaciones es clara, no se encuentran currículos completos de esta materia (si bien es cierto que tanto en las titulaciones a extinguir -titulaciones técnicas/superiores en Informática o Telecomunicaciones- como en los nuevos grados aprobados ya hay algunas asignaturas dedicadas a aspectos básicos de la seguridad de la información). Además, no existe en la actualidad ningún máster universitario de seguridad con orientación profesional e investigadora en el entorno universitario catalán. Estos hechos generan un vacío de enseñanzas regladas en esta temática.

Las causas por las que no hay una profundización en este ámbito en enseñanzas regladas son diversas, pero las más relevantes son por un lado, la falta de tiempo en los grados para incluir las temáticas de seguridad y por otro lado, la dificultad de encontrar recursos especializados (es decir, profesorado experto en la materia) que pueda impartir estas asignaturas con un buen nivel de calidad.

El MISTIC nace con la vocación de vencer estas dos causas. En primer lugar, se crea una propuesta sólida de formación especializada en seguridad TIC, un máster completo, que responda a la demanda de la sociedad en este sector. En segundo lugar, se pretende aprovechar la experiencia de las diferentes universidades del entorno catalán en el campo de la seguridad de las TIC. De esta manera, se prevé que cada universidad participante imparta las asignaturas de las que su profesorado es experto.

El conocimiento de los grupos de investigación que impulsan el Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones viene avalado por su trayectoria en la investigación en este ámbito. Como dato específico, la práctica totalidad de los

grupos de investigación interesados en participar en el máster interuniversitario forman parte del proyecto ARES, el único proyecto CONSOLIDER que el Ministerio ha financiado hasta el momento sobre la temática relativa a la seguridad informática. Este hecho es un buen indicador de la calidad de los equipos integrantes y de su conocimiento de la materia.

Por otro lado, la UOC, la UAB y la URV disponen de una amplia oferta de posgrado en el ámbito de las tecnologías de la información y de las comunicaciones. Los programas que se ofrecen en este ámbito son los siguientes:

UOC:

- Máster universitario en Software Libre
- Másteres y posgrados no oficiales:
  - Dirección y gestión de las TIC
  - Seguridad informática
  - Business Intelligence
  - SAP
  - .NET
  - Cisco
  - Multimedia
  - Bioinformática y bioestadística
  - Ingeniería del software
  - Videojuegos
  - Sistemas de información geográfica y geotelemática
  - Software libre
  - Tecnología y accesibilidad
  - Interacción persona-ordenador
  - Sistemas TIC salud
  - Telemedicina
  - Educación y TIC
  - Administración electrónica

UAB:

- Máster universitario en Ciencia e Ingeniería Computacional
- Máster universitario en Computación de Altas Prestaciones
- Máster universitario en Diseño de Sistemas de Comunicación
- Máster universitario de Informática Avanzada
- Máster universitario de Visión por Computador e Inteligencia Artificial
- Máster universitario en Tecnologías Multimedia

URV:

- Máster universitario en Ingeniería Informática y de la Seguridad
- Másteres y posgrados no oficiales:
  - Aplicaciones java
  - Aplicaciones .NET
  - Aplicaciones SQL y Oracle

Estudios de mercado

Según un estudio de IDC (2006) sobre el "Mercado de la seguridad en España", el 40% de las empresas sitúa las responsabilidades de seguridad por encima de las asignadas a los directores de TI. Por otro lado, y según el mismo estudio, en 2008, la población mundial de profesionales de seguridad ascenderá a 2,1 millones de personas.

Por otro lado, según el "Estudio sobre el sector de la seguridad TIC en España, 2009" del Instituto Nacional de Tecnologías de la Comunicación (Inteco):

- El mercado mundial de la seguridad ha experimentado fuertes crecimientos en los últimos años, sumando crecimientos importantes de forma ininterrumpida. El mercado español de seguridad ha seguido esta misma tendencia alcanzando en 2006 los 617M€. De esta cifra, los servicios de seguridad representan el 54,9% del mercado, el software de seguridad, un 36,4% y el hardware de seguridad, el 8,7%.

- La prospectiva y tendencias en el mercado de la seguridad es que la inversión en seguridad seguirá incrementándose y el mercado continuará mostrando tasas de crecimiento muy importantes.

- España cuenta con una industria de seguridad TIC muy relevante y desde la Administración se han puesto en marcha algunas iniciativas con potencia tractora suficiente como para desarrollar el sector y contribuir a su posicionamiento en el mercado internacional, un posicionamiento que ya existe, pero que puede mejorarse. Entre los proyectos tractores merece una mención especial el conjunto de iniciativas ligadas al **DNI electrónico**. Iniciativa que puede ser **la base para el desarrollo de un amplio mercado** de productos y servicios. A los esfuerzos para su puesta en marcha y extensión entre la ciudadanía han de sumarse los relativos a los desarrollos (librerías, etc.) que permitan multiplicar y difundir sus usos.

- Uno de los factores inhibidores y de impulso del mercado de seguridad TIC es que los hogares y las empresas no conocen adecuadamente sus necesidades de seguridad TIC, no son conscientes de la evolución de las amenazas y, eventualmente, desconocen sus obligaciones legales. En este escenario parece clara la necesidad de aumentar las **iniciativas formativas y divulgativas** para crear una cultura de la seguridad.

- Sobre la demanda de seguridad TIC en las grandes empresas, aumenta el número de organizaciones que cuenta con directivos específicos en el área de seguridad TIC, de 2006 a 2007 (10%). Este dato parece confirmar que la concienciación sobre la seguridad crece de forma notable entre las grandes empresas y es objeto creciente de un trato diferencial respecto al resto de sistemas de información.

- El 95% de las pymes españolas considera importante o muy importante la seguridad TIC. Este dato no parece verse acompañado por otros indicadores, como el conocimiento de las amenazas. Carencia que puede estar motivada por la **ausencia de personal cualificado en materia de seguridad TIC en las pymes españolas**: únicamente el 16% de las pymes encuestadas declara disponer de expertos en seguridad TIC en su plantilla. Parece **necesario reforzar las acciones de formación emprendidas por los organismos**

públicos para favorecer la implantación entre las pymes de una cultura de seguridad acorde con la importancia que se le concede.

En USA, un informe elaborado por la empresa TNS en abril de 2008, ***Trends in Information Security*****,** (encargado por CompptIA Research), se indica que la formación y certificación en seguridad está "marcando la diferencia" entre las empresas. De hecho, más del 80% de las organizaciones que proporcionaron formación en seguridad afirman que la inversión ha valido la pena y ha aumentado la seguridad de sus activos.

Por otro lado, cabe destacar que en USA la seguridad también continua siendo una prioridad entre la mayoría de organizaciones, las cuales dedican cada vez más recursos a este ámbito. La formación es un foco de atención de muchas empresas, y está ayudando a bajar los riesgos de los fallos de seguridad. Aproximadamente un 60% de las empresas requieren formación de seguridad (IT training) para el personal de los departamentos de informática, y aproximadamente la mitad dan esta formación:

Inserción laboral

Como se ha destacado en el apartado Estudios de mercado, pág. 10, la demanda de profesionales de la seguridad TIC no sólo se mantendrá en los próximos años sino que se prevé que irá en aumento. Las causas son diversas:

- Concienciación de las empresas de la importancia de la seguridad TIC
- Oportunidad de crear nuevas aplicaciones y servicios a partir de la implantación del DNI electrónico. Gran impulso de la administración para migrar todos los trámites con los ciudadanos a través de servicios web que ofrezcan la misma (o más) seguridad que las ventanillas presenciales.
- Evolución de las TIC para proporcionar servicios de red en cualquier momento, cualquier lugar, y desde cualquier dispositivo. Estas nuevas tecnologías y servicios conllevan nuevos riesgos de seguridad que deben ser tratados por profesionales especializados.

El Máster interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC) tiene un modelo de aprendizaje virtual, como el resto de los programas formativos de la UOC. Es por ello que prevemos que el perfil personal del estudiante tendrá unas características muy similares al estudiante UOC. Esto es, el 60% de los alumnos tienen más de 30 años y el 95% trabaja a tiempo completo o parcial. Así pues, el concepto de inserción laboral se trabaja desde la perspectiva de desarrollo profesional y personal. Los diferentes estudios realizados por la UOC en los últimos años muestran que los graduados valoran las posibilidades de promoción o cambio de orientación como elementos de desarrollo.

En este contexto, es significativo el *Estudio de impacto de los graduados* realizado por la UOC en el año 2005, con una muestra de 2.224 titulados de la UOC, de los cuales un 11% correspondían a graduados de las Ingenierías Técnicas en Informática de Gestión y Sistemas. Los resultados mostraron que el 64% de los titulados encuestados habían cambiado de empresa después de haber estudiado en la universidad y un 27% había mejorado su posición dentro de la misma organización, aumentando también su salario. En general, un 41%

consideraba que había mejorado totalmente o bastante a nivel profesional gracias a sus estudios.

A la vista de estos resultados, se puede concluir que el máster que se presenta cumplirá una función muy importante en la formación de profesionales altamente demandados en nuestro país, dando la oportunidad a aquellas personas que ya están trabajando de mejorar su posición o categoría profesional o de reorientar su carrera.

Desde este punto de vista, el perfil preferente de estudiantes a los que va dirigido es el siguiente: directores de sistemas de información, responsables de informática, directores de desarrollo, jefes de proyectos en tecnologías de la información y de las comunicaciones, técnicos de sistemas, analistas, analistas programadores, programadores, administradores de bases de datos, consultores de sistemas de información, expertos en Internet, ingenieros de operaciones en red, etc.

2.1.1. Normas reguladoras del ejercicio profesional vinculado al título

El título presentado no corresponde a ninguna profesión que se vea afectada, en este momento, por normas reguladoras que puedan condicionar la actividad profesional.

2.2. Referentes externos a la universidad proponente que avalen la adecuación de la propuesta a criterios nacionales o internacionales para títulos de similares características académicas

Existen diferentes programas de postgrado, tanto a nivel nacional como internacional, que tratan la seguridad en las TIC. Cada uno de ellos ofrece una intensificación de contenidos en un ámbito concreto, generalmente en seguridad en redes. La titulación presentada se diferencia de las otras por ser una titulación interuniversitaria, y por lo tanto, tener la capacidad de ofrecer asignaturas especializadas en diferentes ámbitos de la seguridad. En concreto, la titulación ofrece tres especialidades profesionalizadoras (redes, aplicaciones, y gestión). El estudiante seguirá una de las especialidades y además adquirirá una visión integral de la seguridad en la empresa que le permitirá liderar las estrategias de seguridad de la misma.

Por otro lado, el máster presentado también tiene la peculiaridad de ofrecer tanto una orientación profesional como de investigación, haciendo hincapié en la búsqueda de soluciones fáciles y usables para resolver problemas reales. La modalidad de los estudios es eminentemente virtual enfocada a la adquisición de competencias mediante una metodología práctica y aplicada.

Referentes nacionales

Existen tres programas nacionales oficiales de máster del ámbito de seguridad TIC, todos ellos con orientación profesional.

Másteres oficiales:

1. **Universidad**: Alfonso X El Sabio

Título: Máster Oficial en Ingeniería de Seguridad de la Información y las Comunicaciones
Créditos: 60 ECTS
Orientación: profesional
Tipo de formación: presencial y virtual (Madrid)
Contenido:

- Tecnologías de red para la seguridad
- Implantación de sistemas seguros
- Gestión de la seguridad
- Aspectos legales de la seguridad

2. **Universidad**: Deusto
Título: Máster Oficial en Seguridad de la Información
Créditos: 60 ECTS
Orientación: profesional
Tipo de formación: presencial (Bilbao)
Contenido:
    - Calidad, innovación tecnológica y Responsabilidad Social
    - Seguridad de sistemas de información
    - Seguridad de redes de comunicación
    - Seguridad en servicios de aplicación
    - Tecnologías de seguridad
    - Seguridad de la información a nivel de aplicación
    - Legislación
    - Criptografía avanzada
    - Auditoría de seguridad
    - Administración avanzada de redes
    - Mecanismos de Respaldo y Recuperación de Información
    - Gestión de la Seguridad de la Información

3. **Universidad**: Europea de Madrid
Título: Máster Oficial en Seguridad de las Tecnologías de la Información y las comunicaciones
Créditos: 60 ECTS
Orientación: profesional
Tipo de formación: presencial (Madrid)
Contenido:
    - Arquitecturas y modelos de seguridad de la información
    - Políticas de seguridad
    - Sistemas de gestión de la seguridad
    - Análisis de riesgos
    - La seguridad física y del entorno
    - Técnicas criptográficas
    - Certificación y firma electrónica
    - Gestión de identidades y accesos
    - La seguridad en las comunicaciones y operaciones
    - La seguridad en el software de base y en las aplicaciones

- La seguridad y las personas
- Cumplimiento con el marco jurídico
- El plan de continuidad del negocio

Másteres no oficiales:

Además de estos cuatro programas oficiales de máster que hemos resaltado, también podemos encontrar un conjunto de postgrados en seguridad, generalmente de menor duración.

4. **Universidad**: País Vasco
   Título: Máster en Infraestructuras, Servicios y Seguridad en Redes
   Créditos: 30 ECTS
   Orientación: profesional (Donostia)
   Tipo de formación: virtual
   Contenido:
   - Aspectos legales y regulatorios
   - Diseño de Redes de datos
   - Gestión de la seguridad
   - Infraestructuras públicas de comunicaciones
   - Módulos complementarios
   - Redes Basadas en IP
   - Redes de área local y metropolitana
   - Servicios de Red

5. **Universidad**: Zaragoza
   Título: Máster en Servicios Web, Seguridad Informática y Aplicaciones de Comercio Electrónico
   Créditos: 53 ECTS
   Orientación: profesional
   Tipo de formación: presencial (Zaragoza)
   Contenido:
   - Web semántica
   - Negocio y comercio electrónico
   - Programación avanzada
   - Conceptos y arquitectura de servicios web
   - Interacción persona-ordenador
   - Seguridad Informática
   - Redes
   - Seminarios y talleres
   - Lenguajes web
   - Programación servicios web

6. **Universidad**: Politécnica de Madrid
   Título: Máster en Seguridad informática
   Créditos: 60 ECTS
   Orientación: profesional
   Tipo de formación: presencial (Madrid)

Contenido:

- La seguridad lógica y los SGBD
- Reglamento de Certificación y Evaluación de la Seguridad de la TI
- Responsabilidades del comprador de productos y servicios de seguridad de TI
- Prácticas de diseño e implantación de la seguridad en redes y en entornos departamentales
- Prácticas de seguridad en aplicaciones de Negocio Electrónico
- La Seguridad en las aplicaciones móvil
- La Gestión integrada de la Seguridad
- El Documento de Seguridad de la LOPD
- Plan de Continuidad
- La Práctica de la Seguridad y Auditoria en las Organizaciones

7. **Universidad**: Politécnica de Madrid
   Título: Máster en Dirección y Gestión de la Seguridad de la Información
   Créditos: 60 ECTS
   Orientación: profesional
   Tipo de formación: presencial (Madrid)
   Contenido:
   - Análisis y Gestión de Riesgos, Métodos y Herramientas
   - Seguridad en el Diseño y Desarrollo de Sistemas.
   - Tecnologías Aplicadas a la Seguridad de la Información
   - Seguridad en el Diseño y Desarrollo de Sistemas.
   - Seguridad en las Arquitecturas de Red y Comunicaciones
   - Normas y Estándares de Seguridad de las TIC
   - Cumplimiento Legislativo en la Seguridad y la Protección de la Información.
   - Fundamentos y Conceptos Empresariales
   - Habilidades para la dirección y el liderazgo.
   - El Gobierno de TI
   - La Política de Seguridad de la Información
   - El Sistema de Gestión de la Seguridad de la Información
   - Protección de la Plataforma TI
   - La Auditoria de Sistemas de Información.

8. **Universidad**: Politécnica de Madrid
   Título: Máster en Sistemas de Comunicación e Información para la Seguridad y la Defensa
   Créditos: 36 ECTS
   Orientación: profesional
   Tipo de formación: presencial y virtual (Madrid)
   Contenido:
   - Aplicaciones y servicios de información y colaboración en el web
   - Comunicaciones móviles
   - Comunicaciones, localización y radionavegación por satélite
   - Fundamentos matemáticos: teoría de la señal y las comunicaciones, teoría de la información
   - Gestión de proyectos de seguridad y defensa

- Guerra electrónica en comunicaciones
- Introducción a las redes y servicios de telecomunicación
- Introducción a los sistemas de información
- Las tecnologías de la información y las comunicaciones: concepto, evolución, tendencias
- Mando y control
- Seguridad de los sistemas de información
- Seguridad de redes de comunicaciones
- Sensores radar y electroópticos
- Servicios y redes tcp/ip
- Tecnologías de la información y comunicacionesSistemas de comunicación

- Sistemas sensores
- Sistemas de información
- Guerra electrónica

9. **Universidad**: Pontificia de Salamanca
   Título: Máster en Seguridad Informática
   Créditos: 70 ECTS
   Orientación: profesional
   Tipo de formación: presencial (Madrid)
   Contenido:
   - Seguridad en las TIC
   - Consultoría en Seguridad Informática
   - Auditoría Informática
   - Desarrollo de aplicaciones web comunes

Referentes europeos

Se han tenido en cuenta los programas formativos de dos iniciativas **interuniversitarias**:

- NordSecMob, formado por: Helsinki University of Technology (TKK) in Finland, Technical University of Denmark (DTU), The Royal Institute of Technology (KTH) in Sweden, The Norwegian University of Science and Technology (NTNU) and the University of Tartu (UT) in Estonia. Ofrece el Máster's Programme in Security and Mobile Computing
- Kerckhoffs Institute for Computer Security, formado por: University of Twente, the Eindhoven University of Technology, y the Radboud University Nijmegen). Ofrece un máster in computer security.

Otros programas europeos:

- University of Tampere: Máster´s Programme in Security Management
- Luleå University of Technology: Máster Programme in Information Security
- Royal Holloway, University of London: MSc Information Security
- University College of London: MSc. on Information Security
- University of Liverpool, MSc in Computer Security
- University of Birmingham, MSc in Computer Security
- University of Surrey, MSc in Security Technologies and Applications

- University of Bedfordshire, MSc in Computer Security and Forensics
- University of Greenwich, MSc in Computer Security Forensics and Risk Management
- Kingston University, MSc in Network and Information Security
- Liverpool John Moores University: MSc in Computer Network Security
- University of Leicester, MSc Security and Risk Management
- University of Kent, MSc Information Security and Biometrics
- ETH Zurich. MSc Computer Sciencie. Track on information security.

Referentes internacionales

Programas de Universidades estadounidenses:

- The New York Institute of Technology (NYIT). Máster of Science in Information, Network and Computer Security
- DePaul University, Máster of Science in Computer, Information and Network Security
- Western Governors University: M.S. Information Security and Assurance
- Kaplan University: Máster of Science in Information Technology in Information Security and Assurance
- East Stroudsburg University: Máster of Science in Information Security
- Nova Southeastern University: M.S. in Information Security
- Stevens Institute of Technology: Máster of Science in Security Management
- American InterContinental University: Máster of Information Technology with a Concentration in Internet Security
- James Madison University: M.S. Information Security
- Johns Hopkins University: Máster of Science in Security Informatics
- Capitol College: M.S. - Information Assurance

Programas de las certificaciones empresariales de seguridad:

- Certified Information Systems Security Professional (CISSP), from International Information Systems Security Certification Consortium, Inc., (ISC)²
- Cisco Certified Security Professional (CCSP)
- Security Certified Programm Certifications (SCNS, SCNP, SCNA)

Otros referentes

- Las recomendaciones de la Generalitat de Catalunya respecto a la formación en una tercera lengua de los estudiantes universitarios.
- Las competencias transversales de la UOC, UAB y URV, por lo que se refiere a la comunicación en una lengua extranjera, el uso y aplicación de las TIC y la comunicación escrita en el ámbito académico y profesional.
- Los ámbitos de investigación principales de los departamentos y estudios participantes en el máster, que incluyen ámbitos de investigación en seguridad TIC.
- El programa de doctorado de la UOC, UAB y URV, y el papel relevante que juega la investigación en seguridad TIC dentro de estos programas de doctorado.
- La misión de la UOC de dar formación a lo largo de la vida.
- El perfil de los estudiantes del máster de Seguridad de la UOC.

2.3. Descripción de los procedimientos de consulta internos y externos utilizados para la elaboración del plan de estudios

Proceso de reflexión metodológica

A continuación se detalla el proceso de reflexión metodológica realizado por las tres universidades participantes en el máster.

Universitat Oberta de Catalunya (UOC)

En el caso de la UOC, dos factores han sido determinantes en el proceso general de diseño de los planes de estudio conducentes a la obtención de las titulaciones adaptadas al EEES: por un lado, los planes piloto de adaptación al EEES llevados a cabo en el curso 2005/6 y siguientes y, por otro, el proceso de evaluación de las titulaciones oficiales de la UOC a partir del curso 2006/07.

La UOC respondió a la convocatoria, impulsada por la Generalitat de Catalunya, para la presentación de Planes piloto de adaptación al EEES con el inicio de dos programas en el curso 2005/06. Estos grados fueron diseñados con anterioridad al Real decreto 1393/2007 en el que se establece la ordenación de las enseñanzas universitarias oficiales y, por tanto, no constituyen en la actualidad una oferta de Grado. Esta primera adaptación permitió a la universidad acumular cierta experiencia en el diseño de titulaciones adaptadas al EEES y ha contribuido positivamente a la presentación de los grados adaptados ya al RD 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales.

Estas titulaciones piloto han seguido el procedimiento establecido por la Agencia de Calidad del Sistema Universitario Catalán (AQU) para la certificación de la adaptación de las titulaciones piloto de las universidades del sistema universitario de Cataluña al Espacio Europeo de Educación Superior y cuentan ya con la resolución favorable en cuanto cumplen los criterios establecidos de implantación completa, transparencia documental e indicadores de calidad.

Por último, destacamos que el diseño y puesta en marcha de los programas pilotos ofrecieron a la universidad la posibilidad de iniciar internamente un proceso de reflexión previo sobre aspectos fundamentales del modelo de enseñanza-aprendizaje (el sistema de créditos ECTS, las competencias, el sistema de evaluación, el aula virtual…) de gran utilidad también en el diseño actual de titulaciones adaptadas al EEES.

Este proceso de análisis sirvió de base para actualizar algunos elementos concretos del modelo. En marzo de 2007, se inició un proceso de reflexión general y sistematizada sobre el impacto de los planteamientos del EEES en la metodología de la universidad y la estructura de las nuevas enseñanzas. Se crearon 8 grupos de trabajo para abordar las temáticas siguientes:

- Crédito ECTS
- Competencias
- Plan docente
- Evaluación
- Reconocimiento académico de la experiencia profesional (RAEP)
- Materiales didácticos

- Aula
- Trabajo fin de grado / trabajo fin de máster y prácticas

Para cada uno de los temas se definen y se concretan unos objetivos y se constituyen los diferentes equipos de trabajo formados por profesores de los diferentes estudios de la universidad, y por personal no académico directamente implicado en el diseño, el desarrollo y la evaluación de los programas, y pertenecientes a distintas áreas de gestión docente (Área de Operaciones de Gestión Docente, Área de Incorporación y Seguimiento del Estudiante, Área de Biblioteca, unidad de Gestión de Contenidos, Área de Planificación y Evaluación, Tecnología Educativa). En total, participan directamente setenta personas en el análisis, la reflexión y la síntesis de los ocho temas mencionados anteriormente.

A finales del mes de junio de 2007, cada uno de los grupos de trabajo elabora un documento que recoge las conclusiones provisionales de cada tema y un conjunto de propuestas sometidas a debate en diferentes comisiones de la universidad: comisión académica, comisión de programas y comisión de gestión.[2] Finalmente, en julio de 2007 se dispone de un documento de conclusiones: *Conclusiones finales al debate sobre la adaptación metodológica al EEES*.

A partir de septiembre de 2007 se abren dos líneas de trabajo para dar un nuevo impulso a la innovación metodológica relacionada con la actividad docente. Por una parte, se diseña un plan de comunicación para dar a conocer y extender formalmente a todo el profesorado y al personal de gestión afectado las conclusiones finales del debate metodológico, por medio de un plan de formación y comunicación que se lleva a cabo a lo largo de 2008. Por otra parte, se ha puesto en marcha una segunda fase de análisis, que da continuidad a los ocho temas mencionados, para llevar a cabo el diseño operativo y la implementación de las conclusiones de los temas tratados en la primera fase, tanto en relación con aspectos metodológicos como con elementos de gestión necesarios para su realización; ante la detección de nuevos temas que deben ser analizados por parte de equipos de trabajo transversales, se está reflexionando en torno a los recursos docentes y los docentes colaboradores.

Universidad Rovira i Virgili (URV)

La URV se ha implicado en la implantación de metodologías modernas en los procesos de enseñanza/aprendizaje, de acuerdo con el espíritu de la Declaración de Bolonia. Desde el inicio del proceso de Bolonia, organizó Jornadas y conferencias, dirigidas al conjunto de la comunidad universitaria, pero especialmente a sus dirigentes, dando a conocer los puntos principales del proceso a medida que éste se iba desarrollando (jornadas sobre acción tutorial, sobre presentación del proyecto Tunning, por citar solo dos ejemplos) con la participación de expertos nacionales y europeos.

Desde hace tres cursos, la URV ha ido adaptando sus planes de estudio al Espacio Europeo de Educación Superior, a partir de la implantación de unos planes piloto de grado y máster, en respuesta a una convocatoria del Departamento de Universidades de la Generalitat de Cataluña, y a continuación, implantando el sistema ECTS de manera progresiva en el resto de las enseñanzas que imparte. Este proceso ha implicado una amplia revisión de nuestros planes

[2] Comisión Académica: constituida por los directores de estudio; Comisión de Programas: constituida por los directores de programa; Comisión de Gestión: constituida por los directores de las áreas de gestión académica.

de estudio, que ha generado numerosas reuniones y discusiones a diferentes niveles (la propia Universidad, en su Claustro, Consejo de Gobierno, Comisión de Ordenación Académica, Comisión de Docencia; los distintos centros, los departamentos y entre los estudiantes).

Asimismo, el Vicerrectorado de Política Docente y Convergencia al EEES de esta universidad ha desarrollado una amplia labor con el objetivo de coordinar el proceso de armonización Europa de la universidad. Para ello ha realizado una serie de reuniones con los responsables de las enseñanzas para ir implementando paso a paso el nuevo sistema que a su vez implica un nuevo concepto de cultura universitaria. A su vez, los responsables se han encargado de transmitir y coordinar en su enseñanza el citado proceso.

Universitat Autónoma de Barcelona (UAB)

Por su parte, la UAB ha desarrollado distintas iniciativas para la reflexión e implementación de las nuevas metodologías desde la puesta en marcha de la adaptación de las titulaciones a las nuevas características surgidas del EEES.

La Universitat Autónoma de Barcelona participó también en la prueba piloto impulsada por la Generalitat de Catalunya, para la presentación de Planes piloto de adaptación al EEES con el inicio de dos programas en el curso 2005/06. Propuso la definición y el desarrollo de, entre otros, un título propio de Informática en el que se empezó a trabajar inmediatamente sobre los grandes retos impuestos por la convergencia al EEES en lo que se refiere a las metodologías docentes: la visión del alumno como centro del proceso de aprendizaje o las competencias que van más allá los conocimientos, como parte necesaria de la formación universitaria, entre otras.

La visión del alumno como centro neurálgico del proceso de aprendizaje lleva a unas metodologías docentes basadas en el trabajo del alumno. La implantación de una metodología de este tipo requiere una alta dedicación del profesorado a las tareas cas de tutorización, corrección, evaluación, preparación de casos prácticos, etc.,

Para ello, la UAB cuenta con una unidad especializada en formación del profesorado (Unitat d'Innovació Docent en Educació Superior – IDES) que desde hace ya muchos años asesora a los docentes en las nuevas metodologías docentes que sirven de base para el correcto desarrollo del nuevo Espacio Europeo de Educación Superior.

El Vicerrectorado de Política Académica, responsable último de las titulaciones impartidas en la universidad, trabaja junto con la Oficina de Planificación y Calidad de la universidad, para que las distintas titulaciones de la universidad sigan un mismo enfoque metodológico que permita un desarrollo satisfactorio del nuevo EEES.

Procedimientos de consulta internos

La UOC, la UAB y la URV han decidido impulsar la titulación del MISTIC en el marco del espacio europeo de educación superior, de acuerdo con los criterios fijados por el Real decreto 1393/2007, de 29 de octubre, por el cual se establece la ordenación de las enseñanzas universitarias oficiales. En este proceso previo de definición del nuevo máster han participado activamente todos los profesores de la UOC, UAB y URV implicados en él, y también el personal de gestión asociado a los estudios y al posgrado.

Para trabajar la definición del Máster se creó una **comisión de titulación** formada por:

- Rafael Macau, director de los Estudios de Informática, Multimedia y Telecomunicación de la UOC
- Helena Rifà, directora del Máster
- Jordi Herrera, coordinador del programa de doctorado en Informática de la UAB
- Francesc d´Assís Serratosa, coordinador del programa de doctorado en Informática de la URV
- Robert Clarisó, director académico del área de posgrado en Informática, Multimedia y Telecomunicación
- Josep Prieto, director de programa de la Ingeniería Técnica en Informática de Sistemas
- Jordi Serra, director académico del programa de máster de Seguridad de la UOC
- Carles Garrigues, director académico del programa de máster Universitario en Software Libre de la UOC
- Marta Borrás, administradora de los Estudios de Informática, Multimedia y Telecomunicación

El diseño de la nueva titulación interuniversitaria empezó en mayo de 2009 con una reunión de la comisión de titulación. Desde mayo de 2009, todos los profesores relacionados con el Máster han participado en el diseño de la titulación. El profesorado se ha dividido en grupos según su área de conocimiento para trabajar en cuatro puntos clave del diseño del nuevo Máster:

1. La definición de las competencias específicas del máster
2. La definición de las competencias relacionadas con el área de conocimiento
3. La definición de los contenidos
4. El diseño de las materias/asignaturas

Se han tenido en cuenta las opiniones de los estudiantes del actual máster de seguridad de la UOC, a los cuales se les han hecho consultas directas, encuestas de final de semestre, y un estudio del perfil del alumnado.

Los miembros de la comisión de titulación han recogido las propuestas del profesorado de sus universidades juntamente con las aportaciones realizadas por los agentes internos y externos, y se han reunido periódicamente para realizar la propuesta, coordinar el proceso de diseño de la titulación, y elaborar la memoria.

Procedimientos de consulta externos

Los días 27, 28 y 29 de octubre, se celebró en el Parador de San Marcos de León, el III Encuentro Nacional de la Industria de Seguridad en España (ENISE), dedicado a la Innovación en Seguridad de la Información. Asistieron al evento 520 personas y 110 empresas e instituciones relacionadas con el sector de la seguridad. En foro fue un buen lugar para reflexionar sobre las necesidades del sector. Una de las críticas de las empresas fue lo mucho que les cuesta encontrar profesionales cualificados para trabajar en proyectos de seguridad, y la necesidad que desde las universidades se trabajen los intereses reales de la sociedad y de la industria.

Se debatió la propuesta del máster con algunas de las empresas asistentes y la propuesta fue bien recibida. Las empresas destacaron la importancia de definir un máster universitario de seguridad, y valoraron positivamente las especialidades profesionalizadoras definidas.

Documento de alegaciones al Informe de Evaluación Provisional emitido por AQU

Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones por la Universitat Oberta de Catalunya

Id. título: 4312898

A continuación se exponen las alegaciones de la Universitat Oberta de Catalunya al Informe Previo de Evaluación emitido por la Agència per a la Qualitat del Sistema Universitari de Catalunya (AQU), para el Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones por la UOC (Id. título: 4312898)

La Comisión de titulación ha valorado las motivaciones recogidas en el Informe, al objeto de completar y mejorar el plan de estudios, y expone las siguientes argumentaciones para su toma en consideración.

MODIFICACIONES REQUERIDAS:

DESCRIPCIÓN DEL TÍTULO
Aportar el convenio de colaboración entre la UOC, la UAB y la URV, debidamente firmado.
El convenio de colaboración está actualmente en trámite de valoración del clausulado por las diferentes universidades y será debidamente aportado tan pronto como esté firmado. Por el momento, se aporta el compromiso por escrito de las universidades a participar en esta oferta interuniversitaria.
Corregir la errata relativa al número de créditos ECTS de matrícula máxima a tiempo parcial establecidos por la UAB.
Se ha corregido la errata, pues se había introducido en la aplicación 600 en lugar de 60.

COMPETENCIAS
Especificar en el apartado 3 de la memoria la especialidad a la que se encuentra vinculada cada competencia específica.
Se ha incluido en el apartado 3 de la memoria la especialidad a la que se encuentra vinculada cada competencia.
Revisar el perfil de competencias incorporando los aspectos especificados en el apartado de competencias del presente informe con el objetivo de mejorar su adecuación al contenido disciplinario del título. Una vez revisado el conjunto de competencias, deben introducirse las modificaciones pertinentes en el plan de estudios con el objetivo de asegurar la coherencia interna de los contenidos. A continuación se detallan los aspectos que deben incorporarse para considerar una completa adecuación del perfil de formación: - El marco normativo legal, dado que éste condiciona el uso de las tecnologías y sistemas de seguridad. - Habilidades directivas, dado que los profesionales expertos en seguridad ocupan posiciones cada vez más elevadas en el organigrama empresarial. - Estructuras normalizadoras, evaluadoras y certificadoras y las normas correspondientes que regulan los ámbitos de la seguridad (principalmente ISO/IEC pero también CEN/CENELEC/ETSI). - Capacidad para elaborar un plan de seguridad, incluyendo aspectos tales como el análisis y gestión de riesgos, políticas de seguridad, planes de recuperación y planes de formación y sensibilización.
- El marco normativo legal se trabaja en la materia de “Legislación y Regulación” que es comuna y obligatoria a todos los estudiantes del máster. Por lo tanto, todos ellos adquirirán formación con respecto al marco normativo legal, obteniendo las competencias 12 y 13 que se reflejan en la memoria del máster.

- El MISTIC proporciona una formación especializada en el ámbito de la seguridad informática, incluyendo entre sus salidas profesionales la de Oficial de Seguridad Informática de una corporación. La introducción de habilidades directivas en el perfil formativo del MISTIC permitirá a los estudiantes del máster ocupar posiciones directivas con las competencias adecuadas para ello. Es por este motivo que en el plan docente del máster, se ha añadido la materia "Dirección Estratégica de Sistemas y Tecnologías de la Información (SI/TI)", que proporcionará a los estudiantes las competencias siguientes:
    - Capacidad para la dirección de proyectos de investigación, desarrollo e innovación, en empresas y centros tecnológicos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.
    - Capacidad para la integración de tecnologías, aplicaciones, servicios y sistemas propios de la Ingeniería Informática, con carácter generalista, y en contextos más amplios y multidisciplinares.
    - Capacidad para la planificación estratégica, elaboración, dirección, coordinación, y gestión técnica y económica en los ámbitos de la ingeniería informática relacionados, entre otros, con: sistemas, aplicaciones, servicios, redes, infraestructuras o instalaciones informáticas y centros o factorías de desarrollo de software, respetando el adecuado cumplimiento de los criterios de calidad y medioambientales y en entornos de trabajo multidisciplinares.

  La materia de "Dirección Estratégica de Sistemas y Tecnologías de la Información (SI/TI)" formará parte del módulo de optativas del máster, y podrá ser cursada por cualquier estudiante de las especializaciones profesionales del máster.
- La materia de Sistemas de Gestión de la Seguridad de la Información no trata las normas CEN/CENELEC/ETSI, dado que se trata de estándares de elevada especialización técnica, concretamente en los siguientes campos:
    - CENELEC: comité europeo de electrotecnia
    - ETSI: Instituto europeo de normas de telecomunicación
    - CEN: comité europeo de normalización; engloba el resto de sectores técnicos que no están bajo la órbita de CENELEC y ETSI.

  La materia de Sistemas de Gestión de Seguridad de la Información habla de cómo implantar un sistema de gestión según el modelo PDCA (plan-do-check-act), y no entra a concretar cómo se tienen que implantar las medidas de seguridad técnicas que la ISO 27002 recoge. Es decir, la ISO 27002 hace una descripción detallada de las medidas genéricas de seguridad a implantar, pero sin a entrar a describir bajo qué estándares o con qué tecnología estas medidas se tienen que poner en práctica. Para poner un ejemplo, la norma puede hablar de la necesidad de establecer comunicaciones seguras e incluso, puede hablar de cifrado, pero en ningún caso establece cuál es el algoritmo de cifrado a implantar, el cual podría ser perfectamente el objeto de alguna de estas normas.
  Por lo tanto, este conjunto de normas técnicas específicas no son objeto de esta asignatura.
- La materia de Sistemas de Gestión de la Seguridad de la Información dedica buena parte del temario a la implantación de un SGSI, describiendo la elaboración del Plan de Seguridad en la parte final de la fase PLAN del ciclo de Deming, y explicando la implantación y puesta en práctica del Plan de Seguridad en la fase DO del ciclo de Deming. Los estudiantes que cursen la materia tendrán la capacidad para elaborar un plan de seguridad, incluyendo aspectos tales como el análisis y gestión de riesgos, políticas de seguridad, planes de recuperación y planes de formación y sensibilización, y así lo hemos reflejado en la competencia 29.

ACCESO Y ADMISIÓN DE ESTUDIANTES

Completar la tabla de asignaturas de complementos de formación indicando los créditos correspondientes a cada una de las asignaturas.

Se ha incorporado esta información en la tabla de asignaturas de los complementos de formación. Todas las asignaturas son de 6 créditos.

PLANIFICACIÓN DE LAS ENSEÑANZAS

Revisar los contenidos académicos específicos de algunos módulos/materias, incluyendo los aspectos que se detallan en el apartado de planificación de la titulación del presente informe.

1. Módulo de formación obligatoria: en la materia 'Legislación y regulación', aun cuando se cita la LOPD, se recomienda incluir los contenidos referidos al RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Esta carencia se detecta también en la materia 'Auditoria técnica'

2. Módulo de especialidad en Seguridad en servicios y aplicaciones: la materia 'Biometría', tiene un contenido en ECTS demasiado elevado, 6 ECTS, teniendo en cuenta las necesidades en la práctica profesional de los expertos en seguridad. Se recomienda disminuir la asignación de créditos.

3. Módulo de especialidad en Gestión y auditoría de la seguridad informática: en el conjunto de contenidos no se hace referencia a la elaboración de un plan de seguridad. Sin embargo, cualquier medida de seguridad debe estar enmarcada en un plan, cuya elaboración, mantenimiento y actualización es una tarea relevante para los profesionales expertos en seguridad. Se recomienda la inclusión de dichos contenidos.

4. Por otro lado, la materia 'Análisis forense' requiere de conocimientos en seguridad en sistemas operativos. Dado que éste aspecto está recogido como materia que forma parte del módulo de la especialidad en 'Seguridad en redes y sistemas', podría contemplarse la posibilidad de que parte de dicha materia fuera cursada también en el marco de la materia de 'Análisis forense'.

5. Por último y, al menos para los estudiantes que cursen esta especialidad, seria pertinente la inclusión de una materia relacionada con habilidades directivas, ya que los expertos en seguridad suelen ocupar posiciones de dirección en las empresas.

1. En la materia "Legislación y regulación", dentro del apartado de legislación relativa a la protección de datos de carácter personal, se hace un estudio detallado de la LOPDP y el nuevo reglamento de desarrollo de la LOPDP: el RD 1720/2007. Para que quede correctamente reflejado en la memoria del máster, lo hemos indicado en la descripción de la materia en la pág.65.

   Por otro lado, aunque los contenidos del real decreto no se vuelven a explican en detalle en la materia de "Auditoria técnica", sí se hace énfasis en la importancia de cumplir con la normativa de datos de carácter personal.
2. La biometría es una ciencia con orígenes muy antiguos pero es una técnica emergente para el reconocimiento de las personas y la seguridad de los sistemas. Hoy día se considera una pieza clave en muchos sistemas donde la seguridad es un factor esencial. Es importante resaltar dos aspectos importantes que relacionan la seguridad con la biometría. El primero es que la biometría se aplica para aumentar la seguridad de los sistemas y las personas. El segundo es la seguridad que se debe garantizar en los propios sistemas biométricos. Es decir, que los sistemas biométricos, instalados para aumentar la

seguridad también pueden ser objeto de ataque informático. La vulnerabilidad de los sistemas biométricos así como las herramientas informáticas para garantizar su protección son temas que se deben explicar en detalle.

Dado el enorme impacto de la biometría sobre los sistemas informáticos, y en concreto sobre los sistemas de identificación y autenticación, es necesario explicar en detalle no sólo las técnicas biométricas sino su aplicación práctica y como garantizar que no son objeto de ataques informáticos. Por este motivo, el temario es denso y la materia tiene una carga docente de 6 ECTS.

3. La elaboración e implantación de un plan de seguridad se trabaja en la materia de "Sistemas de Gestión de la Seguridad" dentro de cada una de las fases de planificación, implantación, revisión, y mejora del sistema de gestión de la seguridad de la información. Además, dentro de la asignatura del "Proyecto fin de máster", uno de los temas que se trabaja es la elaboración de un plan de seguridad.
4. Los contenidos de Análisis Forense están enfocados principalmente a estudiar la metodología de la informática forense para la preparación de informes periciales a usar ante un tribunal de justicia. Esto significa que las técnicas informáticas de los análisis forenses se trabajan sólo en algunas de las actividades de evaluación continua. Por ello, los estudiantes pueden superar esta materia habiendo cursado sólo la materia obligatoria de "Vulnerabilidades de Seguridad". Aún así, el hecho de haber superado "Seguridad en Sistemas operativos" permite al estudiante tener una visión más profunda y técnica en las prácticas y es por ello que el equipo de tutores del MISTIC se encargará de recomendar a los estudiantes que quieran realizar Análisis Forense, que cursen previamente como optativa la asignatura de Seguridad en Sistemas Operativos.
5. Como se ha comentado en el punto anterior de "Competencias", el MISTIC incorporará una nueva materia en habilidades directivas, llamada: "Dirección Estratégica de Sistemas y Tecnologías de la Información (SI/TI)"

Asegurar la adecuación de las actividades formativas de carácter práctico requeridas en las materias detalladas en el apartado de planificación de la titulación del presente informe
(Vulnerabilidades de seguridad, Seguridad en redes, Biometría y Análisis forense).

Vulnerabilidades de seguridad:

En lo que se refiere a las actividades formativas que requieren un enfoque práctico, cabe destacar que, en ciertas materias, el modelo de enseñanza a distancia brinda una oportunidad única a los estudiantes para aplicar en un entorno real los conocimientos adquiridos.

Son un ejemplo de estas materias aquellas relacionadas con las vulnerabilidades y la seguridad de las redes, puesto que no se puede olvidar que la mayoría de los ataques a sistemas informáticos se realizan a distancia utilizando como medio, las redes de comunicaciones. En la materia de Vulnerabilidades de seguridad, para realizar las actividades formativas que requieren un enfoque práctico, se dispondrá de distintos servidores en los que se implementaran varios sistemas con vulnerabilidades concretas con el fin que los estudiantes, simulando ataques remotos, puedan verificar la explotación de dichas vulnerabilidades. Se trabajará también con escáneres de vulnerabilidades, como por ejemplo Nessus, con el fin de auditar los sistemas que estén en explotación, identificar posibles amenazas y analizar las configuraciones más idóneas para la eliminación de las amenazas. El acceso a estos escáneres se realizará de forma remota.

Seguridad en redes:

En las prácticas de seguridad en redes se trabajará con diferentes herramientas que permitan escanear, monitorizar, tracear y identificar ataques en la red. Ello se hará de forma local utilizando distribuciones LiveCD de Linux. Además, de forma similar a Vulnerabilidades de

seguridad, se utilizaran servidores remotos en los que se simularan diferentes ataques.

Biometría:
Las prácticas de biometría no requieren que los alumnos usen hardware específico como podrían ser los escáneres de dedo o iris o cámaras de video. Esto es debido a que todos estos sistemas generan una imagen y para la comprensión de la técnica es suficiente trabajar directamente sobre dicha imagen. Por este motivo, las prácticas usaran base de datos públicas de huellas dactilares, iris o caras. Las imágenes de estas bases de datos tienen la ventaja que son imágenes normalizadas y clasificadas. Usualmente están compuestas por un conjunto de individuos y de cada individuo, tenemos unas ocho muestras. De este modo es más fácil comprender los conceptos de similitud entre imágenes de un mismo dedo, iris o cara. Además, se pueden calcular las tasas de falsos aceptados o falsos descartados.
Las técnicas de adquisición de las imágenes de las huellas dactilares, iris, caras,… se explican en el temario junto con la descripción de los sensores. También se detallan las marcas de sensores actuales para que el alumno esté familiarizado con ellos.

Análisis forense:
En la asignatura de análisis forense, las actividades formativas de carácter práctico se realizan utilizando una imagen de una máquina virtualizada que se distribuye a los estudiantes en DVD. Esta imagen está preparada para que los estudiantes puedan realizar sobre la misma los ejercicios de análisis forense planteados por el docente. El estudiante puede realizar estos ejercicios ejecutando la máquina virtual en su propio equipo.

Indicar las instituciones con las que se prevé establecer los convenios de movilidad de los estudiantes.

Actualmente la UOC mantiene acuerdos con otras universidades para fomentar la movilidad, como es el caso del proyecto Intercampus y el convenio Metacampus:

- Intercampus es un proyecto de un conjunto de universidades catalanas que tiene como objetivo desarrollar una experiencia de intercambio de asignaturas que se imparten a través de Internet.
- Metacampus es un convenio firmado entre la Universidad Autónoma de Barcelona y la Universitat Oberta de Catalunya, mediante el cual se ofrece la posibilidad a los estudiantes de la UOC de cursar virtualmente asignaturas de libre elección en la UAB y a la inversa.

En esta línea, la UOC quiere fomentar la promoción de nuevos acuerdos bilaterales o multilaterales con otras instituciones universitarias que deben orientarse principalmente a un mayor número de asignaturas de intercambio en la oferta de movilidad de los programas, el desarrollo de titulaciones conjuntas y la fijación de un sistema de reconocimiento de créditos para estudiantes residentes fuera del territorio que hagan formación presencial en programas del lugar de residencia.

Por otro lado, la UOC solicitó en febrero de 2007 la Carta universitaria Erasmus, que le fue concedida en julio de 2007 por la Dirección General de Educación y Cultura de la Comisión Europea. En el marco de la Carta universitaria Erasmus, la UOC quiere ampliar y consolidar un conjunto de convenios que favorezcan la movilidad de estudiantes y encajen en el modelo de enseñanza-aprendizaje de la universidad.

Así, pues, la línea que la universidad quiere seguir orienta a la potenciación de la movilidad individual de los estudiantes mediante los programas Erasmus.

Mecanismos para el aseguramiento de la movilidad

El criterio de elección de las universidades con las que se formalizan acuerdos de movilidad es académico, previo análisis de los planes de estudio y de los calendarios académicos, teniendo en cuenta los objetivos y las competencias descritos en cada programa.

Las acciones de movilidad se articulan mediante acuerdos específicos. Estos acuerdos regulan (total o parcialmente) los siguientes aspectos.

- Aspectos generales: marco de colaboración, objetivos del acuerdo, duración del acuerdo…
- Pactos académicos: asignaturas afectadas por el acuerdo de movilidad, pactos académicos, tablas de equivalencias o de reconocimiento de créditos, pactos de calendarios académicos, comisión de seguimiento del acuerdo...
- Pactos administrativos: circuitos para el posterior reconocimiento de los créditos mediante intercambio de información entre secretarías…
- Pactos económicos: acuerdos entre universidades, condiciones especiales para alumnos, condiciones de facturación, plazos de tiempo estipulados…
- Pactos legales: cláusulas para la protección de datos personales, tiempo de vigencia y condiciones de renovación, causas de rescisión y circuitos para la resolución de los conflictos.

En función de cada acuerdo pueden existir cláusulas adicionales a las descritas (propiedad de los contenidos, intercambio de profesorado…).

Una vez firmados los acuerdos, se dan a conocer a los estudiantes susceptibles de poder acogerse al programa de movilidad, especificando las condiciones de matrícula, los trámites y el posterior reconocimiento en el programa de origen. Esta puesta en conocimiento se articula por medio del tutor del programa, quien puede asesorar al alumno sobre las dudas que les surjan en lo relativo al programa de movilidad en el marco de los estudios que cursa.

PERSONAL ACADÉMICO

Indicar la ratio prevista de profesor colaborador por asignatura.

Tal y como se explica en el anexo correspondiente al apartado 7 de la solicitud, Recursos Materiales y Servicios, hay tres tipos de asignaturas principales: estándar, de especial dedicación y el Trabajo de fin de Máster (TFM):

En las asignaturas estándar, la acción docente sigue un plan de aprendizaje común, la atención se realiza principalmente por medio de los buzones personales de cada estudiante, los buzones grupales y la dinamización del colaborador docente en el aula. El ratio de

estudiantes por aula virtual en las asignaturas estándar es de un máximo de 75 estudiantes.

En las asignaturas con especial dedicación priman los elementos de individualización sobre los grupales, de manera que cada estudiante o grupos reducidos de estudiantes siguen un itinerario de aprendizaje diferenciado. La ratio de estudiantes en las asignaturas con especial dedicación es recomendable que sea inferior a las de las asignaturas estándar.

En las asignaturas de Trabajo fin de Máster (TFM) se precisa realizar un trabajo de seguimiento y tutoría individualizado y personalizado. La ratio de estudiantes por aula en las asignaturas de Trabajo fin de Máster (TFM) es recomendable que también sea inferior a las de la tipología de asignaturas antes mencionadas.

Por otro lado, nos gustaría clarificar que los 250 estudiantes por curso que constan en la solicitud se refieren a una previsión de máximo de estudiantes, y no a una oferta cerrada de plazas que necesariamente deba cubrirse. La UOC es una institución que tiene como misión facilitar la formación de las personas a lo largo de su vida. El objetivo primordial de la Universidad es conseguir que cada persona pueda satisfacer sus necesidades de aprendizaje aprovechando al máximo su esfuerzo. Siendo esta la razón de ser de la Universidad, no se oferta un número de plazas limitado para estudiantes de nuevo acceso. Todos los estudiantes que soliciten el acceso a un Master y cumplan con los requisitos de acceso a ese Master tendrán derecho a matricularse.

La oferta de plazas del Master que se detalla en la siguiente tabla se ha calculado teniendo en cuenta, por un lado, los recursos de la Universidad (docentes, económicos y técnicos) y, por otro lado, los análisis de necesidades de mercado.

La propuesta de plazas para los 2 próximos cursos se presenta en términos de mínima y máximo:

Curso académico	Mínimo	Máximo
2011-2012	20	250
2012-2013	20	250

Las cifras expresadas en el cuadro anterior reflejan, por tanto, la previsión de matrículas de nuevo acceso hasta el curso 2012-2013, y no la oferta cerrada de plazas para esta titulación.

Sin embargo, debe tenerse en cuenta que el número de plazas del programa no es fijo. La flexibilidad del modelo pedagógico y organizativo de la Universidad permite valorar el incremento de esta oferta a partir de los resultados obtenidos en los próximos cursos y ajustarla a una demanda más real, sin perjuicio de la calidad de los recursos disponibles para el desarrollo del programa.

Garantizar la presencia de personal docente experto en gestión y auditoria de la seguridad informática.

Como se detalla en el punto 6 del anexo, los profesores responsables de las asignaturas cuentan con los colaboradores docentes, los cuales prestan la atención docente individualizada a los estudiantes y se responsabilizan del proceso de evaluación. La relación

de estos colaboradores con la UOC se formaliza mediante un contrato civil de prestación de servicio o bien en el marco de convenios que la universidad coordinadora tiene firmados con otras universidades.

La necesidad de colaboradores docentes viene determinada por el número real de estudiantes matriculados. Estas necesidades se determinan en cada curso y, a partir de la definición de los perfiles académicos y profesionales previstos por los estudios, se inicia la convocatoria para la selección de docentes colaboradores dando publicidad tanto en medios públicos como en el propio sitio web de la universidad.

Las asignaturas correspondientes a la Especialidad de Gestión y auditoría de la seguridad estarán coordinadas por la UOC, la cual contratará dichos colaboradores docentes en función del número de estudiantes matriculados. En este caso, la UOC se compromete a priorizar para estas asignaturas aquellos perfiles con experiencia profesional en el ámbito de la Gestión y auditoría de la seguridad.

Clarificar si la titulación cuenta con profesorado de la Universitat de les Illes Balears.

La Universitat de les Illes Balears (UIB) participará con su profesorado en la docencia de la asignatura “Comercio electrónico”. Puesto que su colaboración es en una única asignatura, no forma parte de las universidades solicitantes del título y su colaboración vendrá regulada por una adenda al convenio interuniversitario entre la UOC, UAB y URV.

RECURSOS MATERIALES Y SERVICIOS

Aportar un modelo de convenio de prácticas en empresas.

Se aporta un ejemplo de convenio de prácticas en empresa, que se ha utilizado en el actual Máster universitario de Software libre. Los convenios del MISTIC seguirán este modelo.

PROPUESTAS DE MEJORA:

COMPETENCIAS

Se recomienda revisar el lenguaje utilizado en la redacción de las competencias.

A fin de mejorar el plan de estudios del máster, se ha revisado el lenguaje utilizado en la redacción de las competencias para que no incluyan la utilización de verbos como conocer que no implican un resultado que sea visible y que pueda ser evaluado.

PLANIFICACIÓN DE LAS ENSEÑANZAS

Se recomienda considerar la conveniencia de la modificación sugerida en el apartado de planificación de la titulación del presente informe relativa a las asignaturas del bloque de especialidad en investigación.

Las materias de “Metodologías de investigación en TIC” y “Técnicas de investigación en TIC” permiten al estudiante comprender cómo realizar un proyecto de investigación y qué herramientas y recursos son apropiados para llevar a cabo dicha investigación. En la primera se abordan los procesos y metodologías que se aplican en los proyectos de investigación de las áreas TIC, incluidos los tipos de preguntas de investigación, las estrategias de investigación, los ejemplos y modelos de investigación, y la análisis y evaluación de la actividad de investigación. En la segunda se cubren las diferentes técnicas y herramientas que se utilizan en la investigación TIC, incluyendo cómo escribir trabajos científicos, hacer publicaciones, o recibir financiación pública para proyectos de investigación y herramientas de apoyo.
El hecho que estas dos materias tengan un creditaje total de 12 ECTS responde a diferentes motivos:

- Dar una formación de alta calidad en las metodologías y técnicas de investigación que permita al estudiante iniciar sus estudios de doctorado con las competencias básicas necesarias para poder planificar y llevar a cabo una tesis doctoral en el período de 3 años.
- Unificar los conocimientos de los estudiantes que quieran seguir sus estudios de doctorado a través de un programa a distancia, en concreto, el Programa de Doctorado en Tecnologías de la Información y de las Redes que ofrecerá la UOC. Todos los másteres que dan acceso a este doctorado tienen unas materias de iniciación a la investigación básicas de 12 ECTS.

Se recomienda la elaboración de una guía y una normativa del Trabajo de Fin de Máster que defina los aspectos relativos a su diseño, ejecución, supervisión, evaluación y posterior publicidad.

El hecho de tener una guía y una normativa para el Trabajo de Fin de Máster permitirá desarrollar unos mejores proyectos y evaluarlos objetivamente. Nos comprometemos a elaborar la guía y a hacerla pública para estudiantes y supervisores.

OTROS CAMBIOS

COMPLEMENTOS DE FORMACIÓN

Se han modificado dos de los complementos de formación del máster. Estos cambios son los siguientes:
1) Asignaturas del área de matemáticas: cambio de la asignatura "Iniciación a las matemáticas para la ingeniería" por la asignatura de "Lógica".

La asignatura de iniciación a las matemáticas es una asignatura muy básica que se incluyó como complementos de formación para reforzar los conocimientos de aquellos estudiantes que no habían trabajado mucho las matemáticas durante los últimos años. De todos modos, hemos valorado que esta asignatura es incluso demasiado básica para aquellos alumnos que

quieran cursar un máster en TIC, y consideramos que los alumnos que no tengan estos conocimientos no podrán acceder al máster. Así pues, hemos decidido anular la "Iniciación a las matemáticas para la ingeniería" de los complementos de formación. Por otra parte, en los complementos incluiremos la asignatura de "Lógica" que proporciona las competencias básicas para entender las asignaturas de criptografía y grafos, necesarias para cursar el máster.

2) Asignaturas del área de programación: cambio de la asignatura "Arquitectura de computadores" por "Estructura de computadores"

Este cambio viene motivado por un error en el nombre de la asignatura.

RECONOCIMIENTO DE CRÉDITOS

En la tabla de equivalencias entre las asignaturas del máster en Seguridad de la UOC y las materias del máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones por la UOC, UAB, y URV, se han añadido unas equivalencias (ver pág. 46 de la memoria):

- Seguridad en Sistemas Operativos por Seguridad en Sistemas Operativos
- Seguridad en Bases de Datos por Seguridad en Bases de Datos
- Auditoría técnica y de certificación por Auditoría técnica
- Análisis forense y evidencia digital por Análisis forense

Estas equivalencias estaban implícitamente incluidas en la tabla dentro del reconocimiento de grupos de asignaturas por especialidades del máster. Sin embargo, detallamos explícitamente la paridad de las asignaturas para poder reconocer los créditos a aquellos estudiantes que no tengan completada una especialización del máster, pero si hayan cursado asignaturas equivalentes que puedan ser reconocidas.

ANEXOS : APARTADO 3

Nombre : P4_Memoria_MISTIC_F2.pdf

HASH SHA1 : 83fwZqqyu9CFYG/5cE+onw/DnFk=

Código CSV : 4590361786657764761233 6

4. ACCESO Y ADMISIÓN DE ESTUDIANTES

4.1. Sistemas de información previa a la matriculación y procedimientos accesibles de acogida y orientación de los estudiantes de nuevo ingreso para facilitar su incorporación a la universidad y la titulación

Perfil de ingreso recomendado

El MISTIC va dirigido a ingenieros, ingenieros técnicos, licenciados o graduados en el área de las Tecnologías de la Información y las Comunicaciones.

Se recomienda que las personas que deseen cursar el máster tengan un nivel de competencia en inglés equivalente al nivel A2 del marco común europeo de lenguas y un nivel de competencia a nivel de usuario en el uso de las tecnologías de la información y la comunicación.

Para facilitar al estudiante la comprobación del propio conocimiento de la lengua extranjera, la UOC pone a su disposición, por medio de los tutores, una prueba de nivel de conocimiento de inglés. La prueba permite al estudiante verificar si su nivel es el recomendado para iniciar sus estudios en este máster (nivel A2 o superior). Esta prueba no es excluyente ni requisito previo. En el caso de que el nivel del estudiante no sea el recomendado, este puede escoger libremente iniciar sus estudios asumiendo la responsabilidad de su falta de nivel inicial o, por medio de la recomendación del tutor, reforzar este nivel a partir de cursos complementarios que las propias universidades participantes en el máster ofrecen como formación continua al público en general.

Sistemas de información y acogida

La UOC, la UAB y la URV, a través de sus canales de comunicación habituales, ofrecerán información sobre el programa formativo del MISTIC. En el convenio interuniversitario se detallan las reglas de colaboración entre las tres universidades. Véase anexo 1- Convenio interuniversitario.

La universidad coordinadora del máster, la UOC, será la responsable del proceso de acceso y matrícula. Esta universidad cuenta para ello con un proceso de acogida para los nuevos estudiantes que contempla de forma amplia los siguientes aspectos:

- La información sobre el programa: objetivos, condiciones de acceso, itinerarios formativos, salidas profesionales...
- La información sobre el entorno virtual de aprendizaje: el Campus Virtual y la metodología de aprendizaje.
- Asesoramiento para la matrícula por medio del tutor o la tutora.
- Herramientas para la resolución de dudas y consultas, por medio de canales virtuales o de los centros de apoyo.

Periódicamente se revisan estos canales de información para garantizar que facilitan el conocimiento de los contenidos del programa, así como los perfiles personales y académicos que más se adecuan a cada titulación.

La solicitud de acceso al máster se hará a través del portal web de la UOC. A partir del momento en que el futuro estudiante haga su solicitud de acceso e incluya la información de toda la documentación que deba presentar, se iniciará el proceso de tramitación de dicha solicitud. La tramitación positiva implicará su alta en el Campus Virtual, con un perfil específico de «incorporación» que facilita el acceso a la información relevante de acogida y orientación para los estudiantes de nuevo ingreso, y además con la asignación de un tutor o tutora de inicio, que le dará apoyo y orientaciones en el momento de formalizar su primera matrícula.

El sistema de orientación capaz de dar respuesta a las necesidades específicas de los estudiantes en un entorno de formación virtual tiene como elemento fundamental al tutor o la tutora, una figura especializada en la orientación académica y profesional, y conocedora de la totalidad del programa de estudios. El tutor, dependiendo de cuál sea el perfil personal y académico del estudiante, orientará la propuesta de matrícula que el estudiante quiere realizar, valorando tanto la carga docente en créditos que este puede asumir en un semestre como los contenidos y las competencias de las distintas materias propuestas, en función de sus conocimientos previos, experiencia universitaria y expectativas formativas.

Tal como se describe más adelante y en detalle (véase el apartado 4.3), el modelo de tutoría de la UOC se dota de un plan de tutoría que permite ajustar las características de la acción tutorial a las diferentes fases de la trayectoria académica del estudiante, y también a los diferentes momentos de la actividad del semestre: matrícula, evaluación... Asimismo, se ajusta a la singularidad de cada una de las titulaciones por medio de planes de tutoría específicos para cada programa.

Los tutores son, pues, para los estudiantes un referente académico y profesional del programa.

La UOC dispone de un **operativo para la función tutorial** que desarrolla acciones de formación para los tutores sobre el mismo modelo de tutoría y también para el desarrollo de los planes de tutoría que se materializan en su actividad. Asimismo, el operativo facilita las herramientas y los recursos necesarios para el desarrollo del plan de acción tutorial mencionado.

Por otro lado, desde la dirección académica del programa de máster se lleva a cabo la coordinación de los tutores para ajustar sus acciones a la singularidad de cada programa.

La UOC dispone, además, de diversos mecanismos para conocer la opinión de los estudiantes sobre la acción de sus tutores. El principal es la encuesta institucional que se administra directamente a los estudiantes al final de cada curso.

Sumándose a la acción del tutor, y para atender cuestiones no exclusivamente docentes de la incorporación del estudiante (información relativa a aplicaciones informáticas, material impreso…), la UOC pone a disposición de los estudiantes el Servicio de Atención que aglutina el Servicio de atención de consultas y el Servicio de ayuda informática. El Servicio de atención a consultas es el responsable de resolver cualquier duda académica o administrativa.

El Servicio de ayuda informática es el responsable de asesorar a los usuarios del campus virtual en relación a las posibles dudas o incidencias que puedan surgir en la utilización del

campus virtual, los problemas de acceso a los materiales y el software facilitado por la universidad. El servicio de ayuda informática se efectúa de manera digital, pero se habilita un servicio de consulta directo de manera que el estudiante también puede tener acceso a través de vía telefónica.

El acceso al servicio de atención de consultas es único para el estudiante -siempre accede desde la misma aplicación informática disponible desde el campus- y es atendido por un mismo equipo. Este será el responsable de buscar la respuesta a la consulta hecha y de facilitarla al estudiante.

4.2. Acceso y admisión

Las vías de acceso al Máster son las previstas en la normativa aplicable.

Las solicitudes de acceso y admisión serán gestionadas por los órganos administrativos de la UOC, que garantizarán el cumplimiento de las condiciones de acceso legalmente establecidas, así como de las condiciones de admisión.

El tutor podrá recomendar la realización de formación compensatoria a la vista del expediente académico y experiencia profesional del estudiante con el objetivo de aproximarle al perfil de ingreso recomendado.

Criterios de acceso

De acuerdo con lo establecido en el Real decreto 861/2010, del 2 de julio, que modifica el apartado 1 del artículo 16 del Real decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales, para poder acceder a las enseñanzas oficiales de Máster es necesario estar en posesión de un título universitario oficial español u otro expedido por una institución de educación superior perteneciente a otro Estado integrante del Espacio Europeo de Educación Superior que faculte en el mismo para el acceso a enseñanzas de Máster.

Además, en virtud de lo dispuesto en la disposición adicional cuarta del Real decreto 1393/2007, quienes estén en posesión del título oficial de Diplomado, Arquitecto Técnico, Ingeniero Técnico, Licenciado, Arquitecto o Ingeniero podrán acceder a estas enseñanzas oficiales de Máster.

Asimismo, podrán acceder los titulados conforme a sistemas educativos ajenos al EEES, sin necesidad de la homologación de sus títulos, previa comprobación por parte de la Comisión de Coordinación de que se acredita un nivel de formación equivalente a los correspondientes títulos oficiales españoles y que facultan en el país expedidor del título para el acceso a enseñanzas de postgrado. El acceso por esta vía no implicará, en ningún caso, la homologación del título previo ni su reconocimiento a otros efectos que el de cursar las enseñanzas de Máster.

Criterios de admisión

Los criterios de admisión se establecen en función del perfil de ingreso (titulación académica y experiencia profesional previa) del estudiante. Pueden ser admitidas al Máster las personas que hayan cursado los siguientes estudios:

1. Titulados en Ingeniería Informática (Graduados, Ingenieros, Ingenieros Técnicos).
2. Titulados del área de Ingeniería y Arquitectura (Graduados, Ingenieros, Ingenieros Técnicos, Licenciados, Diplomados) en especialidades vinculadas a las tecnologías de la información y de las comunicaciones. Por ejemplo, Telecomunicaciones o Multimedia.
3. Titulados en el área de Ciencias, en las especialidades de Matemáticas, Física y Estadística (Graduados, Licenciados, Diplomados).
4. Otros titulados.

Los dos primeros grupos de titulados (Ingenieros informáticos e Ingenieros del área TIC) no necesitarán cursar ningún complemento de formación para iniciar el MISTIC, mientras que el tercer grupo (Titulados en el área de Ciencias) es probable que tenga que cursar créditos de formación compensatoria (como máximo 30 ECTS). Para los restantes titulados (cuarto grupo), siempre y cuando cumplan las condiciones de acceso legalmente previstas, su admisión al máster quedará supeditada al número de créditos de complementos de formación que debieran cursar.

La superación de estos complementos de formación, previstos para los grupos 3 y 4, será un requisito necesario para la consecución del título.

En el tercer grupo (titulados en el área de Ciencias, en las especialidades de Matemáticas, Física y Estadística), la identificación de los créditos necesarios a cursar como complementos de formación se realizará mediante una tutorización y evaluación personalizada de la formación y experiencia previa de cada estudiante, y será aprobada por la Comisión de Coordinación del máster. La composición de dicha Comisión viene detallada en el convenio de colaboración (véase anexo 1 – Convenio interuniversitario).

En el cuarto grupo (quienes estén en posesión de otros títulos), los candidatos serán evaluados por la Comisión de Coordinación del máster, la cual determinará su admisión en función de su formación previa y experiencia profesional. Para evaluar su admisión, la Comisión de Coordinación analizará las evidencias aportadas por el estudiante sobre sus competencias en el área (certificaciones en seguridad, minors académicos, etc.). En cualquier caso, la admisión de estos estudiantes estará supeditada al número de créditos de complementos de formación necesarios para alcanzar el perfil de entrada: sólo se admitirá a los estudiantes que puedan alcanzar el perfil de entrada con, como máximo, 60 ECTS de formación compensatoria.

El listado de complementos de formación se presenta en la tabla siguiente y está compuesto por asignaturas del Grado en Ingeniería Informática de la Universitat Oberta de Catalunya.

Complementos de formación (0-60 ECTS entre las siguientes asignaturas de 6 cr cada una)	
• Fundamentos de programación	• Prácticas de programación

• Diseño y programación orientada a objetos	• Lógica
• Álgebra	• Grafos y complejidad
• Fundamentos de computadores	• Redes y aplicaciones Internet
• Criptografía	• Estructura de computadores
• Sistemas operativos	• Administración de redes y sistemas operativos
• Uso de bases de datos	• Seguridad en redes de computadores
• Sistemas distribuidos	• Fundamentos de sistemas de información

En caso que se considere que el estudiante no puede alcanzar el perfil de ingreso al máster con una formación complementaria de 60 créditos, no se le admitirá en el programa.

Incorporación

Como se ha explicado anteriormente, una vez obtenido el acceso al máster, el estudiante recibirá su alta en el Campus Virtual, con un perfil específico de «incorporación» que facilita el acceso a la información relevante de acogida y orientación para los estudiantes de nuevo ingreso, y además con la asignación de un tutor o tutora de inicio, que le dará apoyo y orientaciones en el momento de formalizar su primera matrícula.

Estudiantes con discapacidad

El MISTIC utilizará el modelo educativo de la UOC. Éste se basa en la personalización y el acompañamiento permanente al estudiante, más allá de las limitaciones del tiempo y del espacio. Se trata, pues, de un modelo que consigue intrínsecamente elevadas cotas de igualdad de oportunidades en el acceso a la formación, al que se suman los esfuerzos necesarios para responder a las necesidades de los estudiantes con discapacidad.

Desde sus inicios, la UOC ha dedicado un importante esfuerzo a adaptar su tecnología para facilitar el acceso a la universidad de las personas con discapacidad. El propio sistema virtual permite la participación de personas con discapacidad auditiva o motriz de forma natural, ya que se basa en la escritura y en la conexión remota asíncrona. En este sentido, se han adaptado las interfaces del aula virtual con el fin de cumplir con la estandarización WAI AA del Consorcio W3C (www.w3c.org/WAI), que se recomienda para permitir una buena navegación por las interfaces web.

En cuanto a las acciones relacionadas directamente con el aprendizaje, se ha buscado aproximar sus contenidos docentes a todo el mundo, de manera que facilita la documentación de las asignaturas en formato PDF para permitir una lectura automática a partir de herramientas TTS (TextToSpeech). Actualmente, además, está en curso el proyecto de transformación de los contenidos de la UOC al formato DAISY (formato de libro hablado). Este formato permite a las personas con discapacidad visual trabajar con el contenido audio como si se tratara de un libro, pasar página o avanzar al siguiente capítulo con facilidad.

Igualmente dispone de un catálogo de servicios para atender las necesidades especiales en las acciones formativas desarrolladas presencialmente: encuentros presenciales y realización de exámenes. Se cuida la accesibilidad de todos los estudiantes, ofreciendo puntos de trabajo adaptados con lector de pantalla y línea braille según las necesidades.

Entre el colectivo de estudiantes con un grado de minusvalía superior al 33%, se aplicarán en los precios del máster las mismas exenciones y descuentos que se aplican en los programas del conjunto de universidades públicas catalanas.

Más concretamente, los servicios que ofrece la universidad coordinadora a los estudiantes del MISTIC con discapacidad son los siguientes:

- Acogida y seguimiento: Todos los estudiantes, desde el momento en que solicitan el acceso a la universidad, de manera previa a la matrícula, hasta su graduación, tienen a su disposición un tutor que se encargará de orientarlos y asesorarlos de manera personalizada. De esta manera los estudiantes con discapacidad pueden tener incluso antes de matricularse por primera vez información sobre el tipo de apoyo que para cada caso pueden obtener de la universidad.

- Materiales didácticos de las asignaturas: Los materiales didácticos tiene como objetivo permitir que el estudiante pueda estudiar sean cuales sean las circunstancias en las que deba hacerlo, independientemente del contexto en el que se encuentre (biblioteca, transporte público, domicilio, etc.), del dispositivo que esté utilizando (PC, móvil, etc.), o de las propias características personales del estudiante. Por este motivo se ha trabajado en diversos proyectos que han permitido avanzar en la creación de materiales en formato XML a partir del cual se generan versiones de un mismo contenido en múltiples formatos, como pueden ser materiales en papel, PDF, HTML, karaoke, libro hablado, libro electrónico. Cada uno de estos formatos está diseñado para ser utilizado en un determinado momento o situación, y se está trabajando para garantizar que este abanico de posibilidades se encuentra disponible para los materiales de todas las asignaturas. Por ejemplo, el libro hablado resulta muy interesante para responder a las necesidades de las personas con discapacidad visual, ya que el formato DAISY que utiliza les permite trabajar con el contenido en audio como si se tratará de un libro, pasando página o avanzando hasta el siguiente capítulo con facilidad. La versión HTML permite realizar búsquedas en el contenido del material y el formato PDF permite una lectura automática a partir de herramientas TTS (TextToSpeech). Se sigue investigando en como elaborar nuevos formatos que se adapten a las necesidades de los distintos estudiantes cada vez con una mayor precisión, con el objetivo de avanzar hacia una universidad cada vez más accesible e inclusiva.

- Plataforma de aprendizaje. Campus de la UOC: Desde sus inicios la UOC siempre ha dedicado un importante esfuerzo a adaptar su tecnología con el objetivo de facilitar el acceso de las personas con discapacidad a la universidad. Ya su propio sistema virtual permite la participación de personas con discapacidad auditiva o motriz de forma natural, al estar basado en la escritura y en la conexión remota asíncrona. Además, se han adaptado las distintas interfaces del campus virtual para cumplir con la estandarización WAI AA del consorcio w3c (www.w3c.org/WAI), recomendada para permitir una buena navegación por las interfaces web en el caso de personas con discapacidad visual.

- Actos presenciales: La UOC es una universidad a distancia donde toda la formación se desarrolla a través de las herramientas de comunicación y trabajo que proporciona el campus virtual. Sin embargo, semestralmente se desarrollan determinadas actividades presenciales. Algunas son voluntarias, como la asistencia al encuentro de inicio de

semestre o al acto de graduación, y otras son obligatorias, como la realización de las pruebas finales de evaluación.

- Encuentro de inicio de semestre y Acto de graduación. Los estudiantes con discapacidad pueden dirigirse al servicio de la UOC responsable de la organización de estos actos para hacerles llegar sus necesidades. A demanda del estudiante, se buscarán los medios necesarios para que su asistencia sea lo más fácil y satisfactoria posible. Toda solicitud es siempre aceptada. En la página web informativa de estos actos se haya toda la información sobre la posibilidad de realizar este tipo de peticiones, así como el enlace que facilita a los estudiantes realizar su solicitud. Los servicios que pueden solicitarse son, entre otros:
    - Rampas y accesos adaptados
    - Aparcamiento reservado
    - Acompañamiento durante el acto
    - Intérprete de lenguaje de signos

- Pruebas presenciales de evaluación: En la secretaria del campus los estudiantes encuentran información sobre el procedimiento a seguir para solicitar adaptaciones para la realización de las pruebas presenciales. Han de rellenar un formulario. El estudiante puede solicitar cualquier tipo de adaptación, que se concederá siempre que sea justificada documentalmente. Las adaptaciones más solicitadas en el caso de las pruebas presenciales de evaluación son las siguientes:
    - Rampas y accesos adaptados
    - Programa Jaws o Zoomtext
    - Enunciados en Braille
    - Realizar las pruebas con ayuda de un PC
    - Realización de pruebas orales
    - Enunciados adaptados
    - Más tiempo para realizar las pruebas

4.3. Sistemas de apoyo y orientación de los estudiantes una vez matriculados

La universidad coordinadora del máster, la UOC, cuenta con una infraestructura que permite un sistema personalizado de apoyo y orientación a los estudiantes. Los profesores, docentes colaboradores y tutores de la UOC, UAB y URV darán apoyo y orientación al estudiante al largo de todos sus estudios.

El estudiante, una vez matriculado, tiene acceso a las aulas virtuales de las asignaturas que cursa. La responsabilidad sobre las asignaturas del máster es lo que definimos con el rol de profesor responsable de asignatura (PRA). Cada PRA se responsabiliza de un grupo de asignaturas dentro de su área de conocimiento y es el responsable de garantizar la docencia que recibe el estudiante, por lo que está presente en todo el proceso de enseñanza/aprendizaje, desde la elaboración, supervisión y revisión de los materiales docentes hasta la selección, coordinación y supervisión de los colaboradores docentes, el diseño del plan docente, la planificación de todas las actividades del semestre y la evaluación de los procesos de aprendizaje de los estudiantes.

El docente colaborador, bajo la dirección y coordinación del profesor responsable de asignatura, es para el estudiante la figura que le orientará en el proceso de enseñanza-aprendizaje, y en su progreso académico. Es la guía y el referente académico del estudiante, al que estimula y evalúa durante el proceso de aprendizaje, y garantiza una formación personalizada. Su papel se centra en lo siguiente:

- Ayudar al estudiante a identificar sus necesidades de aprendizaje.
- Motivarle para mantener y reforzar su constancia y esfuerzo.
- Ofrecerle una guía y orientación del proceso que debe seguir.
- Resolver sus dudas y orientar su estudio.
- Evaluar sus actividades y reconocer el grado de consecución de los objetivos de aprendizaje y del nivel de competencias asumidas, proponiendo, cuando sea necesario, las medidas para mejorarlas.

Además del docente colaborador, el tutor ofrece apoyo a los estudiantes durante el desarrollo del programa.

En función del progreso académico del estudiante durante el desarrollo del programa, la acción tutorial se focaliza en aspectos diferentes de la actividad del estudiante. Así, en un primer momento, al inicio de su formación, el tutor se encarga de acoger e integrar al estudiante en la comunidad universitaria y de asesorarle respecto de las características académicas y docentes del programa al que quiere acceder; le acompaña en su adaptación al entorno de aprendizaje; le presenta los diferentes perfiles e itinerarios del programa de formación, y le orienta en relación con la coherencia de los contenidos que tiene que alcanzar, remarcando su sentido global, asesorándole sobre especialidades académicas y profesionales más adecuadas en función de los conocimientos y la experiencia profesional previa. El tutor desarrolla estas funciones teniendo en cuenta las especiales características de cada estudiante con respecto a su lengua, país de origen, intereses y motivaciones, y de acuerdo con su situación personal.

En un segundo momento le ayuda a adquirir autonomía y estrategias de aprendizaje mediante el modelo y la metodología de aprendizaje virtual. Durante el desarrollo de la actividad le orienta en función de la elección de contenidos hasta la consecución de los objetivos propuestos dentro del programa. También participa en la definición y la valoración de los proyectos de aplicación que realicen los estudiantes promoviendo el pensamiento crítico en torno a la profesión.

El equipo de tutores es coordinado por el director del programa, que realiza un seguimiento continuado del mismo en las diferentes acciones. El plan de tutoría se ajusta a la singularidad de cada una de las titulaciones. Los tutores elaboran una propuesta de plan de tutoría -a partir de las especificidades de cada programa- que cuenta para su desarrollo con la aprobación del Director del Programa y la validación del equipo de Desarrollo de la Función Tutorial de la universidad coordinadora. Son los tutores los que tienen la función de llevar a cabo el plan de tutoría a lo largo del semestre, a través de las aulas de tutoría del Campus Virtual.

En paralelo, el Grupo de Desarrollo de la Función Tutorial apoya a los tutores facilitándoles las herramientas y las informaciones necesarias con el fin de que puedan dar una respuesta

adecuada a las necesidades de los estudiantes, principalmente en aquellos aspectos más transversales y vinculados a los servicios y a las informaciones de la universidad coordinadora.

El Grupo de Desarrollo de la Función Tutorial recopila, de forma sistemática, la actividad del estudiante en relación con el seguimiento de la docencia y también las acciones que lleva a cabo el tutor para asesorarlo.

Al finalizar el semestre, el director del programa y el Grupo de Desarrollo de la Función Tutorial, valoran el funcionamiento y los resultados obtenidos (rendimiento y satisfacción) con el fin de poder introducir cambios, en el siguiente semestre, en el plan de tutoría del programa y de esta manera poder dar una mejor respuesta a las necesidades de los estudiantes.

El director del Programa y el Grupo de Desarrollo de la Función Tutorial celebran reuniones presenciales con los tutores con el fin de hacer seguimiento de su actividad y compartir las propuestas de acciones de mejora. Son los responsables de que se apliquen las mejoras propuestas y de hacer un seguimiento de sus resultados.

Conviene recordar que el Comité de Evaluación Externo del proceso de Evaluación institucional seguido por la universidad, bajo las directrices de AQU Catalunya, valoró muy adecuadamente el funcionamiento de la acogida definido por la universidad, teniendo en cuenta “el buen desarrollo del plan tutorial: su alto grado de formalización, su evolución, y valoración por los diferentes colectivos, motivo por el cual se valoran como muy adecuados los mecanismos de aseguramiento de calidad de la acogida”.

Como mecanismo de apoyo a los estudiantes, también podemos mencionar otros servicios de los que puede beneficiarse el estudiante de la universidad una vez matriculado. Básicamente destacamos los servicios de biblioteca y recursos de la UOC, la UAB y la URV, así como los servicios de ayuda informática, atención de consultas y servicios territoriales de la universidad coordinadora.

Los estudiantes tienen a su disposición, desde el inicio del semestre, todo el material y documentación de referencia de cada una de las asignaturas de las que se ha matriculado. Los estudiantes encuentran en los materiales y recursos didácticos los contenidos que contribuyen, juntamente con la realización de las actividades que han sido planificadas desde el inicio del semestre, a la obtención de los conocimientos, las competencias y las habilidades previstas en las asignaturas. Todos estos contenidos han sido elaborados por un equipo de profesores expertos en las diversas áreas de conocimiento y de la didáctica, y de acuerdo con los principios del modelo pedagógico de la UOC. Los materiales pueden presentarse en diferentes formatos: papel, web, vídeo, multimedia… en función de la metodología y del tipo de contenido que se plantee. Igualmente los estudiantes pueden disponer de otros recursos a través de la biblioteca virtual que ofrece los servicios de consulta, préstamo, servicio de documentos electrónicos servicio de información a medida. Además, ofrece formación a los usuarios para facilitar el uso de los servicios.

Del mismo modo, la UOC pone a disposición de los estudiantes el Servicio de Atención que aglutina el Servicio de atención de consultas y el Servicio de ayuda informática. El Servicio de atención a consultas es el responsable de resolver cualquier duda académica o administrativa. El Servicio de ayuda informática es el responsable de asesorar a los usuarios del campus

virtual en relación a las posibles dudas o incidencias que puedan surgir en la utilización del campus virtual, los problemas de acceso a los materiales y el software facilitado por la universidad. El servicio de ayuda informática se efectúa de manera digital, pero se habilita un servició de consulta directo de manera que el estudiante también puede tener acceso a través de vía telefónica.

El acceso al servicio de atención de consultas es único para el estudiante -siempre accede desde la misma aplicación informática disponible desde el campus- y es atendido por un mismo equipo. Este será el responsable de buscar la respuesta a la consulta hecha y de facilitarla al estudiante.

Por último para contribuir a mejorar la atención personalizada y presencial a los estudiantes, la UOC dispone de diecisiete centros de apoyo y también de cuarenta y siete puntos de información. Estos centros además de puntos de información son centros de servicios académicos y administrativos que facilitan la recogida de sugerencias, demandas o necesidades. Por otro lado, a parte de la universidad coordinadora, el resto de universidades participantes en el máster (UAB y URV) también ofrecerán información y a través de los puntos de información de sus campus universitarios.

4.4. Transferencia y reconocimiento de créditos: sistema propuesto por la universidad

- **Reconocimiento de créditos:**

El MISTIC entiende por reconocimiento de créditos ECTS la aceptación por parte de la universidad coordinadora de los créditos obtenidos en enseñanzas universitarias de carácter oficial, ya sea en la UOC, UAB, URV o en otra universidad, para que computen en otros estudios a los efectos de obtener una titulación universitaria de carácter oficial.

Asimismo, y de acuerdo con el artículo 6 del RD 1393/2007, de 29 octubre, según redacción otorgada por el RD 861/2010, de 2 de julio, la experiencia laboral y profesional acreditada, así como los créditos obtenidos en enseñanzas universitarias conducentes a la obtención de títulos no oficiales, también podrán ser reconocidos en forma de créditos que computarán a efectos de la obtención del MISTIC, siempre que dicha experiencia o títulos estén relacionados con las competencias inherentes al Máster.

La unidad básica del reconocimiento será el crédito ECTS (sistema europeo de transferencia de créditos), regulado en el Real decreto 1125/2003, de 5 de septiembre, por el cual se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y con validez en todo el territorio nacional.

Los créditos ECTS serán susceptibles de ser incorporados al expediente académico del estudiante y serán reflejadas en el Suplemento Europeo al Título, en virtud de lo establecido en el artículo 6 del Real decreto 1393/2007, de 29 de octubre, por el cual se establece la ordenación de las enseñanzas universitarias oficiales.

Los estudios previos y la experiencia laboral y profesional aportados serán susceptibles de reconocimiento en función del programa de Máster de destino. Por tanto, el reconocimiento de

créditos ECTS podrá ser diferente si los mismos estudios de origen se aportan a otro programa de Máster de destino.

Las asignaturas reconocidas, transferidas, convalidadas y adaptadas, en la medida que tienen la consideración de asignaturas superadas, también serán susceptibles de reconocimiento.

Los criterios en materia de reconocimiento de asignaturas de titulaciones oficiales que se han establecido, cuando los estudios de destino sean enseñanzas oficiales de Máster, son los siguientes:

1. Cuando los estudios aportados sean enseñanzas universitarias conducentes a la obtención del título oficial de Diplomado, Ingeniero Técnico, Arquitecto Técnico o de Graduado, no serán susceptibles de reconocimiento al no existir adecuación entre el nivel de competencia exigido en las enseñanzas aportadas y el previsto en el programa de Máster de destino.

2. Cuando los estudios aportados sean enseñanzas universitarias conducentes a la obtención del título de Licenciado, Ingeniero, Arquitecto, Máster Universitario o Doctorado, las asignaturas aportadas serán susceptibles de reconocimiento si, a criterio de la dirección de programa de Máster correspondiente, existe equivalencia o adecuación entre las competencias y los conocimientos asociados a las asignaturas cursadas en los estudios aportados y los previstos en el programa de Máster de destino.

Los estudiantes del máster de Seguridad Informática de la UOC (título propio) podrán obtener el reconocimiento de créditos académicos del plan de estudios del MISTIC, en función de las asignaturas o grupo de asignaturas superadas hasta el momento por el estudiante de acuerdo con la tabla de equivalencias que se detalla a continuación.

Tabla 2. Equivalencias entre el máster en Seguridad de la UOC y el MISTIC

Máster Seguridad UOC			**MISTIC**		
Asignatura	**Cr**	**Tp**	**Materia**	**Cr**	**Tp**
Explotación de vulnerabilidades	6	C	Vulnerabilidades de seguridad	6	C
Aspectos legales	6	C	Legislación y regulación	6	C
Seguridad en redes	6	P	Seguridad en redes	6	OE
Seguridad en sistemas operativos	6	P	Seguridad en sistemas operativos	6	OE
Seguridad en bases de datos	6	P	Seguridad en bases de datos	6	OE
Sistemas de gestión de la seguridad de la información	6	C	Sistemas de gestión de la seguridad	6	OE
Auditoría técnica y de certificación	6	P	Auditoría técnica	6	OE
Análisis forense y evidencia digital	6	P	Análisis forense	6	OE
Grupos de asignaturas (3 de 4)	**Cr**		**Especialidad**	**Cr**	
- Sistemas de gestión de la seguridad de la información - Planes de continuidad de negocio - Auditoria técnica y de certificación - Análisis forense y evidencia digital	18		Gestión y auditoria de la seguridad	18	
Grupos de asignaturas (3 de 5)	**Cr**		**Especialidad**	**Cr**	
- Seguridad en redes	18		Seguridad en redes y sistemas	18	

- Seguridad en aplicaciones web - Seguridad en bases de datos - Seguridad en sistemas operativos - Programación segura					

"C": asignatura común
"OE": asignatura obligatoria de especialidad
"P": asignatura optativa

Los criterios para el reconocimiento de competencias a través de la experiencia profesional y laboral son las siguientes:

1. Cuando el estudiante aporte evidencias de experiencia profesional de un mínimo de un año en puestos de administración de redes y servicios, programación de aplicaciones seguras, o en consultoría de sistemas de gestión de la seguridad de la información, se le reconocerá la materia de Prácticas profesionalizadoras, de 3 ECTS.

2. Cuando el estudiante aporte evidencias de experiencia profesional de un mínimo de dos años en los puestos anteriores y además pueda demostrar que ha alcanzado las competencias asociadas a una de las materias del MISTIC, se le reconocerá dicha materia (a excepción del Trabajo fin de máster, que no es susceptible a reconocimientos). Solamente se otorgaran créditos por el aprendizaje mostrado, no por la simple experiencia acumulada.

Para la evaluación del reconocimiento de la experiencia profesional se tendrán en cuenta todas aquellas evidencias que el estudiante pueda aportar, tanto para demostrar su actividad profesional (p.e. contratos de trabajo, certificado de vida laboral de la Tesorería General de la Seguridad Social, certificados de empresa donde conste la duración del contrato, las actividades realizadas y la duración de las mismas), como para demostrar las características y la calidad de las actividades desarrolladas (p.e. cartas de recomendación, evidencias de los resultados del trabajo –muestras, fotos, videos, ..-).

- **Transferencia de créditos:**

Las asignaturas transferidas se verán reflejadas en el expediente académico del estudiante y en el Suplemento Europeo al Título, en virtud de lo establecido en el artículo 6.3 del Real decreto 1393/2007, de 29 de octubre, por el cual se establece la ordenación de las enseñanzas universitarias oficiales.

- **Sistema de gestión del reconocimiento y transferencia de créditos**

La evaluación de estudios previos (EEP) es el trámite que permite a los estudiantes valorar su bagaje universitario anterior y obtener el reconocimiento -o en su caso la transferencia- de los créditos cursados y superados en alguna titulación anterior, en la UOC, UAB, URV, o en cualquier otra universidad.

Las solicitudes de EEP son evaluadas y resueltas por la Comisión de Evaluación de Estudios Previos. La Comisión de Evaluación de Estudios Previos (EEP) es el órgano competente para

emitir las resoluciones correspondientes a las solicitudes de evaluación de estudios previos realizadas por los estudiantes.

La Comisión de EEP está formada por un representante de cada universidad participante en el MISTIC, el director académico del mismo, y es presidida por el Vicerrector de Ordenación Académica y Profesorado de la UOC. Actúa como secretario/a de la Comisión de EEP el responsable de este trámite de la Secretaria Académica.

Las funciones específicas de la Comisión de EEP son las siguientes:

1. Evaluar la equivalencia o adecuación entre las competencias y los conocimientos asociados a las asignaturas cursadas en los estudios aportados y los previstos en el plan de estudio de la titulación de destino.
2. Emitir las resoluciones de EEP.
3. Resolver las alegaciones formuladas por los estudiantes a la resolución de la solicitud de evaluación de estudios previos emitida, valorando la correspondencia entre las asignaturas y competencias adquiridas en los estudios aportados y los previstos en el plan de estudio de destino.
4. Velar por el cumplimiento de los criterios de reconocimiento y transferencia de créditos aprobados por la universidad, y por el correcto desarrollo del proceso de EEP.

Los estudiantes pueden realizar un número ilimitado de solicitudes de EEP, incluso aportando los mismos estudios previos.

Las solicitudes de EEP son válidas si el estudiante introduce sus datos en el repositorio de estudios previos, abona la tasa asociada al trámite y envía la documentación requerida dentro de los plazos establecidos.

Para poder realizar una solicitud de EEP es necesario haber introducido previamente los datos de los estudios aportados en el repositorio de estudios previos. El repositorio es un reflejo del estudio previo aportado por el estudiante, donde se indican las asignaturas superadas, el tipo de asignatura (básica, obligatoria, optativa, troncal o de libre elección), los créditos, la calificación obtenida, el año de superación y si se trata de una asignatura semestral o anual.

Una vez introducidos los datos en el repositorio, el estudiante ya podrá realizar una solicitud de EEP en los plazos establecidos en el calendario académico de la UOC.

Realizada la solicitud de EEP, el estudiante dispone de un plazo máximo de 15 días naturales para aportar la documentación correspondiente y abonar la tasa asociada a dicho trámite. Emitida la resolución por parte de la Comisión de EEP, el estudiante recibe notificación de la misma a través de un correo electrónico a su buzón personal. Una vez notificada la resolución de EEP, si el estudiante no está de acuerdo, dispone de un plazo de 15 días naturales para alegar contra el resultado de la resolución de EEP.

ANEXOS : APARTADO 4

Nombre : TP_Memoria_MISTIC.pdf

HASH SHA1 : 9s2t94mlolPQpNtF1ayVLuDIlUU=

Código CSV : 4260834157231419435051 8

Anexo 1: Enseñanzas no oficiales a extinguir: Máster en Seguridad Informática por la UOC

A1.1. Introducción al programa

La sociedad de la información y las nuevas tecnologías de comunicación plantean la necesidad de mantener la usabilidad y confidencialidad de la información que soportan los sistemas de sus organizaciones; para ello, es especialmente importante elegir e implantar los sistemas y métodos de seguridad más idóneos, que protejan sus redes y sistemas ante eventuales amenazas, ya sean presentes o futuras.

El programa de Máster en Seguridad Informática persigue convertir al participante en un auténtico experto en seguridad, con lo que pueda hacer frente a una de las profesiones más demandadas y competitivas del mercado laboral actual. Gracias a la diversidad temática del programa, el estudiante puede especializarse en diferentes tecnologías y conocimientos.

Este máster permite obtener conocimientos que se pueden desarrollar en los ámbitos profesionales de:

- Responsable de red informática o responsable de seguridad informática.
- Profesionales, administradores y responsables de áreas de informática y comunicaciones en ámbitos empresariales, comerciales, industriales, académicos y el sector público.
- Profesores, consultores y asesores en las áreas de informática, comunicaciones, sistemas y demás áreas relacionadas con la seguridad de los sistemas y la información.

A1.2. Objetivos

Los objetivos académicos del programa son los siguientes:

- Conocer los diferentes tipos de vulnerabilidad que presentan las redes TCP/IP.
- Conocer los principales ataques que puede recibir un sistema informático, así como los posibles métodos de protección, detección y políticas de seguridad que permitan evitar el daño al sistema o minimizar su repercusión.
- Saber configurar la prevención contra los ataques más frecuentes.
- Conocer la configuración experta de los servidores de GNU/Linux.
- Conocer la configuración experta de Windows 2003 Server.
- Saber las técnicas principales de seguridad en los sistemas operativos.
- Conocer el marco normativo de la protección de datos a través de textos normativos.
- Conocer las obligaciones legales respecto a las medidas de seguridad.
- Conocer la legitimación de ficheros y datos, y la jurisdicción que comporta la protección de éstos.
- Conocer la visión completa y actual de la posibilidad de la puesta en marcha del plan de gestión de la seguridad en la empresa para mejorar el entorno de los sistemas informáticos. Abordar modelos de estudio de costes y factibilidad de sistemas informáticos de seguridad.
- Saber identificar y dimensionar amenazas de sistemas informáticos: elaborar planes de contingencia, evaluación/análisis de riesgos, implantación de políticas de seguridad.
- Conocer las ISO de seguridad (27001, 27002…).

- Saber hacer una auditoría de seguridad en un sistema informático.
- Saber elaborar un análisis forense de cualquier sistema informático; PC, móviles, routers, etc.
- Saber identificar las vulnerabilidades de las aplicaciones web, proyecto OWASP (Open Web Application Security Proyect).

A1.3. Requisitos de admisión

El Máster en Seguridad Informática se dirige a titulados universitarios con conocimientos previos sobre sistemas operativos, hardware, software y programación, que necesiten obtener unos conocimientos avanzados sobre seguridad informática.

Los conocimientos necesarios para acceder al máster son conocimientos básicos de redes (estructura paquete IP, nociones de comunicaciones entre ordenadores, etc.), conocimientos básicos de administración de Windows, de Linux a nivel de usuario avanzado y de redes, y conocimientos de protocolos de redes (SMTP, Samba, DHCP, SSH, HTTP).

Para acceder al programa, es necesario disponer de una titulación universitaria legalizada. En el caso de no tenerla, un comité de admisión valorara los conocimientos y la experiencia de solicitudes a partir de su curriculum.

A1.4. Metodología

El modelo pedagógico de la UOC se basa en el participante, que trabaja con autonomía, gestionando su tiempo y construyendo su propio itinerario de aprendizaje por medio de la interacción y el trabajo cooperativo.

Mediante el Campus Virtual, se consigue un aprendizaje profundo y flexible, sin barreras de espacio ni de tiempo, desde cualquier lugar y en cualquier momento. Este modelo permite una atención personalizada por parte de profesionales, docentes y expertos de reconocido prestigio, que acompañan a cada participante de forma individual y al grupo en su conjunto hacia la construcción del nuevo conocimiento.

Los materiales y recursos didácticos incluyen e integran contenidos, aplicaciones prácticas y herramientas directamente relacionadas con el entorno y las actividades laborales concretas. En este programa se utiliza una variada combinación de metodologías, considerando que los participantes son profesionales en activo y que el intercambio de sus propias experiencias profesionales será un aspecto muy relevante para conseguir los objetivos académicos.

Los participantes que acceden por primera vez al entorno del campus virtual realizarán una formación paralela al inicio del programa docente, basada en un breve curso introductorio para aprender a navegar por el entorno, conocer sus funcionalidades y utilización de los espacios destinados a la comunicación y la docencia.

El material se compone de diferentes módulos didácticos en formato papel. También se proporciona al estudiante software de apoyo o complementario en soporte CD para la realización de las prácticas y demás ejercicios de evaluación.

A1.5. Sistema de evaluación

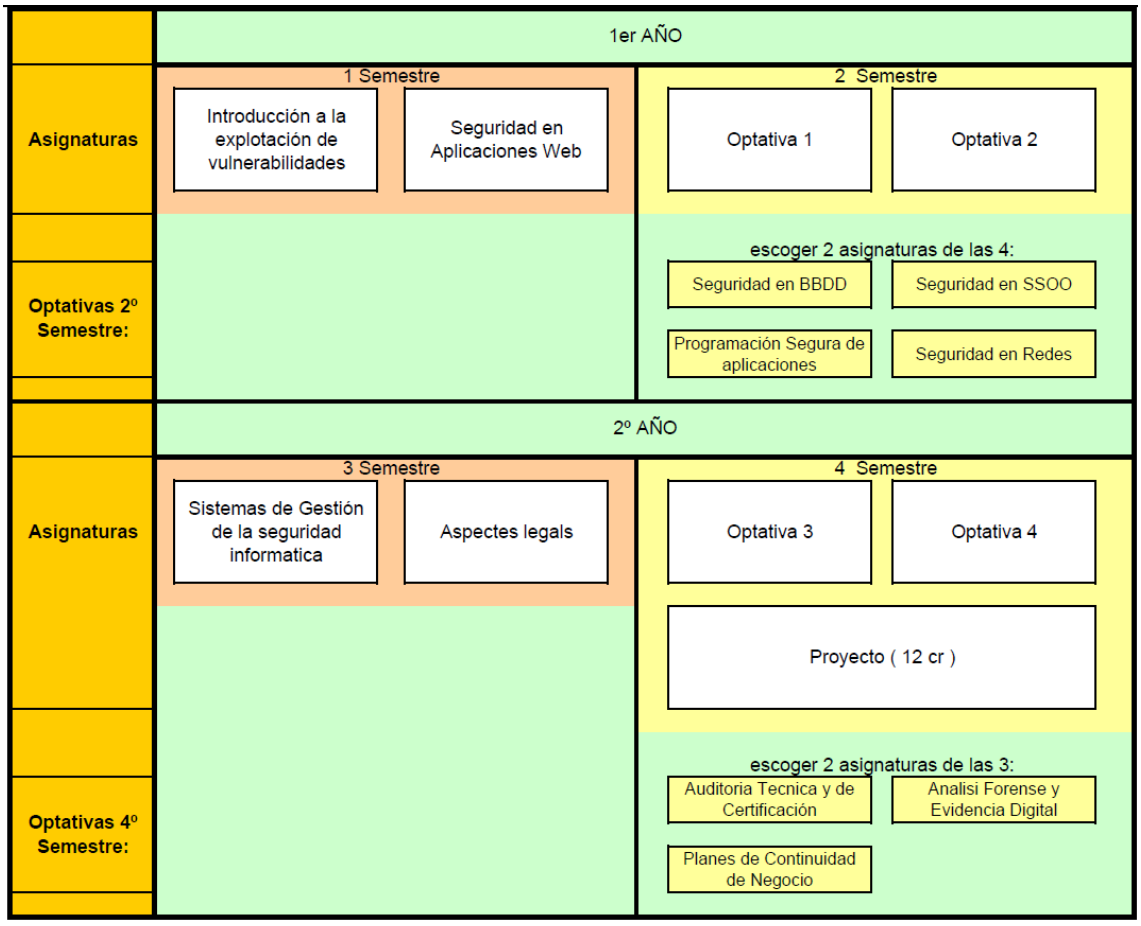
La evaluación del proceso de aprendizaje es continua y se centra mayoritariamente en trabajos que facilitan la integración del conocimiento y la adquisición de competencias para la praxis profesional de cada estudiante.

Una vez concluido el Máster, en función de las notas obtenidas en las diferentes asignaturas y de su evolución, el director del programa calificará a cada estudiante con una nota final de Máster.

A1.6. Estructura y contenidos del programa

El máster tiene una duración de 2 años (1500 horas), y una carga de 60 ECTS. Para superar el máster es necesario cursar 8 asignaturas de 6 ECTS y realizar un proyecto fin de máster de 12 ECTS.

La estructura del máster es la que se muestra en la figura siguiente:



A continuación se detalla el contenido de las asignaturas del programa.

Seguridad en redes

- Ataques contra las redes TCP/IP
  - Seguridad en redes TCP/IP
  - Actividades previas a la realización de un ataque
  - Escuchadores de red
  - Ataques de denegación deservicio
  - Deficiencias de programación
- Mecanismos de prevención
  - Sistemas cortafuegos
  - Construcción de sistemas cortafuegos
  - Zonas desmilitarizadas
  - Características adicionales de los sistemas cortafuegos

- Mecanismos de protección
  - Sistemas de auto-identificación
  - Protección del nivel de red: IPsec
  - Protección del nivel de transporte: SSL/TLS
  - Redes privadas virtuales
- Aplicaciones seguras
  - El protocolo SSH
  - Correo electrónico seguro
- Sistemas para la detección de intrusiones
  - Necesidad de mecanismos adicionales
  - Sistemas de detección de intrusos
  - Escáneres de vulnerabilidad
  - Sistemas de detección
  - Prevención de intrusiones
  - Detección de ataques distribuidos

Seguridad en sistemas operativos

- Introducción a la seguridad
  - La seguridad en la empresa
  - Modelos y políticas de seguridad
- Administración de servidores
  - Análisis de requisitos
  - Configuraciones hardwarere comendadas
  - Listas de compatibilidad de hardware
  - Consideraciones software
  - Planificación de la instalación
  - Sistemas de archivos
  - Administración de discos
  - Instalación del servidor
  - Activación de servicios y protocolos de red
  - Protocolos y sistemas de autenticación de usuarios
  - Administración y mantenimiento del servidor
  - Altas/bajas/modificaciones de usuarios
  - Cuotas de disco
  - Herramientas básicas
- La seguridad pasiva
  - Política de backups
  - Planes de contingencia
  - Sistemas de recuperación
- La seguridad activa
  - Certificados y sistemas de claves públicas y privadas
  - IPSEC
  - Redes privadas virtuales
  - Monitorización de la red
  - Herramientas de comprobación
- Configuración de servicios
  - Servidores de ficheros e impresoras
  - Configuración
  - Análisis de riesgos
  - Prevención
  - Servidor de correo
  - Configuración
  - Análisis de riesgos
  - Prevención
  - Servidores web y Ftp
  - Configuración
  - Análisis de riesgos
  - Prevención

- Mantenimiento
  - Actualizaciones
  - Monitorización de evento
  - Automatización de tareas

Aspectos legales
- LOPD
  - Generalidades
  - Principios fundamentales
  - Las bases de la protección de datos
  - Ficheros de titularidad pública y privada
  - Derechos de los interesados
  - Infracciones y sanciones
  - APD Agencia de Protección de Datos
  - Reglamento de medidas de seguridad (¿Qué hay que hacer?)
- LSSI
  - Principios y definiciones
  - Obligaciones impuestas
  - Resolución de conflictos
  - Infracciones y sanciones

Sistemas de gestión de la seguridad de la información
- Gestión de la seguridad informática
  - Seguridad de la información
  - Principios de seguridad
  - Normativas de seguridad
  - Grado de implantación de estas normativas
- Análisis de riesgos
  - Ciclo de vida de la seguridad
  - Análisis de riesgos
  - Metodologías: MARGERIT,NIST, CRAMM, OCTAVE
- Sistemas de gestión de la seguridad de la informática
  - Normativas de seguridadde la información
  - Sistemas de gestión de laseguridad de la información
  - Medidas de seguridad: ISO
  - Implantación de un SGSI

Planes de continuidad de negocio
- Planes de continuidad
  - La gestión de la continuidad de negocio
  - El BIA, el análisis de riesgos y las estrategias
  - Desarrollo de un plan de continuidad
  - La gestión operativa del plan de continuidad

Auditoría técnica y de certificación
- Introducción
- Tipos de auditorías
- Auditorías de certificación (SGSI)
  - Introducción
  - Objetivos
  - Fases: documental/presencial/documentación
  - Certificación

- Auditoría técnica de sistemas de información
  - Objetivos de las auditorías técnicas de seguridad
  - Metodologías de auditoría
  - Ejecución de auditorías de seguridad
  - Herramientas

Análisis forense y evidencia digital
- Introducción
- Recuperación de información
- Análisis forense
- Metodología
    - Adquisición de datos
    - Análisis e investigación de datos
    - Documentación del proceso
- Situación legal
- Ejemplos de aplicación
- Herramientas

Programación segura
- Programación segura de aplicaciones web
    - Seguridad en el navegador
    - Cómo programar aplicaciones inmunes a SQL injection
    - Cómo programar aplicaciones inmunes a Cross Site Scripting
    - Prevención de vulnerabilidades LFI y RFI
    - Almacenamiento seguro de recursos en servidor
    - Autenticación y autorización en aplicaciones multiusuario
- Programación segura de aplicaciones locales
    - Prevención de desbordamientos de Stack y Heap
    - Prevención de vulnerabilidades de tipo format strings
    - Prevención de vulnerabilidades off-by-one
    - Prevención de condiciones de carrera
    - Programación con mínimos privilegios
- Programación segura de aplicaciones en red
    - Criptografía en las comunicaciones
    - Almacenamiento de logs remoto
    - Programación inmune a denegaciones de servicio
- Otros aspectos de la programación
    - Manejo seguro decodificación de caracteres internacionales
    - Problemas de programación específicos de algunos lenguajes
    - Criptografía general

Seguridad en Bases de Datos
- Introducción
    - Importancia de las bases de datos
    - Evolución del mercado
    - Evolución de los ataques
    - Perspectivas
- Principales arquitecturas
    - Introducción
    - Oracle
    - Microsoft SQL
    - MySQL
    - DB2
    - Otros sistemas de bases de datos
- Vulnerabilidades
    - Introducción
    - Inyección SQL
    - Inyección SQL ciega
    - Inyección de código
    - Denegación de servicio
    - Desbordamiento debuffer/ejecución de código
    - Backdoors y rootkits
    - Otros ataques

  - Historial de lasprincipales vulnerabilidades
- Fortificación
  - Introducción
  - Servicios
  - Permisos, usuarios ycontraseñas
  - Tablas Principales
  - Procedimientosalmacenados
  - Criptografía
  - Prevención de desastres
  - Otros aspectos
  - Análisis forense
  - Uso de herramientas parala securización
- Intrusión
  - Introducción
  - Detección eidentificación de objetivos
  - Inyección SQL
  - Denegación de servicio ydesbordamiento de buffer
  - Ataques de fuerza sucia
  - Ataques internos
- Desarrollo seguro
  · Introducción
  · Arquitecturas seguras
  · Técnicas básicas dedesarrollo seguro
  · Busca de problemas alcódigo fuente
  · Otras consideraciones

Seguridad en aplicaciones web
- Arquitectura de aplicaciones web
  - Arquitectura en capas
  - La capa de presentación
  - La capa de negocios
  - La capa de datos
  - Estándares
- Ataques a aplicaciones web
  - Ataques de inyección descripts
  - Cross-Site Scripting
  - Hijacking
  - Cross-Site RequestForgery
  - Clickjacking
  - Ataques de inyección decódigo
  - SQL Injection
  - Manipulación de recordset
  - Serialized SQL Injection
  - Basado en errores ODBC
  - Blind SQL Injection
  - Time-based BlindSQL Injection
  - Arithmetic BlindSQL Injection
  - RFD (Remote FileDownloading)
  - LDAP Injection
  - AND LDAP Injection
  - OR LDAP Injection
  - Blind LDAP Injection
  - Xpath Injection
  - Xpath, Xquery
  - Blind Xpath Injection
  - Ataques de PathTransversal
  - Descarga de ficheros
  - Ataques de inyección deficheros

  - Local File Inclusion
  - Remote File Inclusion
  - WebShells AndWebtrojans
  - Otros ataques aaplicaciones web
  - Decompiladores Flash,Java y .NET
  - Ruptura de sesión
  - Fuzzing deaplicaciones web
- Auditoría y desarrollo seguro
  - OWASP (Open Web Application Security Project)
  - Code Analysis Tools
  - Scanners de vulnerabilidad de caja negra
  - Acunetix
  - W3af
  - WAF (Web Applicaton Firewalls)
  - Mod Security

Introducción a la explotación de vulnerabilidades

- Gestión de memoria
  - Segmentos
  - Utilización de la pila
- Ejecución de procesos
  - Espacio de usuario/sistema
  - Llamadas a funciones
- Conceptos básicos de lenguaje máquina
- Herramientas
  - Debuggers
  - Syser (Reemplazo Soft ICE- Windows)
  - OllyDbg (Windows)
  - RR0D (Debugger multiplataforma)
  - Fenris (Linux)
  - Compiladoras/Lenguajes
  - C
  - Ensamblador
- Exploits
  - Locales/Remotos
  - Alteraciones básicas
  - Integer overflow
  - Static data overflow
  - Heap overflow
  - Buffer overflow
  - Shellcodes
  - Escalada de privilegios
  - Detección y/o protección de ataques
  - Dependencias con sistemas operativos

ANEXOS : APARTADO 5

Nombre : P5_Memoria_MISTIC_F2.pdf

HASH SHA1 : eN+s3hNQWZXAr6Rmw/yCDbZY26E=

Código CSV : 45903627205942001400351

5. PLANIFICACIÓN DE LAS ENSEÑANZAS

5.1. Estructura de las enseñanzas

El MISTIC tiene 60 ECTS.

El máster está formado por 4 especialidades, 3 de las cuales son de orientación profesional y 1 es de orientación investigadora. El alumno está obligado a seguir una de estas cuatro especialidades.

5.1.1. Distribución del plan de estudios en créditos ECTS, por tipo de materia

El plan de estudios del MISTIC contiene 18 ECTS de materias comunes y obligatorias para todos los alumnos del máster, 18 ECTS de materias obligatorias de especialidad, 12 ECTS de materias optativas, y 12 ECTS de trabajo fin de máster y prácticas. La Tabla 2 ilustra el contenido del plan de estudios.

Tabla 2: Resumen de las materias y la distribución en créditos ECTS

	Orientación profesional	Orientación investigadora
Tipo de materia	**Créditos**	**Créditos**
Obligatorias Comunes	18	
Obligatorias de Especialidad	18	
Optativas	12	
Prácticas profesionalizadoras	3	0
Trabajo fin de máster	9	12
Total	60	

Especialidades profesionalizadoras

Especialidad 1: Seguridad en redes y sistemas
Especialidad 2: Seguridad en servicios y aplicaciones
Especialidad 3: Gestión y auditoría de la seguridad informática

Especialidad de investigación

Especialidad 4: Investigación

La Figura 4 muestra un esquema del formato del programa.

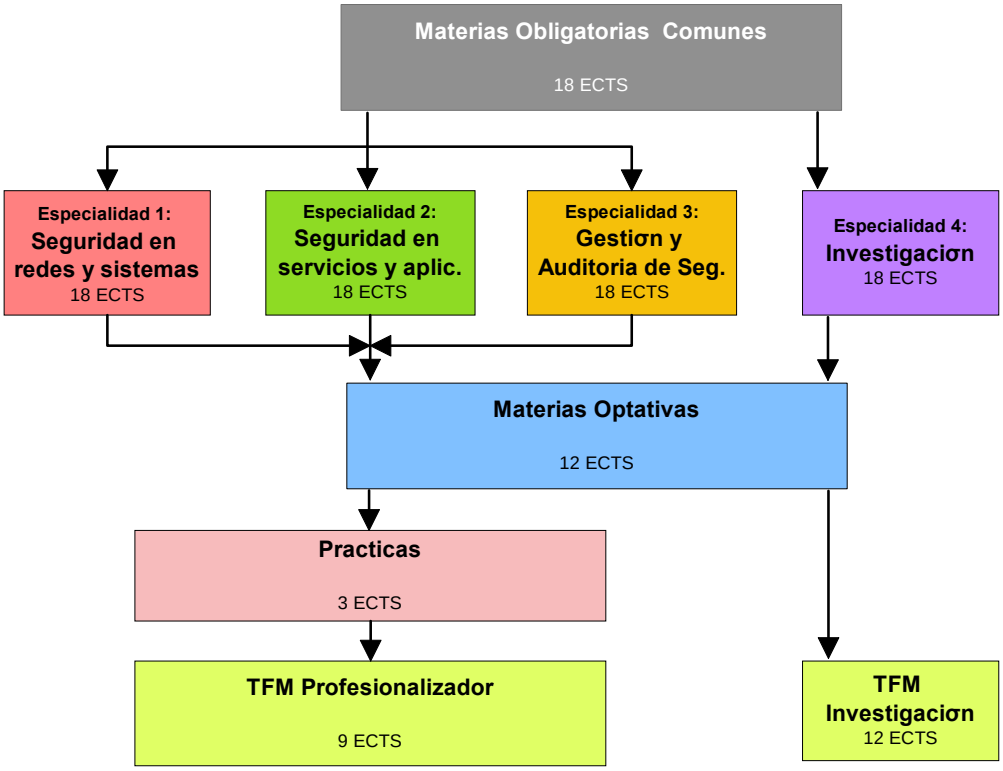


Figura 4: Esquema del programa del MISTIC

Los contenidos del máster se agrupan en módulos según las competencias específicas que trabajan. En concreto, se han definido ocho módulos: uno de materias comunes a todos los estudiantes del máster; cuatro módulos de materias de especialización correspondientes a los perfiles de las especialidades; uno de materias exclusivamente optativas (no forman parte de la parte obligatoria de ninguna especialización); un módulo de prácticas; y finalmente un módulo asociado al trabajo fin de máster.

La oferta de materias optativas que los estudiantes pueden cursar está formada por las materias del módulo de optativas juntamente con las materias de los módulos de las otras especialidades distintas a la que él haya escogido como itinerario de especialización.
La siguiente tabla muestra los módulos del máster y las materias asociadas a cada uno de ellos.

Estructura de la Enseñanza del Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (60 ECTS)
Módulo de formación Obligatoria: *Comunes (18 ECTS)*
• Legislación y regulación (6 ECTS) • Vulnerabilidades de seguridad (6 ECTS) • Identidad digital (6 ECTS)
Módulo de Especialidad 1: *Seguridad en Redes y Sistemas (18 ECTS)*
• Seguridad en redes (6 ECTS) • Seguridad en sistemas operativos (6 ECTS) • Seguridad en bases de datos (6 ECTS)
Módulo de Especialidad 2: *Seguridad en Servicios y Aplicaciones (18 ECTS)*
• Comercio electrónico (6 ECTS) • Programación de código seguro (6 ECTS) • Biometría (6 ECTS)
Módulo de Especialidad 3: *Gestión y Auditoría de la Seguridad Informática (18 ECTS)*
• Sistemas de gestión de la seguridad (6 ECTS) • Auditoría técnica (6 ECTS) • Análisis forense (6 ECTS)
Módulo de Especialidad 4: *Investigación (18 ECTS)*
• Criptografía avanzada (6 ECTS) • Metodologías de investigación (6 ECTS) • Técnicas de investigación (6 ECTS)
Módulo de Optativas: *Optativas (12 ECTS)*

- Técnicas de marcado de la información (6 ECTS)
- Dirección Estratégica de Sistemas y Tecnologías de la Información (SI/TI) (6 ECTS)

Nota: *El estudiante debe cursar 12 ECTS de materias optativas. La oferta de materias optativas para cada estudiante, además de las materias propias de este módulo, incluye las materias de todos los módulos de especialidad que no formen parte de la propia especialidad del estudiante.*

Prácticas

Prácticas profesionalizadoras (3 ECTS)

Para especialidades profesionalizadoras:

- Prácticas profesionalizadoras (3 ECTS)

Módulo Trabajo Fin de Máster

TFM (21 ECTS)

Para especialidades profesionalizadoras:

- Trabajo Fin de Máster (aplicación profesional, 9 ECTS)

Para la especialidad de investigación:

- Trabajo Fin de Máster (investigación básica o aplicada, 12 ECTS)

Mapa de competencias

A continuación, en la Tabla 3 se detalla la distribución de las competencias entre los módulos que componen el Máster. La tabla muestra las materias donde se trabajan más profundamente y evalúan las 45 competencias presentadas en el punto 3.1 de esta memoria. Aunque algunas de estas competencias se trabajan en menor grado en otras materias, en el mapa se pretende mostrar aquellas materias cruciales para el desarrollo de dichas competencias.

	C. transversales							C. específicas																																								
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
Módulo Comunes	X	X	X	X		X	X	X	X	X		X	X	X	X						X																											
Vulnerabilidades de Seguridad	X	X	X	X		X	X	X	X	X											X																											
Legislación y regulación		X					X					X	X																																			
Identidad digital	X	X		X	X	X	X							X	X																																	
Módulo Seguridad en Redes y Sistemas	X	X	X	X	X	X	X	X								X	X	X	X	X	X																											
Seguridad en redes	X		X	X	X	X	X	X								X	X				X																											
Seguridad en sistemas operativos	X	X		X	X	X	X											X		X	X																											
Seguridad en bases de datos	X	X				X													X		X																											
Módulo Seguridad en Servicios y Apl.	X	X	X	X	X	X	X															X	X	X	X	X	X																					
Comercio electrónico	X	X	X	X	X	X	X																	X	X																							
Programación de código seguro	X				X																	X	X																									
Biometría		X		X		X	X																			X	X																					
Módulo Gestión y Auditoría de la Seg.	X	X	X	X	X	X	X																					X	X	X	X	X	X	X	X													
Sistemas de gestión de la seguridad	X	X	X	X		X	X																					X	X	X	X																	
Auditoría técnica	X	X	X	X	X	X																										X	X		X													
Análisi forense	X	X	X		X	X																												X	X													
Módulo Investigación en Seguridad TIC	X	X	X	X	X	X	X																													X	X	X	X	X	X	X	X					
Metodologías de Investigación				X	X		X																															X	X		X	X						
Técnicas de investigación		X	X		X		X																													X	X	X										
Criptografía avanzada	X	X		X	X	X	X																																	X	X	X	X					
Módulo Optativas	X	X		X	X	X	X																																					X	X	X	X	X
Técnicas de marcado de la información	X	X		X	X	X	X																																					X	X			
Dirección Estratégica SI/TI		X	X	X			X																																							X	X	X
Módulo Prácticas	X	X		X	X	X																																										
Prácticas profesionalizadoras	X	X		X	X	X																																										
Módulo PFC	X	X	X	X	X	X	X				X																												X									
TFM Profesionalizador	X	X	X	X	X	X	X				X																																					
TFM Investigación	X	X	X	X	X	X	X				X																												X									

Tabla 3: Mapa de competencias

5.1.2. Explicación general de la planificación del plan de estudios

El estudiante puede realizar el plan de estudios en un año (dos semestres), en el caso de cursarlo a tiempo completo, o bien dos años, si se dedica al estudio a tiempo parcial.

A la vista de la trayectoria del estudiante y de la orientación profesional que éste quiera dar a sus estudios, el tutor le orientará -atendiendo a su perfil personal y profesional- hacia la matrícula de determinadas asignaturas optativas que le permitan consolidar un nivel superior de aquellas competencias que se adecuen a sus necesidades y expectativas.

a) Planificación en un año lectivo

Si el MISTIC se cursa en un año lectivo de dos semestres, la distribución recomendada de las materias es la siguiente:

- **Primer semestre**: **30** créditos ECTS: 18 créditos de materias comunes y 12 créditos de materias obligatorias de especialidad.

- **Segundo semestre**: **30** créditos ECTS: 6 créditos de materias obligatorias de especialidad, 12 créditos de asignaturas optativas, 3 créditos de prácticas profesionalizadoras (sólo en el caso de cursar una especialidad profesionalizadora) y 9-12 créditos del Trabajo Fin de Máster según se curse una especialidad profesionalizadora o de investigación.

Especialidad Seguridad en redes y sistemas

Sem 1	Vulnerabilidades de seguridad (6)	Legislación y regulación (6)	Identidad digital (6)	Seguridad en SO (6)	Seguridad en BBDD (6)
Sem 2	Seguridad en redes (6)	Optativas (6)	Optativas (6)	TFM+Prácticas (12)	

Especialidad Seguridad en servicios y aplicaciones

Sem 1	Vulnerabilidades de seguridad (6)	Legislación y regulación (6)	Identidad digital (6)	Comercio electrónico (6)	Programación código seg. (6)
Sem 2	Biometria (6)	Optativas (6)	Optativas (6)	TFM+Prácticas (12)	

Especialidad Gestión y auditoría de la Seguridad Informática

Sem 1	Vulnerabilidades de seguridad (6)	Legislación y regulación (6)	Identidad digital (6)	Sistemas de gestión (6)	Auditoría técnica (6)
Sem 2	Análisis forense (6)	Optativas (6)	Optativas (6)	TFM+Prácticas (12)	

Especialidad Investigación

Sem 1	Vulnerabilidades de seguridad (6)	Legislación y regulación (6)	Identidad digital(6)	Técnicas investigación(6)	Metodologías investigación(6)

Sem 2	Criptografía avanzada (6)	Optativas (6)	Optativas (6)	TFM (12)

b) Planificación en dos años lectivos

Si el MISTIC se cursa en dos años lectivos la distribución propuesta de las asignaturas es la siguiente:

- **Primer semestre**: **18** créditos ECTS de materias comunes.
- **Segundo semestre**: **12** créditos ECTS: 6 de materias obligatorias de especialidad, y 6 de optativas.
- **Tercer semestre**: **12-15** créditos ECTS.

  Si se cursa una especialidad con orientación profesional, la distribución de créditos es: 12 créditos de asignaturas obligatorias de especialidad, y 3 créditos de prácticas.

  Si se cursa una especialidad con orientación investigadora, se realizaran 12 créditos de asignaturas obligatorias de especialidad.
- **Cuarto semestre**: **15-18** créditos ECTS:

  Si se cursa una especialidad con orientación profesional, la distribución de créditos es: 6 créditos de asignaturas optativas y 9 créditos del Trabajo Fin de Máster de tipo profesionalizador.

  Si se cursa una especialidad con orientación investigadora, se realizaran 6 créditos de asignaturas optativas y 12 créditos del Trabajo Fin de Máster de tipo investigación.

Especialidad Seguridad en redes y sistemas

Sem 1	Vulnerabilidades de seguridad (6)	Legislación y regulación (6)	Identidad digital (6)
Sem 2	Seguridad en redes (6)	Optativas(6)	
Sem 3	Seguridad en SO (6)	Seguridad en BBDD (6)	Prácticas (3)
Sem 4	Optativas (6)	TFM (9)	

Especialidad Seguridad en servicios y aplicaciones

Sem 1	Vulnerabilidades de seguridad (6)	Legislación y regulación (6)	Identidad digital (6)

Sem 2	Biometría (6)	Optativas (6)	
Sem 3	Programación código seguro (6)	Comercio electrónico (6)	Prácticas (3)
Sem 4	Optativas (6)	TFM (9)	

Especialidad Gestión y auditoría de la Seguridad Informática

Sem 1	Vulnerabilidades de seguridad (6)	Legislación y regulación (6)	Identidad digital (6)
Sem 2	Análisis Forense (6)	Optativas (6)	
Sem 3	Sistemas de Gestión (6)	Auditoría Técnica (6)	Prácticas (3)
Sem 4	Optativas (6)	TFM (9)	

Especialidad Investigación

Sem 1	Vulnerabilidades de seguridad (6)	Legislación y regulación (6)	Identidad digital (6)
Sem 2	Criptografía avanzada (6)	Optativas (6)	
Sem 3	Metodologías investigación (6)	Técnicas investigación (6)	
Sem 4	Optativas (6)	TFM (12)	

Cabe destacar que el estudiante no debe ceñirse obligatoriamente a esta planificación, sino que puede adaptar su ritmo de estudio a sus necesidades y circunstancias personales y profesionales.

Esto se garantiza mediante el proceso establecido para la matriculación semestral de créditos en la titulación. El proceso se inicia con una propuesta de matrícula por parte del estudiante que debe ser valorada y aprobada por su tutor antes de que sea administrativamente formalizada. Es en este momento del proceso, durante la validación tutorial, en el que se realizan las orientaciones oportunas con la finalidad de asegurar la eficacia de la adquisición de todas las competencias de la titulación por parte del estudiante.

Mecanismos de coordinación docente

La responsabilidad última sobre la calidad que recibe el estudiante en cada asignatura corresponde al profesor responsable de asignatura (PRA). El profesor responsable de asignatura es quien vela por la calidad y la actualización del contenido y de los recursos de la asignatura, con especial atención a su diseño e innovando para garantizar el desarrollo adecuado de la actividad docente y su adecuación a los estándares de calidad definidos por las universidades participantes. Se encarga del diseño del plan docente o plan de aprendizaje,

planifica la actividad que debe desarrollarse a lo largo del semestre y revisa y evalúa la ejecución.

Para garantizar la coordinación docente dentro del programa, el director de programa y los profesores responsables de las asignaturas del máster se reúnen periódicamente con el objetivo de analizar los elementos de transversalidad que pueden presentar las asignaturas encadenadas y las asignaturas complementarias. Estas asignaturas comparten, en la mayoría de los casos, las competencias que trabajan, por lo que actividades y sistemas de evaluación pueden ser comunes y compartidos.

Asimismo, el profesor responsable de asignatura es el responsable de coordinar a los distintos consultores que interactúan en una misma asignatura, siendo su competencia evaluar de manera conjunta el funcionamiento, los resultados y el grado de alcance de los objetivos de la asignatura.

Finalmente, para poder garantizar la efectiva coordinación entre todos los actores implicados en el proceso de aprendizaje de los estudiantes, estos se reúnen periódicamente con objeto de tratar los temas y las problemáticas de interés común, establecer criterios y evaluar el desarrollo del programa.

Paralelamente, al inicio y al final de cada semestre, se llevan a cabo reuniones de cada profesor responsable de asignatura con el equipo de consultores que coordina, y del director académico del programa con el equipo de tutores, donde se comparten los resultados de las evaluaciones, encuestas e indicadores de calidad, y se toman las decisiones pertinentes para cada una de las materias.

Además, una vez al año (como mínimo) se realiza un encuentro de todos los consultores y tutores con el profesorado, el director académico de programa y el director de estudios, con el objetivo de tratar los temas de profundización necesarios para el buen funcionamiento del máster.

5.2. Planificación y gestión de la movilidad de estudiantes propios y de acogida

La movilidad de los estudiantes y titulados es uno de los elementos centrales del proceso de Bolonia. El Comunicado de Londres de mayo de 2007 dejó constancia del compromiso en el ámbito nacional de avanzar en dos direcciones: por un lado, los procedimientos y las herramientas de reconocimiento, y, por otro, estudiar mecanismos para incentivar la movilidad. Estos mecanismos hacían referencia a la creación de planes de estudios flexibles, así como a la voluntad de alentar el incremento de programas conjuntos.

Movilidad en la UOC

La movilidad que se efectuará en el MISTIC se centrará en el intercambio de estudiantes con otras universidades mediante acuerdos articulados en convenios interuniversitarios, contemplando el posterior reconocimiento de créditos en la titulación de origen del estudiante.

Los acuerdos de movilidad podrán efectuarse en ambos sentidos; siendo el MISTIC tanto emisor o receptor de estudiantes. Los acuerdos de movilidad podrán afectar tanto a la docencia virtual como a la presencial:

- En los casos en los que el máster actúe como emisor de estudiantes, los acuerdos podrán afectar tanto a asignaturas presenciales como a asignaturas virtuales de la universidad receptora.

- En los casos en los que el máster actúe como receptor de estudiantes, la movilidad será virtual, aunque podría considerarse algún caso excepcional que afectase a actividades presenciales organizadas desde las universidades participantes en el máster (UOC, UAB y URV).

Asimismo, el propio modelo no presencial de la Universitat Oberta de Catalunya que se aplica en esta titulación permite dotar de movilidad al programa en su conjunto. En este sentido, el modelo de la UOC basado en el uso de las nuevas tecnologías, y por medio de un campus virtual accesible desde internet, permite ofrecer formación a estudiantes que residen en cualquier lugar donde sea posible la conexión a la red.

Actualmente la UOC mantiene acuerdos con otras universidades para fomentar la movilidad, como es el caso del proyecto Intercampus y el convenio Metacampus:

- Intercampus es un proyecto de un conjunto de universidades catalanas que tiene como objetivo desarrollar una experiencia de intercambio de asignaturas que se imparten a través de Internet.
- Metacampus es un convenio firmado entre la Universidad Autónoma de Barcelona y la Universitat Oberta de Catalunya, mediante el cual se ofrece la posibilidad a los estudiantes de la UOC de cursar virtualmente asignaturas de libre elección en la UAB y a la inversa.

En esta línea, la UOC quiere fomentar la promoción de nuevos acuerdos bilaterales o multilaterales con otras instituciones universitarias que deben orientarse principalmente a un mayor número de asignaturas de intercambio en la oferta de movilidad de los programas, el desarrollo de titulaciones conjuntas y la fijación de un sistema de reconocimiento de créditos para estudiantes residentes fuera del territorio que hagan formación presencial en programas del lugar de residencia.

Por otro lado, la UOC solicitó en febrero de 2007 la Carta universitaria Erasmus, que le fue concedida en julio de 2007 por la Dirección General de Educación y Cultura de la Comisión Europea. En el marco de la Carta universitaria Erasmus, la UOC quiere ampliar y consolidar un conjunto de convenios que favorezcan la movilidad de estudiantes y encajen en el modelo de enseñanza-aprendizaje de la universidad.

Así, pues, la línea que la universidad quiere seguir orienta a la potenciación de la movilidad individual de los estudiantes mediante los programas Erasmus.

Mecanismos para el aseguramiento de la movilidad

El criterio de elección de las universidades con las que se formalizan acuerdos de movilidad es académico, previo análisis de los planes de estudio y de los calendarios académicos, teniendo en cuenta los objetivos y las competencias descritos en cada programa.

Las acciones de movilidad se articulan mediante acuerdos específicos. Estos acuerdos regulan (total o parcialmente) los siguientes aspectos.

- Aspectos generales: marco de colaboración, objetivos del acuerdo, duración del acuerdo…
- Pactos académicos: asignaturas afectadas por el acuerdo de movilidad, pactos académicos, tablas de equivalencias o de reconocimiento de créditos, pactos de calendarios académicos, comisión de seguimiento del acuerdo...
- Pactos administrativos: circuitos para el posterior reconocimiento de los créditos mediante intercambio de información entre secretarías…
- Pactos económicos: acuerdos entre universidades, condiciones especiales para alumnos, condiciones de facturación, plazos de tiempo estipulados…
- Pactos legales: cláusulas para la protección de datos personales, tiempo de vigencia y condiciones de renovación, causas de rescisión y circuitos para la resolución de los conflictos.

En función de cada acuerdo pueden existir cláusulas adicionales a las descritas (propiedad de los contenidos, intercambio de profesorado…).

Una vez firmados los acuerdos, se dan a conocer a los estudiantes susceptibles de poder acogerse al programa de movilidad, especificando las condiciones de matrícula, los trámites y el posterior reconocimiento en el programa de origen. Esta puesta en conocimiento se articula por medio del tutor del programa, quien puede asesorar al alumno sobre las dudas que les surjan en lo relativo al programa de movilidad en el marco de los estudios que cursa.

5.3. Descripción detallada de los módulos o las materias de enseñanza-aprendizaje de que consta el plan de estudios

Descripción del sistema de evaluación y sistema de calificaciones

La **metodología de enseñanza-aprendizaje** utilizada en el presente máster se basa en un modelo educativo caracterizado por la asincronía en espacio y tiempo canalizada a través de un campus virtual.

Por tanto, la metodología de enseñanza-aprendizaje que se utilizará en el máster sitúa al estudiante como impulsor de su propio proceso de aprendizaje. Esta metodología se caracteriza por proporcionar al estudiante unos recursos adaptados a sus necesidades. Estos recursos deben garantizar que el estudiante pueda alcanzar los objetivos docentes y trabajar las competencias marcadas en cada una de las materias que realiza.

Entre los recursos que la universidad pone a disposición de los estudiantes en el marco del Campus Virtual es preciso destacar los siguientes.

- El espacio donde desarrollamos la docencia: el aula virtual.

- Los elementos de planificación de la docencia: plan docente o plan de aprendizaje.
- Los elementos de evaluación de la enseñanza: pruebas de evaluación continua (PEC), pruebas de evaluación final.
- Los recursos disponibles: módulos didácticos, guías de estudio, casos prácticos, biblioteca, lecturas, artículos...
- Las personas que facilitan el aprendizaje: profesores y docentes colaboradores.

En el marco de este modelo pedagógico, el **modelo de evaluación** del máster persigue adaptarse a los ritmos individuales de los estudiantes facilitando la constante comprobación de los avances que muestra el estudiante en su proceso de aprendizaje. Por ello, el modelo de evaluación establecido es el de la **evaluación continua**, que ha de garantizar que la evaluación sea formativa pero sin renunciar a su dimensión acreditativa. A su vez, ha de ser flexible y viable.

La opción de este modelo se justifica en el marco del espacio europeo de educación superior porque ofrece al estudiante una pauta de actividades que debe realizar y sugiere un ritmo de trabajo concreto que garantiza la mejor consecución de los objetivos en el tiempo de que dispone; asegura su participación activa en la construcción del propio conocimiento y facilita la guía y la orientación del profesor en el proceso de aprendizaje, permitiendo obtener de manera gradual una calificación académica.

Este modelo, pues, se construye a partir de cuatro aspectos básicos: la función formativa de la evaluación, la función acreditativa, la flexibilidad y la viabilidad. Atendiendo a estas características, este programa contempla un método de evaluación de las competencias tanto específicas como transversales basado en:

- el trabajo de los estudiantes con los contenidos tanto teóricos como prácticos por medio de actividades, las cuales contemplan la progresión de los aprendizajes que tienen que lograr y se plantean de forma continuada en el tiempo;
- el *feedback* formativo y personalizado por parte del colaborador docente, que favorece la autorregulación, por parte de los estudiantes, de estos aprendizajes;
- una tipología de actividades diversa que permite el trabajo de las competencias que tienen que adquirir;
- un sistema de valoración a cinco niveles, que permite calificar los resultados de los aprendizajes de cada actividad de evaluación continua de manera cualitativa. Al finalizar el semestre, el estudiante obtiene una calificación global cualitativa de la evaluación continua, que tiene su correspondencia cuantitativa según lo establecido en el artículo 5.4 del Real decreto 1125/2003, de 5 de septiembre, por el cual 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. Así, estas calificaciones cualitativas llevan asociadas las siguientes calificaciones cuantitativas:

    1. Matrícula de Honor (M): 10 puntos.
    2. Sobresaliente (SB): 9,5 puntos.
    3. Notable (NO): 8 puntos.
    4. Aprobado (A): 6 puntos.
    5. Suspenso (SU): 2,5 puntos.

Los estudiantes que no realicen las pruebas de evaluación establecidas obtendrán la calificación de No presentado (NP), la cual lleva asociada una calificación cuantitativa de cero puntos.

El número de calificaciones finales con Matrícula de Honor que podrá otorgar la Junta de Evaluación, en ningún caso podrá exceder del cinco por ciento de los estudiantes matriculados en la materia, salvo que el número de estudiantes matriculados sea inferior a 20, en cuyo caso sólo se podrá conceder una calificación final con Matrícula de Honor.

Atendiendo al perfil previsto de los estudiantes y a la flexibilidad que caracteriza al modelo de evaluación propuesto, el estudiante puede optar por dos vías de evaluación para la superación de cada asignatura: el seguimiento del sistema de evaluación continua o bien la realización de una única prueba final de evaluación. La opción recomendada a los estudiantes, considerando su perfil de formación y profesional, es la de ir alcanzando y superando los aprendizajes por la vía de pruebas de evaluación continua hasta llegar a la realización y entrega de un trabajo fin de máster.

El sistema, los métodos y los instrumentos de evaluación de aquellos aprendizajes que los estudiantes deberán alcanzar en esta titulación se han diseñado en el marco del modelo de evaluación de aprendizajes basados en las competencias de las universidades integrantes del máster. El modelo de evaluación de competencias de carácter formativo persigue adaptarse a las características de cada materia y asignatura y facilitar, en este marco, flexibilidad para que el estudiante siga su proceso de aprendizaje. El proceso de evaluación de competencias está configurado por actividades de inicio, actividades de seguimiento y actividades de síntesis.

El correcto seguimiento del sistema de evaluación continua implicará la realización de las actividades propuestas, guiadas y evaluadas por los profesores de las asignaturas, que deben realizarse durante el semestre y que se exponen en la planificación de cada asignatura al inicio del semestre de manera individual y original. Los criterios y requisitos para superar de forma satisfactoria la evaluación continua o las pruebas finales de evaluación serán expuestos, de manera general, en el plan docente de la asignatura.

Por medio del plan docente de cada una de las asignaturas, que se hace público en el espacio del aula al inicio del semestre, los estudiantes conocen cuáles son las actividades de aprendizaje y de evaluación propuestas, qué recursos didácticos tienen al alcance, qué seguimiento y ayuda pedagógica recibirán del equipo docente, cuáles serán los criterios para evaluar su rendimiento y la adquisición de competencias, y cuál es el sistema de valoración de cada una de las actividades.

El proceso de evaluación se centra en las siguientes tipologías:

- **Evaluación continua (EC) + Prueba de síntesis (PS) / Examen final**
  Consiste en diferentes procesos evaluativos de seguimiento de las actividades o prácticas realizadas, más una prueba final que certifica la asimilación de los contenidos y la obtención de las competencias. La nota final de EC se obtiene con la media ponderada de las calificaciones correspondientes a cada una de las pruebas de evaluación continua. En el modelo de evaluación con PS, el estudiante que ha superado la EC realiza una prueba calificable cuya nota es objeto de cruce con la obtenida en la EC. Aquellos estudiantes que, por diferentes causas, no han podido

completar o superar el proceso de evaluación continua, tienen la opción de presentarse al Examen final.

- **Evaluación continua + Examen final**.
  Consiste en diferentes procesos evaluativos de seguimiento de las actividades o prácticas realizadas, más una prueba final que certifica la asimilación de los contenidos y la obtención de las competencias relacionadas con la asignatura. La nota final se obtiene mediante el cruce de la nota de la evaluación continua y la nota obtenida en la prueba final.

- **Evaluación continua + Prueba de síntesis**
  Consiste en diferentes procesos evaluativos de seguimiento de las actividades o prácticas realizadas, más una prueba final calificable cuya nota es objeto de cruce con la obtenida en la EC. La nota final de evaluación continua se obtiene con la media ponderada de las calificaciones correspondientes a cada una de las pruebas de evaluación continua.

- **Evaluación continua**
  Consiste en diferentes procesos evaluativos de seguimiento de las diferentes actividades o prácticas realizadas. La nota final se obtiene con la media ponderada de cada una de las calificaciones correspondientes.

La decisión del modelo de evaluación a aplicar se toma en función de las características propias de la materia a evaluar. Las materias con un elevado componente práctico se evalúan mediante prácticas, con entregas periódicas de carácter obligatorio. En aquellos casos en que se considera necesario, estas materias se evalúan virtual o presencialmente mediante un examen final o una prueba de síntesis.

Atendiendo al perfil previsto de los estudiantes y a la flexibilidad que caracteriza el modelo de evaluación propuesto, se recomienda a los estudiantes —considerando su perfil de formación y profesional— el seguimiento de la evaluación continua, con el fin de que vayan alcanzando y superando los aprendizajes paulatinamente hasta llegar a la realización y entrega del Trabajo de fin de máster.

Los mecanismos para el aseguramiento de la calidad respecto a la evaluación de los aprendizajes se basan en:

- Encuestas a estudiantes.
- Seguimiento del proceso docente por parte de profesores responsables de asignatura, directores de programa y estudios, y consiguiente cambio en los planes de objetivos personales.
- Coordinación de todos los equipos implicados en el proceso de enseñanza.

El modelo pedagógico del máster, como ya se ha comentado, apuesta por la **evaluación continua** como un medio para ayudar al estudiante no presencial a seguir de manera adecuada el programa previsto. Por ello, se realiza un seguimiento del grado de implementación de la evaluación continua en las asignaturas y el porcentaje de estudiantes que optan por este modelo de evaluación, así como los resultados obtenidos.

Las **pruebas de evaluación** (tanto las pruebas de evaluación continua como, si es necesario, la prueba de síntesis) se actualizan semestralmente y constituyen un sistema coherente que evita distorsiones en la evaluación, en tanto que existe relación directa entre las actividades desarrolladas durante el curso y las pruebas de evaluación. Como garantía del proceso existe un procedimiento de revisión de exámenes y de pruebas de síntesis, que es bien conocido por

parte de los estudiantes y que se explicita, se publica y al que se accede desde el Campus Virtual.

A continuación se presenta la descripción detallada de los módulos de enseñanza-aprendizaje de que consta el plan de estudios.

Módulo de formación obligatoria: Comunes	**(18 ECTS OBLIGATORIOS)**
COMPETENCIAS ESPECÍFICAS Y RESULTADOS DEL APRENDIZAJE QUE EL ESTUDIANTE ADQUIERE CON DICHO MÓDULO [8] Capacidad para analizar las técnicas de explotación de vulnerabilidades de una red y los puntos débiles de un sistema. [9] Capacidad para identificar, evaluar y gestionar los principales riesgos de un dominio informático, tanto tecnológicos como procedentes de la ingeniería social. [10] Capacidad para usar técnicas y contramedidas básicas de seguridad para la prevención de ataques derivados de la ingeniería social. [12] Capacidad para aplicar el marco jurídico que afecta a la gestión de la seguridad de sistemas informáticos, teniendo en cuenta la legislación relativa a la propiedad intelectual, el comercio electrónico, la firma electrónica y la protección de datos de carácter personal. [13] Poseer y comprender conocimientos de las estructuras normalizadoras, evaluadoras, certificadoras, y las normas correspondientes que regulan los ámbitos de la seguridad. [14] Poseer y comprender conocimientos de las arquitecturas más importantes de AAA (Authentication, Authorization, Accounting), así como sistemas de federación de identidades y de autenticación única (SSO-Single Sign On). [15] Capacidad para identificar las vulnerabilidades de privacidad de los sistemas (especialmente en aplicaciones web) y capacidad para protegerlos.	
REQUISITOS PREVIOS Los requisitos de acceso al máster.	
RESULTADOS DEL APRENDIZAJE • Conocer la importancia de la seguridad en Internet, en términos de sus implicaciones en diferentes sectores: comercio electrónico, banca electrónica, distribución de contenidos, redes sociales, publicidad, spam. • Conocer las bases de la seguridad informática en diferentes ámbitos: vulnerabilidades y ataques en redes y sistemas, necesidades de seguridad en el desarrollo de aplicaciones, consideraciones legislativas de la seguridad. • Conocer los fundamentos jurídicos sobre seguridad informática • Describir los requerimientos de seguridad de un sistema y la criticidad de cada uno de ellos.	

Materia
Vulnerabilidades de seguridad
6 ECTS

Contenido
- Explotación de vulnerabilidades
- Ingeniería social

Materia
Legislación y regulación
6 ECTS

Contenido
Aspectos legales de la seguridad, nacionales e internacionales

Materia
Identidad digital
6 ECTS

Contenido
- **Técnicas de autenticación, autorización, y gestión de usuarios**
- **Privacidad y anonimato**

Actividades formativas con su contenido en ECTS, su metodología de enseñanza-aprendizaje y su relación con las competencias que debe adquirir el estudiante.

Competencias específicas	Actividades formativas	Nº Créditos ECTS
[8]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	0,5
	PRÁCTICAS	0,5
[9]	PREGUNTAS TEÓRICAS	0,5
	RESOLUCIÓN DE PROBLEMAS	0,5
	ESTUDIO DE CASOS	0,5
	PRÁCTICAS	0,5
[10]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	1
	ESTUDIO DE CASOS	1
	PRÁCTICAS	0,5
	BÚSQUEDA DE INFORMACIÓN	1
[12]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	0,5
	ESTUDIO DE CASOS	0,5
[13]	PREGUNTAS TEÓRICAS	1
	ESTUDIO DE CASOS	0,5
[14]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	1
	ESTUDIO DE CASOS	1
[15]	PREGUNTAS TEÓRICAS	1
	BÚSQUEDA DE INFORMACIÓN	1
	PRÁCTICAS	1

Nota: las competencias transversales se trabajan paralelamente a las competencias específicas, a través de las actividades formativas indicadas.

Aparte de las actividades citadas es importante resaltar que en los créditos asignados están incluidas aquellas actividades que por su papel de instrumento metodológico nuclear se repiten de forma sistemática a lo largo de todas las unidades de docencia:
- Lectura de materiales docentes
- Participación en foros y otras actividades de comunicación

- Realización de pruebas y ejercicios de evaluación

Todas las actividades propuestas se orientan a guiar el proceso de aprendizaje, estimular y motivar al estudiante y facilitar el aprendizaje para alcanzar el nivel competencial propuesto. Sin embargo, no todas ellas tienen por finalidad la evaluación del estudiante.

El sistema, los métodos y los instrumentos de evaluación de los aprendizajes que los estudiantes tendrán que alcanzar en este programa formativo se han diseñado en el marco del modelo de evaluación de aprendizajes basados en competencias de la UOC descrito al inicio de este apartado.

Atendiendo al perfil de los estudiantes previsto y a la flexibilidad que caracteriza al modelo de evaluación propuesto en este **máster**, en general, el estudiante puede optar por dos vías de evaluación para la superación de cada asignatura o materia: el seguimiento del sistema de evaluación continua con una prueba final –que es la vía que la UOC promueve–, o bien la realización de una única prueba final de evaluación. Sin embargo, también se despliega un sistema adicional en algunas asignaturas o materias con una clara vocación aplicada o profesionalizadora, el cual contempla el seguimiento adecuado de las actividades de evaluación continua como única alternativa de evaluación.

Con carácter general hay que señalar que el estudiante, a lo largo de su itinerario académico, desarrollará un amplio número de actividades de evaluación continua, las cuales podrán estar basadas en la resolución de casos prácticos fundamentados en situaciones reales de negocio, en la realización de ejercicios de autoevaluación, en actividades individuales y de trabajo en equipo, en ejercicios de evaluación y en la elaboración de informes de prácticas.

Vista la carga de trabajo del estudiante prevista a lo largo de todo el programa y el conjunto de competencias y conocimientos que se trabajan y que se acreditan, se garantiza que haya una coherencia entre la carga de trabajo de las diferentes actividades programadas en las materias y los créditos de la propia materia, ponderando el número de actividades y su dificultad.

Sistema de evaluación de la adquisición de las competencias y sistema de calificaciones

El correcto seguimiento del sistema de evaluación continua implicará la realización de las actividades propuestas, guiadas y evaluadas por el consultor de la asignatura, que se tienen que hacer durante el semestre y que se exponen en la planificación de cada asignatura al inicio de semestre de manera individual y original. Los criterios y requisitos para superar de forma satisfactoria la evaluación continua o las pruebas finales de evaluación estarán expuestos, de manera general, en el plan docente de la asignatura.

Por medio del plan docente de cada una de las asignaturas, que se hace público en el espacio del aula al inicio de semestre, los estudiantes conocen cuáles son las actividades de aprendizaje y de evaluación propuestas, qué recursos didácticos tienen al alcance, qué seguimiento y ayuda pedagógica recibirán del consultor, cuáles serán los criterios para evaluar su rendimiento y la adquisición de competencias, y cuál es el sistema de valoración de cada una de las actividades.

Sin embargo, al inicio de cada actividad o prueba final de evaluación, las propuestas están expuestas y son presentadas extensamente por el consultor en el aula.

El diseño de este máster asegura que las competencias específicas y transversales se trabajan, se movilizan y se adquieren a los niveles definidos, por un lado, por la tipología de actividades de aprendizaje evaluables y no evaluables, y, por otro lado, por la metodología docente y el planteamiento de cada ejercicio o tarea que el estudiante tiene que realizar.

La tipología de actividades que se propone es la siguiente: reflexión y discusión sobre conceptos

fundamentales, análisis comparativo, trabajo de síntesis, realización de mapas conceptuales, recogida y tratamiento de la información, análisis de casos, actividades orientadas a proyecto, actividades de autoevaluación, actividades de evaluación entre iguales.

Como ya hemos dicho, el modelo de evaluación que se promueve en este máster es el de evaluación continua. Por lo tanto, la valoración de la consecución de los objetivos tiene lugar en diversos momentos del proceso formativo en cada uno de los módulos de las diferentes especialidades, y no sólo al final del proceso.

Aunque no se dispone de esta información, debido a la novedad del programa, sobre la cantidad y la distribución de actividades evaluativas, se tendrá en cuenta para su programación que haya coherencia entre la carga de trabajo de las diferentes actividades programadas en las materias y los créditos de la propia materia, por lo que se ponderarán el número de actividades y su dificultad.

Existe un registro de calificaciones de la evaluación continua (EC) y nota final de EC que es visible para el estudiante, el cual, en todo momento del semestre, puede conocer las evaluaciones emitidas por el consultor de la asignatura. Esta aplicación web, a la cual sólo el consultor tiene acceso, es donde habrá que introducir las calificaciones de cada una de las actividades de evaluación continua propuestas a los estudiantes y la calificación final de evaluación continua para cada estudiante.

Para las evaluaciones de cada módulo, así como para la calificación final que el máster otorga, hay previstos mecanismos de evaluación colectiva (junta de evaluación) y mecanismos de revisión de las calificaciones (los procesos de revisión de exámenes y pruebas de evaluación).

La **junta de evaluación** está integrada por los profesores, consultores y tutores del máster, y presidida por el director académico de programa o la persona en quien delegue.

En una primera fase, a la junta de evaluación le corresponde proponer a la dirección de programa la calificación final de la asignatura, teniendo en cuenta el cuadro de cruces, y debatir la calificación final de una asignatura cuando la tabla de cruce dé como resultado más de una posibilidad (sobresaliente / matrícula de honor, notable / aprobado).

Finalmente, en una segunda fase, a la junta de evaluación le corresponde validar todas las calificaciones finales otorgadas y resolver los casos donde el cuadro de cruce dé como resultado más de una posibilidad. Por lo tanto, en este sentido, dictaminará si es procedente o no la concesión de matrículas de honor.

Validadas las calificaciones finales otorgadas por la junta de evaluación, la dirección de programa las asignará de manera provisional y las publicará en los expedientes académicos de los estudiantes dentro del plazo establecido en el calendario académico. Finalizado el periodo de revisión de las pruebas finales de evaluación, el director académico de programa asignará las calificaciones finales de manera definitiva y procederá al cierre de actas.

Si el plan docente de la asignatura contempla la realización de una prueba final de evaluación, los estudiantes tendrán derecho a solicitar la revisión de esta prueba una vez publicadas las calificaciones finales de las asignaturas. Los estudiantes tendrán que solicitar la **revisión de sus pruebas finales de evaluación** dentro de los plazos establecidos en el calendario académico de la UOC y por medio de los canales designados a tal efecto.

Una vez publicados los resultados de la revisión de las pruebas finales de evaluación, y a la vista de los resultados, los estudiantes tendrán derecho a solicitar, si lo consideran justificado, una alegación a este resultado. Los estudiantes tendrán que solicitar la **alegación al resultado de la revisión de sus pruebas finales de evaluación** dentro de los plazos establecidos en el calendario académico de la UOC y por medio de los canales designados a tal efecto.

El **sistema de evaluación de la adquisición de las competencias y sistema de calificaciones** descrito en este apartado es válido para el conjunto de módulos que conforman el máster y que se detallan a continuación.

Breve descripción de contenidos de cada materia

En este módulo se trabajan los conocimientos básicos de la seguridad informática desde el punto de vista técnico y legal. Así, las materias que conforman el módulo tratan las vulnerabilidades de seguridad en redes, los conceptos de identidad digital y las aplicaciones del dni electrónico, y la legislación y regulación relacionada con la seguridad informática.

- **Vulnerabilidades de Seguridad (6ECTS)**: Esta materia hace un repaso a las amenazas, vulnerabilidades y ataques de seguridad en redes y sistemas. La materia incide en el aprendizaje de metodologías y herramientas para identificar y minimizar las vulnerabilidades desde una perspectiva práctica y aplicada. Se expondrá a los estudiantes a una variedad de ataques actualmente presentes: virus, troyanos, gusanos, rootkits, bootnets. Asimismo, se analizarán las técnicas utilizadas para llevar a cabo ataques basados en Ingeniería social y se estudiarán las contramedidas de seguridad que pueden ayudar a prevenirla.

- **Identidad digital (6 ECTS)**: Esta materia se focaliza en las técnicas de gestión de las identidades digitales y su protección frente a los riesgos de privacidad y a los ataques de falsificación de datos. Se introducen protocolos y herramientas de autentificación fuerte, sistemas de autorización, sistemas de “single sign-on” y servicios de federación. También se aprenden los conceptos y métodos para la creación de tecnologías y políticas que garanticen la protección de la privacidad al mismo tiempo que permitan que la sociedad pueda compartir información personal para propósitos específicos y acordados. Los métodos incluyen procesos relacionados con la identidad de los datos, la vinculación de los registros, generar perfiles a partir de los datos, fusión de datos, datos de anonimato, especificación y aplicación de políticas, y data mining preservando la privacidad.

- **Legislación y regulación (6 ECTS)**: En esta materia se describen los aspectos de la legislación nacional e internacional que están relacionados con la seguridad informática. Se introducen los fundamentos jurídicos, el derecho penal y los tipos de delitos existentes. Se hace un amplio análisis de las leyes LOPDP, LSSICE, firma digital, y facturación electrónica. Se estudia también en detalle el nuevo reglamento de desarrollo de la LOPDP –el RD 1720/2007-.

Comentarios adicionales

El módulo da a los estudiantes una visión general de los problemas de seguridad presentes en los sistemas informáticos actuales y las estrategias para prevenirlos y combatirlos, tanto desde el punto de vista técnico como legal.

Módulo de Especialidad 1: Seguridad en Redes y Sistemas
(18 ECTS OBLIGATORIOS DE ITINERARIO)

COMPETENCIAS ESPECÍFICAS Y RESULTADOS DEL APRENDIZAJE QUE EL ESTUDIANTE ADQUIERE CON DICHO MÓDULO

[8] Capacidad para analizar las técnicas de explotación de vulnerabilidades de una red y los puntos débiles de un sistema.

[16] Capacidad para comprender y saber usar herramientas para la administración y

protección de redes cableadas e inalámbricas, y la gestión de alertas de seguridad.
[17] Capacidad para concebir, desplegar, organizar y gestionar redes de comunicaciones en contextos residenciales, empresariales o institucionales, responsabilizándose de la seguridad del sistema y la protección de los datos de los usuarios.
[18] Poseer y comprender conocimientos de las técnicas principales de seguridad en los sistemas operativos.
[19] Capacidad para configurar y administrar una base de datos a nivel físico y lógico, a fin de asegurar la integridad, disponibilidad y confidencialidad de la información almacenada.
[20] Capacidad para realizar una configuración experta de un servidor GNU/Linux o Windows.
[21] Capacidad para diseñar soluciones integrales apropiadas en escenarios complejos que combinen las técnicas y contramedidas conocidas para la prevención, detección y disuasión de ataques.

REQUISITOS PREVIOS

Para cursar las asignaturas del módulo, es necesario que el estudiante tenga conocimientos básicos sobre las vulnerabilidades y los mecanismos de prevención y protección de redes TCP/IP. Estos conocimientos se adquieren en la materia de Vulnerabilidades de Seguridad del módulo de materias comunes del máster.

RESULTADOS DEL APRENDIZAJE

- Conocer las herramientas para analizar la seguridad de una red y saber elegir la más apropiada en cada situación.
- Evaluar y proteger un sistema informático frente a ataques de seguridad.
- Detectar de forma rápida y eficiente las incidencias de seguridad en los sistemas, así como analizar de forma rigurosa su origen y los rastros de infección.
- Conocer dónde buscar información puntualmente actualizada de las vulnerabilidades de seguridad que los sistemas presentan.
- Saber actualizar los conocimientos de seguridad en redes, sistemas operativos y bases de datos, forma rápida y constante.

Materia
Seguridad en redes
6 ECTS

Contenidos

- Diseño y planificación de redes seguras, con especial atención a la redes distribuidas, sin hilos, y abiertas.

Materia
Seguridad en sistemas operativos
6 ECTS

Contenido

- Estudio y configuración de computadores en diversos S.O. para poder disponer de equipos seguros.

Materia
Seguridad en bases de datos
6 ECTS

Contenido

- Ataques de seguridad en bases de datos y configuración segura.

Actividades formativas con su contenido en ECTS, su metodología de enseñanza-aprendizaje y su relación con las competencias que debe adquirir el estudiante.

Competencias específicas	Actividades formativas	Nº Créditos ECTS
[8]	PREGUNTAS TEÓRICAS	0,5
	RESOLUCIÓN DE PROBLEMAS	0,5
	PRÁCTICAS	0,5
[16]	PREGUNTAS TEÓRICAS	0,5
	RESOLUCIÓN DE PROBLEMAS	0,5
	ESTUDIO DE CASOS	0,5
	PRÁCTICAS	0,5
	BÚSQUEDA DE INFORMACIÓN	0,5
[17]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	0,5
	ESTUDIO DE CASOS	1
	PRÁCTICAS	1
[18]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	1
	ESTUDIO DE CASOS	0,5
[19]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	1
	PRÁCTICAS	1
[20]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	0,5
	PRÁCTICAS	1
[21]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	0,5
	PRÁCTICAS	1

Nota: las competencias transversales se trabajan paralelamente a las competencias específicas, a través de las actividades formativas indicadas.

Aparte de las actividades citadas es importante resaltar que en los créditos asignados están incluidas aquellas actividades que por su papel de instrumento metodológico nuclear se repiten de forma sistemática a lo largo de todas las unidades de docencia:

- Lectura de materiales docentes
- Participación en foros y otras actividades de comunicación
- Realización de pruebas y ejercicios de evaluación

Todas las actividades propuestas se orientan a guiar el proceso de aprendizaje, estimular y motivar al estudiante y facilitar el aprendizaje para alcanzar el nivel competencial propuesto. Sin embargo, no todas ellas tienen por finalidad la evaluación del estudiante.

El sistema, los métodos y los instrumentos de evaluación de los aprendizajes que los estudiantes tendrán que alcanzar en este programa formativo se han diseñado en el marco del modelo de evaluación de aprendizajes basados en competencias de la UOC descrito al inicio de este apartado.

Atendiendo al perfil de los estudiantes previsto y a la flexibilidad que caracteriza al modelo de evaluación propuesto en este **máster**, en general, el estudiante puede optar por dos vías de evaluación para la superación de cada asignatura o materia: el seguimiento del sistema de evaluación continua con una prueba final –que es la vía que la UOC promueve–, o bien la realización de una única prueba final de evaluación. Sin embargo, también se despliega un sistema adicional en algunas asignaturas o materias con una clara vocación aplicada o profesionalizadora, el cual contempla el seguimiento adecuado de las

actividades de evaluación continua como única alternativa de evaluación.

Con carácter general hay que señalar que el estudiante, a lo largo de su itinerario académico, desarrollará un amplio número de actividades de evaluación continua, las cuales podrán estar basadas en la resolución de casos prácticos fundamentados en situaciones reales de negocio, en la realización de ejercicios de autoevaluación, en actividades individuales y de trabajo en equipo, en ejercicios de evaluación y en la elaboración de informes de prácticas.

Vista la carga de trabajo del estudiante prevista a lo largo de todo el programa y el conjunto de competencias y conocimientos que se trabajan y que se acreditan, se garantiza que haya una coherencia entre la carga de trabajo de las diferentes actividades programadas en las materias y los créditos de la propia materia, ponderando el número de actividades y su dificultad.

Sistema de evaluación de la adquisición de las competencias y sistema de calificaciones

El sistema de evaluación de la adquisición de las competencias y sistema de calificaciones se describen en el primer módulo.

Breve descripción de contenidos de cada materia

En este módulo se trabajan los conocimientos propios de las tecnologías de seguridad en sistemas operativos, bases de datos, redes, y sistemas distribuidos. Las materias que conforman el módulo son: seguridad en redes, seguridad en sistemas operativos y seguridad en bases de datos. A continuación se detalla el contenido de dichas materias:

- **Seguridad en redes (6 ECTS)**: Esta materia se centra en el diseño y planificación de redes seguras. Se hace un repaso a las arquitecturas de cortafuegos y redes privadas virtuales, y se analiza la seguridad de los protocolos Internet (ARP, DNS, IPSec,..). Se presentan las vulnerabilidades de las redes inalámbricas y se analizan los sistemas y protocolos para proteger las comunicaciones en este entorno. Se estudian protocolos de redes PAN (Bluetooth, Zigbee), LAN (wifi), MAN (wimax, ad hoc) y WAN (celulares). Finalmente, en esta materia se trabaja cómo diseñar y verificar que un sistema de comunicación es seguro.

- **Seguridad en sistemas operativos (6 ECTS)**: Esta materia se focaliza en el estudio de la seguridad en diferentes sistemas operativos. Se introducen los mecanismos de seguridad pasiva y activa, se presentan los modelos y políticas de seguridad empresarial, y se detalla cómo realizar configuraciones de servidores. En concreto, el alumno aprenderá a realizar configuraciones expertas en servidores GNU/Linux y Windows.

- **Seguridad en bases de datos (6 ECTS)**: Esta materia se focaliza en el estudio de las arquitecturas de bases de datos, sus vulnerabilidades, y los mecanismos de fortificación. Se introducen los mecanismos de seguridad pasiva y activa, se presentan los modelos y políticas de seguridad empresarial, y se detalla cómo realizar configuraciones.

Comentarios adicionales

El módulo permite a los estudiantes adquirir las competencias propias de los administradores y responsables de la seguridad informática de un sistema empresarial.

Módulo de Especialidad 2: Seguridad en Servicios y Aplicaciones
(18 ECTS OBLIGATORIOS DE ITINERARIO)

COMPETENCIAS Y RESULTADOS DEL APRENDIZAJE QUE EL ESTUDIANTE ADQUIERE CON DICHO MÓDULO

[22] Capacidad para aplicar metodologías y buenas prácticas de programación de código robusto, así como capacidad de modelar las amenazas de un sistema para evaluar la seguridad de las aplicaciones desarrolladas.
[23] Capacidad para analizar, diseñar y desarrollar aplicaciones y servicios web seguros.
[24] Poseer y comprender conocimientos de los sistemas que forman parte de una arquitectura de comercio electrónico, y capacidad para desplegar una.
[25] Capacidad para comprender y analizar los sistemas de facturación electrónica, de pago y de micro-pago.
[26] Comprender las técnicas de reconocimiento de las personas a través de características físicas: cara, huellas dactilares, orejas, iris, manos, forma de caminar, voz, etc.
[27] Capacidad para diseñar aplicaciones reales con acceso biométrico. Conocer el software y hardware actual para desarrollar aplicaciones.

REQUISITOS PREVIOS

Para cursar las materias del módulo es necesario que el estudiante haya superado la materia de Identidad digital del módulo de materias comunes del máster.

RESULTADOS DEL APRENDIZAJE

- Conocer y poner en práctica las metodologías de programación de código seguro.
- Conocer las librerías de programación de servicios de seguridad en diferentes tecnologías y saber elegir la más adecuada en cada situación.
- Demostrar comprensión por las plataformas de pago electrónico.
- Ser capaz de diseñar e implementar un sistema de comercio electrónico.
- Manejar las técnicas de reconocimiento biométrico.

Materia
Programación de código seguro
6 ECTS

Contenido
- Metodologías y herramientas para el desarrollo de código robusto a ataques de seguridad

Materia
Comercio electrónico
6 ECTS

Contenido
- Facturación electrónica, sistemas de pago

Materia
Biometría
6 ECTS

Contenido
- Descripción de diferentes sistemas biométricos

Actividades formativas con su contenido en ECTS, su metodología de enseñanza-aprendizaje y su relación con las competencias que debe adquirir el estudiante.

Competencias específicas	Actividades formativas	Nº Créditos ECTS
[22]	PREGUNTAS TEÓRICAS	1
	DEBATE	1
	PRÁCTICAS	1
[23]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	1
	ESTUDIO DE CASOS	1
	BUSQUEDA DE INFORAMACIÓN	1
[24]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	1
	DEBATE	1
[25]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	1
	BÚSQUEDA DE INFORMACIÓN	1
[26]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	0,5
	ESTUDIO DE CASOS	1
[27]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	0,5
	PRÁCTICAS	1

Nota: las competencias transversales se trabajan paralelamente a las competencias específicas, a través de las actividades formativas indicadas.

Véase una explicación de la metodología de enseñanza-aprendizaje en el módulo 1

Sistema de evaluación de la adquisición de las competencias y sistema de calificaciones

Véase explicación del módulo 1

Breve descripción de contenidos de cada materia

En este módulo se trabajan los conocimientos asociados al desarrollo de aplicaciones seguras. Las materias que conforman el módulo son: programación de código seguro, comercio electrónico, y biometría. A continuación se detalla el contenido de dichas materias:

- **Programación de código seguro (6 ECTS):** Esta materia se focaliza en el ámbito de la programación de aplicaciones de seguridad. Por un lado, se describirán las técnicas de programación para evitar la presencia de vulnerabilidades durante el proceso de ejecución. Se incidirá en los riesgos más comunes (desbordamientos del buffer y la pila, inyección de código, cross site scripting, etc.), y los procesos de seguridad básicos: cómo gestionar la memoria, el formato y el encapsulado de datos, la certificación de los compiladores y sus métodos de verificación, y la gestión de los flujos de información. Se presentarán las metodologías y herramientas para identificar y eliminar los agujeros de seguridad, y se explicaran las directrices esenciales para crear software seguro: como diseñar software pensando en la seguridad desde el inicio del desarrollo e integrar sistemas de análisis y gestión del riesgo en todo el ciclo de vida del software.

- **Comercio electrónico (6 ECTS):** Esta materia hace un repaso de los estándares de firma electrónica y las bases para la seguridad en el comercio electrónica. El contenido central de la materia es la facturación electrónica y las arquitecturas de comercio electrónico. Se analizará la seguridad de los protocolos de transacciones electrónicas y los sistemas de pago electrónico y móvil.

- **Biometría (6 ECTS):** En esta materia se presentan los métodos para reconocer las personas mediante técnicas biométricas así como el impacto que estos métodos suponen en nuestra sociedad. Se explican, entre otros, el reconocimiento de caras, de huellas, del iris, y de la voz. Se discute sobre las consideraciones de seguridad de estos sistemas.

Comentarios adicionales

El módulo permite a los estudiantes adquirir las competencias propias de un jefe de proyectos de desarrollo y despliegue de software, y de un analista/programador de aplicaciones con requerimientos de seguridad críticos.

Módulo de Especialidad 3: Gestión y Auditoria de la seguridad informática
(18 ECTS OBLIGATORIOS DE ESPECIALIDAD)

COMPETENCIAS Y RESULTADOS DEL APRENDIZAJE QUE EL ESTUDIANTE ADQUIERE CON DICHO MÓDULO

[28] Capacidad para identificar y analizar los procesos críticos de una organización, así como el impacto que produciría la interrupción de estos procesos.
[29] Capacidad para elaborar un plan de seguridad, teniendo en cuento todo el proceso de inventario y clasificación de activos, estudio de amenazas, análisis de riesgos y definición del plan de acción con el presupuesto asociado para la aprobación de la dirección.
[30] Capacidad para desarrollar un Plan de Continuidad, conocer sus fases y el personal que debe implicarse en su desarrollo. Conocer las normas y estándares de referencia relacionados con la Continuidad de Negocio
[31] Capacidad para implantar un Sistema de Gestión de la Seguridad de la Información siguiendo las fases del ciclo de Deming.
[32] Capacidad para gestionar la certificación de un sistema de gestión de la seguridad de la información, así como capacidad para comprender, interpretar y explicar las ventajas que aporta la certificación de estos sistemas.
[33] Capacidad de elaborar e implementar un plan de auditoría. Uso de las herramientas habituales para realizar una auditoría técnica de seguridad.
[34] Capacidad para realizar un análisis forense de cualquier sistema informático (PC, móviles, routers, etc.) y presentarlo en una sede judicial.
[35] Capacidad para aplicar las consideraciones legales adquiridas para realizar la gestión de un incidente de seguridad.

REQUISITOS PREVIOS

Para cursar las materias del módulo es necesario que el estudiante haya superado la materia de Legislación y Regulación del módulo de materias comunes del máster.

RESULTADOS DEL APRENDIZAJE

- Evaluar con rigor los procesos de una organización para identificar los puntos críticos de seguridad.
- Saber elaborar un sistema de gestión de la seguridad de la información.
- Demostrar conocimiento de las fases de desarrollo de un Plan de Continuidad y las

herramientas para llevarlo a cabo.
- Desarrollar una auditoría técnica y de certificación.
- Realizar el informe de un análisis forense.

Materia
Sistemas de gestión de la seguridad
6 ECTS

Contenido
- Sistemas de gestión de la seguridad de la información

Materia
Auditoría técnica
6 ECTS

Contenido
- Auditoría técnica y de certificación

Materia
Análisis forense
6 ECTS

Contenido
- Análisis forense

Actividades formativas con su contenido en ECTS, su metodología de enseñanza-aprendizaje y su relación con las competencias que debe adquirir el estudiante.

Competencias específicas	Actividades formativas	Nº Créditos ECTS
[28]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	1
[29]	PREGUNTAS TEÓRICAS	1
	DEBATE	1
	PRÁCTICAS	1
[30]	PREGUNTAS TEÓRICAS	1
	ESTUDIO DE CASOS	1
	PRÁCTICAS	1
[31]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	0,5
	DEBATE	0,5
[32]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	0,5
	PRÁCTICAS	0,5
[33]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	0,5
	ESTUDIO DE CASOS	1
[34]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	0,5
[35]	PREGUNTAS TEÓRICAS	0,5
	RESOLUCIÓN DE PROBLEMAS	0,5
	BUSQUEDA DE INFORMACION	0,5
	PRÁCTICAS	0,5

Nota: las competencias transversales se trabajan paralelamente a las competencias específicas, a través de las actividades formativas indicadas.

Véase una explicación de la metodología de enseñanza-aprendizaje en el módulo 1

Sistema de evaluación de la adquisición de las competencias y sistema de calificaciones

Véase explicación del módulo 1

Breve descripción de contenidos de cada materia

En este módulo se trabajan los conocimientos relacionados con la gestión de la seguridad. Las materias que conforman el módulo son: sistemas de gestión de la seguridad, auditoría técnica, y análisis forense. A continuación se detalla el contenido de dichas materias:

- **Sistemas de gestión de la seguridad (6 ECTS)**: El objetivo de esta materia es aprender a realizar la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI). Se introducen los principios y normativas de seguridad empresarial, se aprende a hacer un análisis de riesgos con las metodologías más usadas (MARGERIT, NIST,CRAMM, OCTAVE), se presentan las medidas de seguridad ISO, y se estudian las fases de implantación de un SGSI.

- **Auditoría técnica (6 ECTS):** En esta materia se presentan los diferentes tipos de auditorías. La materia se centra en las auditorías técnicas y de certificación. Se explican los objetivos y las fases (documental/presencial/documentación) de la auditoría, así como el proceso de certificación. Se presentan las metodologías de auditoría así como los herramientas apropiadas para llevarlas a cabo.

- **Análisis forense (6 ECTS):** Esta materia se focaliza en los aspectos técnicos que se deben llevar a cabo para realizar un análisis forense, y la documentación que se debe generar. Se presentan las técnicas de recuperación de información y la metodología de un análisis, es decir, adquisición de datos, análisis e investigación de datos, y documentación del proceso. Se describe el marco legal de los análisis forenses. Se aprenden a usar las herramientas propias de un análisis de este tipo.

Comentarios adicionales

El módulo permite a los estudiantes adquirir las competencias propias de profesionales especializados en las nuevas tecnologías de seguridad que implementan y gestionan de manera eficaz sus sistemas.

Módulo de Especialidad 4: Investigación **(18 ECTS OBLIGATORIOS DE ESPECIALIDAD)**

COMPETENCIAS Y RESULTADOS DEL APRENDIZAJE QUE EL ESTUDIANTE ADQUIERE CON DICHO MÓDULO

[36] Capacidad para planificar, administrar, dirigir y coordinar proyectos de investigación en el campo de las TIC.
[37] Capacidad para diseñar y llevar a cabo la investigación según las normas del conocimiento científico en el campo de las TIC.
[38] Capacidad para redactar documentación científica, y sintetizar y presentar los resultados de un proyecto de investigación.
[39] Capacidad para determinar las características relevantes de un sistema TIC para su modelado y simulación, así como capacidad para sintetizar y presentar los resultados.
[40] Comprender los fundamentos teóricos de la criptografía moderna y el funcionamiento de los protocolos criptográficos actualmente en uso.
[41] Capacidad para analizar los distintos sistemas criptográficos que se utilizan habitualmente y criticar su aplicabilidad, así como entender la no aplicabilidad de otros sistemas teóricamente

interesantes.
[42] Capacidad para interpretar, analizar y explicar las diferencias conceptuales y su aplicabilidad entre los diversos esquemas propuestos para resolver un mismo problema criptográfico.
[43] Capacidad para comprender y utilizar las aplicaciones criptográficas existentes basadas en técnicas avanzadas.

REQUISITOS PREVIOS

No existen requisitos previos para cursar las asignaturas de este módulo.

RESULTADOS DEL APRENDIZAJE

- Escribir de forma correcta y apropiada para el ámbito investigador.
- Conocer el proceso de investigación, así como sus técnicas y métodos asociados
- Elaborar documentos científico-técnicos de forma rigurosa: organizar, estructurar, sistematizar y argumentar la información.
- Saber buscar información eficiente y eficazmente.
- Saber analizar un conjunto de datos o información rigurosamente, tanto de forma cualitativa como cuantitativa.
- Demostrar conocimientos teóricos sobre criptografía avanzada.

Materia
Metodologías de investigación
6 ECTS

Contenido
- Metodologías de investigación en las TIC

Materia
Técnicas de investigación
6 ECTS

Contenido
- Técnicas de investigación en las TIC

Materia
Criptografía avanzada
6 ECTS

Contenido
- Curvas elípticas, criptografía cuántica

Actividades formativas con su contenido en ECTS, su metodología de enseñanza-aprendizaje y su relación con las competencias que debe adquirir el estudiante.

Competencias específicas	Actividades formativas	Nº Créditos ECTS
[36]	PREGUNTAS TEÓRICAS	0,5
	REDACCIÓN DE TEXTOS	1
[37]	PREGUNTAS TEÓRICAS	0,5
	RESOLUCIÓN DE PROBLEMAS	1
	ESTUDIO DE CASOS	1
[38]	PREGUNTAS TEÓRICAS	1
	ACTIVIDADES PRÁCTICAS	0,5

	BUSQUEDA DE INFORAMACIÓN	0,5
[39]	PREGUNTAS TEÓRICAS	1
	DEBATE	0,5
	REDACCIÓN DE TEXTOS	0,5
	PRESENTACIONES ORALES	1
	ACTIVIDADES PRÁCTICAS	1
[40]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	0,5
	PRÁCTICAS	0,5
[41]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	0,5
	ESTUDIO DE CASOS	0,5
[42]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	0,5
	ACTIVIDADES PRÁCTICAS	0,5
[43]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	0,5
	BUSQUEDA DE INFORMACION	0,5

Nota: las competencias transversales se trabajan paralelamente a las competencias específicas, a través de las actividades formativas indicadas.

Véase una explicación de la metodología de enseñanza-aprendizaje en el módulo 1

Sistema de evaluación de la adquisición de las competencias y sistema de calificaciones

Véase explicación del módulo 1

Breve descripción de contenidos de cada materia

En este módulo se trabajan los conocimientos básicos para iniciar proyectos de investigación en seguridad de la información y las comunicaciones. En concreto, este módulo prepara a los alumnos que quieran seguir sus estudios en programas de doctorado. Las materias que conforman el módulo son: metodologías de investigación, técnicas de investigación y criptografía avanzada. A continuación se detalla el contenido de dichas materias:

- **Metodologías de Investigación en TIC (6 ECTS):** Esta materia se centra en presentar las fases de un proceso de investigación, y las metodologías para llevar a cabo un proyecto. Se hace una introducción al proceso de investigación (propósito y productos de la investigación, proceso de investigación, aspectos éticos, revisión de la literatura) y se presentan las metodologías de investigación (encuestas, diseño y creación, experimentos, estudio de casos, *action research*, prueba formal). Se definen las estrategias de investigación (entrevistas, observación, cuestionarios, documentos), se detallan las técnicas de análisis cuantitativo y cualitativo, y se describen los métodos de prueba formal.
- **Técnicas de Investigación en TIC (6 ECTS):** Esta materia se centra en presentar las fases de un proceso de investigación, y las técnicas para llevar a cabo un proyecto. Se introduce al estudiante en la redacción de textos científicos. Se presentan los características principales de las publicaciones científicas (proceso de peer review, categorías de publicaciones: revistas indexadas y no indexadas, factores de impacto, índices científicos y bibliométricos, congresos, workshops, ...). y la selección de publicaciones en una área. Se estudia cómo gestionar proyectos de investigación y se aprende a manejar herramientas de apoyo a la investigación: procesadores de textos científicos, gestores de bibliografía, editores de presentaciones, bases de datos (ISI WoK, Google Scholar, DBLP), herramientas de análisis cuantitativo y cualitativo, herramientas de gestión de proyectos. También se introducen nociones sobre la propiedad intelectual: patentes, propiedad intelectual, derechos de autor. Finalmente, se aprende a presentar los resultados de una

investigación, en forma de informes, artículos o presentaciones orales.

- **Criptografía avanzada (6 ECTS)**: La criptografía avanzada incluye aquellos aspectos sobre dicha técnica que por su especificidad, complejidad o por que abarcan o relacionan diversos tópicos, se escapan a los cursos de criptografía básicos. En esta materia se hace un recorrido por las bases matemáticas que soportan dichos esquemas avanzados, cuerpos finitos, curvas elípticas, Tate pairings, etc. y se especifican los más importantes esquemas criptográficos, así como sus aplicaciones (por ejemplo, las firmas de grupo o de anillo, signaturas ciegas, cifrado basado en identidad, criptografía cuántica y post-cuántica, etc.)

Comentarios adicionales

Los estudiantes deberán disponer de un nivel suficiente de inglés (el nivel indicado en las condiciones de ingreso al Máster en el apartado 4.1), para poder leer y escribir documentación técnica y científica en este idioma.

Todo el profesorado y los docentes colaboradores que realicen docencia en las asignaturas de este módulo tendrán el título de doctor.

Módulo de Optativas **(6 ECTS OPTATIVOS)**

COMPETENCIAS Y RESULTADOS DEL APRENDIZAJE QUE EL ESTUDIANTE ADQUIERE CON DICHO MÓDULO

[44] Poseer y comprender conocimientos de las diferencias conceptuales entre los diferentes dominios de marcado de la información digital (dominio temporal/espacial y transformado). Capacidad crítica para analizar la bondad de distintos sistemas de marcado.
[45] Capacidad para integrar conocimientos de las aplicaciones existentes para las técnicas de marcado de la información
[46] Capacidad para la dirección de proyectos de investigación, desarrollo e innovación, en empresas y centros tecnológicos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.
[47] Capacidad para la integración de tecnologías, aplicaciones, servicios y sistemas propios de la Ingeniería Informática, con carácter generalista, y en contextos más amplios y multidisciplinares.
[48] Capacidad para la planificación estratégica, elaboración, dirección, coordinación, y gestión técnica y económica en los ámbitos de la ingeniería informática relacionados, entre otros, con: sistemas, aplicaciones, servicios, redes, infraestructuras o instalaciones informáticas y centros o factorías de desarrollo de software, respetando el adecuado cumplimiento de los criterios de calidad y medioambientales y en entornos de trabajo multidisciplinares.

REQUISITOS PREVIOS

No existen requisitos previos para cursar las asignaturas de este módulo.

RESULTADOS DEL APRENDIZAJE

- Demostrar conocimientos sobre la problemática de la esteganografía en diferentes soportes (audio, imagen, video).
- Comprender y evaluar las técnicas de marcado de la información.
- Conocer el funcionamiento, la organización y la dirección estratégica de los diferentes departamentos que utilizan sistemas de información
- Comprender la gestión estratégica de los sistemas y tecnologías de la información, desde la planificación hasta la implantación en el día a día.

Materia **Técnicas de marcado de la información** **6 ECTS** **Contenido** • Esteganografía y marcas de agua	**Materia** **Dirección Estratégica de SI/TI** **6 ECTS** **Contenido** • Planificación, organización, y dirección estratégica en sistemas y tecnologías de la información (SI/TI)

Nota: *La oferta de materias optativas para cada estudiante, además de las materias propias de este módulo, incluye las materias de todos los módulos de especialidad que no formen parte de la propia especialidad del estudiante.*

Actividades formativas con su contenido en ECTS, su metodología de enseñanza-aprendizaje y su relación con las competencias que debe adquirir el estudiante.

Competencias específicas	Actividades formativas	Nº Créditos ECTS
[44]	PREGUNTAS TEÓRICAS	1
	BUSQUEDA DE INFORAMACION	1
	RESOLUCIÓN DE PROBLEMAS	1
[45]	PREGUNTAS TEÓRICAS	1
	RESOLUCIÓN DE PROBLEMAS	1
	PRÁCTICAS	1
[46]	PREGUNTAS TEÓRICAS	0,5
	ESTUDIO DE CASOS	1
	DEBATE	0,5
[47]	PREGUNTAS TEÓRICAS	1
	ESTUDIO DE CASOS	0,5
	DEBATE	0,5
[48]	PREGUNTAS TEÓRICAS	1
	ESTUDIO DE CASOS	0,5
	DEBATE	0,5

Nota: las competencias transversales se trabajan paralelamente a las competencias específicas, a través de las actividades formativas indicadas.

Véase una explicación de la metodología de enseñanza-aprendizaje en el módulo 1

Sistema de evaluación de la adquisición de las competencias y sistema de calificaciones

Véase explicación del módulo 1

Breve descripción de contenidos de cada materia

En este módulo se trabajan conocimientos específicos sobre alguna de las áreas de seguridad. La materia

que conforma este módulo es: técnicas de marcado de la información. A continuación se detalla el contenido de dicha materia:

- **Técnicas de marcado de la información (6 ECTS)**: Dicha materia incluye todas aquellas técnicas que se utilizan para el marcado de la información digital. Se estudian los esquemas de marcas de agua más utilizados hasta el momento tanto en contenidos de imágenes como de audio. Por otro lado, se estudian también las distintas aplicaciones que tienen las técnicas de marcado, como pueden ser el rastreo de la información digital, la detección de copia o la detección de manipulación.

Dirección estratégica de Sistemas y Tecnologías de la Información (6 ECTS): Dicha materia estudia los conceptos básicos de la estrategia de empresa y el papel que tienen los sistemas y tecnologías de la información (SI/TI) en la consecución de los objetivos de negocio. En particular se trabaja la planificación estratégica de SI/TI, la organización estratégica de departamentos de SI/TI, y la dirección estratégica de SI/TI.

Comentarios adicionales

Los estudiantes deberán disponer de un nivel suficiente de inglés (el nivel indicado en las condiciones de ingreso al Máster en el apartado 4.1), para poder leer y escribir documentación técnica y científica en este idioma.

Módulo de Prácticas
(3 ECTS OBLIGATORIOS DE LAS ESPECIALIDADES PROFESIONALIZADORAS)

COMPETENCIAS Y RESULTADOS DEL APRENDIZAJE QUE EL ESTUDIANTE ADQUIERE CON DICHO MÓDULO

En este módulo se trabajan fundamentalmente las competencias transversales del máster:

[1] Capacidad de análisis y síntesis de la seguridad de un sistema.

[2] Capacidad para ejercer la actividad profesional de acuerdo al código ético y a los aspectos legales actuales en el entorno de las TIC.

[3] Capacidad de comunicación tanto a público especializado como no especializado de modo claro y sin ambigüedades.

[4] Capacidad de aprendizaje autónomo consultando información.

[5] Capacidad para seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas en entornos nuevos.

[6] Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática.

REQUISITOS PREVIOS

Este módulo requiere haber superado como mínimo 30 ECTS de las materias del máster.

RESULTADOS DEL APRENDIZAJE

- Demostrar los conocimientos técnicos, éticos y legislativos para ejercer la actividad profesional en el ámbito de la seguridad de la información.

- Saber adaptarse de forma eficiente y eficaz a nuevos entornos de trabajo y herramientas no experimentadas con anterioridad
- Conocer el funcionamiento, la organización y la dirección estratégica de los diferentes departamentos que utilizan sistemas de información

Materia
Prácticas
3 ECTS

Contenido obligatorio

- Prácticas profesionalizadoras

Actividades formativas con su contenido en ECTS, su metodología de enseñanza-aprendizaje y su relación con las competencias que debe adquirir el estudiante.

Competencias transverales	Actividades formativas	Nº Créditos ECTS
[1,2,3,4,5,6]	ACTIVIDADES PRÁCTICAS	2,5
	INFORME DE APRENDIZAJE	0,5

Véase una explicación de la metodología de enseñanza-aprendizaje en el módulo 1

Sistema de evaluación de la adquisición de las competencias y sistema de calificaciones

Véase explicación del módulo 1.

Breve descripción de contenidos de cada materia

- **Prácticas profesionalizadoras (3 ECTS):** Por sus características especiales, las prácticas profesionalizadoras no tienen asociadas contenidos específicos. El desarrollo de éstas se nutrirá de los contenidos ya vistos a lo largo de los estudios más la documentación *ad hoc* que se requiera en función del tipo de práctica o tarea a llevar a cabo.

Comentarios adicionales

Uno de los objetivos principales del MISTIC es formar a expertos en seguridad que sean capaces de gestionar, diseñar e implementar nuevas soluciones innovadoras que permitan proteger y reducir el riesgo sobre los activos empresariales. Los estudiantes del máster deben ser capaces de atender las demandas empresariales, y es por ello que es fundamental reforzar el vínculo del máster con el ámbito más práctico y profesional.

Las prácticas del máster están programadas como un módulo obligatorio de las especialidades profesionalizadoras. Las prácticas podrán desarrollarse en alguna de las siguientes modalidades:

- Prácticas vinculadas al entorno profesional
- Prácticas con convenios

<u>Prácticas vinculadas al entorno profesional</u>

Las prácticas vinculadas al entorno profesional consistirán en la ejecución de un trabajo asociado a un problema de origen empresarial. Estos proyectos estarán dirigidos por consultores de perfil profesional que propondrán a los estudiantes la resolución de problemas vigentes y reales en sus empresas. Se realizaran en modalidad on-line dentro del marco del campus virtual de la UOC utilizando la metodología y las

herramientas propias de la empresa que ha originado el proyecto.

La práctica ha de permitir poner en juego algunas de las competencias específicas del máster así como todas las competencias transversales, especialmente el trabajo en equipo. La práctica deberá fijar unos objetivos generales, unos resultados de aprendizaje y un plan de actuación. El profesor responsable de las prácticas será quien determinará en cada caso los criterios e indicadores para su valoración final.

Prácticas con convenios

Una parte considerable de los estudiantes de la UOC actualmente ya está activa en el mercado de trabajo. Es por ello que el MISTIC fomentará que el programa de prácticas profesionalizadoras pueda desarrollarse en el lugar de trabajo del estudiante. Evidentemente, estas prácticas también se sustentarán en el mismo sistema de tutoría, seguimiento y evaluación ya en funcionamiento. De ese modo, se conseguirá fomentar las aptitudes emprendedoras de estas personas al mismo tiempo que se facilitará un mayor vínculo entre la universidad y el sistema productivo.

Módulo del Trabajo fin de máster **21 ECTS OBLIGATORIOS**

COMPETENCIAS Y RESULTADOS DEL APRENDIZAJE QUE EL ESTUDIANTE ADQUIERE CON DICHO MÓDULO

[11] Capacidad para realizar, presentar y defender ante un tribunal interuniversitario, un ejercicio original realizado individualmente consistente en un proyecto integral de Seguridad de las Tecnologías de la Información y de las Comunicaciones de naturaleza profesional o de investigación en el que se sinteticen las competencias adquiridas en las enseñanzas.

[39] Capacidad para determinar las características relevantes de un sistema TIC para su modelado y simulación, así como capacidad para sintetizar y presentar los resultados.

REQUISITOS PREVIOS

Este módulo requiere haber superado como mínimo 30 ECTS de las materias del máster.

RESULTADOS DEL APRENDIZAJE

- Demostrar comprensión detallada en un ámbito especializado dentro de la seguridad de la información.
- Saber analizar diferentes alternativas y elegir la más adecuada, justificando su elección.
- Saber evaluar y discutir decisiones tomadas, ya sea por uno mismo o por otros.
- Elaborar y defender un documento que sintetice un trabajo original en el ámbito de la seguridad de la información.
- Saber transmitir de forma eficiente y eficaz las partes más importantes de un contenido voluminoso a diferentes audiencias.
- Leer y escribir con corrección en inglés

Proyecto especialidades profesionalizadoras **9 ECTS** Trabajo fin de máster	**Proyecto especialidad de investigación** **12 ECTS** Trabajo de fin máster

Actividades formativas con su contenido en ECTS, su metodología de enseñanza-aprendizaje y su relación con las competencias que debe adquirir el estudiante.

Competencias específicas	Actividades formativas	Nº Créditos ECTS
[11]	BÚSQUEDA DE INFORMACIÓN	1
	ACTIVIDADES PRÁCTICAS	2
	REDACCION DE INFORMES	1
	LECTURA DE TEXTOS Y ARTÍCULOS	1,5
	PROYECTO	3
	PRESENTACIÓN ORAL	0,5
[39]	REDACCIÓN ARTÍCULO CIENTÍFICO	3

Nota: las competencias transversales se trabajan paralelamente a las competencias específicas, a través de las actividades formativas indicadas.

Véase una explicación de la metodología de enseñanza-aprendizaje en el módulo 1

Sistema de evaluación de la adquisición de las competencias y sistema de calificaciones

El Trabajo fin de máster, dada su singular naturaleza, requiere un proceso de evaluación diferente al modelo usado en el resto de asignaturas. El estudiante seleccionará su Trabajo fin de máster a partir de un conjunto de trabajos ofertados o realizará una propuesta de definición del mismo. Al estudiante se le asignará un director de Trabajo fin de máster que se encargará de realizar el seguimiento y la evaluación del desarrollo del mismo. Los Trabajos fin de máster de los estudiantes que realicen la especialidad de investigación serán dirigidos por profesores doctores.

El modelo de evaluación del Trabajo fin de máster se basa en un modelo de evaluación continua con el objetivo de realizar un seguimiento personalizado y una evaluación de las competencias generales del trabajo. A tal efecto, se definen tres tipos de actividades evaluativas: actividades de inicio, actividades de seguimiento y actividades de síntesis.

Las actividades de inicio se centrarán en la documentación, búsqueda de información, definición de objetivos del propio proyecto. Todo esto debe dar como resultado el plan de trabajo que el estudiante seguirá durante el desarrollo del mismo. Así, las actividades de inicio tienen por objetivo valorar y/o conocer el conocimiento previo del estudiante, tanto de las competencias instrumentales como de las competencias específicas de otras asignaturas con las que el Trabajo fin de máster esté especialmente vinculado.

Las actividades de seguimiento se corresponden con la ejecución del Trabajo fin de máster propiamente. Durante esta fase el estudiante irá realizando entregas al director del trabajo con el objetivo de facilitar el seguimiento y la evaluación del mismo. Las actividades de seguimiento guían el proceso de aprendizaje y permiten acreditar la adquisición de las competencias previstas y la consecución de los objetivos de aprendizaje fijados. Así, estas actividades constituyen el núcleo del proceso de evaluación e incluyen las tareas para trabajar las diferentes competencias de acuerdo con la tabla definida anteriormente.

Finalmente, el estudiante deberá realizar las actividades de síntesis a fin de cerrar el Trabajo fin de máster. Estas actividades incluyen la entrega de la memoria del trabajo, así como su presentación y defensa. En general, las actividades de síntesis persiguen aplicar las competencias trabajadas a lo largo del proceso con el objetivo de poder hacer una valoración de conjunto.

La evaluación de los Trabajos fin de máster la realizará un tribunal interuniversitario formado por 3 miembros, y como mínimo uno de ellos pertenecerá a una universidad diferente a la del estudiante. El presidente del tribunal de Trabajos fin de máster será el director/tutor del trabajo.

Los alumnos que realicen la totalidad de su trabajo fin de máster en una empresa, deberán entregar una memoria y una presentación de su trabajo en la universidad. Los profesores evaluarán el trabajo del estudiante siguiendo el mismo procedimiento que se ha descrito.

Se han definido dos tipos de Trabajos fin de máster según la orientación de la especialidad cursada por el estudiante: Profesionalizador o Investigación.

- **TFM Profesionalizador (9 ECTS):** El objetivo de esta materia es la elaboración de un trabajo escrito y opcionalmente, un prototipo de software, en los que se pone en práctica y se profundiza en las competencias generales del máster y las transversales de la especialización cursada por el estudiante. Asimismo, durante la elaboración de dicho trabajo se intenta fomentar el desarrollo de competencias similares a las de la práctica profesional. Del mismo modo, resaltar que se hará especial énfasis en los aspectos relacionados con la planificación, seguimiento, búsqueda de información, habilidades comunicativas, su impacto en el mundo real, análisis económico, etc.

- **TFM Investigación (12 ECTS):** En esta materia se ponen en práctica y se profundizan las competencias del módulo de investigación del máster mediante la elaboración de un artículo científico. Además, destacar que en función de la temática del trabajo fin de máster, el estudiante profundizará sus conocimientos en las competencias relacionadas con dicha temática. Durante la elaboración del trabajo se fomentará el desarrollo de competencias para ser un buen investigador, y se sentarán las bases para realizar una tesis doctoral.

ANEXOS : APARTADO 6

Nombre : P6_Professorat_Memoria_MISTIC.pdf

HASH SHA1 : 8qmzf2RcSfiBWZPyRGhKUX25b30=

Código CSV : 4260836826980427097 4038

6. PERSONAL ACADÉMICO

6.1. Profesorado y otros recursos humanos necesarios y disponibles para llevar a cabo el plan de estudios propuesto

La UOC, la UAB, la URV y la UIB disponen de una estructura académica que garantiza el buen funcionamiento del máster y un programa docente de calidad.

De acuerdo con la ordenación académica de la UOC, los profesores responsables de asignatura se encargarán de la planificación, definición de los contenidos y recursos, y del proceso de evaluación del estudiante, así como de la selección y coordinación de los docentes colaboradores de cada asignatura. Estas funciones serán asumidas por profesorado de la UOC, UAB, URV y UIB según establece el convenio de colaboración (anexo 1).

La dirección académica del programa se encargará a un profesor doctor de los Estudios de Informática, Multimedia y Telecomunicación de la UOC.

La gestión del programa será asumida por las diferentes áreas de gestión de la UOC, que cuenta en la actualidad con más de cuatrocientos profesionales contratados, de perfiles diversos y divididos funcionalmente en áreas de especialización, que se configuran como ámbitos de apoyo a la actividad docente: Área de Operaciones de Gestión Docente, Área de Incorporación y Seguimiento del Estudiante, Área de Biblioteca, Área de Alumni, Área de Servicios al Estudiante, Área de Personas, Área de Planificación y Evaluación y Unidad de Recursos de Aprendizaje.

6.1.1. Personal académico disponible

El personal académico del máster está formado por:

- Profesorado de la UOC, UAB, URV y UIB
- Docentes colaboradores

Profesorado

Coordinación

Los Estudios de Informática, Multimedia y Telecomunicación de la UOC serán los responsables de la coordinación del Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones. Estos Estudios cuentan en la actualidad con un total de 50 profesores a tiempo completo. Los estudios están dirigidos por el director de estudios, que es el responsable de toda la oferta de los estudios y es miembro de la Comisión Académica.

De los 50 profesores a tiempo completo que conforman los Estudios, un 66% son doctores. De éstos últimos, un 70% ha obtenido la evaluación positiva de la Agencia para la Calidad del Sistema Universitario de Cataluña (AQU).

En relación a la experiencia del profesorado, cabe destacar que un 38% cuenta con más de 10 años de experiencia docente, mientras que un 50% lleva entre 5 y 10 años realizando dichas funciones.

En lo referente a su experiencia investigadora, la UOC está actualmente en proceso de definición de las categorías investigadoras de su equipo docente y, por el momento, 10 profesores disponen de un tramo de investigación. Asimismo, es importante destacar que los 50 profesores de los Estudios de Informática, Multimedia y Telecomunicación son activos en investigación y que la mayoría forma parte de redes profesionales o científicas de su ámbito de conocimiento, tanto a nivel nacional como internacional. A pesar de que los Estudios se crearon hace poco más de diez años, la participación en redes científicas ha aumentado a buen ritmo y en la actualidad se participa en un buen número de convocatorias competitivas de investigación (programa Consolider-Ingenio 2010, Plan Nacional I+D, Proyectos del VIº y VIIº programas marco de investigación y desarrollo de la Comisión Europea y proyectos FIT del Ministerio de Industria, Turismo y Comercio, entre otros)

Finalmente, hay que mencionar que un 40% posee experiencia profesional diferente a la académica o investigadora, sea en el ámbito empresarial o en el de la administración pública.

Dirección académica

Tabla resumen CV					
Profesorado	**Categoría / nivel contractual**	**Titulación académica**	**Líneas de investigación**	**Experiencia académica y/ o profesional**	**Ámbito del conocimiento**
Rifà Pous, Helena (UOC)	Profesor agregado (UOC)	Doctora en Telecomuni-caciones	Seguridad en redes inalámbricas (ad hoc, cognitve), redes distribuidas, PKI	Experiencia académica (5-10) y profesional (5-10)	Redes de telecomunicación, seguridad en aplicaciones

Relación de profesorado dedicado al Máster
A continuación se presenta una relación del profesorado que participará en el despliegue del MISTIC.

Tabla resumen CV profesorado del máster					
Profesorado	**Categoría / nivel contractual**	**Titulación académica**	**Líneas de investigación**	**Experiencia académica y/ o profesional**	**Ámbito del conocimiento**
Arnedo Moreno, Joan (UOC)	Profesor agregado (UOC)	Doctor en Informática	Redes P2P, seguridad en peer groups, seguridad en JXTA	Experiencia académica (5-10) y profesional (1-5)	Redes, seguridad, programación
Castellà Roca, Jordi (URV)	Profesor agregado (AQU)	Doctor en Informática	Protocolos criptogràficos, Seguridad en comercio electrónico (pagos electrónicos),	Experiencia académica (5-10) y profesional (5-10)	Redes de computadores, Seguridad, Criptografia, Privacidad,

			Privacidad, Votación electrónica, y Detección de fraude e intrusiones.		Programación
Garrigues Olivella, Carles (UOC)	Profesor agregado (UOC)	Doctor en Informática	Desarrollo asistido de aplicaciones, Protección de agentes móviles, Sistemas distribuídos, Código móvil, Entornos ubicuos	Experiencia académica (1-5) y profesional (1-5)	Seguridad informática, Redes de computadores, Legislación informática
Herrera Joancomartí, Jordi (UAB)	Profesor agregado (AQU)	Doctor en Matemáticas	Seguridad en redes ubicuas, redes sociales, seguridad de la información	Experiencia académica (+10) y profesional (1-5)	Criptografía, seguridad de la información, seguridad en redes
Rifà Coma, Josep (UAB)	Profesor catedrático (ANECA)	Doctor en Matemáticas	Criptografía, teoría de códigos, combinatoria	Experiencia académica (+10)	Teoría de la información, criptografía, codigos
Robles Martínez, Sergi (UAB)	Profesor titular (ANECA)	Doctor en Informática	Seguridad en agentes móviles, sistemas de detección de intrusiones, seguridad en redes DTN	Experiencia académica (+10)	Ingeniería del software, redes
Serra Ruiz, Jordi (UOC)	Profesor (UOC)	Ingeniero Informático, DEA	Seguridad de la información y seguridad en redes, Software y conocimientos libres	Experiencia académica (+10) y profesional (1-5)	Software libre, Seguridad informática, Sistemas operativos
Serratosa Casanelles, Francesc (URV)	Profesor titular (ANECA)	Doctor en Informática	Reconocimiento de patrones, visión por computador, biometría	Experiencia académica (+10)	Computadores, Biometría
Ferrer Gomila, Josep Lluís (UIB)	Profesor titular (ANECA)	Doctor en Informática	Comercio electrónico, protocolos criptográficos	Experiencia académica (+10)	Ingeniería telemática

Descripción de las categorías y nivel contractual del profesorado

La relación contractual del profesorado de la UOC es de carácter laboral y tiene definidas las siguientes categorías con sus funciones asociadas.

- Profesor ayudante: se trata de una posición inicial de profesorado, en la que se empiezan a desarrollar tareas docentes combinadas con la formación doctoral.

- Profesor: es la posición que ocupa el profesorado doctor que está en proceso de desarrollo de sus capacidades docentes y de investigación, con especial énfasis en el modelo educativo de la UOC y en las líneas de investigación prioritarias establecidas por la universidad.

- Profesor agregado: es la posición que ocupa el profesorado con unas capacidades docentes y de investigación evidenciadas y acreditadas (con especial énfasis en el modelo educativo de la UOC y sus objetivos de innovación e investigación). Los profesores agregados cuentan con la evaluación positiva emitida por la Agencia para la Calidad del Sistema Universitario Catalán (AQU) como profesores de la UOC.

- Catedrático: únicamente puede acceder a esta categoría el profesorado agregado de la UOC con una carrera docente e investigadora plenamente consolidada o bien los profesores procedentes de otras universidades que dispongan de unos requisitos equivalentes.

Las categorías y funciones del profesorado de la UAB, URV y UIB son las correspondientes a los perfiles de profesorado de las universidades públicas españolas y, en el caso de la UAB y URV, también los perfiles de profesorado aprobados por la Generalitat de Catalunya. Los profesores de las universidades públicas españolas pueden ser funcionarios (en las categorías de profesores titulares de escuela universitaria, profesores titulares de universidad, catedráticos de escuela universitaria y catedráticos de universidad) o bien contratados (en las categorías de ayudante, profesor ayudante doctor, profesor contratado doctor, profesor asociado, profesor visitante y profesor emérito). En ambos casos, el acceso se realiza mediante concursos públicos. Los candidatos deben poseer la acreditación válida para el puesto emitida por la Agencia Nacional de Evaluación de la Calidad y Acreditación (ANECA). Por otro lado, la Generalitat de Catalunya, establece unas categorías laborales estables de profesorado permanente (catedrático, agregado y colaborador). Los profesores contratados por esta vía han sido acreditados por la Agencia para la Calidad del Sistema Universitario Catalán (AQU).

Docentes colaboradores

En función del número de estudiantes matriculados cada semestre, los profesores cuentan con la colaboración de los tutores y de los colaboradores docentes, encargados de prestar la atención docente individualizada a los estudiantes y del proceso de evaluación. La estructura académica del MISTIC contará con las figuras de docentes colaboradores y tutores de la UOC para el desarrollo de la actividad docente. La relación de estos colaboradores con la UOC se formaliza mediante un contrato civil de prestación de servicio o bien en el marco de convenios que la universidad coordinadora tiene firmados con otras universidades.

Funciones

El colaborador docente actúa como agente facilitador del aprendizaje, por lo que hace de mediador entre los estudiantes y los diferentes materiales didácticos en el contexto del Campus

Virtual. Su actuación tiene que servir de estímulo y de guía a la participación activa de los estudiantes en la construcción de sus conocimientos, y tiene que permitir, al mismo tiempo, que el proceso de enseñanza se ajuste a los diferentes ritmos y posibilidades de los estudiantes. Los ámbitos básicos de actuación que caracterizan a los diferentes encargos de colaboración docente agrupan el desarrollo de las siguientes acciones.

- Llevar a cabo tareas de orientación, motivación y seguimiento.
- Tomar iniciativas de comunicación con las personas asignadas que favorezcan un primer contacto y, periódicamente, la continuidad de una relación personalizada.
- Hacer un seguimiento global del grado de progreso en el estudio de la acción formativa desarrollada y valorar los éxitos y las dificultades que ha encontrado el estudiante.
- Coordinarse con el profesor responsable de la asignatura y mantener contactos con otros colaboradores docentes de la misma materia o titulación.
- Resolver consultas individuales generadas a lo largo del programa de formación: dudas sobre contenidos o procedimientos, decisiones sobre la evaluación, solicitudes de ampliación de información o de recursos complementarios, etc.
- Atender consultas sobre incidentes en el estudio o seguimiento de la acción formativa.
- Dirigir a los estudiantes a las fuentes o personas más adecuadas, con respecto a consultas generales o administrativas que sobrepasan sus atribuciones.
- Desarrollar la evaluación de los aprendizajes adquiridos durante el proceso, en función del tipo de evaluación diseñada por el profesor responsable de la asignatura.

Los profesores de la UAB y URV realizarán las funciones de docente colaborador de como mínimo una aula de las asignaturas de las que son responsables.

El tutor, por su parte, tiene el encargo de orientar, guiar y asesorar al estudiante sobre cuestiones relacionadas con los siguientes aspectos.

- La planificación de su estudio.
- El diseño de su itinerario curricular.
- El ajuste de su ritmo de trabajo a sus posibilidades reales.
- El conocimiento de la normativa académica.
- El conocimiento del calendario académico.
- El conocimiento de los derechos y los deberes de los estudiantes y de los canales de atención que tienen a su disposición.
- El conocimiento del funcionamiento de la institución en términos generales.

Perfil de los docentes colaboradores

El MISTIC sustituirá el máster propio en "Seguridad informática" que la UOC ofrece desde el curso 2004/05. Los docentes colaboradores y tutores del nuevo máster tendrán un perfil similar al de los docentes que actualmente realizan dichas funciones en el máster propio, de los cuales un 50% cuenta con experiencia docente y un 67% con experiencia profesional en el ámbito de docencia del máster.

Asimismo, se garantizará que todos los docentes colaboradores de la especialidad de investigación sean doctores, mientras que en las especialidades profesionales se priorizarán aquellos perfiles con experiencia profesional en el ámbito en el que realizarán la docencia.

Como hemos apuntado, la necesidad de tutores y colaboradores docentes viene determinada por el número real de estudiantes matriculados. Estas necesidades se determinan en cada curso y, a partir de la definición de los perfiles académicos y profesionales previstos por los estudios, se inicia la convocatoria para la selección de docentes colaboradores dando publicidad tanto en medios públicos como en el propio sitio web de la universidad.

Movilidad de profesorado

Las tres universidades participantes en el máster poseen la Carta universitaria Erasmus, concedida por la Dirección General de Educación y Cultura de la Comisión Europea.

Este documento abre la puerta a las Universidades para participar como coordinadoras o socias en proyectos y programas europeos, donde es requisito disponer de la Carta universitaria Erasmus. Por medio de estos programas, las instituciones pueden desarrollar actividades de movilidad de profesores, personal investigador, estudiantes y personal de gestión mediante el establecimiento de convenios bilaterales de colaboración con otras universidades que también dispongan de la Carta.

Además la UOC, en el marco de las convocatorias del Plan de ayudas internas del Internet Interdisciplinary Institute (IN3), ofrece ayudas a la movilidad de profesorado e investigadores con el fin de facilitar la asistencia a acontecimientos, reuniones científicas o estancias en otras universidades o institutos de investigación.

En el marco de la Carta universitaria Erasmus, la UOC estudia cómo ampliar y consolidar un conjunto de convenios que aún favorezcan en mayor grado la movilidad del profesorado.

6.1.2. Otros recursos humanos disponibles

El MISTIC cuenta, dentro de los Estudios de Informática, Multimedia y Telecomunicaciones de la UOC, con el apoyo directo de un equipo de gestión formado por los siguientes perfiles:

- Administrador de estudios
- Gestor de actividad de posgrado
- Técnico de gestión académica
- Secretaría

El perfil principalmente implicado en el diseño y el apoyo a la garantía de la calidad de los programas es el administrador de estudios. Como figura de apoyo a la ordenación académica de la universidad y a la Dirección de Estudios, y desde su responsabilidad de gestión, contribuye al alcance de los objetivos académicos y de investigación participando en los procesos de aseguramiento de la calidad tanto docentes como administrativos, en la gestión de equipos, en el apoyo al diseño de programas docentes y a las actividades de análisis, y en la proyección social o difusión derivadas de estas actividades. Esta función se desarrolla de manera coordinada entre todos los administradores de acuerdo con las políticas del Vicerrectorado de Ordenación Académica y Profesorado, bajo la Dirección de Ordenación académica.

ANEXOS : APARTADO 6.2

Nombre : P6_Otros_Recursos_Memoria_MISTIC.pdf

HASH SHA1 : evnoivQ0eTr5WBio9GcVh3C1pZo=

Código CSV : 42608373291104417990909

Como hemos apuntado, la necesidad de tutores y colaboradores docentes viene determinada por el número real de estudiantes matriculados. Estas necesidades se determinan en cada curso y, a partir de la definición de los perfiles académicos y profesionales previstos por los estudios, se inicia la convocatoria para la selección de docentes colaboradores dando publicidad tanto en medios públicos como en el propio sitio web de la universidad.

Movilidad de profesorado

Las tres universidades participantes en el máster poseen la Carta universitaria Erasmus, concedida por la Dirección General de Educación y Cultura de la Comisión Europea.

Este documento abre la puerta a las Universidades para participar como coordinadoras o socias en proyectos y programas europeos, donde es requisito disponer de la Carta universitaria Erasmus. Por medio de estos programas, las instituciones pueden desarrollar actividades de movilidad de profesores, personal investigador, estudiantes y personal de gestión mediante el establecimiento de convenios bilaterales de colaboración con otras universidades que también dispongan de la Carta.

Además la UOC, en el marco de las convocatorias del Plan de ayudas internas del Internet Interdisciplinary Institute (IN3), ofrece ayudas a la movilidad de profesorado e investigadores con el fin de facilitar la asistencia a acontecimientos, reuniones científicas o estancias en otras universidades o institutos de investigación.

En el marco de la Carta universitaria Erasmus, la UOC estudia cómo ampliar y consolidar un conjunto de convenios que aún favorezcan en mayor grado la movilidad del profesorado.

6.1.2. Otros recursos humanos disponibles

El MISTIC cuenta, dentro de los Estudios de Informática, Multimedia y Telecomunicaciones de la UOC, con el apoyo directo de un equipo de gestión formado por los siguientes perfiles:

- Administrador de estudios
- Gestor de actividad de posgrado
- Técnico de gestión académica
- Secretaría

El perfil principalmente implicado en el diseño y el apoyo a la garantía de la calidad de los programas es el administrador de estudios. Como figura de apoyo a la ordenación académica de la universidad y a la Dirección de Estudios, y desde su responsabilidad de gestión, contribuye al alcance de los objetivos académicos y de investigación participando en los procesos de aseguramiento de la calidad tanto docentes como administrativos, en la gestión de equipos, en el apoyo al diseño de programas docentes y a las actividades de análisis, y en la proyección social o difusión derivadas de estas actividades. Esta función se desarrolla de manera coordinada entre todos los administradores de acuerdo con las políticas del Vicerrectorado de Ordenación Académica y Profesorado, bajo la Dirección de Ordenación académica.

El perfil principalmente implicado en la gestión del desarrollo de los programas es el técnico de gestión académica (TGA). Los estudios cuentan con un número determinado de estos profesionales en función del número de programas que ofrecen y del número de créditos desplegados. Existe una dirección coordinada de todos los técnicos de gestión académica de la UOC, en torno a la vicegerencia, con el fin de asegurar una visión transversal de los procesos relacionados con la gestión de la docencia: programación académica semestral, asignación a las aulas de colaboradores docentes, gestión en el aula de los recursos docentes y los materiales, seguimiento de incidencias y gestión de trámites de estudiantes.

Además del personal de gestión directamente implicado en el máster, la UOC pone a disposición de los estudiantes del MISTIC su estructura propia de gestión, que permite dar respuesta a la organización administrativa de los diferentes programas. La gestión se realiza tanto en relación directa con los programas desde diferentes equipos de gestión –como los de Operaciones de Gestión, Servicio a los Estudiantes, Recursos de Aprendizaje, o Planificación y Evaluación, entre otros– como de forma indirecta, desde el resto de grupos operativos que dan servicio en ámbitos como el mantenimiento de los sistemas de información en la universidad o los aspectos de gestión económica.

Los equipos de gestión de la UOC con relación directa con la gestión docente o de programas son los siguientes:

- Área de Operaciones de Gestión Docente
- Área de Incorporación y Seguimiento del Estudiante
- Área de Biblioteca
- Área de Alumni
- Área de Servicios al Estudiante
- Área de Personas
- Área de Planificación y Evaluación
- Unidad de Recursos de Aprendizaje

El Área de **Operaciones de Gestión Docente** (OGD) es el área responsable de posibilitar la gestión docente de la universidad. OGD apoya los procesos de gestión vinculados al profesorado y facilita soluciones técnicas para la correcta impartición de la docencia. Gestiona, además, el entorno virtual y los encargos realizados a los colaboradores docentes, y facilita los materiales en el aula para que la docencia y su evaluación sean posibles.

Gestiona los calendarios y las hojas personales de exámenes y pruebas de síntesis en las que los estudiantes pueden elegir día, hora de sus pruebas principales y la sede en la que quieren realizarlas, y coordina la realización de las pruebas virtuales que realizan estudiantes con necesidades especiales o residentes en el extranjero. Organiza la logística de todas las sedes de exámenes, no sólo en Cataluña sino también en el resto del territorio español, y posibilita los diferentes modelos de evaluación que ofrece la universidad.

OGD realiza también la gestión académica de los expedientes, asegurando su óptima gestión desde el acceso del estudiante a la universidad hasta su titulación. Posibilita los trámites ligados a la vida académica del estudiante, establece calendarios, diseña circuitos que garanticen una eficiente gestión de la documentación recibida, emite los documentos solicitados por los estudiantes (certificados, títulos oficiales, propios, progresivos, etc.),

gestiona la asignación de becas, autorizaciones, convenios de trabajo de final de máster y prácticas, y los traslados de expediente solicitados por el estudiante. Desde OGD se gestiona la tramitación de la evaluación de estudios previos, desde las solicitudes hasta la resolución y sus posibles alegaciones.

El Área de **Incorporación y Seguimiento de los Estudiantes** garantiza la óptima incorporación y acogida de los nuevos estudiantes y de su progresión. Por medio del Campus Virtual, el estudiante accede a toda la información académica necesaria, cuenta con el asesoramiento personal de su tutor, puede visualizar en todo momento el estado de su expediente y tiene la opción de efectuar consultas en línea –incluso las relativas a temas relacionados con la informática de su punto de trabajo o de los materiales. Todo ello debe entenderse como un sistema integral de comunicación y atención que comprende no sólo la información del Campus, sino también un completo sistema de atención de las consultas individuales y un eficaz sistema de tratamiento de quejas, si estas se producen.

El Área es la responsable de los procesos de información pública de los planes de estudios y también, mediante su unidad de Análisis e Investigación de Mercado, del análisis de las necesidades y expectativas de la sociedad en relación con la oferta que pueda desarrollar la UOC.

La tutorización del estudiante se realiza mediante la asignación de un tutor personal para cada estudiante, que le acompañará en sus primeras andaduras en la universidad, así como a lo largo de toda su vida académica. El tutor asesora y orienta a sus estudiantes; de forma permanente, realiza su seguimiento académico, conoce su rendimiento académico y, en definitiva, es conocedor de su progresión en los estudios.

La Universidad facilita también al estudiante un acompañamiento de tipo relacional-social, proporcionando los elementos necesarios para el enriquecimiento de la vida universitaria más allá de lo estrictamente académico o docente. El estudiante encontrará en el Campus Virtual toda una serie de ventajas culturales y comerciales, así como servicios pensados para cubrir sus necesidades. Por ejemplo, tiene la posibilidad de chatear, participar en alguno de los cuatrocientos foros de debate sobre todo tipo de temas, realizar compras por medio de la cooperativa o buscar su promoción laboral y profesional por medio de la bolsa de trabajo.

En el **Área de Biblioteca**, la UOC cuenta con una Biblioteca Virtual, que tiene como principal objetivo proporcionar a estudiantes, docentes e investigadores acceso a la información necesaria para el desarrollo de sus funciones. La Biblioteca Virtual ofrece un conjunto de recursos y servicios a los distintos miembros de la comunidad universitaria y apoya especialmente a los estudiantes en el desarrollo de su actividad de aprendizaje facilitándoles la documentación requerida para superar con éxito la evaluación continua y los exámenes.

El acceso a los contenidos y servicios de la Biblioteca Virtual se realiza mediante la página web, que recoge, además de información general del servicio, el catálogo que da acceso al fondo bibliográfico de la universidad, otros catálogos universitarios nacionales e internacionales, la colección digital (acceso a información en formato electrónico) y servicios que proporcionan acceso directo al préstamo, encargo de búsqueda documental y otros servicios de información a medida.

El **Área Alumni**, creada en el año 2008, es responsable de la comunidad de graduados, creando servicios, formación y actividades orientadas al desarrollo personal y profesional de dicho colectivo.

El **Área de Servicios al Estudiante**, coordina todos los servicios que se ofrecen a los estudiantes a partir del Plan Director de Servicios, garantizar que los estudiantes cuentan con toda la información necesaria para cursar sus estudios en la universidad, y por último de la atención personalizada tanto en relación a los trámites académicos, ayuda informática, y la recogida de las quejas y recomendaciones. Es importante destacar que desde a finales del curso 2007/08 la universidad cuenta con el Defensor universitario, cuyas funciones y designación constan en el artículo 44 de las Normas de Organización y Funcionamiento.

El **Área de Personas** apoya al profesorado en el proceso de selección de los colaboradores docentes y tutores, y en el ámbito de la gestión de su vinculación contractual con la universidad. La contratación de los docentes colaboradores se efectúa por una doble vía: convenios o acuerdos privados con universidades y contratos civiles de prestación de servicios. Anualmente, se abre un proceso de selección ordinario para adaptar los recursos a las necesidades y perfiles requeridos, teniendo en cuenta la evolución de la matrícula. Igualmente, el Área de Recursos Humanos colabora con los órganos de gobierno de la institución, y especialmente con el Vicerrectorado de Ordenación Académica y Profesorado, en todos los aspectos relacionados con la selección, el desarrollo profesional y la vinculación contractual del profesorado, en los términos previstos en las políticas generales de gestión de personas de la universidad y, específicamente, en el documento de política de profesorado.

La **unidad de Recursos de Aprendizaje** es responsable de asegurar la gestión integral de los contenidos desde el proceso de creación a la planificación y producción final, buscando la máxima eficiencia en el proceso y asegurando la calidad de los contenidos.

El **Área de Planificación y Evaluación** está implicada principalmente en los procesos de verificación y evaluación de programas, así como en los procesos de evaluación de la actividad docente del profesorado. También recae en esta unidad el aseguramiento de los sistemas internos de garantía de la calidad.

Por su parte, la UAB y URV ponen a disposición de los estudiantes del MISTIC la estructura propia de gestión de las bibliotecas, salas de estudio y salas de informática.

El **servicio de Biblioteca de la URV** dispone de 61 trabajadores de personal de administración y servicios, número suficiente para su correcto funcionamiento y adecuado para la atención personalizada a los usuarios. Las Salas de estudios de los diferentes Campus están abiertas a toda la comunidad universitaria vigiladas periódicamente por conserjería y por becarios. Estos últimos están físicamente ubicados en las Salas de Usuarios (salas de informática), donde se encargan principalmente de las siguientes funciones: abrir y cerrar la sala, mantener el orden y custodiar los equipos informáticos, asesorar informáticamente y en cuestiones básicas a los usuarios, detectar i comunicar a la dirección de los centros incidencias y necesidades detectadas

En relación al **personal de administración y servicios de la UAB** que de forma directa o indirecta prestarán servicio al nuevo título de Máster, se identifican los siguientes: Apoyo

Informático de la Escuela de Ingeniería (1 técnico responsable y 6 técnicos de apoyo), Biblioteca de Ciencia y Tecnología (1 técnico responsable y 17 personas de apoyo), Gestión Académica, Servicio Logístico y Punto de Información (1 gestor responsable y 10 personas de apoyo), Gestión Económica (1 gestor responsable y 2 personas de apoyo), Administración del Centro (1 administradora laboral y 1 secretaria de dirección), Secretaría de la Dirección (1 secretaria de dirección) y Unidad Integrada de Apoyo Administrativo Departamental (1 administrativo responsable de la unidad y 2 personas de apoyo).

6.1.3. Previsión de profesorado y otros recursos humanos necesarios

En el MISTIC participarán 9 profesores y profesoras (la cifra incluye la directora académica del programa), provenientes de las diferentes universidades que participan en el mismo, así como por las personas implicadas en tareas de gestión detalladas en el apartado 6.1.2. Para llevar a cabo el desarrollo del programa se cuenta, además, con el equipo externo de docentes colaboradores: tutores y colaboradores docentes, en función del número de estudiantes matriculados para cada período docente.

El sistema de selección, formación y evaluación del profesorado y docentes colaboradores de la UOC sigue un proceso claramente definido en el Sistema de Garantía Interno de la Calidad y que queda recogido en el manual correspondiente (AUDIT). El Vicerrector de Política de Universitaria y Profesorado de dicha universidad planifica el proceso de selección de profesorado y docentes colaboradores a partir de las necesidades de despliegue de los programas. Esta planificación es aprobada por el Consejo de Gobierno que hace la convocatoria pública de las plazas y nombra el Comité de Selección, que serán los encargados de seleccionar los profesores y docentes colaboradores en función de los perfiles necesarios y los candidatos presentados.

6.1.4. Mecanismos de que se dispone para asegurar la igualdad entre hombres y mujeres y la no-discriminación de personas con discapacidad

A continuación se detallan los mecanismos de los que disponen las tres universidades participantes en el MISTIC para asegurar la igualdad y la no-discriminación por discapacidad entre sus recursos humanos.

Universitat Oberta de Catalunya (UOC)

Mecanismos de igualdad

1. Agente para la igualdad

La UOC dispone desde 2006 de la figura de una agente para la Igualdad. La agente para la igualdad tiene como responsabilidad velar por la correcta aplicación de la Ley orgánica para la igualdad efectiva entre mujeres y hombres (3/2007), así como desplegar las acciones del plan de igualdad propio de la universidad.
En este sentido, la UOC ha sido pionera con la instauración de esta figura en sus estructuras orgánicas.

2. Plan de igualdad

La UOC dispone desde 2007 de un plan de igualdad para el periodo 2007-2010. Este plan recoge un análisis sociodemográfico sobre la situación del género en la universidad y desarrolla acciones específicas para mejorar las situaciones con mayor desequilibrio entre mujeres y hombres, tanto en el ámbito organizativo (relaciones laborales, lenguaje, marketing, imagen corporativa...) como en el ámbito académico (paridad de género en las comisiones científicas y en los contenidos de las titulaciones, ejes de investigación, etc.).

3. Comisión de género

La UOC dispone desde 2006 de una comisión de género integrada por profesores y profesoras. Dicha comisión participa en la Comisión Interuniversitaria de Género de las universidades catalanas. Tiene el encargo de identificar desequilibrios entre géneros en relación con las cuestiones de ámbito académico y científico (paridad en la representación científica, presencia de la perspectiva femenina en los contenidos y materiales de estudio, etc.).

4. Políticas de recursos humanos

La UOC incorpora la perspectiva de género en la totalidad de las políticas de gestión de las personas (selección, comunicación interna, retribución, contratación, formación y desarrollo) y posee medidas específicas para el fomento de la conciliación entre vida personal y profesional. Es Premio Nacional Empresa Flexible 2007 y participa en diversos foros donde se comparten prácticas sobre igualdad y conciliación.

No-discriminación por discapacidad

En cumplimiento de la legislación vigente, y como medida de integración del colectivo de trabajadores discapacitados, algunos trabajadores de la plantilla de la UOC son personas con una discapacidad reconocida. Para el cumplimiento de dicha medida en toda su extensión, no obstante, se han solicitado además medidas alternativas, que se llevan a cabo en diferentes ámbitos de actividad de la universidad.

También se han establecido acuerdos con diferentes intermediadores del mercado de trabajo que gestionan candidaturas de personas con discapacidad para la publicación de ofertas laborales –entre otros: Fundosa, ONCE, Addecco, Sélect y la red de Oficinas de Trabajo de la Generalitat– con el objetivo de facilitar el acceso a los procesos de selección abiertos a personas con discapacidad.

Universitat Autónoma de Barcelona (UAB)

Desde el año 2006, la UAB dispone de mecanismos para asegurar la igualdad y la no-discriminación por discapacidad entre sus recursos humanos. Concretamente, el 4 de mayo de 2006 se aprobó el “Primer plan de acción para la igualdad entre mujeres y hombres de la UAB”. En dicho plan se especifican los objetivos y las acciones necesarias para promover el acceso al trabajo y a la promoción profesional en igualdad de condiciones. Dicho plan se concreta en los siguientes objetivos i acciones:

Objetivo 1

Garantizar que la normativa de la UAB relativa a los criterios de contratación, de evaluación de currículos y de proyectos de investigación no contenga elementos de discriminación indirecta.

Acciones:

- Revisar los anuncios publicitarios y las convocatorias de la universidad desde la perspectiva de género.
- Presentar desagregadas por sexo los datos de aspirantes y de ganadores de plazas convocadas por la universidad, y de composición de las comisiones.
- Velar por la igualdad en la composición de los tribunales de los concursos de profesorado. Delante de la elección de candidatos con méritos equivalentes, aplicar la discriminación positiva a favor del sexo menos representado.

Objetivo 2
Eliminar la segregación horizontal por sexo en departamentos y facultades.

Acciones:

- Revisar los reglamentos internos de contratación para que no contengan elementos favorecedores de discriminación indirecta.
- Revisar los procedimientos de promoción y contratación para garantizar que no se produce discriminación indirecta de género.

Objetivo 3
Eliminar la segregación vertical por sexo en departamentos y facultades.

Acciones:

- Identificar por sexo el tipo de participación académica y de gestión del profesorado en los departamentos.
- En las nuevas contrataciones o cambios de categoría, en igualdad de condiciones, incentivar el equilibrio entre la proporción de mujeres y de hombres en las diversas categorías del profesorado.

Objetivo 4
Diagnosticar el estado de los becarios y las becarias de la UAB en relación con el sexismo.

Acción:

- Llevar a cabo un estudio monográfico sobre las condiciones de trabajo del colectivo de becarios y becarias por sexo y grupo.

Objetivo 5
Diagnosticar el estado de la plantilla de las empresas concesionarias de la UAB en relación con el sexismo.

Acciones:

- Asegurar que los convenios de la UAB con empresas concesionarias tengan en consideración el acceso a los datos y a la información sobre la política de igualdad de oportunidades y organización del trabajo desde la perspectiva de género.

- Diagnosticar las condiciones específicas de la plantilla de las empresas concesionarias.

Objetivo 6
Fomentar la investigación y la publicación entre las mujeres.

Acción:

- Estimular una presencia creciente de mujeres expertas en los proyectos internacionales.

Objetivo 7
Potenciar la carrera académica de las mujeres.

Acción:

- Impulsar medidas para incentivar que las mujeres se presenten a las convocatorias para la evaluación de los méritos de investigación.

Objetivo 8
Incluir la igualdad como indicador de calidad en los tres estamentos universitarios (personal académico, personal de administración y servicios i alumnado).

Acciones:

- Promover los recursos orientados al asesoramiento psicológico, la prevención y la detección precoz de situaciones de discriminación y violencia de género.
- Recoger la información sobre situaciones eventuales de discriminación, acoso sexual o trato vejatorio a la UAB.

Objetivo 9
Potenciar la presencia pública de las mujeres en el contexto universitario.

Acciones:

- Potenciar el incremento del número de expertas en las comisiones de ámbito supraunivesitario.
    - Incrementar el número de expertas en las comisiones del Claustro de la UAB.
    - Incrementar el número de mujeres entre los expertos, conferenciantes e invitados a los actos institucionales de la UAB, los centros y los departamentos.
    - Incrementar gradualmente el número de profesores visitantes hasta llegar al equilibrio.
    - Incrementar gradualmente el número de mujeres en doctorados honoris causa.

Universitat Rovira i Virgili (URV)

Para garantizar que la contratación del profesorado y del personal de apoyo se realiza atendiendo a los criterios de igualdad entre hombre y mujeres, la URV aplica lo establecido en el convenio colectivo del PDI laboral, según el cual:

Artículo 17. Comisión e selección (…/..).

3. Siempre y cuando la composición de la plantilla del campo de conocimiento lo permita, en igualdad de condiciones, se priorizarán la presencia de personal docente e investigador laboral y la igualdad de género en las comisiones de selección.

Disposición adicional primera. Política de género
1. Las universidades desarrollarán las acciones necesarias e instrumentarán aquellos mecanismos que favorezcan la igualdad de género a la institución, de manera que se priorice el acceso de la mujer a todos aquellos ámbitos y órganos donde actualmente su presencia es deficitaria.

2. Particularmente, en aquello que afecta este convenio, “se impulsarán políticas activas en la selección del personal docente e investigador laboral y de soporte a la carrera académica de las mujeres.”

3. Asimismo, los sindicatos firmantes desarrollarán medidas para favorecer la paridad de género en los órganos de representación colectiva del personal docente e investigador laboral.

Además de la aplicación del convenio colectivo, recientemente la URV ha elaborado, a partir de los resultados indicativos de diversas desviaciones o diferencias que se debían cambiar o mejorar, el “Pla d’Igualtat entre homes i dones de la URV”. Este plan incorpora, considerando el marco legal que afecta y la Ley de Igualdad, una relación de seis ejes con las acciones más adecuadas para alcanzar los objetivos previstos. Dicho plan de igualdad se puede consultar en el siguiente link:

http://wwwa.urv.cat/la_urv/3_organs_govern/secretaria_general/links_claustre/annexos/sessio240507/3_pla_igualtat.pdf

El eje 2 del plan hace referencia al acceso en igualdad de condiciones de trabajo y promoción de profesionales.

Eje 2: El acceso en igualdad de condiciones al trabajo y la promoción profesional. Organización de las condiciones del trabajo con perspectiva de género.

Este eje incluye las siguientes medidas:

Medida 2.1 Revisar los anuncios y las convocatorias públicas de la universidad con perspectiva de género.
Medida 2.2 Presentar desagregados por sexo los datos de aspirantes y las personas seleccionadas convocadas por la universidad y de composición de las comisiones.
Medida 2.3 Velar por el equilibrio en la composición de los tribunales de los concursos de profesorado. Ante la elección de aspirantes con méritos equivalentes, aplicar la acción positiva en favor del sexo menos representado.
Medida 2.4 Revisar los procedimientos de promoción y contratación para garantizar que no se produzca discriminación indirecta de género.
Medida 2.5 Identificar por sexo el tipo de participación académica y de gestión del profesorado en los departamentos.

Medida 2.6 En las nuevas contrataciones o cambios de categoría, en igualdad de condiciones, incentivar el equilibrio entre la proporción de mujeres y de hombres en las diversas categorías del profesorado.
Medida 2.7 Elaborar un estudio sobre el colectivo de becarios y becarias.
Medida 2.8 Introducir en la valoración de los convenios y contratos de la URV con empresas concesionarias su situación sobre política de igualdad de oportunidades entre hombres y mujeres.
Medida 2.9 Promover los recursos orientados al asesoramiento psicológico, la prevención y la detección precoz de situaciones de discriminación y violencia de género.
Medida 2.10 Detectar los riesgos sanitarios y psicosociales que afectan el bienestar de las mujeres.

Con el fin de implicar a centros y departamentos, la URV recoge en el Plan de igualdad las propuestas siguientes:

- Hacer un acto de reconocimiento a la persona, departamento o centro del ámbito URV que se haya distinguido por la defensa de los derechos de las mujeres.
- Presentar, desagregadas por sexo, los datos relacionados con la elaboración de los acuerdos internos de planificación de centros, departamentos e institutos.
- Incentivar que los centros adopten estrategias de captación específicas, especialmente en aquellas enseñanzas actualmente muy feminizados o masculinizados.
- Convocar anualmente una jornada sobre el estado de la investigación en género por ámbitos de conocimiento, centros y/o departamentos.
- Incrementar el número de mujeres entre los expertos, conferenciantes e invitados a los actos institucionales de la URV, los centros y los departamentos.

En lo que concierne al acceso de personas con discapacidad, la URV debe respetar en las convocatorias el porcentaje que la normativa vigente establece en cuanto a la reserva de plazas para personas con discapacidad.

ANEXOS : APARTADO 7

Nombre : P7_Memoria_MISTIC_F2.pdf

HASH SHA1 : ye8RVK4CWuDtKeYp0bKQNi64D7A=

Código CSV : 45903638646068865521746

7. RECURSOS MATERIALES Y SERVICIOS

7.1. Justificación de la adecuación de los medios materiales y servicios disponibles

Espacios docentes y específicos para el aprendizaje

El MISTIC se basa en el modelo de enseñanza a distancia de la Universitat Oberta de Catalunya.

Este modelo, centrado en el estudiante, utiliza las tecnologías de la información y la comunicación (TIC) para facilitarle espacios, herramientas y recursos que le permiten la comunicación y el desarrollo de su actividad académica. El espacio principal donde esto tiene lugar es el Campus Virtual. En él, el aula es el espacio virtual en el que el estudiante accede al plan docente de las asignaturas (objetivos, planificación, criterios de evaluación, actividades y recursos), se relaciona con los profesores y con los compañeros de grupo de modo permanente y vive la experiencia de aprender y de generar conocimiento compartiendo sus ideas o propuestas.

El aula virtual cuenta con tres espacios de comunicación básicos: el tablón del profesor, el foro y el debate. Asimismo, y en lo que se refiere a la evaluación de los aprendizajes, el aula permite el acceso al registro de resultados de la evaluación continua y final de todas y cada una de las asignaturas.

La tipología de aulas para las asignaturas puede ser estándar, de especial dedicación y el trabajo fin de máster (TFM).

En las asignaturas estándar, la acción docente sigue un plan de aprendizaje común, la atención se realiza principalmente por medio de los buzones personales de cada estudiante, los buzones grupales y la dinamización del colaborador docente en el aula. El ratio de estudiantes por aula virtual en las asignaturas estándar es de un máximo de 75 estudiantes.

En las asignaturas con especial dedicación priman los elementos de individualización sobre los grupales, de manera que cada estudiante o grupos reducidos de estudiantes siguen un itinerario de aprendizaje diferenciado. La ratio de estudiantes en las asignaturas con especial dedicación es recomendable que sea inferior a las de las asignaturas estándar.

En las asignaturas de Trabajo fin de Máster (TFM) se precisa realizar un trabajo de seguimiento y tutoría individualizado y personalizado. La ratio de estudiantes por aula en las asignaturas de Trabajo fin de Máster (TFM) es recomendable que también sea inferior a las de la tipología de asignaturas antes mencionadas.

Prácticas profesionalizadoras

Tal como se explicita en el punto 5 de la memoria, las especializaciones profesionales de este máster contemplan la realización de 3 créditos ECTS de prácticas obligatorias en entornos profesionales.

En la descripción de los módulos del máster (apartado 5.3) se establecen los requisitos de formación previos necesarios para que el estudiante pueda formalizar la matrícula correspondiente a las prácticas profesionales.

El tutor orientará al estudiante sobre las prácticas más adecuadas de acuerdo con su perfil, preferencias y expectativas, así como sobre el proceso que hay que seguir para realizar la matrícula de esta materia.

Las figuras internas dedicadas a la gestión de las prácticas son los técnicos de gestión del programa y los técnicos de gestión docente.

Las figuras docentes implicadas en el diseño y desarrollo de los procesos relacionados con las prácticas son el profesor responsable de la asignatura y el colaborador docente de la asignatura.

Los estudiantes que quieran realizar las prácticas en un centro externo a la universidad, deberán presentar su propuesto a la dirección de programa. Ésta (o en quien delegue) validará que tanto el centro como el proyecto sean los adecuados, y se comunicarán al centro las solicitudes asignadas. Para cada uno de estos estudiantes se firmará un convenio de cooperación educativa entre la universidad coordinadora y la empresa u organización donde realizará las prácticas, en el cual se concretará el proyecto a realizar, las condiciones y las personas que harán el seguimiento y la evaluación del estudiante. La Universidad coordinadora tiene los mecanismos adecuados (actividades de difusión de los propios estudios, red de empresas asociadas) para gestionar esta actividad. Igualmente, el perfil del estudiante del máster permite prever que en muchos casos se podrá realizar la actividad en la propia empresa o institución donde trabaja el estudiante, lo cual beneficia en muchos casos tanto al propio estudiante como a la empresa.

Con el fin de realizar los proyectos en colaboración con el entorno empresarial y profesional, la universidad coordinadora dispone de una red de Empresas e Instituciones Asociadas, con las cuales ha suscrito un convenio. A continuación se detalla el listado de empresas e instituciones con las que se ha firmado convenio y que permitirían el desarrollo de las prácticas del máster:

- ABAST SOLUTIONS, S.A.
- ABYLIGHT
- ALTRAN
- ALTRIUM
- ASOCIACIÓN DE TÉCNICOS DE INFORMÁTICA
- ATOS ORIGIN
- AUREN
- BANC SABADELL
- BARCELÓ CORPORACIÓ EMPRESARIAL
- CAIFOR
- CAIXA D'ENGINYERS
- CAIXA GIRONA
- CAIXA SABADELL
- CAJA ESPAÑA

- CAPGEMINI ESPAÑA
- CENTUM
- CONFEDERACIÓN ESPAÑOLA DE CAJAS DE AHORROS
- CONSELL INSULAR DE MALLORCA
- CORPORACIÓ CATALANA DE MITJANS AUDIOVISUALS
- DATADIAR
- DESARROLLO DE TELESERVICIOS
- DIGITAL 360
- DOC6
- DOMINION
- DRECERA
- 2M2 CONSULTING
- EDS ESPAÑA, S.A.
- ELOGIA
- ERCROS
- EVERIS
- EXPECTRA TECHNOLOGY
- FRAPE BEHR
- FUNDACIÓN ONCE
- GENOS OPEN SOURCE
- GLOBALIA
- GRUPO GMV
- GRUPO ICA
- GRUPO INTERCOM
- IBERMÁTICA
- INK CATALUNYA
- INTERNET SECURITY AUDITORS, S.L.
- INTERPARTNER CONSULTING
- IN2
- MICROART
- NEXTRET, S.L.
- OPEN ALLIANCE PROJECT
- PRIMAVERA BUSINESS SOFTWARE SOLUTIONS
- RACC
- RAONA ENGINEERS
- SADIEL
- SETTING CONSULTORIA, S.L.
- SISTEMAS DIGITALES DE TELEFONÍA
- SOFTTEK INFORMATION SERVICES DA. DE CV
- SPECIALIST COMPUTER CENTRES
- STERIA ESPAÑA
- SUN MICROSYSTEMS ESPAÑA
- TECNOCOM ESPAÑA SOLUTION
- TECSIDEL, S.A.
- T-SYSTEMS
- ZURICH

El listado detallado se irá ampliando y modificando en función de las necesidades, tanto de las empresas como de las universidades participantes.

Laboratorio virtual

El MISTIC dispone de dos tipos de laboratorios virtuales, uno en el que se da soporte a las materias asociadas a la especialidad profesional y otro que se utiliza en las materias ligadas a la especialidad de investigación. Estos laboratorios virtuales tienen como objetivo servir de apoyo, y están destinados a vehicular el soporte práctico de las materias que involucran algún tipo de software en su actividad y/o contenidos. Este laboratorio facilita la interacción entre los estudiantes y un docente de laboratorio con el objetivo de tratar cuestiones relacionadas con un lenguaje de programación determinado, problemas de instalación o funcionamiento de un software de base o de aplicación.

En el MISTIC el modelo de educación se desarrolla sobre el entorno de aprendizaje virtual de la UOC, donde la comunicación entre profesores y alumnos se realiza de manera asíncrona a través de Internet. Así pues, este tipo de laboratorio también se realiza en un entorno de educación asíncrona, tanto en el tiempo como en el espacio.

Este laboratorio es un espacio virtual interactivo que incorpora todos los recursos tecnológicos, pedagógicos y humanos necesarios para dar soporte a la realización de las actividades prácticas de las asignaturas y que están adaptados a las necesidades de los estudiantes y profesores. El laboratorio virtual está compuesto de los siguientes recursos:

- Entorno virtual de comunicación: correo electrónico, foros, blog, wiki, chat, videoconferencia, acceso remoto al escritorio, pizarra digital interactiva e información presencial.
- Corrector automático de programas: permite corregir el código fuente, en C, Java o PHP, automáticamente a través de un servidor. También permite detectar copias.
- Máquina virtual: Una máquina virtual es un programa que permite simular máquinas donde se instalan diferentes sistemas operativos (como Microsoft Windows, GNU/Linux, DOS, BSD o Mac OS) simultáneamente en un mismo equipo de trabajo, proporcionando transparencia al estudiante para mantener la compatibilidad con aplicaciones heredadas, reduciendo de esta manera el tiempo de configuración y instalación para realizar las practiques desde su punto de trabajo habitual.
- Software específico: el software de cualquier tipo que necesita el estudiante y que se le envía antes del inicio del curso.

En relación a los recursos pedagógicos y estratégicos utilizados en los laboratorios para el aprendizaje de los estudiantes, se cuenta con:

- Ejercicios prácticos.
- Documentación y materiales de soporte.
- Metodología de aprendizaje.

El profesor de Laboratorio tiene un perfil especializado y muy técnico que ayuda al estudiante en la realización de las prácticas.

La UOC tiene 11 años de experiencia trabajando con laboratorios virtuales en las titulaciones de Informática, Multimedia y Telecomunicación y 7 años de experiencia en la impartición de un máster propio de seguridad, sin que en ningún caso haya representado un problema la adquisición de competencias prácticas a través de dichos laboratorios virtuales.

Recursos de aprendizaje

Los estudiantes tendrán a su disposición todos los recursos de aprendizaje necesarios para alcanzar cada una de las competencias del máster. Todos estos recursos son elaborados por un equipo de expertos de reconocido prestigio en lo que respecta al conocimiento correspondiente a cada asignatura y en la didáctica educativa, de acuerdo con los principios del modelo pedagógico de la UOC.

El material didáctico de las asignaturas se estructura en unidades didácticas o módulos con esquemas de inicio, donde se pueden visualizar los contenidos básicos de cada unidad. Además, los módulos dan acceso a los glosarios, índices bibliográficos, ejercicios de autoevaluación, materiales de lectura, casos prácticos, etc., toda la información necesaria para que los estudiantes alcancen el conocimiento y las competencias definidas por los objetivos de la asignatura.

El material didáctico tiene diversos formatos: web, papel, CD-ROM o DVD. El formato del material didáctico es, en cada momento, el más adecuado para alcanzar los objetivos y las competencias fijadas.

En el caso del MISTIC el uso de software específico es indispensable para la adquisición de las competencias de la titulación. Este software se pone a disposición del estudiante desde el inicio de semestre, bien a través del envío de CD o DVD por correo postal, bien a través del Campus Virtual.

A continuación se detalla el software que se ha planificado para el máster en el momento de la realización de esta memoria. Es importante destacar que esta relación se irá modificando y ampliando según las necesidades de los estudiantes y profesorado y de acuerdo con la evolución que vayan experimentando los ámbitos de conocimiento a los que hacen referencia.

Software	**Asignaturas**
Conexión remota a laboratorio con equipos reales	Seguridad en Sistemas Operativos
Planificación y gestión de proyectos (Open Project / MS Project)	Técnicas de investigación Prácticas profesionalizadoras Trabajo de fin de máster
Hoja de cálculo (Excel / Calc) y Presentaciones (PowerPoint / Impress)	Técnicas de investigación Prácticas profesionalizadoras Trabajo de fin de máster
Procesadores de textos científicos (LaTeX)	Técnicas de investigación Trabajo de fin de máster
Herramientas de Gestión	Técnicas de investigación

Bibliográfica (RefWorks, BibTeX)	Trabajo de fin de máster
Herramientas de análisis cualitativo y cuantitativo (SPSS, Matlab, Scilab, NVivo, Atlas …)	Técnicas de investigación Trabajo de fin de máster

Bibliotecas

Los estudiantes del MISTIC tendrán acceso a las bibliotecas de las tres universidades responsables del Máster (UOC, UAB y URV).

La Biblioteca Virtual de la UOC es accesible por Internet para toda la comunidad universitaria desde el portal de la UOC. Asimismo, se accede a ella directamente desde las aulas del Campus Virtual por medio del espacio *Recursos*, que reúne y proporciona una selección rigurosa y esmerada de recursos básicos y de apoyo, preparada conjuntamente entre el profesorado y el equipo de apoyo de la Biblioteca. Este espacio de recursos está presente en todas las asignaturas, y facilita a los estudiantes el seguimiento de las actividades propuestas y les permite tener una visión global de las fuentes y las herramientas de la rama de especialización. Los recursos que se incluyen en el aula son de tipología diversa: artículos, bases de datos, libros electrónicos, revistas electrónicas, software, ejercicios de autoevaluación, enlaces a la bibliografía recomendada, recursos de información electrónica gratuitos, etc. De esta forma los estudiantes disfrutan de una biblioteca a medida para cada asignatura.

Los recursos del aula y la bibliografía recomendada de la asignatura son revisados cada semestre por el profesor responsable con el apoyo técnico del equipo de Biblioteca, por medio de un procedimiento preestablecido que se inicia dos meses antes del comienzo del semestre académico. Dicha revisión se lleva a cabo de forma centralizada por medio de una herramienta de atención de incidencias definida institucionalmente mediante la cual el profesorado hace llegar a la Biblioteca las modificaciones que hay que realizar en dicho espacio. La Biblioteca es responsable de gestionar esta documentación: incorporar, modificar o dar de baja títulos en la bibliografía recomendada; incorporar, modificar o dar de baja fuentes de información o ejercicios de apoyo, etc.

Este máster permite alcanzar competencias de un alto grado de especialización técnica y científica. Para conseguir estos objetivos, se ha previsto la utilización intensiva de los siguientes recursos disponibles en la Biblioteca Virtual de la UOC:

Recurso	**Asignaturas**
Acceso a base de datos de consultoría y prospectiva tecnológica (Gartner)	Trabajo de fin de máster
Acceso a bases de datos de publicaciones científicas (ISI Web of Knowledge, ACM Portal, IEEExplore, Elsevier Science Direct, SpringerLink, Emerald, Google Scholar…)	Metodologías de investigación Técnicas de investigación Trabajo de fin de máster

La Universitat Autónoma de Barcelona pone a disposición de los estudiantes del Máster los recursos bibliográficos de la Escuela de Ingeniería de esta universidad, ubicados en la Biblioteca de Ciencias, Biociencias y de Ingenierias.

Su fondo especializado en las diferentes disciplinas de las ciencias puras y aplicadas está constituido por más de 100.000 libros y cerca de 3.300 títulos de revistas. Por otro lado la Biblioteca digital de la UAB pone a disposición de todos los usuarios del campus un conjunto de recursos documentales de casi 12.000 títulos de revistas electrónicas y 8.700 libros digitalizados.

Esta biblioteca también organiza sesiones de formación de usuarios para que los alumnos saquen el máximo rendimiento de los recursos que se les ofrece. La mayor parte de los recursos bibliográficos pueden consultarse libremente en las salas llamadas de primer y segundo ciclo, donde hay 30 puntos informatizados con conexión a Internet.

Asimismo, la biblioteca cuenta con el servicio de préstamo, que permite a los usuarios disponer de material bibliográfico durante dos semanas. También se ofrece un servicio de préstamo de ordenadores portátiles dentro del recinto de la propia biblioteca por dos horas renovables y de memorias USB por tres días no renovables.

La URV, por su parte, pone a disposición la Biblioteca del Campus Sescelades**,** con una superficie de 1.900 m^2 y capacidad para unas 500 personas. Actualmente esta biblioteca cuenta con unas 1.500 revistas y más de 90.000 ejemplares de libros. A través de la página web, se puede acceder electrónicamente a los catálogos de las más prestigiosas editoriales científicas y de Ingeniería. Además del tradicional servicio de préstamo de libros y revistas, esta biblioteca dispone también de un servicio de préstamo de ordenadores portátiles. Adjuntos a la biblioteca hay espacios de lectura y trabajo, con un área de 1.036 m^2. Toda la biblioteca cuenta con conexión a la red inalámbrica y cableada.

La biblioteca ha iniciado desde hace años un profundo cambio y adaptación a las nuevas tecnologías y metodologías docentes para transformarse en un Centro de Recursos para el Aprendizaje y la Investigación. Este centro será el espacio donde estudiantes y PDI encontrarán de forma integrada los productos y servicios que necesitan para desarrollar sus actividades de aprendizaje, docencia, investigación y formación continuada. Se pretende convertir la biblioteca en un entorno que haga posible la integración de servicios informáticos, bibliotecarios, pedagógicos, de información institucional, audiovisual y lingüística, entre otros. Para ello se han habilitado salas de trabajo que permiten a los estudiantes y PDI del centro aprovechar los recursos disponibles:

- Sala de usuarios: en la planta baja del edificio de la biblioteca, el centro cuenta con una sala de informática de 378 m^2 con 106 ordenadores para los estudiantes. El curso 2008-09 se ha puesto a disposición de los estudiantes un servicio de impresión en la modalidad de prepago que se ha adjudicado mediante el correspondiente concurso público, a una empresa externa. Ocupa aproximadamente 550 m^2 y está equipada con más de 100 ordenadores. Dispone de un servicio de impresión de prepago.

- Sala de estudios: En la misma planta baja del edificio de la biblioteca, el centro dispone de una sala de estudio de 1.100 m^2. Esta sala está a disposición de los alumnos para estudiar de forma individual o colectiva y cuenta con conexión a la red inalámbrica y cableada. Su capacidad es de 324 plazas, distribuidas en mesas de cuatro, seis, ocho y doce personas.

Sedes

Los estudiantes del MISTIC podrán hacer uso de la red de sedes y centros de información de la UOC, los cuales ofrecen sus servicios a los futuros estudiantes, estudiantes y conjunto de la comunidad universitaria.

Estos servicios son:

- Asesoramiento personalizado respecto de la oferta formativa de la universidad.
- Apoyo a la gestión académica, con la entrega y recogida de documentación, entrega de títulos, resolución de dudas académicas, etc.
- Servicio de retorno y préstamo bibliográfico.
- Centro de recursos, con la puesta a disposición y utilización en los centres de apoyo de conexión a internet, equipamiento audiovisual, salas de estudio y salas de reuniones.

La UOC cuenta en la actualidad con un total de 17 sedes.

Las sedes participan además en determinados procesos de la universidad como son, la organización de las sedes pruebas finales presenciales, la organización de actividades y la dinamización de les Comisiones de centro formadas por estudiantes y graduados de su territorio.

Para hacer más efectiva la presencia en el territorio, la UOC cuenta también con los puntos de información como extensión de las sedes que permiten completar el despliegue territorial. Los servicios que ofrecen son:

- Información general sobre la oferta formativa de la Universidad.
- Devolución de los préstamos del fondo bibliográfico.
- Conexión a Internet y uso de salas de estudio.

Actualmente existen más de 40 puntos de información. En total pues la universidad cuenta con la siguiente red territorial:

17 sedes
Manresa, Salt, Barcelona, Reus, Lleida, Sabadell, Terrassa, Sant Feliu de Llobregat, Tortosa, Vilafranca del Penedès, Vic, L'Hospitalet del Llobregat, Granollers, Vilanova i la Geltrú, Madrid, Sevilla y Valencia.

47 centros de información
Amposta, Andorra, Badalona (Can Casacuberta y Llefià), Banyoles, Barcelona (Les Corts, Vila Olímpica, Sant Andreu y Horta-Guinardó), La Bisbal d'Empordà, Berga, Blanes, Ciutadella, Coma-ruga, Eivissa, Figueres, Gandesa, L'Alguer, Igualada, Manacor, Martorell, Mataró,

Montblanc, Mora d'Ebre, Olot, Palafrugell, La Pobla de Segur, Puigcerdà, Ripoll, Rubí, Santa Coloma de Farners, La Seu d'Urgell, Solsona, Sort, Tarragona, Tàrrega, Valls, Barberà del Vallès, Manlleu, Masquefa, Ribes de Freser, La Fatarella, La Pobla de Segur, Santa Bàrbara, Vallirana, Vidreres, Tremp y Pont de Suert.

Los mecanismos existentes de mejora y supervisión de los servicios que se ofrecen en esta red se detallan a continuación:

- Comisiones de sedes, formada por los representantes de los estudiantes de la zona territorial que representa cada centro de apoyo, escogidos por votación entre los propios estudiantes. Las funciones de las comisiones de centro (que preside el director del centro correspondiente) son proponer mejoras de los servicios que se ofrecen y proponer actividades a realizar.
- Buzón de sugerencias en cada centro de apoyo.
- Plan de mantenimiento anual de los espacios (infraestructuras), que supervisan los diferentes directores territoriales.
- Plan de mantenimiento de las infraestructuras tecnológicas (sustitución de los equipos informáticos cada 5 años como máximo).
- Encuesta a los estudiantes usuarios de los centros de apoyo.
- Detección de las necesidades de los estudiantes directamente a través de los comentarios que envían al personal de atención de los centros de apoyo.

Inversiones

Por la propia naturaleza de la UOC, la universidad coordinadora, no existen inversiones específicas para los programas.

Las inversiones en equipamientos de la UOC son de carácter general y se distribuyen en inversiones en las oficinas de gestión, en las inversiones en los centros de soporte y sus bibliotecas, y en las inversiones en aplicaciones informáticas y el Campus Virtual (en el que se imparte la docencia) y que afectan por igual a todos los programas de formación.

Seguridad

El espacio donde se desarrolla toda la actividad docente es el Campus Virtual de la UOC, que es también el espacio de comunicación.

El Campus Virtual ha experimentado desde su puesta en marcha sucesivas mejoras para dar respuesta a las necesidades de la comunidad universitaria. Así, el Campus ha garantizado el acceso de los estudiantes a pesar del incremento de usuarios (de los 200 usuarios del curso 1995-1996 a los más de 40.000 del curso 2006-2007), para lo cual ha incrementado las funcionalidades en relación con la actividad docente y de investigación, y ha mejorado los planes de seguridad y confidencialidad de los usuarios, así como su accesibilidad y usabilidad.

La Universidad dispone de un sistema de seguimiento de las incidencias que se producen en el Campus Virtual que permite conocer y resolver los errores y paradas que puedan haber perjudicado la accesibilidad de los estudiantes. Los niveles de servicio se sitúan por encima del 99%, estándar de calidad de servicio en internet.

7.2. Previsión de adquisición de los recursos materiales y servicios necesarios

Política de financiación y asignación de recursos

La Universitat Oberta de Catalunya inició el año 1998 el establecimiento de los compromisos presupuestarios con la Generalitat de Catalunya por medio de los correspondientes contratos programa. Este instrumento permite valorar la actividad que se llevará a cabo por parte de la universidad, que incluye la programación de nueva oferta, y establece las necesidades de transferencia anual para la realización de dicha actividad en el marco estratégico de la universidad y condicionado a la implantación de acciones de mejora de la calidad.

El 5 de marzo de 2009, la Universitat Oberta de Catalunya firmó un nuevo Contrato Programa con el Departamento de Innovación, Universidad y Empresa, para los periodos de 2009 a 2014, que recoge los objetivos de adaptación de la actual oferta formativa de la universidad –que es donde queda circunscrita la propuesta de máster que aquí se presenta–, así como la creación de nueva oferta, también en el marco de la implantación del EEES, y las necesidades de subvención que este despliegue implica.

Estas necesidades se determinan a partir de la relación de costes para el desarrollo de la actividad en lo que se refiere a transferencia corriente, y a las necesidades de inversión en materiales didácticos para el aprendizaje, en tecnología y aplicaciones para el Campus virtual y en infraestructura tecnológica para su mantenimiento, por lo que corresponde a la subvención de capital.

Las necesidades de materiales didácticos para el programa que se presenta, se determinan anualmente a través del Plan de despliegue de la titulación que se refleja en esta memoria en el capítulo 10.

Plan de viabilidad

El plan de viabilidad económica que se presenta, tiene en cuenta la estructura de gasto variable directamente asociado a la titulación en cada curso y que se detalla bajo los epígrafes de:

- tutoría y docentes colaboradores, cuya necesidad viene determinada por el número real de matriculados,
- replicación y envío de materiales docentes (gastos no asociados a la inversión), y
- comisiones de cobro de la matrícula (gastos financieros).

Estos capítulos se rigen por una fórmula de gasto variable, asociada al número de alumnos y créditos de matrícula. La evolución de la matrícula y la rematrícula de estudiantes y créditos para el Programa se han estimado por parte del Área de marketing de la universidad y sus valores permiten determinar el ingreso estimado del programa derivado de los derechos de matrícula.

Además se han estimado las inversiones para la elaboración de los nuevos recursos docentes del programa.

El cálculo que se presenta no incluye las necesidades transversales de gestión y tecnológicas, así como las necesidades de profesorado detectadas.

MISTIC				
	2011	**2012**	**2013**	**2014**
Estudiantes nueva incorporación	50	93	96	98
Estudiantes rematriculados	0	92	187	206
Estudiantes computables	47	179	275	296
INGRESOS DE MATRICULA	36.930	141.064	220.429	241.852
GASTOS VARIABLES	11.334	47.915	79.978	89.478
Tutoría	2.400	10.273	17.138	19.170
Consultoría	7.499	32.056	53.588	59.941
Gastos en materiales	1.310	5.091	8.447	9.449
Gastos financieros y otros	125	495	805	918
INVERSION EN RECURSOS DOCENTES	124.774	219.962	92.088	0

c 3727

Convenio de colaboración

Empresa asociada UOC

Universitat Oberta de Catalunya

Auditoría y Consultoría de Privacidad y Seguridad SL

PARTES

De una parte, la Universitat Oberta de Catalunya, (de ahora en adelante UOC), domiciliada en Barcelona, avenida del Tibidabo, 39, representada en este acto por la señora Imma Tubella Casadevall, que actúa como rectora.

De otra parte, Auditoria y Consultoria de Privacidad y Seguridad SL (de ahora en adelante PriSE), con el CIF B91827733, domiciliada en Sevilla, Plaza Ruiz de Alda 11, representada en este acto por el señor Daniel García Franco, que actúa como administrador.

MANIFESTACIONES

1. La Fundació per la Universitat Oberta de Catalunya (de ahora en adelante FUOC), con CIF G-60-667813, es titular de la Universitat Oberta de Catalunya, reconocida por la Ley del Parlamento de Cataluña 3/1995, de 6 de abril. El Patronato de la FUOC otorga poderes legales al Sr. Òscar Aguer Bayarri como director de la FUOC y gerente de la UOC el 22 de diciembre de 2005 y los eleva a públicos por la notaria de Barcelona Sra. M. Isabel Gabarró Miquel, según escritura con número de protocolo 4128 del 22 de diciembre de 2005.

2. La UOC es una universidad surgida de la sociedad del conocimiento que tiene por misión facilitar la formación de las personas a lo largo de la vida, utilizando las nuevas tecnologías para superar las barreras del tiempo y del espacio. Es objetivo de la UOC hacer avanzar la creatividad de las personas y el progreso de la sociedad, impulsando la investigación en torno a la sociedad del conocimiento.

3. La UOC tiene la voluntad de establecer alianzas con empresas e instituciones que compartan sus objetivos y valores con el objetivo de crear una red relacional que permita el intercambio de experiencias orientadas al desarrollo de los profesionales y a la mejora de la competitividad de las organizaciones en el marco de la sociedad del conocimiento, y con esta finalidad se crea el canal relacional Empresas Asociadas UOC.

4. PRiSE es una empresa dedicada a la privacidad, identidad digital y seguridad informática, enmarcada en dos linias diferenciadas, ambas incorporando ofertas de formación:

a. Identidad digital: el equipo de PRiSE ha participado en el diseño y desarrollo de escenarios como una federación de identidad digital (el Servicio de Identidad de RedIRIS), acceso federado a recursos externos que no permitían este tipo de acceso (acceso Web of Knowledge de la FECYT) o bibliotecas virtuales (biblioteca virtual del CSIC). Esto ha permitido obtener un conocimiento técnico muy elevado de estándares como SAML o WS-Trust y de software como Shibboleth, PAPI o simpleSAMLphp.

b. Protección de datos: PRiSE ofrece un catálogo de servicios muy amplio alrededor de la protección de datos dentro de una infraestructura telemática de una empresa. Aunque la protección de datos viene definida por la ley orgánica 15/1999, de

13 de Diciembre, PRiSE apuesta por una definición del escenario desde el punto de vista técnico, por lo que ofrece auditorías y adaptaciones incluyendo soluciones técnicas.

5. PRiSE tiene interés en los mismos objetivos y valores de la UOC y es sensible a ellos, dado que nace de expertos que se han formado tanto en la vida de estudiante como profesionalmente en ambientes universitarios. Y al mismo tiempo se quiere vincular con la Universidad, implicándose y participando de forma activa y comprometida.

6. La UOC y PRiSE quieren firmar un convenio de empresa asociada UOC, en el cual se defina el marco general de colaboración y se apunten los canales de comunicación y de intercambio que quieren impulsar y la línea de compromisos y privilegios que quieren desplegar para hacer prosperar este vínculo.

ACUERDOS

Primero. Este convenio tiene por finalidad nombrar a PRiSE empresa asociada UOC y establecer las condiciones sobre cuya base deberá regirse este vínculo, de forma que se cree un buen marco de relación que nos permita fortalecer las colaboraciones establecidas hasta ahora y, sobre todo, emprender nuevas colaboraciones que nos ayuden a explorar nuevas oportunidades en alguna de las siguientes líneas:

- Asesoramiento en la elaboración de planes formativos para la empresa.
- Diseño y desarrollo de formación a medida.
- Colaboración en el diseño y desarrollo de programas formativos.
- Diseño, desarrollo o dinamización de entornos y comunidades virtuales.
- Colaboración en proyectos de investigación e innovación.
- Colaboración en -o patrocinio de- proyectos o actividades presenciales o virtuales.
- Participación como miembro activo en el consejo asesor de un programa formativo.
- Creación de proyectos de cooperación para el desarrollo y voluntariado virtual solidario.

Segundo. En virtud de este convenio y como empresa asociada UOC, PRiSE disfrutará de -y asumirá- las **prestaciones** y los **compromisos** indicados a continuación, cuyas condiciones se concretarán, siempre que sea necesario, mediante un convenio o una adenda específica, redactados de mutuo acuerdo.

1. Ayudas económicas en las matrículas de formación continua: los profesionales de PRiSE disfrutarán de una beca para el estudio, que se descontará del precio de la matrícula de los programas de formación continua que acuerden ambas instituciones y que dependerá del número de profesionales matriculados.[1]
2. Canal personalizado de atención: PRiSE tendrá un canal personalizado de atención, con un interlocutor único, que buscará los dispositivos más factibles en la gestión de matrículas y en el seguimiento posterior de la formación.
3. Acceso privilegiado a la información: la UOC informará puntualmente a PRiSE de los programas formativos, novedades y noticias que genera la Universidad. Y PRiSE se compromete a ofrecer los mecanismos para que esta información trascienda y se difunda al conjunto de su organización.
4. Acceso privilegiado al conocimiento: los profesionales vinculados a PRiSE podrán consultar los libros que la UOC tiene en catálogo, desde las bibliotecas presenciales de los centros de apoyo de la UOC. Asimismo, podrán asistir a los actos de presentación de resultados de proyectos de investigación, a las actividades presenciales, a congresos, conferencias y mesas redondas que organiza la Universidad para difundir conocimiento, y todo ello en las mismas condiciones que el colectivo de la comunidad de la UOC.
5. Servicio periódico de noticias temáticas: los profesionales de PRiSE se podrán suscribir gratuitamente al servicio de noticias, en forma de boletín de información (*Newsletter*), distribuido por la biblioteca virtual de la UOC, con el fin de estar al día en las áreas de conocimiento de las que la UOC es experta.
6. Participación en los actos sociales de Empresas Asociadas UOC: los representantes de PRiSE podrán asistir a los actos sociales que la UOC organiza en honor a las empresas asociadas UOC, con el objetivo de fortalecer los vínculos, fomentar las relaciones institucionales, establecer relaciones en red (*networking*) y descubrir sinergias entre el colectivo Empresas Asociadas UOC.
7. Acceso a la Bolsa de Trabajo de la UOC: PRiSE podrá canalizar sus ofertas de trabajo a la comunidad de profesionales formados en la Universidad, con el objetivo de captar candidatos para la selección de sus puestos de trabajo.
8. Participación en los programas de cooperación educativa de prácticas universidad-empresa: PRiSE podrá acoger a estudiantes de prácticas de la UOC en su entorno a trabajo para que puedan aplicar los conocimientos teóricos adquiridos en la Universidad.
9. Participación en los programas de emprendedores UOC: PRiSE podrá participar en los proyectos de apoyo al emprendedor UOC, con el objetivo de transferirles notoriedad, ofrecerles apoyo público y constituir un punto de referencia y asesoramiento en sus primeras fases de creación.
10. Participación en los proyectos de formación, difusión e investigación: Ambas partes restarán abiertas a participar en los proyectos de formación, difusión e investigación que surjan de dicha relación y que, englobándose en los ámbitos de trabajo y conocimiento de cada entidad, se consideren de interés mutuo.

[1] Esta prestación sólo se aplicará a partir del momento en que la empresa haya acordado y firmado con la UOC una adenda específica donde se concreten las características de la beca y las condiciones y procedimiento para su concesión.

11. Contribución a los proyectos de solidaridad liderados por la UOC: PRiSE se podrá aproximar al mundo de la paz y la cooperación mediante su colaboración en los proyectos de solidaridad que lidera la UOC.
12. Difusión pública del vínculo: la UOC hará difusión pública del vínculo establecido con este convenio a través del portal de la uoc, www.uoc.edu, con un vínculo directo a la web corporativa de la empresa, www.prise.es, y con la inclusión del nombre de PRiSE en todos los dispositivos gráficos, escritos y digitales en que se identifique la lista de empresas asociadas UOC. Asimismo, PRiSE hará difusión pública e interna de este vínculo utilizando el logo de empresa asociada UOC, en lugares destacados y muy especialmente en la web corporativa e intranet de la organización, www.prise.es, con un vínculo directo a www.uoc.edu.

Tercero. Con el fin de conseguir una relación fluida entre ambas partes, cada institución firmante nombrará a un interlocutor que la represente en las reuniones periódicas que se realicen para la concreción y el seguimiento de este convenio marco y las adendas correspondientes, y para definir las mejores estrategias de colaboración entre ambas entidades.

En representación de la UOC, será Meritxell Santiago, responsable de Empresas Asociadas UOC, que podrá ir acompañada, si fuera necesario, de otras personas de la UOC, según los temas de que se tenga que tratar. Y en caso de que sea necesario, podrá delegar su participación en otras personas de la UOC, tras haberlo comunicado a la otra parte.

En representación de PRiSE, será Elena Galván Fernández.

Cuarto. Este convenio tendrá una vigencia indefinida a contar a partir de la fecha de firma y podrá ser resuelto según lo que se especifica en el acuerdo quinto y sexto.

Quinto. Serán causas de resolución del convenio las siguientes:

a) El mutuo acuerdo de las partes firmantes, manifestado por escrito.
b) La manifestación de cualquiera de las dos partes de la voluntad de resolver el convenio, con un preaviso de tres meses.
c) Las causas generales establecidas en la legislación vigente.

Sexto. Será motivo de rescisión inmediata del presente convenio el uso inadecuado de la imagen de empresa asociada UOC por parte de PRiSE y viceversa.

Séptimo. En el supuesto de que alguno de los acuerdos del convenio se convierta en total o parcialmente nulo o ineficaz, esta nulidad o ineficacia afectará a solamente a la mencionada disposición o a la parte que resulte nula o ineficaz, y subsistirá el convenio en todo lo demás, pero teniéndose por no puesta la mencionada disposición, o la parte afectada.

Octavo. Ninguna modificación o enmienda de este convenio será válida a no ser que se haga por escrito y sea firmada por cada una de las partes.

Noveno. Las dos partes expresan el compromiso de cumplir sus obligaciones respectivas de buena fe y de llevar a buen término todas y cada una de las negociaciones que sean necesarias para cumplir este convenio a satisfacción de ambas.

Para la solución de cualquier cuestión litigiosa derivada de la interpretación o aplicación de los acuerdos establecidos en este convenio, las partes se someten al arbitraje institucional del Tribunal Arbitral de Barcelona, de la Asociación Catalana para el Arbitraje, a quien se encarga la designación del árbitro o árbitros y la administración del arbitraje. El arbitraje será de derecho y las partes se obligan desde ahora al cumplimiento de la decisión arbitral.

Y, en prueba de conformidad con el contenido de este convenio, las partes firman el presente convenio por duplicado, en el lugar y en la fecha más abajo mencionados.

Barcelona, 25 de febrero 2010

Imma Tubella Casadevall
Rectora de la Universitat Oberta de Catalunya

Daniel García Franco
Auditoria y Consultoria de Privacidad y Seguridad

ANEXOS : APARTADO 8

Nombre : P8_Memoria_MISTIC.pdf

HASH SHA1 : ymEAKbR6aiGCIteIBiUBwcHSoig=

Código CSV : 4260840443389508229963 9

8. RESULTADOS PREVISTOS

8.1. Valores cuantitativos estimados para los indicadores y su justificación

El título que se presenta utiliza como referencia base para la previsión de resultados previstos los correspondientes al segundo ciclo de Ingeniería Informática ofrecido por la UOC desde el curso 2001/02 y la experiencia reciente de la misma universidad con los Máster Universitarios (des del curso 2006/07). La estimación de los valores de tasas y resultados académicos y de satisfacción se ha basado en la experiencia de estas titulaciones, concretamente en la evolución de dichos valores desde el curso 2005/06 hasta 2008/09.

- **Tasa de graduación en T+1**

Esta tasa, y de acuerdo con los datos obtenidos de manera periódica desde los sistemas de recogida y análisis de los resultados, ha tenido estos valores:

	2005/06	2006/07	2007/08	2008/09
Máster Universitarios UOC	-	-	16,5%	18,1%

Así pues, se propone que estos valores se estimen en los intervalos siguientes, teniendo en cuenta que se podrá disponer de resultados a partir del curso 2011/12 (T+1):

	2012/13	2014/15	2016/17
MISTIC (el máster se iniciará en el 2011/12)	14%	16%	18%

Será importante, una vez iniciado el máster analizar la composición de las cohortes que se vayan creando para poder hacer una previsión del número de titulados a partir del curso 2011/12 y ajustar la previsión de tasa de graduación, así como establecer esta tasa a partir de la consolidación del programa, mientras este dato no esté consolidado, se considera óptimo el valor de 20%, los objetivos a consolidar deberán situarse en el 25% o superiores.
Debido a las características específicas de los estudiantes de la UOC (mediana de créditos matriculados por curso significativamente inferior al número de créditos teóricos por curso) también se medirá la tasa de graduación en T+2 años, T+3 años,... ya que aportan más información sobre la evolución de la graduación de las diferentes cohortes.

- **Tasa de abandono**

La tasa de abandono en T+1 no tiene sentido para los máster ya que no se tiene abandono hasta el tercer año, T+2.
La tasa de abandono en T+2 años, en los másters universitarios ha tenido estos valores:

Másters universitarios UOC	2008/09
Abandono en T+2 años	24,6%

Se propone que estos valores para el MISTIC se estimen en los intervalos siguientes:

Abandono en T+2 años	Entre un 20 y un 30%

Debido a las características de la formación no presencial, la mejora de dichos valores es compleja y no está siempre asociada al programa de formación. A pesar de ello se deberán proponer acciones para conseguir no superar el 25% y posteriormente mantenerse en valores inferiores.

- **Tasa de eficiencia**

Esta tasa ha tenido estos valores:

	2005/06	2006/07	2007/08	2008/09
2º Ciclo en Ingeniería Informática de la UOC (la titulación se inició en 2001/02)	89,6%	87,6%	nd	nd
Másters Universitarios UOC	-	100%	99,3%	nd

Si tenemos en cuenta que esta tasa está muy relacionada con las tasas de éxito y rendimiento y éstas también se han mantenido estables en los últimos años, tanto en estas titulaciones como en el resto de titulaciones de la universidad, y tenemos en cuenta también que en el proceso de tutoría se orienta al estudiante en la decisión de matrícula, proporcionándole recomendaciones específicas en relación a su situación personal y académica para garantizar un buen rendimiento, la previsión es que la tasa de eficiencia para el MISTIC sea superior al 85%.

- **Tasa de éxito**

La tasa de éxito corresponde al Número de créditos superados/Número de créditos presentados. Esta tasa ha tenido los siguientes valores:

	2005/06	2006/07	2007/08	2008/09
2º Ciclo en Ingeniería Informática	94,4%	94,7%	95,4%	94,6%
Mástes Universitarios	-	96,1%	97,0%	93,6%

La tasa de éxito se ha mantenido estable en los últimos cuatro años tanto en estas titulaciones como en el resto de titulaciones de la universidad, la previsión es que para el MISTIC siga siendo superior al 90%.

- **Tasa de rendimiento**

Esta tasa corresponde al Número de créditos superados/Número de créditos matriculados, Esta tasa ha tenido los siguientes valores:

	2005/06	2006/07	2007/08	2008/09
2º Ciclo en Ingeniería Informática	65,5%	66,9%	69,3%	73,1%
Másters Universitarios	-	79,2%	80,1%	76,9%

La previsión es que la tasa sea superior al 65% en el nuevo MISTIC.

- **Tasa de satisfacción**

Esta tasa, que corresponde al Número de respuestas que valoran 4 o 5 en una escala de 1 a 5/Número de respuestas totales, ha tenido estos valores:

	2005/06	2006/07	2007/08	2008/09
2º Ciclo en Ingeniería Informática	73,7%	76,5%	73,3%	72,4%
Másters Universitarios	-	84,8%	78,4%	76,4%

La tasa de satisfacción se ha mantenido de manera estable alrededor del 75% en el caso del 2º Ciclo en Ingeniería Informática, mientras que en los Máster Universitarios ha disminuido en 8 puntos en tres años, siendo siempre superior al 75%. La adaptación de les mecanismos para la recogida de la satisfacción de los estudiantes puede modificar el tipo de información que se reportará, a pesar de ello se valoraran como resultados satisfactorios medias de satisfacción superiores a 4 entre valores de 1 a 5. Mientras no se disponga de estos nuevos mecanismos se considerará el valor del 80% como satisfactorio

8.2. Progreso y resultados de aprendizaje

Cada final de semestre se facilita con el máximo detalle los resultados a través de los sistemas de información de la UOC, cuyos indicadores quedan recogidos principalmente en su Datawarehouse, que es la fuente básica de información de los resultados de valoración de la docencia para el profesorado. La información se recoge a todos los niveles: programa, asignatura y aula y por tanto va dirigida a diferentes perfiles: director de estudios, director de programa y profesor responsable de asignatura.

Las principales fuentes de información que permiten la obtención de los datos son:

- La gestión académica
- El proceso de recogida de la satisfacción de los estudiantes

Los resultados de estos procesos se cargan semestralmente al Datawarehouse de la universidad, la validación de estos procesos y la idoneidad de los indicadores es una función coordinada por el equipo de evaluación y calidad, que periódicamente se reúne con los administradores de los estudios para asegurar el uso y garantía de los indicadores.

Estos resultados se valoran a nivel de asignatura por el profesor responsable de asignatura, que puede determinar la necesidad de mayor información detallada para conocer las causas de los resultados o analizar las actividades y pruebas de evaluación puesto que todas ellas están accesibles a través de las herramientas del profesor en formato digital.

El director del programa, en el marco de la Comisión de titulación valorará los resultados globales de la titulación, esta valoración incluye la comparación con la información de previsión de resultados. Las valoraciones hechas por la comisión y las posibles acciones de mejora a desarrollar deberán ser recogidas por el director del programa y validadas por su director de estudios.

Los principales resultados que se valoran en la Comisión de la titulación semestralmente corresponden a:

- rendimiento: valorando los ítems de seguimiento de la evaluación continuada, tasa de rendimiento y tasa de éxito
- continuidad: valorando abandono principalmente a partir de la rematricula o las anulaciones voluntarias de primer semestre
- satisfacción: valorando los ítems correspondientes a la acción docente, la planificación, los recursos de aprendizaje y el sistema de evaluación

A final de cada curso además de los resultados expresados, se recogen los correspondientes al balance académico de curso y que presenta el Vicerrector de Ordenación Académica y Profesorado a la Comisión académica y a la Comisión de programas:

- rendimiento: valorando los mismos ítems
- continuidad: valorando los mismos y además la tasa de abandono
- satisfacción: valorando los mismos y además la satisfacción con la UOC, el programa, su aplicabilidad y los servicios
- graduación: tasa de graduación y de eficiencia, en este caso se valora empezar a disponer de estos a partir del curso 2011/12
- inserción o mejora profesional: a partir de los estudios propios elaborados por la universidad cada 2 años y a partir de los resultados obtenidos por los estudios transversales realizados por las universidades catalanas con el apoyo de AQU.

Este conjunto de datos están disponibles para todos los tipos de asignatura, aunque también está previsto disponer de información adicional para los trabajos de final de grado y también de las prácticas. En estos casos es pertinente valorar las memorias y trabajos realizados para valorar la adquisición del conjunto de competencias previstas.

ANEXOS : APARTADO 10

Nombre : P10_Memoria_MISTIC_F2.pdf

HASH SHA1 : 2yd10lzMYKFRLYAOIpp8ttp+UWw=

Código CSV : 459036475899843911470 17

10. CALENDARIO DE IMPLANTACIÓN

10.1. Cronograma de implantación de la titulación

El máster interuniversitario se iniciará el curso 2011-2012. El calendario de implantación que se ha planificado permite al estudiante, de acuerdo con lo establecido en el Real decreto 1393/2007, de 29 de octubre, cursar el máster en 1 año académico (2 semestre lectivos). Dada la existencia de materias que conforman múltiples especialidades, en el primer año se desplegará una de las posibles especialidades, mientras que las otras tres se desplegarán en el segundo año.

Así, el cronograma de implantación es:

- Curso 2011-2012: 54 créditos lectivos + 3 créditos prácticas + 9 créditos TFM
- Curso 2011-2012: 48 créditos lectivos + 12 créditos TFM

Módulo de formación obligatoria: *Comunes*	**créditos**	**curso**
Legislación y regulación	6	2011/12
Vulnerabilidades de seguridad	6	2011/12
Identidad digital	6	2011/12
Módulo de Especialidad 1: *Seguridad en Redes y Sistemas*		
Seguridad en redes	6	2012/13
Seguridad en sistemas operativos	6	2011/12
Seguridad en bases de datos	6	2012/13
Módulo de Especialidad 2: *Seguridad en Servicios y Aplic.*		
Programación código seguro	6	2012/13
Comercio electrónico	6	2012/13
Biometría	6	2012/13
Módulo de Especialidad 3: *Gestión y Auditoría de la Seguridad Informática*		
Sistemas de gestión de la seguridad	6	2011/12
Auditoría técnica	6	2011/12
Análisis forense	6	2011/12
Módulo de Especialidad 4: *Investigación en Seguridad TIC*		
Criptografía avanzada	6	2011/12
Metodologías de investigación	6	2012/13
Técnicas de investigación	6	2012/13
Módulo Optativas		
Técnicas de marcado de la información	6	2012/13
Dirección estratégica de sistemas y tecnologías de la inform.	6	2011/12
Módulo Prácticas		
Prácticas profesionalizadoras	3	2011/12
Módulo Trabajo fin de Máster		
TFM de aplicación profesional	9	2011/12
TFM de investigación básica o aplicada	12	2012/13

10.2. Procedimiento de adaptación, en su caso, de los estudiantes de los estudios existentes al nuevo plan de estudios

No procede la adaptación. Sin embargo, de acuerdo con el art.6(4) del RD 1393/2007, según redacción otorgada por el RD 861/2010, los estudiantes del Máster de Seguridad Informática de la UOC (título propio) podrán obtener el reconocimiento de créditos académicos del plan de estudios del MISTIC, en función de las asignaturas o grupo de asignaturas superadas hasta el momento por el estudiante, de acuerdo con la tabla de equivalencias que se detalla en la página 46 de esta memoria (Tabla 2).

10.3. Enseñanzas que se extinguen por la implantación del correspondiente título propuesto

La implantación de este máster interuniversitario no extinguirá ninguna enseñanza oficial existente actualmente en la UOC, UAB o URV, pero el Máster de Seguridad Informática (título propio) que la Universitat Oberta de Catalunya ha venido ofreciendo desde el curso 2004-2005 dejará de ofrecerse con la implantación del título oficial. En el Anexo 1 se recoge información detallada de este máster propio.