MEMORIA para la solicitud de VERIFICACIÓN DE TÍTULO

MÁSTER UNIVERSITARIO en Ciberseguridad y Privacidad / Cybersecurity and Privacy

Març 2021

UNIVERSITAT OBERTA DE CATALUNYA

INDICE

1. DESCRIPCIÓN DEL TÍTULO

1.1. Datos básicos

Seleccionar Nivel
Máster/ Nivel MECES 3

Indicar Denominación específica
Máster Universitario en Ciberseguridad y Privacidad / Cybersecurity and Privacy

Seleccionar Título Conjunto (carácter interuniversitario)
No

Seleccionar Rama

Ingeniería y Arquitectura

Seleccionar ISCED 1 (International Standard Classification of Education) (Obligatorio)
Seleccionar ISCED 2 (Opcional)

481-Ciencias de la Computación

Seleccionar si habilita para profesión regulada
No

Condición de acceso para título profesional
No

El MU ofrece especialidades?
Sí

Indicar listado de especialidades *(si el programa presenta especialidades)*:

Especialidades (Indicar cada una de ellas)	Créditos optativo
Sistemas	18
Tecnologías	18
Gestión	18

¿Es obligatorio cursar una especialidad de las existentes para la obtención del título?
No

1.2. Distribución de créditos en el título

Créditos totales	**60**
Créditos obligatorios	18
Créditos optativos	30
Créditos Prácticas Externas	0
Créditos de Trabajo Fin de Máster (6-12)	12

1.3. Datos asociados a la Universidad y al Centro

Universidad solicitante
054 – Universitat Oberta de Catalunya

Centro de impartición:
08070118 – Universitat Oberta de Catalunya

Modalidad de la enseñanza
A distancia

Plazas de nuevo ingreso ofertadas

Primer año implantación	500
Segundo año implantación	500

**El número de plazas para el primer año será igual al de la Fitxa PIMPEU, y para los siguientes, igual o superior.*

ECTS de matrícula necesarios según curso y tipo de matrícula:

	Matrícula a Tiempo completo*		**Matrícula a Tiempo parcial**	
	ECTS Matrícula mínima	**ECTS Matrícula máxima**	**ECTS Matrícula mínima**	**ECTS Matrícula máxima**
Primer curso	60	60	6	54
Resto de cursos	0	0	6	54

El número mínimo de matrícula a tiempo parcial ha de coincidir con el número mínimo de créditos de una asignatura, y el número máximo con el global de créditos del programa menos el valor de la asignatura de menos creditaje.

https://seu-electronica.uoc.edu/portal/_resources/ES/documents/seu-electronica/Normativa_academica_EEES_CAST_xvigentx.pdf

Lenguas en las que se imparte
Castellano / Catalán / Inglés

2. JUSTIFICACIÓN

2.1. Justificación del título propuesto, argumentando el interés académico, científico o profesional del mismo con relación a la planificación de las enseñanzas en el marco del sistema universitaria

de Cataluña

La UOC empezó en el curso 2011-2012 un máster interuniversitario en el área de la seguridad informática, el Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones por la UOC, la UAB, y la URV, que ha tenido muy buena acogida y valoración por nuestros estudiantes. El número de nuevos estudiantes fue de casi 200 anuales durante los primeros años, y ha llegado a los 300 en las últimas ediciones. En el curso 2017-2018 el màster tuvo 646 estudiantes activos y se graduaron 148 personas. El número total de graduados del màster ya sube a más de 600. Aunque la satisfacción con el programa es positiva para más del 70% de los graduados, el programa necesita reenfocar parte de su plan de estudios y sus metodologías de trabajo para continuar dando respuesta a las necesidades de un sector pionero y en contínua evolución, y adaptarse a las demandas del mercado. En este sentido, la evolución del máster se lleva a cabo en dos ejes principales: (1) intensificando las competencias profesionales que tienen más salidas laborales y que pivotan sobre la ciberseguridad, (2) incluyendo más competencias en el ámbito de la privacidad para cubrir la demanda de profesionales que está provocando la entrada en vigor de la Ley General de Protección de Datos (LGPD), en Mayo de 2018.

En los siguientes subapartados se exponen los motivos por los que se considera la importancia de ofrecer un programa de máster en el campo de la ciberseguridad y privacidad.

Interés académico

En diciembre del 2017, la Junta de Educación de la *Association for Computing Machinery* (ACM), la mayor asociación académica y profesional sobre informática a nivel mundial, publicó unas pautas curriculares para los programas universitarios en ciberseguridad. Actualmente la ciberseguridad ya se considera una nueva disciplina en los planes de estudio de informática, juntamente con la ciencia de computadores, la ingeniería de computadores, los sistemas de información, las tecnologías de información, y la ingeniería del software.

La ACM ha definido la ciberseguridad como una disciplina basada en la computación que involucra tecnología, personas, información y procesos para permitir operaciones seguras. Engloba la creación, operación, análisis y pruebas de sistemas informáticos seguros. Es un programa de estudio interdisciplinar del ámbito de la informática que incluye aspectos de derecho, política, factores humanos, ética y gestión de riesgos en el contexto de los adversarios.

Interés científico

Vivimos en la era digital donde toda la información está en la red, y donde los ataques sobre los sistemas en tecnologías de la información y las comunicaciones son constantes. Fruto del

incremento de ataques y de su impacto en toda la sociedad, el interés científico en evolucionar los sistemas de protección, prevención, detección e identificación de ataques son de extrema importancia.

Actualmente existen numerosos congresos internacionales de alta calidad en el ámbito de la ciberseguridad. Algunos ejemplos son:

- EUROCRYPT: International Conference on Theory and Applications of Cryptographic Techniques
- SP: IEEE Symposium on Security and Privacy
- FC: International Conference on Financial Cryptography and Data Security
- USENIX Security Symposium
- NDSS: Network and Distribyted Systems Security Symposium

También existen numerosas revistas indexadas de alta calidad, como:

- IEEE Transactions on Information Forensics and Security (IEEE)
- ACM Transactions on Information and System Security (ACM)
- Computers & Security (Elsevier)
- Information and Computer Security (Emerald)
- International Journal of Security and Networks (Interscience Publishers)

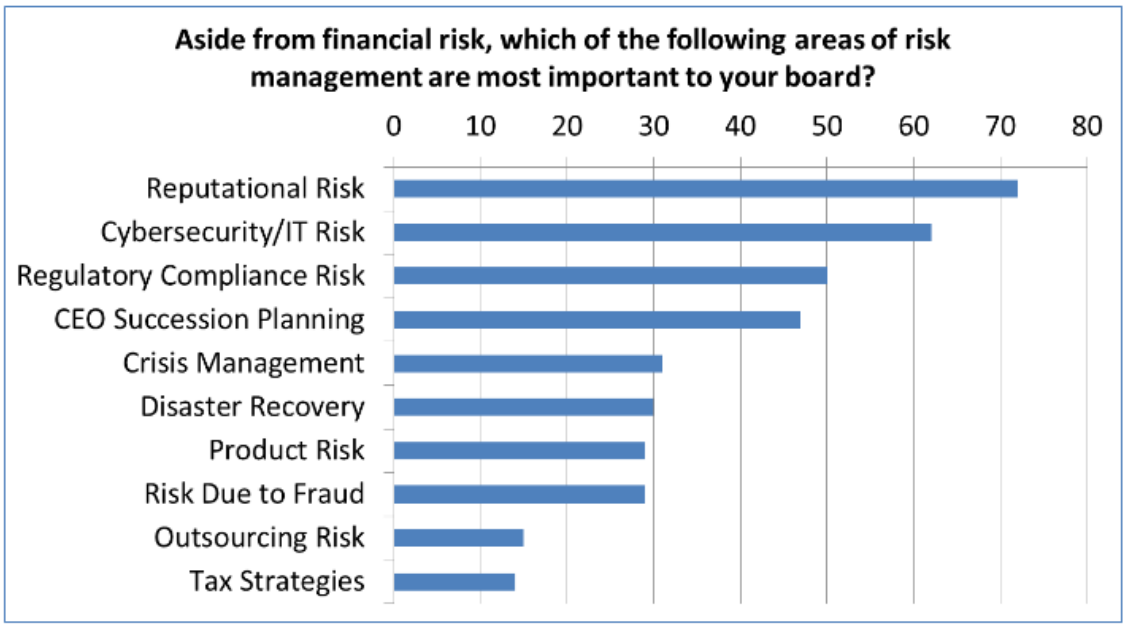
A nivel español, de forma bianual se celebra un congreso del ámbito llamado Reunión Española sobre Criptología y Seguridad de la información (RECSI), que aúna a más de 100 investigadores cada año.

La investigación en seguridad de la información, seguridad de las comunicaciones, y privacidad, es unas de las áreas más activas dentro del ámbito de las tecnologías de la información y de las comunicaciones.

Interés profesional

La ciberseguridad y la protección de la privacidad se han convertido en prioridades muy relevantes para nuestra sociedad. Mantener los sistemas de información y las redes de comunicación seguras es esencial para mantener la economía digital en funcionamiento e incluso para la protección de la democracia.

La ciberseguridad no es solo una preocupación de los departamentos tecnológicos de las empresas sino que es un tema de interés en los consejos de administración. Una investigación realizada por el bufete de abogados EisnerAmper demuestra que las tres principales preocupaciones de los miembros de la juntas de administración de empresas públicas y privadas están relacionadas con la seguridad de la información:



Data Source: EisnerAmper, Concerns About Risks Confronting Boards, Fifth Annual Board of Directors Survey, 2014, page 7.

Según un informe de Gartner del 2018, el incremento del gasto mundial en productos y servicios de seguridad de la información fue de un 12,4% en 2018 y aumentará otro 8,7% en 2019. La oferta de trabajo en el ámbito de la ciberseguridad es muy alta y el sector no encuentra suficientes profesionales formados. Según el informe ***Cybersecurity Talent: The Big Gap in Cyber Protection*** de Capgemini, de las competencias digitales de los profesionales TIC, la ciberseguridad es la que presenta una mayor brecha entre la demanda y la oferta. Un estudio llevado a cabo por el ***Centro para la Ciberseguridad y Educación (ISC)²*** sobre la Fuerza de Trabajo Global en Seguridad de la Información (GISWS) de 2017, revela que faltarán más de 1,8 millones de trabajadores en ciberseguridad a nivel mundial en 2022.

Indicadores adicionales de inserción laboral

Por lo que se refiere al impacto de esta titulación en la inserción laboral de los futuros titulados, ha de tenerse en cuenta que la ocupabilidad en el caso de la UOC es diferente a otras universidades ya que el 95% de sus estudiantes ya son laboralmente activos en el momento de realizar la primera matrícula y, de ellos, el 50% es mayor de 30 años. Con estas cifras, es evidente

que el indicador de la inserción laboral de los graduados de la UOC no es tan relevante como pueden serlo otros factores, tales como la mejora profesional y personal. En otras palabras, el hecho de obtener una titulación universitaria en la UOC facilita a estos estudiantes no tanto la inserción laboral en sí como la posibilidad de promoción dentro de su ámbito de trabajo o el cambio de orientación profesional.

En este contexto, es significativo el Estudio de la inserción laboral de la población titulada de las universidades catalanas, "Universitat i treball a Catalunya", realizado en el año 2017 con la Agencia de Calidad del Sistema universitario catalán (AQU), con una muestra de 4.850 titulados de la UOC de los cursos 2011-2012 y 2012-2013, cuyos resultados a nivel general y su valoración han sido tenidos en cuenta en el diseño de esta propuesta. Los resultados estadísticos de este estudio demuestran que:

- Sólo el 3,6% eran estudiantes a tiempo completo
- Una vez titulados, la tasa de ocupación es del 96,4%
- El 85% de los titulados indican que desarrollan funciones de nivel universitario
- Casi la totalidad de los titulados trabajaba durante los estudios (el 58% en un trabajo relacionado con los estudios)
- Más del 80% de los titulados encuestados repetirían la carrera cursada

En otras palabras, el hecho de obtener este Máster por la UOC facilita a estos estudiantes no tanto la inserción laboral de la que generalmente ya disponen, sino la posibilidad de promoción laboral o cambio de orientación profesional. Por lo tanto, el **perfil preferente de estudiantes a los que va dirigido es fundamentalmente el de ingenieros informáticos** (directores de sistema de información, directores de desarrollo, jefes de proyectos en tecnologías de la información y de las comunicaciones, técnicos de sistemas, analistas, analistas programadores, administradores de bases de datos, consultores de sistemas de información, expertos en Internet, Ingenieros de operaciones de red, oficiales de protección de datos, etc.), pero también ofrece la posibilidad de reciclaje a personas en el ámbito de otras ingenierías TIC (como telecomunicaciones o multimedia), o incluso a graduados en matemáticas o en ciencias de datos que tengan experiencia profesional en el sector o certificaciones que acrediten conocimientos en el ámbito de la informática.

Por todo ello consideramos que está justificado su interés académico/de investigación/práctica profesional dentro del contexto de la programación del sistema universitario.

Normas reguladoras del ejercicio profesional vinculado al título

El título presentado no corresponde a una profesión que se vea afectada, en este momento, por

normas reguladoras que puedan condicionar la actividad profesional.

2.2. Justificación del título propuesto mediante referentes externos e internos (nacionales o internacionales)

Tradicionalmente los programas vinculados a la seguridad informática se han denominado con títulos que enfatizan su vertiente tecnológica. Así, los títulos más comunes eran el de “Seguridad de la Información y de las Comunicaciones” (como el actual máster de la UOC), o “Seguridad Informática”. Sin embargo, desde que ACM empezó a trabajar en un currículum académico en el área de ciberseguridad, éste término ha ido adquiriendo notoriedad y hoy en día, muchos de los nuevos cursos, especializaciones o posgrados, ya llevan la palabra ciberseguridad en su título.

Referentes académicos nacionales

INCIBE, el Instituto Nacional de Ciberseguridad, publica cada año un catálogo con la formación de másteres y grados en el ámbito de la ciberseguridad en España.

Actualmente se ofrecen 60 programas de máster en el ámbito español (23 de los cuales universitarios), y 1 grado. Existen 23 másteres on line, 1 a distancia, y 6 semipresenciales.

Existen 3 másteres universitarios que contienen la palabra **ciberseguridad**:

- Máster Universitario en Ciberseguridad de la UPM. 60 créditos
    - No incluye itinerarios. Ofrece asignaturas del ámbito de las técnicas de ciberseguridad, y de la gestión de ciberseguridad.
- Máster Inter-Universitario en Ciberseguridad por la UVigo y la UDC. 90 créditos
    - No incluye itinerarios. Ofrece asignaturas del ámbito de las técnicas de ciberseguridad, y de la gestión y legislación en ciberseguridad.
- Máster Universitario en Ciberseguridad por la UC3M. 60 créditos
    - Ofrece un itinerario de “Ingeniería de Sistemas Seguros” y un itinerario de “Analista de la Ciberseguridad”.

Solo existe un máster (no universitario) que contenga la palabra **privacidad** en su título:

- Máster en Ciberseguridad y Privacidad, URJC. 60 créditos
    - Programa on line
    - No ofrece optatividad. Ofrece asignaturas del ámbito de las técnicas de

ciberseguridad, de la gestión de la ciberseguridad, y del marco ético y legal de la privacidad.

Actualmente, los másteres con más estudiantes en el ámbito español son:

- Máster Universitario en Seguridad de la Información y de las Comunicaciones por la UOC, UAB y URV. 60 créditos
  - Programa on line
  - Ofrece 3 itinerarios: “Seguridad en redes y sistemas”, “Seguridad en servicios y aplicaciones”, “Gestión de la Seguridad”
- Máster Universitario en Seguridad Informática por la UNIR. 60 créditos
  - programa on line
  - No ofrece optatividad. Ofrece asignaturas del ámbito de las técnicas de ciberseguridad, y de la legislación en ciberseguridad.

Referentes académicos europeos

Uno de los másteres europeos más reconocidos en el ámbito de la ciberseguridad son los de la **Royal Holloway**. En concreto, su oferta es la siguiente:

- MSc in Information Security
  - 1 año a tiempo completo. Presencial
- MSc in Information Security with Year in Industry
  - 2 años a tiempo completo. Presencial.
- MSc in Information Security
  - 1 año a tiempo completo. On line
- MSc in Mathematics of Cryptography and Communications
  - 1 año a tiempo completo. Presencial

Otras de las universidades reconocidas con programas de máster en ciberseguridad son:

- University of York: MSc in Cyber Security
  - 1 año a tiempo completo. Presencial.
- University of York: online MSc in Computer Science with Cyber Security
  - 2 años a tiempo parcial. On line
- University of Surrey: MSc in Information Security
  - 1 año a tiempo completo. Presencial.

- University of Birmingham: MSc in Cyber Security
  - 1 año a tiempo completo. Presencial.
- University of Southampton: MSc in Cyber Security Risk Management
  - 1 año a tiempo completo. Presencial
- Belgium interuniversity: Master in CyberSecurity
  - Universidades: Ecole Royale Militaire, Université Libre de Bruxelles, Université Catholique de Louvain, Université de Namur, Haute Ecole de Bruxelles, Haute Ecole Libre de Bruxelles
  - 2 años a tiempo completo. Presencial
- University of Liverpool: Online MSc in Cyber Security
  - 2 años a tiempo parcial. On line
- Lancaster University: MSc in Cyber Security
  - 1 año a tiempo completo. Presencial
- Programa conjunto de universidades de Suiza: Master en Cybersécurité
  - Universidades: École Polytechnique Fédérale de Lausanne y Eidgenössische Technische Hochschule (ETH) de Zürich
  - 2 años a tiempo completo. Presencial
- Université de Rennes: Master 2 cybersécurité
  - Especialización de un año de estudios de máster. Presencial.

A parte de las referencias aquí expuestas, existen muchas otras universidades europeas con programas de máster en el ámbito de la ciberseguridad.

Informes de asociaciones o colegios profesionales que avalan la propuesta

El contenido del máster sigue las guías temáticas que ha elaborado la *Association for Computing Machinery* (ACM), la mayor asociación académica y profesional sobre informática a nivel mundial, sobre estudios universitarios en ciberseguridad.

Colectivos y expertos externos consultados

El Máster Universitario en Seguridad de la Información y de las Comunicaciones que la UOC ofrece actualmente es un programa interuniversitario. Para renovar el programa y diseñar el Máster Universitario en Ciberseguridad y Privacidad hemos consultado con los grupos de investigación que colaboraban con nosotros en el programa y cuyos expertos son de los más reconocidos en el sector:

- Grupo CRISES de la Universitat Rovira y Virgili: Expertos en privacidad y promotores de la cátedra UNESCO de privacidad de datos.

- Grupo SENDA de la Universitat Autònoma de Barcelona: Expertos en seguridad de redes y aplicaciones distribuidas
- Grupo SECOM de la Universitat de les Illes Balears: Expertos en protocolos de comercio electrónico

Prácticamente todos los investigadores de estos grupos han formado parte de la red de excelencia ARES y del proyecto ARES-CONSOLIDER (el único proyecto CONSOLIDER que el Ministerio financió sobre la temática de seguridad informática), cuyo hecho es un buen indicador de la calidad de los equipos y de su conocimiento en la materia.

Por otro lado, la Universidad Oberta de Catalunya forma parte del *Centre de Recerca en Ciberseguretat de Catalunya* (CyberCat), y el plan de estudios del programa ha sido consultado con los expertos que forman parte del centro.

Dentro del marco del màster de seguridad, periódicamente la UOC organiza la UOC-Con, el congreso de ciberseguridad de la UOC. En esta jornada invitamos a empresas del sector para que hagan ponencias sobre los últimos avances en una determinada temática (el curso 2017-2018 el tema fue móviles y seguridad). Este congreso nos permite trabajar estrechamente con expertos del sector y obtener información de cuáles son sus demandas de recursos profesionales, además de servir como evento de networking entre empresas y estudiantes y de permitir exponer algunos de los trabajos finales de más interés profesional.

Descripción de los procedimientos de consulta internos utilizados para la elaboración del plan de estudios

El proceso de diseño de los planes de estudio de la UOC se fundamenta en dos procesos previos, por un lado los planes pilotos de adaptación llevados a cabo en Cataluña en el curso 2005/06 y su posterior implantación, y por otro el proceso interno de reflexión y análisis de algunos de los conceptos básicos del EEES y su impacto en nuestra universidad. Los conceptos identificados y abordados por 8 grupos de trabajo interdisciplinares fueron:

- Créditos ECTS
- Competencias
- Plan docente
- Sistemas de evaluación
- Reconocimiento de la experiencia profesional
- Recursos de aprendizaje
- Aula virtual
- Trabajos final de Grado/Máster

Para cada uno de estos grupos se concretaron objetivos de trabajo y se presentaron los documentos de conclusiones a mediados del 2007, en julio de 2007 se concretan todas las propuestas en el documento: Conclusiones finales al debate sobre la adaptación metodológica al EEES.

Para trabajar la definición del Máster Universitario en Ciberseguridad y Privacidad se ha seguido el protocolo interno de la UOC para la elaboración de las propuestas, con la consecuente creación de una **comisión de titulación** que cuenta con el apoyo de los diferentes equipos implicados en el diseño e implantación del programa. En este proceso previo de definición del nuevo Máster han participado activamente todos los profesores de los Estudios de Informática, Multimedia y Telecomunicación de la UOC implicados en él, y también el personal de gestión asociado a los estudios.

La Comisión de la Titulación está formada por la Directora del programa del Máster en Ciberseguridad y Privacidad, la Dra. Helena Rifà, los profesores Dr. Jordi Serra, Dr. Carles Garrigues, Dr. Víctor García y Dra. Montse Serra, y la mánager del programa de los Estudios de Informática, Multimedia y Telecomunicación, la Sra. Sílvia Puigbó. Esta comisión se ha reunido de forma periódica y han trabajado intensamente en la definición final de aspectos destacados en la propuesta como el perfil profesional, las orientaciones, la definición de las competencias específicas del Máster y el plan de estudio propuesto, y a partir de los referentes descritos en el punto 2.2. y de las aportaciones realizadas por los agentes internos y externos.

Respecto a la Comisión de Apoyo a la Titulación está integrada por miembros del Área de Programación y Calidad, el Área de Servicios Académicos, el Área de Marketing y Comercial. La finalidad de esta comisión ha sido, a través de procedimientos de información y consulta, velar por la viabilidad metodológica, operativa, económica y de calidad de la propuesta, así como para dotar de coherencia al conjunto de propuestas de nuevo Máster en curso de elaboración.

Por otro lado, se han tenido en cuenta las opiniones de los estudiantes del actual Máster Universitario en Seguridad de la Información y de las Comunicaciones por la UOC, UAB, y URV, a los cuales se les han hecho consultas directas, encuestas de final de semestre, y un estudio del perfil del alumnado.

Los resultados de todo este proceso de participación y consultas tanto externas como internas han sido incorporados en el diseño del Máster, especialmente por lo que respecta a la configuración de los itinerarios y los perfiles de salida del máster.

2.3. Potencial de la institución y su tradición en la oferta de enseñanzas

Adecuación a los objetivos estratégicos de la universidad.

La UOC fue reconocida por la Ley 3/1995, de 6 de abril, del Parlamento de Cataluña, como una nueva realidad, que ha encontrado reconocimiento específico en la Ley 1/2003, de 19 de febrero, de universidades de Cataluña (LUC), y en la Ley orgánica 6/2001, de 21 de diciembre, de universidades (LOU), y se estructura internamente por las NOF (Normas de organización y funcionamiento) aprobadas según el Decreto 273/2003, de 19 de noviembre.

La Fundación para la Universitat Oberta de Catalunya vela por la correcta y eficaz dirección y gestión de la universidad, y lleva a cabo las tareas de inspección, evaluación y control, necesarias para garantizar la máxima calidad del proceso formativo. La Fundación se rige por un patronato integrado por entidades de amplia implantación en todo el territorio y dotadas de un gran prestigio social. La presidencia del Patronato corresponde al consejero de Innovación, Universidad y Empresa de la Generalitat de Cataluña, y la Comisión Permanente está presidida por el director general de Universidades de la Generalitat de Cataluña.

Al igual que el resto de universidades públicas y privadas que han sido reconocidas por el Parlamento de Cataluña, la UOC participa en el Consejo Interuniversitario de Cataluña, órgano de coordinación, consulta y asesoramiento del sistema universitario catalán, que tiene como objetivo principal facilitar la coordinación entre la comunidad universitaria y la Administración educativa.

Coherencia con otros títulos existentes o tradición previa en estudios de naturaleza o nivel similares.

La UOC cuenta con experiencia y una extensa trayectoria en la formación en el ámbito del máster. En el curso 2004/2005 empezó un programa de máster propio en “Seguridad informática” después de años de experiencia ofreciendo cursos de postgrado. En el curso 2011/2012 el programa del Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones por la UOC, UAB, y URV sustituyó el máster própio. El máster que empezamos el curso 2011/2012 ha estado activo hasta la actualidad de forma exitosa, siendo el máster en el ámbito de la seguridad con más graduados del estado español (605 hasta el curso académico 2017-2018), y manteniendo una matrícula de nuevos estudiantes al alza y graduados satisfechos con la titulación.

A nivel de encaje de esta titulación dentro de los Estudios de Informática Multimedia y Telecomunicación, estos cuentan con un conjunto de titulaciones vinculadas, ya sea

temáticamente o que ofrecen una formación generalista que permite alimentar y/o complementar al máster propuesto.

- El Grado de Ingeniería Informática, así como el Máster Universitario de Ingeniería Informática, que establece la formación generalista en la disciplina de las ciencias de la computación.

- El Grado de Tecnologías de Telecomunicación, que establece una formación generalista en la disciplina de la telemática y las redes de comunicaciones móviles.

- El Grado de Ciencia de Datos Aplicada, así como el Máster Universitario en Ciencia de datos, que forman expertos para el análisis de datos masivos y que complementan el máster de seguridad con estas competencias de en tratamiento de la información.

- El Máster Universitario de Desarrollo de Aplicaciones Móviles, que ofrece una visión específica de la programación y entorno de ejecución en el entorno de dispositivos portables.

- El Máster Universitario de Desarrollo de Sitios y Aplicaciones Web, que ofrece competencias específicas para los desarrolladores web.

- El Máster Universitario de Diseño y Programación de Videojuegos, que forma a profesionales en el desarrollo de videojuegos.

- El Máster Universitario de Diseño de Interacción y Experiencia de Usuario (UX), que forma a profesionales con una visión integral del diseño UX y del diseño de interacción e interfaces (UI).

- El Grado de Multimedia y el Máster Universitario en Aplicaciones Multimedia, que se centra en la producción de contenidos digitales, la creatividad, y una excelente experiencia de usuario.

- El Máster Universitario de Gestión Estratégica de la Información y el Conocimiento de las Organizaciones, que se focaliza en el estudio y el liderazgo de la gestión de la información y la gestión del conocimiento en cualquier tipo de empresa o institución.

- El Máster Universitario de Bioinformática y Bioestadística, por la UOC y la UB, que forma a profesionales expertos en el uso de la tecnología para la gestión, el análisis y la interpretación de datos biológicos y médicos.

Líneas de investigación asociadas: grupos de investigación, proyectos en el último trienio, convenios, tesis, publicaciones y, en su caso, reconocimiento de calidad alcanzados.

El grupo K-riptography and Information Security for Open Networks (KISON) es un grupo de investigación creado en la UOC en 2001 centrado en el diseño de tecnologías para la protección de la seguridad de las redes, la información transmitida a través de ellas y la privacidad de sus usuarios. Se trata de un grupo consolidado SGR por la AGAUR de Catalunya que cuenta con más de 8 profesores y 3 investigadores postdoctorales adheridos.

Las líneas de investigación del grupo KISON se centran en la compatibilidad de la seguridad de las redes descentralizadas (por ejemplo, redes ad-hoc, P2P, cloud o IO) y la protección de la información en Internet (especialmente los contenidos multimedia) con los derechos de privacidad de los usuarios. En concreto, las líneas son:

1. Seguridad y privacidad de las redes abiertas
   Despliegue de mecanismos para mejorar la seguridad y la privacidad en varios contextos.
   - Diseño y evaluación de protocolos:
     - mecanismos para estimular la cooperación de los usuarios y garantizar el funcionamiento óptimo de las nueva arquitecturas de redes distribuidas en beneficio de toda la ciudadanía.
     - mecanismos para crear confianza entre las entidades de la red: gestión y distribución de claves, protocolos de autenticación y autorización, protocolos de verificación distribuidos.
     - protocolos de seguridad y privacidad para la interconexión de redes de distinta naturaleza (sensores, domótica, redes de vehiculos, Internet, IoT, ciudades inteligentes, hogares inteligentes, etc.), para proteger la privacidad de la identidad y la localización de los nodos, y permitir una autogestión eficiente de las redes mediante mecanismos escalables.
   - Investigación en ciberseguridad:
     - seguridad de los sistemas informáticos en Internet, incluidos los distintos aspectos de la informática forense, la detección de intrusiones, el control de acceso y la autenticación, la seguridad cognitiva, la banca en línea segura y el comercio electrónico seguro.

2. Seguridad y privacidad de la información
   Diseño de técnicas adecuadas para proteger la información que se transmite en redes abiertas, así y como la privacidad de los usuarios de esta información.
   - Investigación en objetos multimedia:

- sistemas de distribución de contenidos descentralizados, escalables y eficientes con mecanismos para identificar a los redistribuidores ilegales;
- Esquemas de marcas de agua en tiempo real que se pueden ejecutar en dispositivos ligeros (tabletas, teléfonos inteligentes, ordenadores portátiles);
- otras aplicaciones de los sistemas de marca de agua (aparte de la protección de los derechos de autor), como las aplicaciones de segunda pantalla, la detección y localización de manipulaciones o la mejora de la estegoanálisis para detectar comunicaciones secretas.

- Protección de la privacidad:
  - privacidad de los datos médicos, privacidad de los documentos en lenguaje natural, publicación de datos de privacidad, privacidad en el intercambio y publicación de trayectorias, entre otros.

La capacidad y trayectoria científica del grupo en los últimos años es la siguiente:

- Número de artículos publicados (2014-2018): 80
- Número de tesis doctorales leídas (2014-2018): 10
- Número de patentes solicitadas y registradas (2014-2018): 4
- Número de empresas que han colaborado con el grupo con proyectos de I+D+I o a través de contratos de transferencia (2014-2018): 5
- Número de proyectos financiados concedidos (2014-2018): 1
- Número de doctores que forman parte del grupo: 12

A parte del KISON, hay otros grupos en la UOC que tratan de forma más tangencial los problemas de seguridad y privacidad. Son:

- Wireless Networks Research Lab (**WINE**), que promueve las tecnologías que mejoran la manera de comunicarse los dispositivos.
- Systems, Software and Models (**SOM RESEARCH LAB**), que se focaliza en el campo de los sistemas y la ingeniería de programario, sobretodo en la promoción del uso riguroso de modelos de programario y principios de la ingeniería en todas las tareas de diseño de programario.
- Internet Computing & Systems Optimization (**ICSO**), que trata desde la logística y el transporte, a la informática y la colaboración basadas en Internet y en las ciudades inteligentes.
- Communication Networks & Social Change (**CNSC**), donde se especializan en el análisis de las nuevas formas de participación civil (e-democracy) y de la expresión política que aportan los movimientos en red.
- Digital Commons (**DIMMONS**), que investiga las nuevas formas de economía

colaborativa e innovación social.

3. COMPETENCIAS

Veure guia. Només han de figurar les competències que adquiriran tots els estudiants del títol, les associades a una Especialitat no s'han d'incloure en aquest apartat.

3.1. Competencias básicas

Competencias básicas

Les competències bàsiques no es poden canviar, tampoc la seva numeració.

RD 1393/2007, modificado por RD 861/2010

Se garantizarán, como mínimo las siguientes competencias básicas, en el caso de Máster:

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.

3.2. Competencias generales

CG1- Analizar y sintetizar las propiedades de seguridad y privacidad de un sistema.
CG2- Seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas de ciberseguridad en entornos nuevos o poco conocidos.

CG3- Buscar, gestionar y utilizar de manera efectiva la información asociada al proceso de análisis y adaptación de nuevas soluciones tecnológicas.

3.3. Competencias transversales

CT1- Capacidad de iniciativa, de automotivación, y de aprendizaje autónomo a partir de la búsqueda y selección efectiva de información
CT2- Expresarse de forma escrita de forma adecuada al contexto académico y profesional
CT3- Comprensión de textos académicos y profesionales complejos escritos en inglés en el ámbito técnico.

3.4. Competencias específicas

CE1- Ejercer profesionalmente de forma responsable y honesta, actuando de acuerdo al código ético y a los aspectos legales actuales en el entorno de la seguridad y privacidad de datos.
CE2- Analizar y aplicar las técnicas básicas de prevención, protección y detección de ataques a un sistema informático.
CE3- Evaluar y tomar las decisiones más adecuadas en cuanto a la selección y uso de herramientas y tecnologías del mercado en el ámbito de la ciberseguridad y la privacidad.
CE4- Desarrollar, integrar, y evaluar técnicas informáticas que permitan aplicar los principios de privacidad y protección de datos desde el diseño y por defecto que exige el Reglamento General de Protección de Datos (RGPD) a los sistemas, servicios y aplicaciones que traten con datos personales.
CE5- Aplicar el marco jurídico que afecta a la gestión de la seguridad de sistemas informáticos, teniendo en cuenta la legislación relativa a la protección de los datos personales, la propiedad intelectual, la ley de los servicios de la sociedad de la información y el comercio electrónico, así como el derecho penal.
CE6- Identificar, examinar y evaluar los principales riesgos de un dominio informático y diseñar estrategias para gestionarlos.
CE7- Formular y desarrollar soluciones integrales e innovadoras en el ámbito de la ciberseguridad y privacidad, teniendo en cuenta las dinámicas de transformación y las tendencias tecnológicas
CE8- Analizar la implementación y despliegue de soluciones criptográficas para validar su funcionamiento
CE9- Realizar, presentar y defender ante un tribunal universitario un ejercicio original realizado individualmente, consistente en un proyecto integral de Ciberseguridad y privacidad de naturaleza profesional o de investigación, en el que se sinteticen e integren las competencias adquiridas en las enseñanzas.

4. ACCESO Y ADMISIÓN DE ESTUDIANTES

4.1. Sistemas de información previa

Perfil de ingreso recomendado

El perfil de ingreso recomendado para los futuros estudiantes de Máster universitario se corresponde con el establecido por la legislación vigente, así como en la normativa académica de la UOC, tal y como se detalla en el apartado 4.2. Requisitos de acceso y criterios de admisión.

El perfil de acceso recomendado para acceder este Máster es el que corresponde a haber cursado alguno de los estudios que se detallan a continuación:

- Másteres, Grados, Licenciaturas, Ingenierías técnicas, relacionadas con el ámbito de la Ingeniería Informática.
- Másteres, Grados, Licenciaturas, Ingenierías técnicas, relacionadas con el ámbito de la Ingeniería de Telecomunicaciones.
- Másteres, Grados, Licenciaturas, Ingenierías técnicas, relacionadas con el ámbito Multimedia.

También podrán acceder graduados de otras titulaciones afines o equivalentes.

Para aquellos estudiantes que no provengan de estos tipos de titulación, su admisión al máster quedará sujeta al cumplimiento de los criterios de admisión definidos en el Apartado 4.2. En estos casos, se requerirá a los estudiantes acreditar su competencia en el campo de las tecnologías de la información y de las comunicaciones, ya sea a través de programas no oficiales, certificaciones profesionales, o experiencia profesional en el sector.

Con el objetivo de compensar las posibles deficiencias formativas que pudieran existir en cada caso, en función de la titulación de origen de los estudiantes y de su experiencia profesional, se requerirá a los estudiantes la realización de créditos de formación compensatoria de forma previa o simultánea con el Máster. Esta recomendación se realizará mediante una tutorización y evaluación personalizada de las competencias previas de cada estudiante.

La docencia de este Máster se impartirá en catalán, castellano e inglés. Se recomienda a los estudiantes extranjeros ser competentes en la lengua oficial en que vayan a cursar los estudios (catalán, castellano o inglés). En caso necesario, por medio de los tutores también se facilitará la realización de una prueba de nivel de la lengua que corresponda.

Para las personas que cursen el máster en catalán o castellano, se recomienda también un nivel de competencia en lengua extranjera (inglés) equivalente al nivel B2 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.

En este sentido y 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 la lengua extranjera escogida. La prueba permite al estudiante verificar si su nivel es el recomendado para iniciar sus estudios en este Máster (nivel B2 o superior). Esta prueba no es excluyente ni requisito previo.

El estudiante puede optar a una evaluación de estudios previos a partir de titulaciones de escuelas oficiales que acrediten un nivel superior del idioma requerido para el reconocimiento de las competencias de la titulación.

Las solicitudes de acceso y admisión serán gestionadas por los órganos administrativos de la Universidad, que garantizarán el cumplimiento de las condiciones de acceso legalmente establecidas así como de las condiciones de admisión (cuando se hayan establecido).

Sistemas de información y acogida

Para asegurar que la información esté a disposición de toda persona potencialmente interesada en acceder a esta titulación, la UOC ofrece al público en general información completa sobre sus programas formativos y sobre su metodología de enseñanza-aprendizaje como universidad a distancia on-line, a través del portal web de la Universidad. Además ofrece información a través del servicio de atención individualizada de sus centros de apoyo y de las sesiones presenciales informativas de los distintos programas que se realizan en estos centros, así como a través del centro de atención telefónica de la universidad.

Una vez se formaliza la solicitud de acceso a la universidad, podemos decir que el proceso de acogida en la UOC para las nuevos estudiantes contempla de forma amplia los siguientes aspectos:

- La información sobre el programa: Presentación, Requisitos de acceso y titulación, Equipo docente, Plan de estudios, Reconocimiento de créditos, Precio y matrícula, Objetivos, perfiles y competencias, Salidas profesionales.
- La información sobre el entorno virtual de aprendizaje: el Campus Virtual y el Modelo educativo.
- 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.

A continuación explicamos con más detalle el asesoramiento que reciben los futuros estudiantes a partir del momento en que solicitan su acceso a la Universidad y reciben información de toda la documentación que deberá presentar. Se inicia entonces el proceso de tramitación de dicha solicitud, que implica 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. Además, se le asigna un tutor o tutora, que le dará apoyo y orientaciones en el momento de formalizar su primera matrícula, y accede a un aula de tutoría donde encuentra información relevante para su acceso a la universidad. El tutor/a, dependiendo de cuál sea el perfil personal, académico y profesional del estudiante, orientará la propuesta de matrícula, valorando tanto la carga docente en créditos que éste 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. En caso de que sea necesario el tutor le derivará a otros servicios: atención a estudiantes con discapacidad, explicado en el apartado 4.2; recomendación de la prueba de nivel de idiomas oficiales en el caso de estudiantes extranjeros; recomendación de la prueba de nivel de idioma extranjero para estudiantes en general; recomendación de refuerzo formativo en aquellos aspectos que se consideren relevantes

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 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.

Sumándose a la acción del tutor/a, y para atender cuestiones no exclusivamente docentes de la incorporación del estudiante (información relativa a aplicaciones informáticas, material impreso…), la universidad 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 operativa o administrativa. El

Servicio de ayuda informática asesora a los usuarios en relación a las posibles dudas o incidencias que puedan surgir en la utilización del Campus Virtual, los problemas de acceso a los recursos de aprendizaje y el software facilitado por la universidad.

4.2. Requisitos de acceso y criterios de admisión

Las vías de acceso al Máster son las previstas en la normativa aplicable legalmente tal y como quedan recogidos en los artículos 10, 11 y 12 del *Capítulo II. Acceso a estudios universitarios de grado y máster universitario* de la Normativa académica de la Universitat Oberta de Catalunya aplicable a los estudios universitarios EEES, aprobada por el Comité de Dirección Ejecutivo de 18 de diciembre de 2012 y por la Comisión Permanente del Patronato de 9 de abril de 2013:

Capítulo II . Acceso a estudios universitarios de grado y máster universitario

Sección 2.ª Acceso a estudios de máster universitario

Artículo 10. Requisitos de acceso a estudios de máster universitario
1. Pueden acceder a estudios de máster universitario los estudiantes que cumplen con alguno de los siguientes requisitos de acceso:
a. Los estudiantes que están en posesión de un título universitario oficial español o de un título expedido por una institución de educación superior que pertenezca a un estado integrante del espacio europeo de educación superior que faculte para acceder a enseñanzas oficiales de máster.
b. Los estudiantes que están en posesión de una titulación emitida por una institución de educación superior ajena al espacio europeo de educación superior y que han obtenido su homologación con el título universitario oficial español que corresponda.
c. Los estudiantes que están en posesión de una titulación emitida por una institución de educación superior ajena al espacio europeo de educación superior y, sin necesidad de homologación de su título, acreditan en la Universidad un nivel de formación equivalente a los correspondientes títulos oficiales españoles, y que faculta en el país expedidor del título para el acceso a enseñanzas de posgrado.
2. Con relación a la letra a del apartado anterior, los estudiantes que están en posesión de un título oficial de Licenciado, Ingeniero, Arquitecto, Diplomado, Ingeniero Técnico o Arquitecto Técnico pueden acceder a enseñanzas oficiales de máster universitario sin ningún requisito adicional de acceso.
La Universidad puede exigir formación adicional necesaria para el acceso a un máster universitario a los estudiantes que están en posesión de un título de Diplomado, Ingeniero Técnico o Arquitecto Técnico, teniendo en cuenta la adecuación entre las competencias y los

conocimientos derivados de las enseñanzas cursadas en el plan de estudios de origen y los previstos en el plan de estudios del máster universitario de destino, de acuerdo con lo que se haya previsto en la memoria del máster universitario.

Artículo 11. Verificación del nivel de formación de un título de educación superior ajeno al EEES

1. De acuerdo con la vía de acceso prevista en el artículo 10.1.c de esta normativa, los titulados en sistemas educativos ajenos al espacio europeo de educación superior que quieren acceder a un máster universitario sin necesidad de homologación, deben solicitar la verificación de su nivel de formación.

2. La solicitud de verificación del nivel de formación hay que hacerla por los canales y en los plazos establecidos por la Universidad, y acompañarla de la siguiente documentación:

a. Fotocopia del título de educación superior.

b. Fotocopia de la certificación académica o documento oficial que acredita que el título de educación superior permite el acceso a enseñanzas de posgrado. La UOC podrá verificar de oficio el nivel de formación.

Salvo que la documentación haya sido expedida por un estado miembro de la Unión Europea, hay que entregarla correctamente legalizada por vía diplomática o, en su caso, mediante la apostilla del convenio de La Haya de 5 de octubre de 1961. Asimismo, si la documentación original no está en lengua catalana, española o inglesa, se debe entregar legalmente traducida por un traductor jurado, por cualquier representación diplomática o consular del Estado español en el extranjero, o por la representación diplomática o consular en España del país del cual es ciudadano el estudiante o, en su caso, del de procedencia del documento.

3. Los estudiantes que obtienen la verificación de su nivel de formación, pueden acceder a la Universidad por esta vía y formalizar la matrícula en las enseñanzas de máster universitario solicitadas.

4. La admisión a estudios de máster universitario por esta vía en ningún caso implica la homologación del título extranjero de educación superior, ni el acceso a otros estudios distintos a los solicitados.

Artículo 12. Criterios específicos de admisión a máster universitario

1. Los estudiantes pueden ser admitidos a un máster universitario de acuerdo con los requisitos específicos de admisión y los criterios de valoración de méritos establecidos para cada máster universitario.

2. Los requisitos de admisión pueden consistir en la necesidad de superar complementos formativos en ámbitos disciplinarios concretos, en función de la formación previa acreditada por el estudiante. Estos complementos formativos podrán formar parte del máster universitario siempre y cuando en total no se superen los 120 créditos.

Criterios de admisión

No existen criterios específicos de admisión para los perfiles de ingreso recomendados.
Los estudiantes que provengan de otras titulaciones deberán acreditar su competencia en el campo de las tecnologías de la información y de las comunicaciones, ya sea a través de programas no oficiales, certificaciones profesionales, o experiencia profesional en el sector.
Estos estudiantes deberán cursar hasta un máximo de 12 ECTS de complementos formativos para poder ser admitidos al máster. Estos créditos se impartirán en 2 asignaturas:

- (1) Administración de redes y de sistemas operativos (6 ECTS)
- (2) Fundamentos de redes y arquitecturas (6 ECTS)

Mediante una evaluación personalizada de las competencias previas de cada estudiante, según su bagaje profesional y de acuerdo con las certificaciones acreditadas, la Comisión de Admisión valorará en cada caso la admisión de estos estudiantes al programa y los créditos de complementos de formación a cursar.
A continuación se detallan los principales perfiles y certificaciones profesionales válidas para acreditar la competencias de acceso:

a) Perfiles que pueden acceder al programa sin necesidad de cursar complementos de formación:
   - Los siguientes perfiles profesionales que acrediten un mínimo de 3 años de experiencia profesional a tiempo completo:
     - Administrador/a de la red de una organización
     - Analista y técnico/a de administración de bases de datos
     - Ingeniero/a del software
     - Responsable de la seguridad informática de la red empresarial
     - Périto forense de sistemas informáticos
     - Auditor/a de sistemas informáticos
     - Implantador/a de sistemas de gestión de la seguridad de la información
     - Analista/programador
     - Ingeniero/a de comunicación de datos
   - Certificación CISSP de $(ISC)^2$
   - Certificación CCNA/CCNP/CCIE de CISCO
   - Certificación CISA de ISACA

b) Perfiles que pueden acceder al programa y deberán cursar de 6 a 12 ECTS de complementos de formación, según la valoración de la Comisión de admisión, de acuerdo con su experiencia previa y/o certificaciones profesionales aportadas:
   - Los siguientes perfiles profesionales que acrediten un mínimo de 1 año de experiencia profesional a tiempo completo:
     - Diseñador/a de redes de comunicación
     - Programador/a Multimedia
     - Diseñador/a rich-media

  - Especialista en gestión de redes
  - Gestor/a de proyectos
  - Especialista en información de la web
  - Consultor/a de empresas de tecnología de la información
  - Especialista en mantenimiento y apoyo al soporte
  - Perfiles profesionales del apartado (a) con 1 año de experiencia
- Certificaciones CISM de ISACA
- Certificación ISO 27001 Lead Implementer
- Certificación CEPRAL-COETIC-CNA (nivel 2 o superior)
- Certificación CEPRAL-COETIC-NSM (nivel 2 o superior)

La Comisión de admisión valorará otras posibles certificaciones y perfiles profesionales no recogidos en este listado, y que acrediten las competencias necesarias para acceder a la titulación..

Para acreditar los perfiles y certificaciones profesionales de acceso, los estudiantes deberán presentar uno de estos dos grupos de documentación:

a) certificaciones profesionales de CISCO, (ISC)^2, ISACA, del Col·legi Oficial d'Enginyeria Tècnica en Informàtica de Catalunya (COETIC), o del Colegio Profesional de Ingenieros Técnicos en Informàtica de Galicia (CPETIG)
b) un currículum vitae que incluya una breve descripción de los puestos de trabajo vinculados a esta área y las competencias obtenidas; el contrato laboral o certificado de vida laboral que acredite su experiencia profesional, o el certificado profesional que consideren relevante, así como otras evidencias objetivas de sus competencias en el sector (proyectos publicados en github, reconocimientos en el perfil de Linkedin, etc.).

En caso de que el número de solicitudes exceda al de las plazas ofertadas, la admisión se realizará de acuerdo a la siguiente preferencia:

- En primer lugar, titulados en el ámbito de la ingeniería informática, telecomunicación, o titulaciones equivalentes o afines.
- En segundo lugar, los que no siendo titulados de los ámbitos descritos anteriormente evidencien experiencia profesional en el campo de conocimiento del título.
- En igualdad de circunstancias, la asignación de las plazas se hará por orden de solicitud de admisión.

La comisión de Admisión está compuesta por el director académico y el equipo de tutores de la titulación.

La información sobre los complementos formativos queda especificada en el apartado 4.6.

Estudiantes con discapacidad

La misión de la Universitat Oberta de Catalunya es facilitar la formación de las personas a lo largo de la vida. Con el objetivo primordial de satisfacer las necesidades de aprendizaje de cada persona con el máximo acceso al conocimiento, la UOC ofrece un modelo educativo basado en la personalización y el acompañamiento permanente al estudiante, con un uso de las tecnologías de la comunicación y la información que permite romper con las barreras del tiempo y el 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.

El catálogo de servicios que ofrece la universidad a los estudiantes con discapacidad es el siguiente:

- 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 en la UOC información sobre el tipo de apoyo que para cada caso pueden obtener de la universidad.

- Recursos de aprendizaje de las asignaturas: Los recursos de aprendizaje 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 recursos en formato XML a partir del cual se generan versiones de un mismo contenido en múltiples formatos, como pueden ser 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 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 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 acto de graduación, y otras son obligatorias, como la realización de las pruebas finales de evaluación.

    - 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 atender 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 secretaría del campus los estudiantes encuentran información sobre el procedimiento a seguir para solicitar adaptaciones para la realización de las pruebas presenciales. A través de la cumplimentación de 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

Por lo que se refiere a facilidades de tipo económico, la UOC aplica al colectivo de estudiantes con un grado de minusvalía como mínimo del 33% las mismas exenciones y descuentos que el resto de universidades públicas catalanas.

4.3. Apoyo a estudiantes

Una vez el estudiante de nuevo ingreso formaliza su matrícula en la universidad con las orientaciones de su tutor/a, tiene acceso a las aulas virtuales de las asignaturas que cursa durante el semestre.

La responsabilidad sobre las asignaturas del Máster recae en el **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 calidad de 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 recursos de aprendizaje hasta la selección, coordinación y supervisión de los profesores colaboradores, 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 profesor 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 profesor colaborador, y tal y como ya se ha explicado, 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 los itinerarios académicos y profesionales más adecuados 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 sus 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 de la UOC. 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.

Así mismo el estudiante tiene a su disposición, desde el inicio del semestre, todos los recursos de aprendizaje de cada una de las asignaturas de las que se ha matriculado. Los estudiantes encuentran en ellos 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 los resultados de aprendizaje previstos 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. 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 y servicio de información a medida. Además, ofrece formación a los usuarios para facilitar el uso de los servicios.

4.4. Sistema de transferencia y reconocimiento de créditos

Reconocimiento de créditos cursados en Títulos propios (adjuntar plan de estudios del título propio, si es el caso de superar el 15%)	
Mínimo 0	Máximo 48
Reconocimiento de créditos cursados por Acreditación de Experiencia Laboral y Profesional *(hasta un máximo del 15% del total de ECTS de la titulación)***	
Mínimo 0	Máximo* 6 ver apartado 4.4.3

** *La suma conjunta de lo reconocido por título propio más RAEP será como máximo de 9 créditos (o 15% del total de créditos del MU), excepto en el caso que se pueda reconocer más créditos del título propio.*

4.4.1. Reconocimiento de créditos

El reconocimiento de créditos es la aceptación por parte de la UOC de los conocimientos y de las competencias obtenidas en enseñanzas universitarias, cursadas en la UOC o en otra Universidad, para que computen a los efectos de obtener una titulación universitaria de carácter oficial.

Las asignaturas reconocidas mantendrán la misma calificación obtenida en el centro de procedencia.

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 reconocidos podrán ser incorporados, previa matrícula, al expediente académico del estudiante y serán reflejados 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.

Los estudios 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 establecidos por la Universidad, 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.

Se aporta a continuación el texto de la normativa UOC que recoge los aspectos relativos a la transferencia y reconocimiento de créditos.

Título IV. Transferencia y reconocimiento de créditos

Capítulo I. Disposiciones generales
Artículo 59. Ámbito de aplicación
1. Este título tiene por objeto regular la transferencia y el reconocimiento de créditos que se imparten en la UOC.
2. Las normas establecidas en este título se aplican a los créditos obtenidos previamente en el marco de unas enseñanzas universitarias oficiales, unas enseñanzas universitarias propias y otras enseñanzas superiores, en determinadas actividades no programadas en los planes de estudios o por la experiencia profesional.
Artículo 60. Efectos académicos
1. Todos los créditos obtenidos por el estudiante en enseñanzas oficiales cursadas en cualquier universidad, los transferidos, los reconocidos y los superados para la obtención del correspondiente título, se incluyen en el expediente académico del estudiante y quedan reflejados en el suplemento europeo del título.

2. Los créditos reconocidos se incorporan al expediente académico con la calificación obtenida en el centro de procedencia, de acuerdo con el sistema de calificaciones previsto en el artículo 98.2, salvo en los casos siguientes:
a. Cuando el reconocimiento se produce por la aceptación de los créditos correspondientes a más de una asignatura, se otorga la calificación media de estas asignaturas.
b. Cuando se reconocen paquetes de créditos de formación básica, estos créditos no computan a efectos de calificación media del expediente académico.
c. Cuando se reconocen créditos por participación en actividades universitarias culturales, deportivas, de representación estudiantil, solidarias y de cooperación (RECAAU), se incorporan con la calificación «apto» y no computan a efectos de calificación media del expediente.
d. Cuando se reconocen créditos por la experiencia profesional y por enseñanzas propias no se incorpora ninguna calificación y, por lo tanto, no computan en la calificación media del expediente.
e. Cuando se reconocen minors se incorporan con la calificación media de las asignaturas superadas que forman parte del minor.
3. Los créditos reconocidos por estudios universitarios extranjeros se convertirán al sistema de calificaciones previsto en el artículo 98.2.
Artículo 61. Efectos económicos
El reconocimiento y la transferencia de créditos objeto de este título comportan los efectos económicos que se prevén en la normativa económica de la UOC.
Artículo 62. Reconocimiento de créditos
1. El reconocimiento de créditos es la aceptación en un estudio oficial o propio de la UOC de los créditos que, habiendo sido obtenidos en enseñanzas oficiales, en la propia UOC o en otra universidad, son computados a efectos de la obtención de un título oficial. Igualmente, se pueden reconocer créditos obtenidos en otras enseñanzas superiores oficiales, en enseñanzas universitarias conducentes a la obtención de otros títulos no oficiales, y en actividades universitarias no programadas en el plan de estudios en curso. También se pueden reconocer créditos mediante la experiencia profesional.
2. En cualquier caso, no pueden ser objeto de reconocimiento los créditos correspondientes a los trabajos finales de grado (TFG), trabajos finales de máster universitario o máster propio (TFM) y proyectos finales de posgrado (PFP).
3. Tampoco pueden ser objeto de reconocimiento los créditos correspondientes a asignaturas calificadas con "apto para compensación".
Artículo 63. Transferencia de créditos
1. La transferencia de créditos es la incorporación, en los documentos académicos oficiales acreditativos de la enseñanza cursada por un estudiante, de los créditos obtenidos en otras enseñanzas oficiales cursadas con anterioridad, tanto en la UOC como en otras universidades, que no hayan sido tenidos en cuenta en esta enseñanza para la obtención del título oficial correspondiente.

2. Los créditos objeto de transferencia no cuentan para la obtención del título y quedan reflejados únicamente a efectos informativos.
3. Para la transferencia de créditos se seguirá el procedimiento descrito en el capítulo III relativo al procedimiento para el reconocimiento de créditos.
Capítulo II. Criterios para el reconocimiento de créditos
Sección 1ª. Reconocimiento de créditos en programas de grado
Artículo 64. Estudios de grado
El reconocimiento de créditos en los estudios de grado se hará de acuerdo con los siguientes criterios:
I. Cuando la enseñanza universitaria oficial de origen pertenece a la misma rama de conocimiento que el grado de destino:
a. Los créditos de formación básica se reconocen de acuerdo con los siguientes criterios, que se aplicarán de forma jerárquica:
1º Se reconocen los créditos aportados cuando los conocimientos y las competencias adquiridas en el plan de estudios de origen se adecúen a las competencias y los conocimientos de asignaturas del plan de estudios de grado de destino; los créditos reconocidos serán únicamente los de la asignatura reconocida del grado de destino (los créditos aportados que superen el número de créditos reconocidos no darán lugar a ningún tipo de compensación o reconocimiento independiente).
2º El resto de créditos correspondientes a materias de formación básica que no hayan sido objeto de reconocimiento de acuerdo con el criterio mencionado en el apartado anterior, se reconocen mediante paquetes de, como mínimo, seis (6) créditos de formación básica, con indicación de la materia correspondiente, de acuerdo con lo siguiente:
i. En el caso de enseñanzas finalizadas, el estudiante obtendrá el reconocimiento como mínimo, el quince (15) por ciento de los créditos de formación básica de la misma rama de conocimiento del plan de estudios del grado de destino.
ii. En el caso enseñanzas parciales, el estudiante obtendrá el reconocimiento de, como mínimo, el mismo número de créditos de formación básica de la misma rama de conocimiento que haya aportado hasta el número de créditos máximos de formación básica de la misma rama de conocimiento del plan de estudios del grado de destino.
3º El número máximo de créditos de formación básica de la misma rama que se pueden reconocer serán los fijados en el programa de grado de destino.
4º El reconocimiento de créditos de formación básica entre grados de la misma rama solo se evaluará una vez. Si el estudiante realiza una nueva aportación desde el mismo plan de estudios de origen hacia el mismo plan de estudios de destino, solo se tendrá en cuenta la adecuación de competencias y conocimientos entre ambas titulaciones.
5º El estudiante puede optar entre matricularse en los paquetes de créditos reconocidos, o bien cursar las asignaturas de formación básica de la materia correspondiente. Si el estudiante opta

por matricularse en los paquetes de créditos reconocidos, se presume que desiste de cursar las correspondientes asignaturas de formación básica.
b. Los créditos obligatorios y optativos de un grado pueden ser reconocidos teniendo en cuenta la adecuación entre las competencias y los conocimientos adquiridos en el plan de estudios de origen y las competencias y los conocimientos del plan de estudios de destino.
II. Cuando las enseñanzas universitarias oficiales de origen no pertenecen a la misma rama de conocimiento que el grado de destino, el reconocimiento de créditos resultará únicamente de la adecuación entre las competencias y los conocimientos, y de las enseñanzas aportadas y los del plan de estudios de grado de destino. Los créditos reconocidos serán únicamente los de la asignatura reconocida del grado de destino; los créditos aportados que superen el número de créditos reconocidos no darán lugar a ningún tipo de compensación o reconocimiento independiente.
Artículo 65. Enseñanzas universitarias extranjeras
Podrán ser objeto de convalidación los estudios universitarios extranjeros que cumplan los criterios establecidos en el Real decreto 967/2014.
Artículo 66. Títulos universitarios oficiales correspondientes a la anterior ordenación universitaria (LRU)
Los estudios conducentes a la obtención de un título universitario oficial de la anterior ordenación universitaria son susceptibles de reconocimiento si existe adecuación entre las competencias, los conocimientos y los resultados de aprendizaje de las enseñanzas universitarias oficiales aportados y las enseñanzas del grado de destino. Para el reconocimiento de créditos de formación básica se aplican los criterios previstos en el artículo 64.
Artículo 67. Enseñanzas no oficiales y experiencia profesional
1. La experiencia profesional acreditada y los créditos obtenidos en enseñanzas universitarias conducentes a la obtención de otros títulos no oficiales, pueden ser reconocidos en forma de créditos que computan a efectos de la obtención de un título oficial.
2. La experiencia profesional susceptible de reconocimiento académico tiene que estar relacionada con las competencias inherentes al título.
3. El número de créditos que son objeto de reconocimiento a partir de la experiencia profesional y de enseñanza universitarios no oficiales no puede ser superior, en su conjunto, al quince (15) por ciento del total de créditos que constituyen el plan de estudios.
Los créditos reconocidos, una vez matriculados, se incorporan al expediente académico sin calificación y no se tienen en cuenta a efectos del cómputo de la media del expediente académico del estudiante.
Si como consecuencia de la aportación de la experiencia profesional y/o de enseñanzas universitarias no oficiales se reconoce un número de créditos que excede este porcentaje, el estudiante debe elegir qué créditos incorpora al expediente académico para no superar el mencionado porcentaje. Estos créditos, una vez incorporados, no pueden ser objeto de modificación.

4. Excepcionalmente, los créditos procedentes de títulos propios pueden ser objeto de reconocimiento en un porcentaje superior al señalado en el apartado anterior o, en su caso, ser objeto de reconocimiento en su totalidad, siempre que el título propio correspondiente haya sido extinguido y substituido por un título oficial, y la memoria de verificación del título oficial de destino así lo permita.

5. A efectos de calcular el máximo del quince (15) por ciento establecido en el apartado 3, no tienen la consideración de reconocimiento de créditos:

a. Las asignaturas que forman parte de un programa oficial, pero que han sido matriculadas en el marco del @teneo o de la oferta propia de la UOC.

b. Los certificados de escuelas oficiales de idiomas (o títulos equivalentes) o de la Escuela de Lenguas o Centro de Idiomas Modernos de la UOC.

Artículo 68. Reconocimiento de créditos académicos por actividades universitarias (RECAAU)

1. Por la participación en actividades universitarias culturales, deportivas, de representación estudiantil, solidarias y de cooperación (RECAAU), se puede obtener el reconocimiento de hasta un máximo de seis (6) créditos ECTS optativos.

2. El reconocimiento de créditos ECTS solo se puede solicitar con respecto a actividades universitarias realizadas mientras se cursa el plan de estudios conducente a la obtención del título universitario oficial de grado para el cual se solicita el reconocimiento. Solo son susceptibles de reconocimiento de créditos ECTS las actividades universitarias realizadas a partir del curso académico 2007/2008.

3. La relación de actividades universitarias susceptibles de reconocimiento de créditos académicos son las que se indican en el anexo II de esta normativa. Anualmente, la Comisión Académica de la UOC revisa y actualiza el catálogo de actividades universitarias susceptibles de reconocimiento académico.

Artículo 69. Programas o convenios de movilidad

1. La movilidad externa de los estudiantes de la UOC será reconocida académicamente de acuerdo con los criterios generales de movilidad de la titulación y los criterios específicos de cada programa de movilidad o convenio de movilidad.

2. El reconocimiento académico de la movilidad requiere que el programa de estudios que el estudiante pretende cursar y, en su caso, los cambios que se introduzcan en él, hayan sido aprobados por el coordinador de movilidad de los estudios.

3. A efectos de establecer la correspondencia entre asignaturas, hay que atenerse al valor formativo conjunto de las actividades académicas desarrolladas sin que haga falta una identidad completa entre asignaturas y programas.

4. El reconocimiento académico de las asignaturas superadas durante una estancia de movilidad externa se puede hacer por:

a. Asignaturas: los créditos cursados dentro de un programa de movilidad o convenio en el que participe la UOC pueden ser reconocidos e incorporados al expediente del estudiante si se puede

establecer una correspondencia, en conocimientos y competencias, con asignaturas del plan de estudios del estudiante.
b. Las asignaturas superadas durante la estancia de movilidad que no hayan sido objeto de reconocimiento aparecerán en el expediente académico y en el suplemento europeo del título como créditos transferidos.
Artículo 70. Mínors
1. Dentro de los programas de grado, y de acuerdo con el número de créditos previsto para cada uno, la UOC ofrece a los estudiantes la posibilidad de matricularse en mínors, orientados a lograr competencias propias de un ámbito de conocimiento diferente al de la propia enseñanza de grado a través de asignaturas optativas de otros planes de estudios. La Universidad aprueba periódicamente el catálogo de los mínors disponibles para cada programa de grado y lo publica en el Campus Virtual.
2. Una vez superadas todas las asignaturas que forman parte de un mínor, el creditaje del mínor se incorpora al expediente de grado como créditos optativos reconocidos que computan a efectos de la obtención del título.
3. Solo se puede incorporar un mínor por plan de estudios de grado, y de acuerdo con la disponibilidad de créditos establecida para cada programa de grado. Las asignaturas del mínor se tienen que cursar y superar mientras está abierto el expediente de grado.
4. Si no se finaliza el mínor en su totalidad, las asignaturas que se hayan superado no pueden ser objeto de reconocimiento de créditos optativos. No obstante, estas asignaturas constarán como asignaturas transferidas y aparecerán al expediente académico y en el suplemento europeo del título.
Sección 2ª. Reconocimiento de créditos a programas de máster universitario
Artículo 71. Títulos universitarios oficiales
1. Los estudios conducentes a la obtención del título oficial de grado no son susceptibles de reconocimiento de créditos en enseñanzas de máster universitario.
2. Los estudios conducentes a la obtención del título oficial de máster universitario son susceptibles de reconocimiento de créditos cuando sean equivalentes con las competencias y los conocimientos de las asignaturas del máster universitario de destino.
Artículo 72. Enseñanzas universitarias extranjeras
1. Los mismos criterios del artículo 71 son de aplicación con respecto a las enseñanzas universitarias extranjeras.
2. Sin perjuicio de lo previsto en el artículo 11 para el acceso a máster universitario, también se pueden considerar a efectos de reconocimiento los títulos extranjeros de máster que hayan sido homologados con alguno de los títulos españoles oficiales de educación superior, cuando las competencias y los conocimientos de las asignaturas se adecúen a las competencias y los conocimientos de las asignaturas del máster universitario de destino.
Artículo 73. Enseñanzas correspondientes a la anterior ordenación universitaria (LRU)

1. Los estudios conducentes a la obtención del título oficial de Diplomado, Ingeniero Técnico y Arquitecto Técnico no son susceptibles de reconocimiento de créditos en enseñanzas de máster universitario.
2. Los estudios conducentes a la obtención del título oficial de Licenciado, Ingeniero y Arquitecto son susceptibles de reconocimiento de créditos cuando se adecúen a las competencias y los conocimientos de las asignaturas del máster universitario de destino.
Artículo 74. Enseñanzas no oficiales y experiencia profesional
El reconocimiento de créditos por enseñanzas no oficiales y por la experiencia profesional se regula en iguales condiciones que las previstas en el artículo 67, en todo aquello que les sea de aplicación.
Artículo 75. Programas o convenios de movilidad
La movilidad externa de los estudiantes de la UOC será reconocida académicamente en iguales condiciones que las previstas en el artículo 69, en todo aquello que les sea de aplicación.
Sección 3ª. Reconocimiento de créditos en programas propios
Artículo 76. Reconocimiento de créditos en programas propios
Para el reconocimiento de créditos en másteres propios y diplomas de posgrado y de extensión universitaria será de aplicación aquello previsto en la sección 2ª (artículos 71 a 75), no siendo de aplicación el límite del 15% previsto en el artículo 67.3 por remisión del artículo 74. Para estos programas, el máximo de créditos que se pueden reconocer provenientes de enseñanzas no oficiales o por experiencia profesional dependerá de las características y especificidades de cada programa. La experiencia profesional susceptible de reconocimiento académico debe estar relacionada con las competencias inherentes al programa. En ningún caso pueden ser reconocidos los créditos correspondientes al trabajo de final de máster (TFM) o el proyecto final de posgrado (PFP).
Capítulo III. Procedimiento de evaluación de estudios previos (EEP)
Artículo 77. Evaluación de estudios previos (EEP)
El reconocimiento y la transferencia de créditos se solicita a través de una evaluación de estudios previos, trámite académico que permite a los estudiantes reconocer su bagaje formativo, cursado en la UOC o en cualquier otro centro de enseñanza superior.
Artículo 78. Comisión de Evaluación de Estudios y Experiencia Profesional Previos (Comisión de EEEPP)
1. La Comisión de Evaluación de Estudios y Experiencia Profesional Previos es el órgano competente para emitir las resoluciones de las solicitudes de evaluación de estudios previos realizadas por los estudiantes.
2. La Comisión de Evaluación de Estudios y Experiencia Profesional Previos está formada por el vicerrector o vicerrectora con competencias en ordenación académica, que la preside, así como por los directores de programa de la Universidad. Actúa como secretario o secretaria la persona responsable de esta gestión en la Universidad.

3. Las funciones de la Comisión de Evaluación de Estudios y Experiencia Profesional Previos son las siguientes:
a. Evaluar la adecuación entre las competencias, los conocimientos y los resultados de aprendizaje de los estudios aportados y del plan de estudios de destino, de acuerdo con la normativa académica de la Universidad y las disposiciones de carácter general sobre esta materia.
b. Evaluar el reconocimiento académico de la experiencia profesional.
c. Resolver las solicitudes de evaluación presentadas por los estudiantes.
d. Velar por el cumplimiento de los criterios en materia de reconocimiento y transferencia aprobados en esta normativa.
e. Resolver las alegaciones formuladas a sus resoluciones.
f. Cualquier otra función que, en materia de reconocimiento de créditos, se le pueda encomendar.
Artículo 79. Solicitud de evaluación de estudios previos
1. El reconocimiento y transferencia de créditos se formaliza únicamente mediante una solicitud de evaluación de estudios previos, por los canales y en los plazos establecidos por la Universidad. El estudiante puede realizar tantas solicitudes de evaluación de estudios previos como considere necesario.
2. Solo se tendrán en cuenta las solicitudes de evaluación de estudios cuando previamente se hayan realizado los siguientes trámites:
a. Haber introducido los datos de los estudios previos cursados en la aplicación de EEP, detallando toda la información que se solicita (denominación de la asignatura, creditaje, tipología, calificación, convocatoria y duración).
b. Haber abonado el importe del precio asociado a este trámite académico.
c. Haber entregado la documentación requerida de al menos una de las enseñanzas aportadas.
3. Cuando se disponga de una mesa de equivalencia entre los programas de estudios de origen y de destino, en el momento de formalizar la solicitud el estudiante podrá ver la simulación de reconocimiento de créditos. Esta simulación no es vinculante ni condiciona la resolución final de la Comisión de Evaluación de Estudios Previos.
Artículo 80. Tasa asociada a la solicitud de evaluación de estudios previos
1. La solicitud de evaluación de estudios previos tiene asociado un precio, de acuerdo con lo dispuesto en la Normativa económica de la UOC.
2. Los estudiantes que se encuentren en alguna de las condiciones que dan derecho a obtener una bonificación y/o exención en el importe del precio de este trámite académico tienen que acreditar esta condición de acuerdo con lo dispuesto en la Normativa económica de la UOC.
3. Los estudiantes que en su solicitud de evaluación de estudios previos solo aportan enseñanzas cursadas en la UOC, están exentos de abonar el precio de evaluación de estudios previos.
Artículo 81. Documentación asociada a la solicitud de evaluación de estudios previos
1. Si los estudios previos aportados han sido cursados en la UOC, no se requiere aportar ninguna documentación asociada a la solicitud de evaluación de estudios previos.

2. Si los estudios previos aportados han sido cursados en cualquier otra universidad, hay que aportar, junto con la solicitud, la siguiente documentación para cada aportación:
a. Original o fotocopia compulsada del certificado académico, en el que consten las asignaturas, las calificaciones obtenidas, los créditos, el tipo de asignación de la asignatura, la convocatoria y el año de superación de los estudios, tanto si los estudios previos aportados han sido finalizados como si no. Cuando el sistema de calificaciones sea distinto al establecido en el Real decreto 1125/2003, de 5 de septiembre, se deberá incluir la explicación correspondiente del sistema de calificaciones de la universidad de origen.
b. Fotocopia compulsada del título, si los estudios previos aportados han sido finalizados.
c. Fotocopia de los programas de las asignaturas superadas, con el sello del centro de procedencia, solo cuando no haya tabla de equivalencia o esta indique que no se dispone del programa de aquella asignatura.
3. Si los estudios previos han sido cursados en un centro extranjero, salvo que la documentación haya sido expedida por un estado miembro de la Unión Europea, hay que entregarla correctamente legalizada por vía diplomática o, en su caso, mediante la apostilla del convenio de La Haya de 5 de octubre de 1961. Asimismo, si la documentación original no está en lengua catalana, española o inglesa, se debe entregar legalmente traducida por un traductor jurado, por cualquier representación diplomática o consular del Estado español en el extranjero, o por la representación diplomática o consular en España del país del cual es ciudadano el candidato o, en su caso, del de procedencia del documento.
Artículo 82. Resolución de la solicitud de evaluación de estudios previos
1. Las solicitudes de evaluación de estudios previos consideradas válidas son evaluadas y resueltas por la Comisión de Reconocimiento Académico, de acuerdo con los criterios y tablas que se establezcan para cada convocatoria.
2. La resolución de evaluación de estudios previos se notifica al estudiante por correo electrónico en su buzón de la UOC. El estudiante también puede acceder a la resolución consultando su expediente académico.
3. Sobre la base de los créditos reconocidos en la resolución de evaluación de estudios previos, el estudiante puede decidir si incorpora a su expediente los créditos reconocidos, o bien se matricula en ellos para cursar su docencia. Una vez el estudiante se ha matriculado en los créditos reconocidos y los ha incorporado al expediente académico, no se puede modificar el reconocimiento de estas asignaturas.
4. Los estudiantes disponen de un plazo de quince (15) días naturales desde la formalización de la solicitud de evaluación de estudios previos para abonar el importe del precio y para entregar la documentación requerida.
5. Transcurrido este plazo sin haber satisfecho el importe del precio o sin haber entregado la documentación, la solicitud de evaluación de estudios previos se considera inválida y para obtener la evaluación será necesario formalizar una nueva solicitud en el siguiente periodo de evaluación de estudios previos.

6. En la Normativa económica de la UOC se prevén las consecuencias económicas derivadas de una solicitud de estudios previos considerada inválida por no haber entregado la documentación en el plazo establecido, a pesar de haber abonado el precio correspondiente.

Artículo 83. Alegación contra la resolución de la solicitud de evaluación de estudios previos

1. Una vez notificada la resolución de evaluación de estudios previos, el estudiante dispone de un plazo de siete (7) días naturales para poder formular alegaciones.

2. Las alegaciones solo pueden hacer referencia a las aportaciones válidas de la solicitud de evaluación de estudios previos que formalizó el estudiante.

3. La resolución a las alegaciones planteadas por el estudiante se considera definitiva y contra esta no se pueden formular nuevas alegaciones.

Artículo 84. Vigencia de la resolución de evaluación de estudios previos

La resolución de evaluación de estudios previos es válida para el plan de estudios de destino solicitado y es vigente, a efectos de poder incorporar las asignaturas reconocidas al expediente, mientras se mantenga abierto el expediente académico del plan de estudios de destino. Una vez el estudiante se ha matriculado en los créditos reconocidos y los ha incorporado al expediente académico, no se puede modificar el reconocimiento de estas asignaturas.

Capítulo IV. Procedimiento para el reconocimiento académico de la experiencia profesional (RAEP)

Artículo 85. Reconocimiento académico de la experiencia profesional (RAEP)

1. La UOC ofrece a sus estudiantes, de acuerdo con lo dispuesto en el artículo 6.2 del Real decreto 1393/2007, de 29 de octubre, la posibilidad de reconocer créditos académicos a partir de la experiencia profesional que tenga relación con los contenidos y competencias asociados a las materias que hay que reconocer.

2. La Universidad establecerá anualmente para cada programa las asignaturas que pueden ser objeto de reconocimiento de créditos a partir de la experiencia profesional, y los requisitos y documentos que hay que aportar al efecto, así como las pruebas que, si procede, hay que realizar y superar.

Artículo 86. Solicitud de reconocimiento académico de la experiencia profesional

1. El reconocimiento de créditos a partir de la experiencia profesional se formaliza mediante una solicitud por los canales y en los plazos establecidos por la Universidad.

2. Solo se tendrán en cuenta las solicitudes de reconocimiento de la experiencia profesional cuando previamente se hayan realizado los siguientes trámites:

a. Haber indicado la titulación de destino y el rol profesional de origen por el cual se solicita el reconocimiento de la experiencia profesional.

b. Haber abonado el importe del precio asociado a este trámite académico.

c. Haber entregado la documentación requerida.

3. Cuando se haya establecido como requisito para el reconocimiento de la experiencia profesional, el estudiante deberá realizar y superar las pruebas que se hayan establecido.

Artículo 87. Documentación asociada a la solicitud de reconocimiento académico de la experiencia profesional
1. La solicitud de reconocimiento de la experiencia profesional debe ir acompañada de la documentación que la acredite, de acuerdo con lo establecido para cada programa. La UOC actualizará anualmente las tablas de RAEP.
2. La experiencia profesional se puede acreditar por alguno de los siguientes medios:
a. Original o fotocopia del certificado de vida laboral de la Tesorería General de la Seguridad Social.
b. Fotocopia de los contratos de trabajo o nombramiento.
c. Original o fotocopia de certificados de empresa, en el que se especifiquen las funciones y actividades llevadas a cabo.
d. Fotocopia compulsada del título profesional.
e. En el caso de trabajador autónomo o por cuenta propia, original o fotocopia del certificación de la Tesorería General de la Seguridad Social en el correspondiente régimen especial y descripción de la actividad desarrollada.
Artículo 88. Resolución de la solicitud de reconocimiento académico de la experiencia profesional
1. Las solicitudes de reconocimiento de la experiencia profesional son evaluadas y resueltas por la Comisión de Evaluación de Estudios y Experiencia Profesional Previos (EEEPP).. Cuando sea conveniente, dada la especificidad o los requerimientos de una evaluación concreta, se podrá nombrar una comisión específica para realizarla.
2. Las resoluciones de las solicitudes de reconocimiento de la experiencia profesional, su vigencia, así como las alegaciones en su contra, se regulan en las mismas condiciones que las previstas respectivamente en los artículos 82, 83 y 84 de la presente normativa académica.

Este programa reconoce más de un 15% de las titulaciones propias de la UOC de los posgrados del ámbito de la seguridad ofrecidos desde los cursos 2011-2012 a 2019-2020 y que se detallan a continuación. Se reconocerá un máximo de 48 créditos para todos los programas, y un máximo de 24 créditos por posgrado.

1) Posgrado de Gestión y Auditoría de la Seguridad

Posgrado en Gestión y Auditoría de la Seguridad	**Máster universitario en Ciberseguridad y Privacidad**
Legislación y regulación (6 ECTS)	Legislación y protección de datos (6 ECTS)
Sistemas de gestión de la seguridad (6 ECTS)	Sistemas de gestión de la seguridad (6 ECTS)

Análisis forense (6 ECTS)	Análisis forense (6 ECTS)
Auditoría técnica (6 ECTS)	Auditoría técnica (6 ECTS)

2) Posgrado de Seguridad en Redes y Sistemas

Posgrado de Seguridad en Redes y Sistemas	**Máster universitario en Ciberseguridad y Privacidad**
Vulnerabilidades de Seguridad (6 ECTS)	Fundamentos de ciberseguridad (6 ECTS)
Seguridad en redes (6 ECTS)	Arquitecturas y protocolos de seguridad (6 ECTS)
Seguridad en bases de datos (6 ECTS)	Seguridad y pentesting de servidores de datos (6 ECTS)
Seguridad en sistemas operativos (6 ECTS)	Seguridad y pentesting de sistemas (6 ECTS)

3) Posgrado de Seguridad en Servicios y Aplicaciones

Posgrado en Gestión y Auditoría de la Seguridad	**Máster universitario en Ciberseguridad y Privacidad**
Identidad digital (6 ECTS)	Privacidad (6 ECTS)
Programación de código seguro (6 ECTS)	Seguridad del software (6 ECTS)
Biometría (6 ECTS)	Biometría (6 ECTS)

En el documento Anexo se incluye el detalle de los Diplomas de Posgrado susceptibles de reconocimiento: objetivos, perfil profesional, competencias, programa académico y asignaturas que conforman el título.

4.4.2. Transferencia de créditos

La transferencia de créditos consiste en la **inclusión**, en los documentos académicos oficiales acreditativos de las enseñanzas universitarias oficiales cursadas por un estudiante, de las

asignaturas obtenidas, en la UOC o en otra universidad, en enseñanzas universitarias oficiales no finalizadas, que no hayan sido objeto de reconocimiento de créditos ECTS.

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.

4.4.3. Sistema de gestión del reconocimiento y transferencia de créditos

La Evaluación de Estudios Previos (EEP) es el trámite que permite a los estudiantes de la UOC 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 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 los/las directores/as de programa y es presidida por el Vicerrector competente en materia de ordenación académica de la Universidad. Actúa como secretario/a de la Comisión de EEP el responsable de este trámite en la Secretaría 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 (troncal, obligatoria, optativa 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 Universidad.

Realizada la solicitud de EEP, el estudiante dispone de un plazo máximo de 7 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 de la UOC. 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.

Las resoluciones de evaluación de estudios previos son válidas hasta la formalización de la matrícula en el mismo semestre o posteriores y se mantienen vigentes mientras se mantiene abierto el expediente académico del plan de estudios de destinación.

4.4.4. Reconocimiento de la experiencia profesional

La Ley Orgánica 4/2007, de 12 de abril, por la cual se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, abre la puerta al reconocimiento futuro de la experiencia laboral o profesional a efectos académicos. Concretamente, el artículo 36 de la Ley de Universidades -que regula la convalidación o adaptación de estudios, la validación de experiencia, la equivalencia de títulos y la homologación de títulos extranjeros- prevé en su nueva redacción que el Gobierno regule, previo informe del Consejo de Universidades, las condiciones para validar a efectos académicos la experiencia laboral o profesional.

El RD 1393/2007 de 29 de octubre modificado por el RD 861/2010 de 2 de julio, incorpora en el artículo 6 la regulación del reconocimiento de la experiencia profesional o laboral.

En la UOC, el reconocimiento la experiencia profesional se realiza a través de una evaluación que permite valorar las destrezas y los conocimientos adquiridos por el estudiante en su trayectoria profesional.

La UOC, que atiende preferentemente demandas de formación de personas que por motivos profesionales o familiares no pueden cursar aprendizaje universitario mediante metodologías presenciales, ha diseñado un protocolo de evaluación de estos conocimientos y experiencias previas, que ya ha sido aplicado en otros programas formativos y que se corresponde con el nuevo marco normativo.

El reconocimiento de la experiencia profesional se formaliza a través de una solicitud de dicho trámite a través de la Secretaría académica de la universidad, de acuerdo con los plazos establecidos.

Las solicitudes van acompañadas de las evidencias documentales que acreditan la experiencia profesional. Los documentos a entregar son los siguientes:

1. En el caso que el Rol profesional esté acreditado por un certificado oficial de un Colegio Profesional de Ingeniería Informática, la documentación a entregar es simplemente este certificado. La obtención de dicho certificado se gestiona a través del servicio Colegial de Certificación de la Experiencia Profesional para Reconocimientos Académicos y Laborales (CEPRAL) que ofrecen algunos colegios, como por ejemplo,el Col·legi Oficial d'Enginyeries Tècniques i Grau d'Enginyeria en Informàtica de Catalunya (COETIC).
2. En el caso que el estudiante debe acreditar la experiencia profesional a través de evidencias de su vida laboral, la documentación a entregar es la siguiente:
    - Original o fotocopia del certificado de vida laboral de la Tesorería General de la Seguridad Social.
    - Fotocopia de los Contratos de trabajo o Nombramientos.
    - Original o fotocopia de los certificados de empresa en que se especifiquen las funciones y actividades desarrolladas, o fotocopia compulsada del título profesional.
    - En caso de trabajador autónomo o por cuenta propia, el original o fotocopia del certificado de la Tesorería General de la Seguridad Social en el régimen especial correspondiente y descripción de la actividad desarrollada.

Una vez resuelta la solicitud del trámite, en caso de denegación los estudiantes pueden presentar alegación a través de los canales establecidos por la universidad.

Los procedimientos relacionados con el Reconocimiento de la experiencia profesional se recogen en el capítulo IV de la Normativa académica de la universidad, en sus artículos 85, 86, 87 y 88.

Este programa de Máster podrá reconocer hasta un máximo de 6 ECTS por la experiencia profesional previa según lo recogido en la siguiente tabla:

Rol profesional	Asignaturas	Requisitos	Documentación
Auditor ISO 27001	Auditoría técnica (6 ECTS)	Experiencia mínima de 3 años en: - Uso de herramientas MAGERIT, PILAR - Elaboración e implantación de planes de auditoría - Gestión de incidentes de seguridad	1) Vida laboral 2) Autoinforme 3) Evidencias profesionales (p.e. un certificado de empresa detallando las responsabilidades laborales)
Implantador de SGSI	Sistemas de Gestión de la Seguridad (6 ECTS	Experiencia mínima de 3 años en: - Elaboración de planes de seguridad - Elaboración de planes de continuidad de negocio	1) Vida laboral 2) Autoinforme 3) Evidencias profesionales (p.e. un certificado de empresa detallando las responsabilidades laborales)
Analista en Informática forense	Análisis forense (6 ECTS)	Perfil profesional CEPRAL Computer Forensics Analyst (o equivalente)	1) Certificación CFA nivel 6 o superior
Hacker ético	Seguridad y pentesting de servidores de datos (6 ECTS)	Experiencia mínima de 3 años en pentesting de servidores de datos, o	vía 1 1) Vida laboral 2) Autoinforme 3) Evidencias profesionales

		certificación profesional: - Certified Ethical Hacker (CEH) de EC-Council - Certificación de Pentesting en Hacking Ético – PCEH	(p.e. un certificado de empresa detallando las responsabilidades laborales) o vía 2 1) Certificación profesional CEH o PCEH vía 1
Pentester de sistemas	Seguridad y pentesting de Sistemas (6 ECTS)	Experiencia mínima de 3 años en pentesting de sistemas, o certificación profesional: * EC-Council Licensed Penetration Tester (LPT) Master * Global Information Assurance Certification Penetration Tester (GPEN) de GIAC (Global Information Assurance Certification) * GIAC Exploit Researcher & Advanced Penetration Tester (GXPN) també de GIAC * Offensive Security Certified Professional (OSCP)	vía 1 1) Vida laboral 2) Autoinforme 3) Evidencias profesionales (p.e. un certificado de empresa detallando las responsabilidades laborales) o vía 2 1) Certificación profesional LPT, GPEN, GXPN, OSCP

En caso de que se puedan acreditar competencias relacionadas con la titulación a través de actividades no previstas en esta tabla, se estudiará la posibilidad de reconocimientos más allá de los previstos aquí.

4.6. Descripción de los complementos formativos para la Admisión al Máster Universitario

Los estudiantes que provengan de titulaciones distintas al perfil de ingreso recomendado deberán acreditar su competencia en el campo de las tecnologías de la información y de las comunicaciones, ya sea a través de certificaciones profesionales, o experiencia profesional en el sector.
Estos estudiantes deberán cursar hasta un máximo de 12 ECTS de complementos formativos para poder ser admitidos al máster. Estos créditos se impartirán en 2 asignaturas:

- (1) Administración de redes y de sistemas operativos (6 ECTS)
- (2) Fundamentos de redes y arquitecturas (6 ECTS)

Mediante una evaluación personalizada de las competencias previas de cada estudiante, según su bagaje profesional y de acuerdo con las certificaciones acreditadas, la Comisión de Admisión valorará en cada caso la admisión de estos estudiantes al programa y los créditos de complementos de formación a cursar.
A continuación se detallan los principales perfiles de acceso que deberán cursar de 6 a 12 ECTS de complementos de formación, según la valoración de la Comisión de admisión, de acuerdo con su experiencia previa y/o certificaciones profesionales aportadas:

- Los siguientes perfiles profesionales que acrediten un mínimo de 1 año de experiencia profesional a tiempo completo:
    - Diseñador/a de redes de comunicación
    - Programador/a Multimedia
    - Diseñador/a rich-media
    - Especialista en gestión de redes
    - Gestor/a de proyectos
    - Especialista en información de la web
    - Consultor/a de empresas de tecnología de la información
    - Especialista en mantenimiento y apoyo al soporte
    - Perfiles profesionales del apartado (a) con 1 año de experiencia
- Certificaciones CISM de ISACA
- Certificación ISO 27001 Lead Implementer
- Certificación CEPRAL-COETIC-CNA (nivel 2 o superior)
- Certificación CEPRAL-COETIC-NSM (nivel 2 o superior)

La identificación de los complementos formativos correrá a cargo la Comisión de Admisión y se desarrollará de manera personalizada durante el período de incorporación, previo a la primera matrícula. No será obligatoria la realización de dichos complementos para acceder al Máster, pero sí será necesario que se realicen durante el primer o segundo semestre del programa para los estudiantes que lo cursen a tiempo parcial (en más de 1 año) y durante el primer semestre para los estudiantes que lo cursen a tiempo completo (1 año).

5. PLANIFICACIÓN DE LAS ENSEÑANZAS

5.1. Descripción del plan de estudios

Objetivos generales del título

Este máster universitario tiene como principal objetivo la formación de especialistas en el ámbito de la Ciberseguridad y la Privacidad Informáticas que puedan satisfacer la creciente demanda de este tipo de profesionales por parte de empresas, instituciones y universidades.

Para satisfacer este objetivo, se ha diseñado un plan de estudios que dota al estudiante de unos conocimientos sólidos sobre los aspectos fundamentales de la ciberseguridad, la privacidad, y la legislación vigente sobre éste ámbito. El alto nivel de optatividad del máster permite al estudiante elegir su especialización a lo largo del eje que componen tres perfiles: dos perfiles técnicos, uno focalizado en la administración y protección de sistemas, y otro focalizado en la consultoría e implantación de tecnologías de ciberseguridad que puedan ofrecer servicios de valor añadido en este ámbito; y un tercer perfil focalizado en la gestión de la ciberseguridad y la protección de datos.

El máster tiene una clara vocación profesionalizadora, con asignaturas que recogen los fundamentos teóricos y las bases de las tecnologías de ciberseguridad y privacidad, pero que a la vez son muy aplicadas y prácticas. Con ello se quieren formar perfiles que puedan solventar los problemas actuales de la indústria y que puedan crecer y adaptarse a los nuevos retos que aparecerán.

Por otro lado, el máster también ofrece asignaturas optativas más centradas en la investigación, que favorecen el paso hacía unos estudios de doctorado y hacia la práctica científica en el ámbito

académico o profesional.

El resultado final esperado es la formación de profesionales altamente cualificados y competentes de acuerdo a lo especificado en el apartado 1 del documento.

El perfil de formación

Las competencias que se adquieren en el Máster universitario en ciberseguridad y privacidad se han diseñado para aquellos titulados o profesionales el ámbito de la informática y la telemática. Este perfil tiene conocimientos matemáticos para la ingeniería, tiene conocimientos de redes, de sistemas informáticos, y de programación. Además, tiene conocimientos básicos sobre la temática del máster, como son la seguridad en redes y la criptografía. A partir de este perfil, el máster pretende formar a profesionales reflexivos, críticos y autosuficientes, capaces de integrarse en equipos interdisciplinares con los siguientes roles (según la especialidad cursada):

- Especialidad de sistemes: perfiles capaces de liderar el diseño y la implantación tecnológica de políticas de protección, prevención y detección de ataques.
    - Director de sistemas informáticos
    - Consultor de seguridad de sistemas de información
    - Administrador de redes y sistemas
    - Administrador de bases de datos
    - Ingeniero de comunicación de voz y datos
    - Périto forense
- Especialidad de tecnologías: perfiles capaces de diseñar nuevos sistemas y servicios que traten con datos sensibles, confidenciales o privados.
    - Director de tecnología
    - Jefe de proyectos de seguridad TIC
    - Experto en el desarrollo de aplicaciones y servicios web seguros
    - Especialista en sistemas de registro web y control de acceso
    - Consultor de proyectos de administración electrónica
    - Consultor de comercio y banca electrónica
    - Consultor de sistemas blockchain
- Especialidad de gestión: perfiles capaces de definir las prácticas y procedimientos de seguridad y privacidad de acuerdo a las normativas ISO vigentes y a la ley GDPR, así como hacer auditorías de seguridad.
    - Delegado de protección de datos (DPO)
    - Implantador de sistemas de gestión de la seguridad de la información
    - Auditor de seguridad de sistemas de informaciòn

Cabe destacar que este plan de estudios se ha diseñado teniendo en cuenta los derechos

fundamentales y de igualdad de oportunidades entre hombres y mujeres, los principios de igualdad de oportunidades y accesibilidad universal de las personas con discapacidad, los valores propios de una cultura de la paz y de valores democráticos, y los principios de sostenibilidad, conforme a lo dispuesto en la Ley 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres, la Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad, la Ley 27/2005, de 30 de noviembre, de fomento de la educación y la cultura de la paz, y las directrices para la introducción de la sostenibilidad en el currículum elaboradas por la CRUE.

Estructura del Plan de Estudios

El Máster Universitario en Ciberseguridad y Privacidad se estructura en 1 módulo común de fundamentos de 18 créditos, 1 módulo de especialidad formado por 18 créditos, 1 módulo de optatividad de 12 créditos, y 1 módulo obligatorio final del Trabajo final de 12 créditos.

En el módulo de especialidad, el máster ofrece 3 itinerarios posibles: “Sistemas”, “Tecnologías” y “Gestión”

Módulo	Tipología de Asignatura	Créditos
Fundamentos	Obligatoria	18
Especialidad	Optativa	18
Optatividad	Optativa	12
Trabajo final	Obligatoria	12
Total		**60**

La oferta formativa consiste en las siguientes asignaturas:

Módulo	Número total de asignaturas	Número total de créditos
Fundamentos	3	18
Especialidad	9	54
Optatividad	7	42

Trabajo final	1	12
Total		**126**

A continuación se detallan las asignaturas de la oferta formativa, así como su creditaje y temporización.

Módulos	**Asignaturas**	**Tipología de Asignatura**	**ECTS/ Tipología**	**Secuencia**
Fundamentos	Legislación y protección de datos	Obligatoria	6 ECTS	1r semestre
	Fundamentos de ciberseguridad	Obligatoria	6 ECTS	1r semestre
	Privacidad	Obligatoria	6 ECTS	1r semestre
Especialidad: Sistemas	Seguridad y pentesting de servidores de datos	Optativa	6 ECTS	1er semestre
	Seguridad y pentesting de sistemas	Optativa	6 ECTS	2º semestre
	Análisis forense	Optativa	6 ECTS	2º semestre
Especialidad: Tecnologías	Seguridad del software	Optativa	6 ECTS	1er semestre
	Sistemas de Blockchain	Optativa	6 ECTS	1er semestre
	Arquitecturas y protocolos de	Optativa	6 ECTS	2º semestre

	seguridad			
Especialidad: Gestión	Sistemas de gestión de la seguridad	Optativa	6 ECTS	1er semestre
	Gestión de la seguridad en el cloud	Optativa	6 ECTS	2º semestre
	Auditoría técnica	Optativa	6 ECTS	2º semestre
Optatividad	Dirección estratégica de sistemas y tecnologías de la información	Optativa	6 ECTS	1er semestre
	Técnicas de investigación	Optativa	6 ECTS	1er semestre
	Modelos avanzados de minería de datos	Optativa	6 ECTS	1er semestre
	Ciberdelitos: estudio de los tipos delictivos	Optativa	6 ECTS	1er semestre
	Criptografía avanzada	Optativa	6 ECTS	2º semestre
	Biometría	Optativa	6 ECTS	2º semestre
	Técnicas de ocultación de la información	Optativa	6 ECTS	2º semestre
Trabajo final	Trabajo final de máster	TFM	12 ECTS	2º semestre

Se prevé que un estudiante pueda realizar todo el plan de estudios en un año, en el caso de que lo curse a tiempo completo, o en un plazo superior de 2 años según el modelo flexible de la universidad. A continuación se plantean los dos escenarios posibles, ya sea a tiempo completo

o a tiempo parcial en dos años.

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.

a) **Planificación en un año lectivo**

Planificación para los estudiantes que no realicen ninguna especialidad

Sem1 30 ECTS	Legislación y protección de datos	Fundamentos ciberseguridad	Privacidad	Optativa	Optativa
Sem2 30 ECTS	Optativa	Optativa	Optativa	TFM	

Especialidad: Sistemas

Sem1 30 ECTS	Legislación y protección de datos	Fundamentos ciberseguridad	Privacidad	Seguridad y pentesting de servidores de datos	Optativa
Sem2 30 ECTS	Seguridad y pentesting de sistemas	Análisis forense	Optativa	TFM	

Especialidad: Tecnologías

Sem1 30 ECTS	Legislación y protección de datos	Fundamentos ciberseguridad	Seguridad del software	Sistemas de Blockchain	Optativa

Sem2 30 ECTS	Privacidad	Arquitecturas y protocolos de seguridad	Optativa	TFM

Especialidad: Gestión

Sem1 30 ECTS	Legislación y protección de datos	Fundamentos ciberseguridad	Privacidad	Sistemas de gestión de la seguridad	Optativa
Sem2 30 ECTS	Auditoría técnica	Gestión de la seguridad en el cloud	Optativa	TFM	

b) **Planificación en dos años lectivos**

Planificación para los estudiantes que no realicen ninguna especialidad

Sem1 12 ECTS	Legislación y protección de datos	Fundamentos ciberseguridad	
Sem2 18 ECTS	Privacidad	Optativa	Optativa
Sem3 18 ECTS	Optativa	Optativa	Optativa
Sem4 12 ECTS	TFM		

Especialidad: Sistemas

Sem1	Legislación y	Fundamentos

12 ECTS	protección de datos	ciberseguridad	
Sem2 18 ECTS	Seguridad y pentesting de sistemas	Análisis forense	Optativa
Sem3 18 ECTS	Privacidad	Seguridad y pentesting de servidores de datos	Optativa
Sem4 12 ECTS	TFM		

Especialidad: Tecnologías

Sem1 12 ECTS	Legislación y protección	Fundamentos ciberseguridad	
Sem2 18 ECTS	Privacidad	Arquitecturas y protocolos de seguridad	Optativa
Sem3 18 ECTS	Seguridad del software	Sistemas de Blockchain	Optativa
Sem4 12 ECTS	TFM		

Especialidad: Gestión

Sem1 12 ECTS	Legislación y protección de datos	Fundamentos ciberseguridad

Sem2 18 ECTS	Auditoría técnica	Gestión de la seguridad en el cloud	Optativa
Sem3 18 ECTS	Privacidad	Sistemas de gestión de la seguridad	Optativa
Sem4 12 ECTS	TFM		

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.

Programa Erasmus

La UOC solicitó en febrero de 2007 la Carta universitaria Erasmus, que le fue concedida en julio de 2007. A principios del 2009 la UOC entró a formar parte del programa de movilidad docente, al año siguiente se añadió para el personal de gestión.

Desde el curso 2011/12 se han concedido las siguientes becas Erasmus:

	2011/12	**2012/13**	**2013/14**	**2014/15**	**2016/17**	**2017/18**
Formación	7	8	7	9	9	8
Prácticas	0	6	1	4	3	5

Así mismo, entre los cursos 2010/11-2016/17, la universidad también ha recibido estudiantes de movilidad, concretamente 7 de prácticas y 12 de formación.

A nivel general de la UOC existe un grupo de trabajo que reúne a los responsables de movilidad de la universidad y a los coordinadores Erasmus de los diferentes departamentos académicos. Dicha comisión ejerce funciones de coordinación y unifica los criterios de selección de estudiantes y de gestión de los acuerdos académicos entre los estudiantes y las universidades destinatarias. La UOC dispone de un coordinador Erasmus para todos los Estudios que lleva a cabo los contactos para establecer nuevos convenios, participa en el proceso de selección de candidatos a las becas Erasmus, asesora a los estudiantes seleccionados en la elección de asignaturas en la universidad destinataria, firma en nombre del departamento el "learning agreement" de cada estudiante, y mantiene contacto periódico con los estudiantes que se hallen ya realizando su movilidad.

Otros proyectos de movilidad de la UOC

La movilidad que se efectúa en la UOC se centra en el intercambio de estudiantes con otras universidades mediante acuerdos articulados en convenios interuniversitarios, contemplando el posterior reconocimiento de créditos en la universidad origen del estudiante. Los acuerdos de movilidad pueden efectuarse en ambos sentidos; la UOC es emisora o receptora de estudiantes. Los acuerdos de movilidad pueden afectar tanto a la docencia virtual como a la presencial:

- En los casos en los que la UOC actúa como emisora de estudiantes, los acuerdos pueden afectar tanto a asignaturas presenciales como a asignaturas virtuales de la universidad receptora.
- En los casos en los que la UOC actúa como receptora de estudiantes, lo habitual es que la movilidad sea virtual, aunque podría considerarse algún caso excepcional que afectase a actividades presenciales organizadas desde la UOC.

Debe considerarse también la participación en el proyecto piloto europeo e-Move sobre movilidad virtual (MV).

Además, institucionalmente, se promociona la participación activa de la Universitat Oberta de Catalunya en redes de excelencia y alianzas internacionales que permiten facilitar la relación con instituciones universitarias a nivel internacional para el fomento de los convenios de colaboración. Actualmente la UOC es miembro de las siguientes redes europeas e internacionales:

- Academic Cooperation Association (ACA)
- Asociación Universitaria Iberoamericana de Posgrado (AUIP)
- Centro Interuniversitario de Desarrollo (CINDA)
- European Association of Distance Teaching Universities (EADTU)
- European Association for International Education (EAIE)
- European Distance and E-learning Network (EDEN)

- EDUCAUSE-ELI
- European Network for Ombudsmen in Higher Education (ENOHE)
- European University Association (EUA)
- European Association for University Lifelong Learning (EUCEN)
- European Universities Information System (EUNIS)
- Global University network for Innovation (GUNI)
- International Association of Universities (IAU)
- International Council for Distance Education (ICDE)
- IMS Global Learning Consortium (IMS GLC)
- The Observatory on Borderless Higher Education
- Red de Educación Continua de América Latina y Europa (RECLA)
- Red de Organismos Defensores de los Derechos Universitarios (REDDU)
- Talloires Network
- Xarxa Vives d'universitats

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 le surjan en lo relativo al programa de movilidad en el marco de los estudios que cursa.

Mecanismos de coordinación docente

La responsabilidad última 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 la UOC. 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 objeto de tratar los temas y las problemáticas de interés común, establecer criterios y evaluar el desarrollo del programa.

Asimismo, el profesor responsable de asignatura es el responsable de coordinar a los distintos profesores colaboradores 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.

Paralelamente, al inicio y al final de cada semestre, se llevan a cabo reuniones de cada profesor responsable de asignatura con el equipo de profesores colaboradores 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 docentes colaboradores 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.

Origen y reconocimientos obtenidos por la UOC

La UOC fue creada con el impulso del Gobierno de la Generalitat de Catalunya, con la expresa finalidad de ofrecer enseñanza universitaria no presencial, inició su actividad académica en el curso 1995/1996 y desde entonces ha obtenido, entre otros, los siguientes premios y reconocimientos en el ámbito del reconocimiento de la excelencia en e-learning:

- Premio Bangemann Challenge 1997, de la Unión Europea a la mejor iniciativa europea en educación a distancia.

- Premio WITSA 2000, de la World Information Technology and Services Alliance (WITSA), a la mejor iniciativa digital (premio Digital Opportunity) .

- Premio ICDE 2001 a la excelencia, de la International Council for Open and Distance Education (ICDE), que reconoce a la UOC como la mejor universidad virtual y a distancia del mundo.

- Distinción como Centro de excelencia Sun – 2003 (y 2006), entre una selección de instituciones educativas de todo el mundo, por la utilización e integración de las TIC en los procesos formativos.

- 2005 – Premio Nacional de Telecomunicaciones de la Generalitat de Catalunya, por haber sido capaz de poner las telecomunicaciones al servicio de la enseñanza superior, haciendo posible, más que nunca, el acceso universal a la universidad.

- 2009 – Center of Excellence del New Media Consortium, reconoció el liderazgo de la UOC en áreas de la tecnología educativa y los recursos formativos abiertos.

- 2011 – Learning Impact Award for the Best Learning Portal (Bronce), con el proyecto iUOC cuyo objetivo es llevar el Campus Virtual de la Universidad a nuevos escenarios portátiles e interactivos.

- 2014 – Learning Impact Award (Plata). El proyecto galardonado de la UOC es el innovador portal para aprender idiomas SpeakApps

- 2015 – Learning Impact Award (Oro). El proyecto galardonado de la UOC es la herramienta Present@, un videoblog interactivo que permite subir y visualizar de forma fácil presentaciones en vídeo de gran formato.

- 2016 – Learning Impact Award (Mención de Honor). Las aplicaciones de la UOC que recibieron esta distinción son Explica!, Avalua y Lliuraments, que conforman el

ecosistema de apps móviles de la UOC para apoyar a la evaluación continua. Explica! es una app para tabletas que permite generar vídeos con anotaciones gráficas y de voz a partir de un documento PDF o de una pizarra en blanco. Avalua es una app para los colaboradores docentes que facilita el seguimiento de la evaluación de los alumnos desde dispositivos móviles. Finalmente, Lliuraments es una app para el estudiante de la UOC que le permite seguir la actividad de sus PEC desde dispositivos móviles.

- 2016 – European Distance and E-learning Network (EDEN) Premio de excelencia institucional.

Más información:
http://www.uoc.edu/portal/es/universitat/premis/index.html

Modelo pedagógico de la UOC

El modelo educativo de la UOC es el principal rasgo distintivo de la universidad desde sus inicios. Nace con la voluntad de responder de una manera adecuada a las necesidades educativas de las personas que se forman a lo largo de la vida y de aprovechar al máximo el potencial que ofrece la red para aprender en un entorno flexible.

El modelo educativo de la UOC sitúa al estudiante y su **proceso de aprendizaje en el centro**, por lo que el diseño de **actividades de aprendizaje** es el núcleo alrededor del que se organiza la docencia. El modelo de la UOC es **dinámico y flexible** y permite situaciones de aprendizaje diversas. Está pensado para adaptarse y evolucionar en el tiempo de forma constante, a la vez que evoluciona Internet y la sociedad del conocimiento. En este sentido, el modelo garantiza que los estudiantes aprendan de modo parecido a cómo trabajan y se comunican en la red.

La finalidad del proceso de enseñanza-aprendizaje es promover que los estudiantes desarrollen **competencias profesionalizadoras** a través de la evaluación formativa. El modelo educativo de la UOC ofrece un alto grado de personalización y de adaptabilidad que permite al estudiante participar activamente de su propio aprendizaje, y aprender y practicar dentro sus contextos profesionales y/o basándose en sus experiencias previas.

El modelo permite a cada estudiante autoregular su propio proceso de aprendizaje, promoviendo un **aprendizaje autónomo acompañado por los profesores**.

Se basa en cinco pilares fundamentales que configuran la experiencia de aprendizaje: la actividad del estudiante, el acompañamiento docente, la comunidad en red, la evaluación por competencias y las herramientas y recursos.

- **La actividad del estudiante**

  El aprendizaje se concibe como un proceso activo donde el estudiante tiene un papel fundamental tanto en el proceso de construcción del conocimiento como en el desarrollo de competencias. Cuando hablamos de la actividad del estudiante nos referimos no sólo a las actividades que se diseñan para que éste aprenda sino a todas las acciones que éste hace para aprender cómo pueden ser: la planificación de tareas, la gestión del tiempo, o la comunicación con los compañeros. Las actividades de aprendizaje que se ponen al alcance de los estudiantes son diversas y todas ellas buscan fomentar el **aprendizaje activo** mediante **situaciones retadoras y motivadoras**. Se diseñan actividades de aprendizaje de tipología muy diversa, en función de las competencias que se trabajan, del ámbito de conocimiento o del nivel de especialización de la formación que el estudiante realice.

- **El acompañamiento docente**

  Es el conjunto de acciones que hacen los docentes para hacer el seguimiento de los estudiantes y apoyarlos en la planificación de su trabajo, en la resolución de actividades, en la evaluación, y en la toma de decisiones. **El estudiante está acompañado**, en todo momento, por profesorado especializado que tiene como funciones principales el **diseño, orientación, dinamización y evaluación** de todo su proceso educativo. Hay tres perfiles docentes (profesor, profesor colaborador y tutor) que trabajan conjuntamente para asegurar un proceso de aprendizaje de calidad.

- **La comunidad en red**

  El modelo está orientado a la **participación y la construcción colectiva del conocimiento** desde un planteamiento interdisciplinario y abierto a la experiencia formativa, social y laboral de los estudiantes. Se incorpora el **aprendizaje colaborativo** como metodología para que el estudiante se enriquezca de los conocimientos, puntos de vista y experiencias de los compañeros, y para que desarrolle la competencia de **trabajo en equipo para el mundo profesional**. Algunas metodologías que se utilizan para promover este tipo de aprendizaje son: el trabajo por proyectos, el aprendizaje basado en problemas, el aprendizaje indagativo o las metodologías ágiles.

- **La evaluación por competencias**

  La evaluación se concibe como un mecanismo para aprender y retroalimentar el proceso

de aprendizaje. La evaluación, por tanto, es **continua y formativa** y se proporciona durante todo el proceso de aprendizaje. Las actividades de evaluación facilitan el logro de los objetivos de aprendizaje y el desarrollo de las competencias.

- **Las herramientas y los recursos**
  La UOC ofrece un modelo flexible que permite al estudiante **aprender en cualquier lugar y en cualquier momento**. Los estudiantes pueden adaptar el proceso de aprendizaje en función de su estilo de vida y consultar e interaccionar con los recursos de aprendizaje en diferentes formatos y desde múltiples dispositivos. Las herramientas y recursos están al servicio del proceso de aprendizaje del estudiante.

    - En el **Campus virtual** tiene lugar la vida de toda la comunidad universitaria, formada por los estudiantes, profesores, investigadores, docentes colaboradores, y administradores. A través del Campus el estudiante tiene acceso a las **aulas virtuales**, que son los espacios de aprendizaje donde encontrará a los profesores, los compañeros, las actividades, los contenidos y las herramientas para aprender.
    - **Recursos de aprendizaje interactivos y multiformato** (vídeos enriquecidos, hipertextos, audiolibros, videolibros).
    - **Recursos multimedia** (combinando texto, audio, imagen y vídeo).
    - **Espacios virtuales** de aprendizaje en 3D.
    - Diversidad de **herramientas de aprendizaje** (blogs, foros, microblogs, herramientas para grabar y compartir archivos de vídeo y audio).

Herramientas para el aprendizaje

Las herramientas para el aprendizaje son instrumentos que permiten poner en pràctica las metodologías docentes y la realización de las actividades formativas.

Con el objetivo de poder cubrir las diferentes necesidades de aprendizaje que el docente define y garantizar la función **formativa y acreditativa** del sistema de evaluación de la UOC el aula virtual facilita la personalización y la integración de gran variedad de herramientas:

Galería: Espacio que presenta a modo de escaparate archivos en diferentes formatos (audio, vídeo o imagen) con el objetivo de ser evaluados o comentados por los estudiantes.
Langblog: Blog de entradas de audio y vídeo que permite registrar y publicar los archivos de voz y los vídeos de manera que después puedan ser escuchados, vistos y comentados por los compañeros del aula.
Present@: Permite publicar y visualizar actividades de los estudiantes en vídeo o audio. Los estudiantes y el profesorado pueden ver los trabajos y realizar comentarios
VídeoPAC: Permite registrar y enviar actividades en formato de vídeo o audio en el aula. Las

actividades sólo son visibles para el estudiante que las ha realizado y el profesorado.
Blog: Sitio web que permite la publicación cronológica de artículos o apuntes. Se puede incluir todo tipo de información, desde textos, enlaces e imágenes, hasta elementos multimedia.
Multiblog: Blog que facilita que cada estudiante administre su blog dentro del aula. Los blogs son accesibles a través del blog del aula, que contiene una lista de los nombres de los estudiantes enlazados con sus blogs personales.
Foro/Debate: Espacio de discusión que permite a estudiantes y docentes intercambiar información, opiniones, preguntas / respuestas, archivos y toda clase de material sobre varios temas.
Google Apps: Aplicaciones de Google disponibles en el entorno UOC y utilizadas con un objetivo docente (Gmail, Calendar, Drive, Docs, Hangouts, Sites)
Microblog: Sistema que permite el envío de mensajes de texto breves (125 caracteres) y publicarlos en el aula. La herramienta también dispone de una aplicación móvil que facilita la consulta de los mensajes publicados en el aula y en el campus.
Laboratorios virtuales: Facilitan que el estudiante trabaje a cualquier hora y realice todo tipo de simulaciones. Los espacios de trabajo de estos laboratorios son aulas virtuales, en las que el profesor coordina el trabajo de los estudiantes y adapta los contenidos a las necesidades de cada materia o práctica.
Grupos de trabajo: Entorno de trabajo colaborativo dentro de las aulas que permite el trabajo en grupos con espacios de tablero, foro y de intercambio de archivos
Xwiki: Herramienta de *software* abierto para la creación de recursos de aprendizaje en formato wiki.
Moodle: Integración de herramientas del LMS Moodle como por ejemplo: cuestionarios, encuestas, glosario…
Vídedoconferencia: permite programar sesiones de videoconferencia, grabarlas y compartir ficheros y presentaciones.

6.
6.1.

6.1.1. Actividades formativas propias de esta titulación

1	Búsqueda, selección y gestión de la información
2	Presentación y difusión de la información
3	Estudio y resolución de un caso
4	Análisis crítico
5	Resolución de problemas

6	Pruebas objetivas
7	Realización de un trabajo o proyecto
8	Discusión dirigida
9	Simulación
10	Experimentación con objetos reales o laboratorios virtuales

6.1.2. Metodologías docentes propias de esta titulación

1	Aprender haciendo (Learning by doing)
2	Aprendizaje autónomo
3	Trabajo por proyectos
4	Estudio de caso
5	Aprendizaje basado en problemas (PBL)
6	Aprendizaje indagativo

6.1.3. Sistemas de evaluación propios de esta titulación

1	Pruebas de evaluación continua (PEC)
2	Actividades de prácticas
3	Trabajo Final de Máster (TFM)

Descripción del sistema de evaluación y sistema de calificaciones

En el marco de nuestro modelo pedagógico, el **modelo de evaluación** de la UOC 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. Es por ello que la evaluación se estructura exclusivamente en torno a la **evaluación continua**, llevada a cabo a través de las pruebas de evaluación continua (PEC) y las actividades de prácticas . También se prevén modelos de evaluación específicos para los trabajos de fin de Máster.

El modelo concreto de evaluación de cada asignatura se establece semestralmente en el plan docente de cada asignatura, que define:

a. El modelo de evaluación, las actividades de evaluación programadas y el calendario de evaluación.
b. Los criterios generales de evaluación, corrección y notas, y fórmulas de ponderación aplicables.

La información relacionada con el proceso de evaluación se hará pública antes del periodo de matrícula, mediante los canales habituales de comunicación de la UOC.

La normativa aplicable a la evaluación se encuentra en la normativa académica de la UOC, en su capítulo V,:

https://seu-electronica.uoc.edu/portal/_resources/ES/documents/seu-electronica/Normativa_academica_EEES_CAST_consolidada.pdf

La evaluación continua

La evaluación continua (EC) se realiza durante el semestre. Es el eje fundamental del modelo educativo de la UOC y es aplicable a todas las asignaturas de los programas formativos que la UOC ofrece. El seguimiento de la EC es el modelo de evaluación recomendado por la UOC y el que mejor se ajusta al perfil de sus estudiantes.

La EC consiste en la realización y superación de una serie de pruebas de evaluación continua (PEC) establecidas en el plan docente, de acuerdo con el número y el calendario que se concreta. La EC de cada asignatura se ajusta a los objetivos, competencias, contenidos y carga docente de cada asignatura.

El plan docente establece los criterios mínimos y el calendario de entrega para seguir y superar la EC. En todo caso, para considerar que se ha seguido la EC debe haber hecho y entregado como mínimo el 50% de las PEC. El no seguimiento de la EC se califica con una N (equivalente al no presentado).

La práctica es una actividad de evaluación no presencial que forma parte del sistema de evaluación continua de la asignatura. Las prácticas pueden ser obligatorias o no, según lo establecido en el plan docente correspondiente. La nota de prácticas se combina con la nota de la EC para obtener la calificación final de la asignatura, de acuerdo con la tabla de cruce o fórmula ponderada que se establezca en el plan docente.

No se debe confundir esta referencia a las prácticas, entendidas como una actividad que puede formar parte del sistema de evaluación de determinadas asignaturas, con la asignatura específica de prácticas. En el caso de que en un plan de estudios exista una asignatura de este tipo, en el apartado 5, en el módulo correspondiente, se especificará su modelo de evaluación, que se concretará para cada semestre en el plan docente/ de aprendizaje.

Herramientas para el seguimiento de la evaluación continua

Teniendo en cuenta que la evaluación continua se caracteriza por favorecer el **progreso del estudiante** con propuestas de actividades que representen una cierta progresión y utilizar el **feedback formativo y personalizado**, las herramientas específicas que permiten hacer un seguimiento y retroalimentación del proceso de aprendizaje que realiza el estudiante son las siguientes:

- **REC:** Registro de evaluación contínua que unifica en una sola aplicación la entrega de actividades por parte del estudiante y la introducción de calificaciones y comentarios por parte de los profesores colaboradores.
- **eFeedback del REC**: Componente del REC que permite el feedback personalizado en formato audio y vídeo.
- **Explica!:** Aplicación para tabletas digitales que permite realizar comentarios de voz y anotaciones escritas sobre documentos, de manera que la explicación del contenido sea más visual.
- **Evalúa** : Aplicación móvil que permite al profesor colaborador realizar el seguimiento de las actividades formativas y proporcionar feedback formativo.
- **Entregas**: Aplicación móvil que permite a los estudiantes estar al día del estado de las actividades o PEC de sus asignaturas. Con la aplicación pueden recibir al instante y desde cualquier lugar los comentarios y las notas que los docentes realicen sobre las actividades entregadas a los estudiantes.

Trabajo Final de Máster

Los trabajos de fin de Máster (TFM) son objeto de defensa pública ante una comisión de evaluación, de acuerdo con lo establecido en el plan docente de la asignatura.

La evaluación del Trabajo de fin de máster se realizará a través de evaluación continuada y la evaluación de la defensa pública del mismo. En relación a la evaluación continuada, se valorará el trabajo continuado del estudiante a lo largo del semestre y se evaluará a través de entregas parciales relacionadas con el trabajo y la memoria del TFM. Estas entregas se harán a través de las PEC (Pruebas de Evaluación Continua) de la asignatura.

La cantidad de PEC, el alcance de cada una de ellas, y las fechas de entrega, serán definidas por el director del TFM, conjuntamente con el Profesor responsable de la asignatura que definirá el contenido de la primera y última PEC del TFM, que seguirán el mismo formato para todos los estudiantes:

- PEC 1:
    - Introducción y objetivos del proyecto.
    - Planificación del trabajo a lo largo del semestre.
- PEC final (entrega final):
    - Memoria del trabajo.
    - Producto obtenido en la realización del proyecto (si procede).
    - Presentación del proyecto (vídeo).

Después de la fecha de entrega de la PEC final, se establecerá un período de defensa virtual pública en el cual un Tribunal de Evaluación nombrado por el coordinador de la asignatura de TFMs del programa valorará el trabajo. Esta defensa virtual tendrá una duración de una semana, durante la cual los miembros del Tribunal de Evaluación tendrán acceso a la entrega final del TFM y podrán formular preguntas al estudiante en relación a su trabajo. El estudiante dispondrá de 24 horas para responder a cada pregunta formulada.

En la evaluación del TFM, el director del mismo valorará las actividades de evaluación continua del estudiante con un peso del 40% de la nota final. El Tribunal de Evaluación valorará la entrega final, la presentación y la defensa, y tendrá un peso del 60% de la nota final.

Finalmente, una vez finalizado y evaluado el TFM, el estudiante que haya superado la asignatura deberá depositar una copia de su trabajo en el repositorio institucional de la UOC (O2), donde quedará archivado y será de libre consulta para su uso docente y de divulgación. Como autor, el estudiante conservará la propiedad intelectual y podrá escoger la licencia bajo la cual se publicará en abierto. En caso de que el trabajo contenga datos a proteger (tales como datos personales o de secreto empresarial), el estudiante tendrá que retirar esta información del documento antes de su depósito. Según la naturaleza del trabajo, excepcionalmente se puede acordar que el trabajo no sea publicado.

Con la publicación del TFM en el repositorio O2, el trabajo quedará siempre accesible y la UOC

se hará cargo de realizar los cambios de formato necesarios para preservar su accesibilidad en el futuro.

La calificación final de la asignatura. Los modelos de evaluación.

1. La calificación final de la asignatura resulta de las notas obtenidas mediante EC según el modelo de evaluación establecido para cada asignatura y de acuerdo con la tabla de cruce o fórmula ponderada que sea aplicable. El modelo de evaluación y la tabla de cruce o fórmula ponderada aplicable se establecerán semestralmente en el plan docente de la asignatura.

2. Las calificaciones finales se hacen públicas dentro de los plazos establecidos en el calendario académico.

3. Las fórmulas de ponderación se aplicarán según el modelo de evaluación.

La revisión de las calificaciones

El estudiante que no esté de acuerdo con la nota de EC obtenida puede pedir la revisión, de acuerdo con las herramientas y los plazos establecidos.

Derechos y deberes de los estudiantes

1. Información.- Toda la información relativa a los modelos de evaluación de las asignaturas / programas, el calendario de pruebas finales, la elección de las sedes de exámenes, los periodos necesarios para la publicación de las calificaciones finales y para las revisiones debe ser accesible desde Secretaría.

2. Derecho a ser evaluado .- Todo estudiante de la UOC tiene derecho a ser evaluado de las asignaturas de las que se ha matriculado, siempre que no se trate de una asignatura que haya sido reconocida o adaptada, a no ser que haya renunciado a presentarse a las pruebas de evaluación previstas. El estudiante debe estar al corriente de sus deberes económicos con la Universidad para tener derecho a ser evaluado.

3. Convocatorias.-. La matrícula de una asignatura da derecho a una sola convocatoria de evaluación por semestre. El estudiante dispone de cuatro convocatorias para superar cada asignatura. En el caso de asignaturas con prácticas obligatorias o de EC como único modelo de superación de la asignatura corre convocatoria cada vez que el estudiante sigue la EC y no la supera. Por no seguir la EC el estudiante consta en el expediente como no presentado, pero no agota convocatoria. En el caso de asignaturas con prácticas obligatorias o de EC como único

modelo de superación de la asignatura, prevalece lo indicado en el plan docente de la asignatura y, por tanto, sólo se consideran no presentados (y no corre convocatoria) si no entregan el número de PEC o prácticas obligatorias que se especifican en el plan docente.

Agotadas las cuatro convocatorias ordinarias para poder superar una asignatura, el estudiante puede pedir una autorización de permanencia dentro del plazo establecido en el calendario académico de la UOC. Aceptada la autorización de permanencia, el estudiante dispone de una única convocatoria extraordinaria para poder superar la asignatura.

El seguimiento y realización de la evaluación en la UOC queda sujeto a los criterios disciplinarios y sancionadores previstos en la Normativa de Evaluación y en la Normativa de derechos y deberes de la UOC.

Identidad y autoría

Gracias a la evaluación continua, se mantiene un diálogo fluido entre el estudiante y el profesor, el cual se realiza de forma asíncrona principalmente a través de texto, vídeo o audio (con las herramientas especificadas con anterioridad), pudiendo evidenciar, seguir y corregir periódicamente la actividad realizada por cada estudiante, dificultando el fraude y facilitando el seguimiento. Para realizar este seguimiento de manera que se pueda identificar indicios de fraude se cuenta con la siguiente herramienta:

-PEC-plagio: Herramienta que, mediante el uso de inteligencia artificial, es capaz de detectar documentos digitales con contenido semántico similar, ayudando a los profesores a la detección de indicios de plagio en los trabajos entregados por los estudiantes.

Además la UOC lidera el proyecto europeo TeSLA, (Adaptive Trust-based e-assessment System for Learning). Su objetivo es permitir que los estudiantes se puedan evaluar virtualmente en los diferentes momentos del aprendizaje. El proyecto, de tres años de duración y siete millones de presupuesto, cuenta con universidades, centros de investigación y empresas tecnológicas de doce países. El proyecto Tesla desarrollará un sistema de evaluación en línea innovador que permitirá a los estudiantes evaluarse virtualmente gracias a tecnologías integradas y aplicadas en actividades de aprendizaje. El sistema permitirá identificar al estudiante y verificar la autoría gracias a tecnología punta como el reconocimiento facial, el reconocimiento de voz, los patrones de teclado o el antiplagio, entre otros.

https://tesla-project.eu/

Infracción de la normativa

1. Las infracciones de los criterios recogidos en la normativa de evaluación o en el plan docente son valoradas y debidamente sancionadas académicamente y, en su caso, disciplinariamente, de acuerdo con lo establecido a continuación.

2. El profesor responsable de la asignatura (cuando se produzcan dentro del ámbito estricto de una asignatura) o el director de programa correspondiente (cuando se produzcan en el ámbito de diversas asignaturas) está facultado para valorar y, a la vista toda la información recopilada, resolver la sanción académica correspondiente a las conductas siguientes:

- La utilización literal de fuentes de información sin ningún tipo de citación;
- la suplantación de personalidad en la realización de las actividades de evaluación;
- la copia o el intento fraudulento de obtener un resultado académico mejor en la realización de las actividades de evaluación;
- la colaboración, encubrimiento o favorecimiento de la copia en las actividades de evaluación;

Estas conductas pueden dar lugar a las sanciones académicas siguientes:

- nota de suspenso (D o 0) de la PEC/Práctica o de la nota final de EC

Además de la sanción académica correspondiente, el estudiante recibirá una amonestación por escrito del responsable académico recordándole la improcedencia de su actuación y la apertura de un procedimiento disciplinario en caso de reincidencia.

La dirección de programa, a la hora de resolver solicitudes de matrícula excepcional u otras peticiones académicas por parte del estudiante, puede tener en cuenta la información relativa a este tipo de conductas.

3. La infracción de la normativa de evaluación puede dar lugar a la incoación de un procedimiento disciplinario, de acuerdo con la Normativa de derechos y deberes de la UOC. La reincidencia (más de una vez) en las conductas expuestas anteriormente puede ser constitutiva de falta y queda sujeta al procedimiento disciplinario allí previsto.

De acuerdo con la Normativa de derechos y deberes, la Dirección de Programa es competente para iniciar e instruir el procedimiento disciplinario, y el Vicerrectorado responsable de asuntos estudiantiles es competente para resolver en caso de faltas leves y graves y el Rectorado, en caso de faltas muy graves. La sanción resultante del expediente disciplinario constará en todos los expedientes que el estudiante tenga abiertos en la UOC.

5.2. Estructura del Plan de estudios

El Máster universitario en Ciberseguridad y Privacidad ofrece los siguientes módulos:

Id	Denominación		Asignaturas que conforman el módulo
1	Fundamentos		• Legislación y protección de datos • Fundamentos de ciberseguridad • Privacidad
2	Especialidad	Sistemas	• Seguridad y pentesting de servidores de datos • Seguridad y pentesting de sistemas • Análisis forense
		Tecnologías	• Sistemas de blockchain • Seguridad del software • Arquitecturas y protocolos de seguridad
		Gestión	• Sistemas de gestión de la seguridad • Auditoría técnica • Gestión de la seguridad en el cloud
3	Optatividad		• Dirección estratégica de sistemas y tecnologías de la información • Técnicas de investigación • Modelos avanzados de minería de datos • Ciberdelitos: estudio de los tipos delictivos • Criptografía avanzada • Biometría

		• Técnicas de ocultación de la información
4	Trabajo final	• Trabajo final de máster

Módulo 1: Fundamentos

Denominación de la Asignatura • Legislación y protección de datos	
ECTS materia: 6 ECTS	**Carácter:** Obligatoria
Unidad temporal: Semestral	**Despliegue temporal:** 1r semestre
Lenguas en las que se imparte: Catalán/Castellano/inglés	
Resultados de aprendizaje: Al terminar con éxito la asignatura, los estudiantes serán capaces de: • Comprender las repercusiones de carácter jurídico suscitadas por las nuevas tecnologías de la información y, en concreto, de Internet. • Analizar el marco legal, detectar la comisión de hechos ilícitos y tomar decisiones frente a éstos. • Aplicar el marco jurídico que afecta a la gestión de la seguridad de sistemas informáticos, teniendo en cuenta la legislación relativa a la protección de de los datos personales, la propiedad intelectual, la ley de los servicios de la sociedad de la información y el comercio electrónico, así como el derecho penal.	
Contenidos: • Fundamentos jurídicos: repercusiones de las nuevas tecnologías de la información; el ordenamiento jurídico español, riesgos para los derechos y libertades en Internet; el derecho de las nuevas tecnologías • El reglamento europeo de protección de datos (RGPD): ámbito de aplicación, principios, derechos de las personas, medidas de cumplimiento y responsabilidad proactiva; transferencias internacionales de datos; autoridades de control y régimen sancionador • Servicios digitales de la sociedad de la información: propiedad intelectual e Internet, servicios de la sociedad de la información, responsabilidades de los intermediarios prestadores de servicios, firma electrónica	

Observaciones:
Esta asignatura proporciona los conocimientos fundamentales y básicos sobre las repercusiones legales de la seguridad informática. Es una asignatura indispensable dentro de un programa eminentemente técnico que se recomienda cursar al inicio del programa.

Competencias 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.

- CG1- Analizar y sintetizar las propiedades de seguridad y privacidad de un sistema.

Competencias transversales:

- CT1- Capacidad de iniciativa, de automotivación, y de aprendizaje autónomo a partir de la búsqueda y selección efectiva de información
- CT2- Expresarse de forma escrita de forma adecuada al contexto académico y profesional

Competencias específicas:

- CE1- Ejercer profesionalmente de forma responsable y honesta, actuando de acuerdo al código ético y a los aspectos legales actuales en el entorno de la seguridad y privacidad de datos.
- CE5- Aplicar el marco jurídico que afecta a la gestión de la seguridad de sistemas informáticos, teniendo en cuenta la legislación relativa a la protección de de los datos personales, la propiedad intelectual, la ley de los servicios de la sociedad de la información y el comercio electrónico, así como el derecho penal.

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	70	0
Análisis crítico	10	0
Presentación y difusión de la información	20	0
Estudio y resolución de un caso	35	0
Discusión dirigida	15	0

Metodologías docentes:

- Aprender haciendo (Learning by doing)
- Estudio de caso
- Aprendizaje basado en problemas (PBL)

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	100	100

Denominación de la Asignatura

- Fundamentos de ciberseguridad

ECTS materia: 6 ECTS	**Carácter:** Obligatoria
Unidad temporal: Semestral	**Despliegue temporal:** 1r semestre
Lenguas en las que se imparte: Catalán/Castellano/inglés	
Resultados de aprendizaje:	

- Identificar, examinar y gestionar los principales riesgos de un dominio informático.
- Evaluar los sistemas de prevención y protección de ataques.
- Comprender el funcionamiento de los sistemas criptográficos, y validar su implantación en diferentes sistemas.
- Diseñar soluciones integrales apropiadas en escenarios complejos que combinen las técnicas y contramedidas conocidas para la prevención, detección y disuasión de ataques
- Comprender, configurar, y gestionar herramientas para la administración y protección de redes cableadas e inalámbricas, y la gestión de alertas de seguridad.
- Conocer y saber desplegar los diferentes sistemas de detección de intrusiones.

Contenidos:

- Sistemas de prevención y protección de redes: cortafuegos, DMZ, configuración de redes
- Mecanismos de detección de intrusiones: escáneres de vulnerabilidades, sistemas de detección de intrusos, detección de ataques distribuidos
- Criptografía y criptoanálisis: algoritmos de criptografía de clave pública y privada, sistemas de criptoanálisis, protocolos criptográficos
- Vulnerabilidades

Observaciones:
Asignatura que asienta y ordena las bases de la ciberseguridad a partir de conocimientos previos que en diferentes grados de profundidad los alumnos han adquirido en sus estudios técnicos, y refuerza el análisis pormenorizado y crítico para aplicar correctamente este tipo de sistemas.

Competencias 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;
- 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.

- CG1- Analizar y sintetizar las propiedades de seguridad y privacidad de un sistema.
- CG2- Seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas de ciberseguridad en entornos nuevos o poco conocidos.
- CG3- Buscar, gestionar y utilizar de manera efectiva la información asociada al proceso de análisis y adaptación de nuevas soluciones tecnológicas.

Competencias transversales:

- CT1- Capacidad de iniciativa, de automotivación, y de aprendizaje autónomo a partir de la búsqueda y selección efectiva de información
- CT3- Comprensión de textos académicos y profesionales complejos escritos en inglés en el ámbito técnico.

Competencias específicas:

- CE2- Analizar y aplicar las técnicas básicas de prevención, protección y detección de ataques a un sistema informático.
- CE3- Evaluar y tomar las decisiones más adecuadas en cuanto a la selección y uso de herramientas y tecnologías del mercado en el ámbito de la ciberseguridad y la privacidad.
- CE6- Identificar, examinar y evaluar los principales riesgos de un dominio informático y diseñar estrategias para gestionarlos.
- CE8- Analizar la implementación y despliegue de soluciones criptográficas para validar su funcionamiento

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	70	0
Resolución de problemas	25	0
Pruebas objetivas	25	0
Análisis crítico	30	0

Metodologías docentes:

- Aprender haciendo (Learning by doing)
- Aprendizaje autónomo
- Aprendizaje basado en problemas (PBL)

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	100	100

Denominación de la Asignatura ● Privacidad	
ECTS materia: 6 ECTS	**Carácter:** Obligatoria
Unidad temporal: Semestral	**Despliegue temporal:** 1r semestre
Lenguas en las que se imparte: Catalán/Castellano/inglés	
Resultados de aprendizaje: ● Identificar y categorizar información sensible ● Reconocer los problemas de privacidad que surgen en diferentes contextos tecnológicos ● Aplicar tecnologías de mejora de la privacidad (PET) en sistemas de información y de comunicaciones que permitan cumplir con los requerimientos de la GDPR. ● Examinar y hacer análisis críticos sobre los beneficios y posibles pérdidas de utilidad de aplicar técnicas de preservación de la privacidad ● Evaluar el riesgo de reidentificación de sistemas simples y complejos	
Contenidos: ● Modelos de preservación de la privacidad para datos estructurados y no estructurados (aleatorización, técnicas de enmascaramiento y generación de datos sintéticos, k-anonimidad, generalización) ● Evaluación de los riesgos de reidentificación y de su impacto. Test de reidentificación e informe de auditoría ● Preservación de la privacidad en datos que contienen relaciones (grafos), localizaciones, o valores temporales ● Problemáticas específicas y tecnologías de preservación de la privacidad en contextos tecnológicos concretos como el acceso a bases de datos, las comunicaciones, la navegación y los buscadores web, las redes sociales, o los sistemas de pago electrónicos ● Protocolos criptográficos para proteger la privacidad (Pruebas de conocimiento nulo, Transferencia Inconsciente, Recuperación privada de información, Computación segura multiparte)	
Observaciones: Asignatura que proporciona conocimientos básicos y avanzados sobre las técnicas de preservación de la privacidad.	
Competencias 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; ● 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. ● CG1- Analizar y sintetizar las propiedades de seguridad y privacidad de un sistema. ● CG2- Seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas de ciberseguridad en entornos nuevos o poco conocidos. ● CG3- Buscar, gestionar y utilizar de manera efectiva la información asociada al proceso de análisis y adaptación de nuevas soluciones tecnológicas.
Competencias transversales: ● CT3- Comprensión de textos académicos y profesionales complejos escritos en inglés en el ámbito técnico.
Competencias específicas: ● CE3- Evaluar y tomar las decisiones más adecuadas en cuanto a la selección y uso de herramientas y tecnologías del mercado en el ámbito de la ciberseguridad y la privacidad. ● CE4- Desarrollar, integrar, y evaluar técnicas informáticas que permitan aplicar los principios de privacidad y protección de datos desde el diseño y por defecto que exige el Reglamento General de Protección de Datos (RGPD) a los sistemas, servicios y aplicaciones que traten con datos personales. ● CE6- Identificar, examinar y evaluar los principales riesgos de un dominio informático y diseñar estrategias para gestionarlos. ● CE7- Formular y desarrollar soluciones integrales e innovadoras en el ámbito de la ciberseguridad y privacidad, teniendo en cuenta las dinámicas de transformación y las tendencias tecnológicas

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	40	0
Análisis crítico	10	0
Resolución de problemas	30	0
Pruebas objetivas	30	0
Experimentación con objetos reales o laboratorios virtuales	40	0

Metodologías docentes:

- Aprender haciendo (Learning by doing)
- Aprendizaje autónomo
- Aprendizaje basado en problemas (PBL)
- Estudio de caso

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	50	90
Actividades prácticas	10	50

Módulo 2: Especialidad

Denominación de la Asignatura ● Seguridad y pentesting de servidores de datos	
ECTS materia: 6 ECTS	**Carácter:** Optativa
Unidad temporal: Semestral	**Despliegue temporal:** 1r semestre
Lenguas en las que se imparte: Catalán/Castellano/inglés	

Resultados de aprendizaje: ● Conocer dónde y cómo buscar información puntualmente actualizada de las vulnerabilidades de seguridad que los servidores de datos, así como los mecanismos para protegerlos, ● Elegir y manejar de forma adecuada las herramientas para hacer pentesting de servidores de datos ● Detectar de forma rápida y eficiente las incidencias de seguridad en los servidores de datos, así como analizar de forma rigurosa su origen y los rastros de infección.
Contenidos: ● Ataques a bases de datos, SQL injection ● Ataques a aplicaciones web: cross site scripting, clickjacking, ldap injection, xpath, remote file inclusions, webtrojans, etc. ● Auditoría y desarrollo seguro: proyecto OWASP, escáner de vulnerabilidades de caja negra, etc.
Observaciones:
Competencias básicas y generales: ● 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. ● CG1- Analizar y sintetizar las propiedades de seguridad y privacidad de un sistema. ● CG2- Seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas de ciberseguridad en entornos nuevos o poco conocidos. ● CG3- Buscar, gestionar y utilizar de manera efectiva la información asociada al proceso de análisis y adaptación de nuevas soluciones tecnológicas.
Competencias transversales: ● CT1- Capacidad de iniciativa, de automotivación, y de aprendizaje autónomo a partir de la búsqueda y selección efectiva de información ● CT3- Comprensión de textos académicos y profesionales complejos escritos en inglés en el ámbito técnico.
Competencias específicas: ● CE1- Ejercer profesionalmente de forma responsable y honesta, actuando de acuerdo al código ético y a los aspectos legales actuales en el entorno de la seguridad y privacidad de datos. ● CE2- Analizar y aplicar las técnicas básicas de prevención, protección y detección de

ataques a un sistema informático.
- CE3- Evaluar y tomar las decisiones más adecuadas en cuanto a la selección y uso de herramientas y tecnologías del mercado en el ámbito de la ciberseguridad y la privacidad.
- CE6- Identificar, examinar y evaluar los principales riesgos de un dominio informático y diseñar estrategias para gestionarlos.

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	40	0
Pruebas objetivas	30	0
Simulación	40	0
Experimentación con objetos reales o laboratorios virtuales	40	0

Metodologías docentes:

- Aprender haciendo (Learning by doing)
- Aprendizaje autónomo
- Aprendizaje basado en problemas (PBL)
- Estudio de caso

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	40	70
Actividades prácticas	30	60

Denominación de la Asignatura
- Seguridad y pentesting de sistemas

ECTS materia:	**Carácter:**
6 ECTS	Optativa

Unidad temporal: Semestral	**Despliegue temporal:** 2º semestre
Lenguas en las que se imparte: Catalán/Castellano/inglés	
Resultados de aprendizaje: Al terminar con éxito la asignatura, los estudiantes serán capaces de: ● Conocer dónde y cómo buscar información puntualmente actualizada de las vulnerabilidades de seguridad de los sistemas, así como los mecanismos para protegerlos ● Elegir y manejar de forma adecuada las herramientas para hacer pentesting de sistemas operativos ● Aplicar los principios y prácticas del Hacking ético ● 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	
Contenidos: ● Administración de servidores: Windows server, GNU/Linux ● Seguridad pasiva: elementos redundantes, políticas de copias de seguridad, sistemas de recuperación, planes de contingencia ● Seguridad activa: certificados, monitorización de la red, herramientas de comprobación ● Configuración de servicios ● Mantenimiento de sistemas	
Observaciones:	
Competencias básicas y generales: ● 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. ● CG1- Analizar y sintetizar las propiedades de seguridad y privacidad de un sistema. ● CG2- Seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas de ciberseguridad en entornos nuevos o poco conocidos. ● CG3- Buscar, gestionar y utilizar de manera efectiva la información asociada al proceso de análisis y adaptación de nuevas soluciones tecnológicas.	
Competencias transversales:	

- CT1- Capacidad de iniciativa, de automotivación, y de aprendizaje autónomo a partir de la búsqueda y selección efectiva de información
- CT3- Comprensión de textos académicos y profesionales complejos escritos en inglés en el ámbito técnico.

Competencias específicas:

- CE1- Ejercer profesionalmente de forma responsable y honesta, actuando de acuerdo al código ético y a los aspectos legales actuales en el entorno de la seguridad y privacidad de datos.
- CE2- Analizar y aplicar las técnicas básicas de prevención, protección y detección de ataques a un sistema informático.
- CE3- Evaluar y tomar las decisiones más adecuadas en cuanto a la selección y uso de herramientas y tecnologías del mercado en el ámbito de la ciberseguridad y la privacidad.
- CE6- Identificar, examinar y evaluar los principales riesgos de un dominio informático y diseñar estrategias para gestionarlos.

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	40	0
Pruebas objetivas	30	0
Simulación	40	0
Experimentación con objetos reales o laboratorios virtuales	40	0

Metodologías docentes:

- Aprender haciendo (Learning by doing)
- Aprendizaje autónomo
- Aprendizaje basado en problemas (PBL)
- Estudio de caso

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)

Evaluación continua (EC)	40	70
Actividades prácticas	30	60

Denominación de la Asignatura ● Análisis forense	
ECTS materia: 6 ECTS	**Carácter:** Optativa
Unidad temporal: Semestral	**Despliegue temporal:** 2º semestre
Lenguas en las que se imparte: Catalán/Castellano/inglés	
Resultados de aprendizaje: ● Conocer la metodología de la informática forense y cómo aplicarla. ● Conocer de qué manera las diferentes técnicas forenses se relacionan con los sistemas informáticos. ● Aplicar la metodología forense en la preparación del informe pericial para su uso ante el sistema de justicia penal. ● Gestionar de incidentes de una organización correctamente para minimizar los ataques exitosos.	
Contenidos: ● Informática forense y evidencia digital ● Aseguramiento de la escena del suceso ● Identificación y adquisición de la prueba digital ● Análisis de la prueba e investigación ● Laboratorio de informática forense ● Peritación: informe y el dictamen periciales	
Observaciones: ● Para realizar las prácticas de la asignatura, se pondrá a disposición de los estudiantes la herramientas autopsy *Estas herramientas irán actualizándose y adaptándose a las novedades tecnológicas del momento.*	

Competencias 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;
- 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.
- CG1- Analizar y sintetizar las propiedades de seguridad y privacidad de un sistema.

Competencias transversales:

- CT1- Capacidad de iniciativa, de automotivación, y de aprendizaje autónomo a partir de la búsqueda y selección efectiva de información
- CT2- Expresarse de forma escrita de forma adecuada al contexto académico y profesional
- CT3- Comprensión de textos académicos y profesionales complejos escritos en inglés en el ámbito técnico.

Competencias específicas:

- CE1- Ejercer profesionalmente de forma responsable y honesta, actuando de acuerdo al código ético y a los aspectos legales actuales en el entorno de la seguridad y privacidad de datos.
- CE3- Evaluar y tomar las decisiones más adecuadas en cuanto a la selección y uso de herramientas y tecnologías del mercado en el ámbito de la ciberseguridad y la privacidad.

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	40	0
Estudio y resolución de un caso	30	0
Pruebas objetivas	25	0
Resolución de problemas	25	0
Simulación	30	0

Metodologías docentes:

- Aprender haciendo (Learning by doing)
- Aprendizaje basado en problemas (PBL)
- Aprendizaje autónomo

- Estudio de caso

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	40	60
Actividades de prácticas	40	60

Denominación de la Asignatura
- Sistemas de blockchain

ECTS materia: 6 ECTS	**Carácter:** Optativa
Unidad temporal: Semestral	**Despliegue temporal:** 1º semestre

Lenguas en las que se imparte:
Catalán/Castellano/inglés

Resultados de aprendizaje:
- Comprender el funcionamiento de la tecnología blockchain, sus fortalezas y sus limitaciones
- Determinar la idoneidad de integrar un sistema de blockchain en un proyecto complejo
- Evaluar de forma crítica el potencial disruptivo de la blockchain y su encaje junto con otras tecnologías
- Conocer las herramientas y los procedimientos para operar con criptomonedas (ens referim a saber transferir-les, guardar-les, etc?)
- Diseñar e implementar contratos inteligentes y aplicaciones descentralizadas

Contenidos:
- Fundamentos de tecnología blockchain
- Bitcoin
- Ethereum
- Contratos inteligentes
- Blockchain permisionada
- Casos de uso

Observaciones:
Competencias 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; ● 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. ● CG1- Analizar y sintetizar las propiedades de seguridad y privacidad de un sistema. ● CG3- Buscar, gestionar y utilizar de manera efectiva la información asociada al proceso de análisis y adaptación de nuevas soluciones tecnológicas.
Competencias transversales: ● CT1- Capacidad de iniciativa, de automotivación, y de aprendizaje autónomo a partir de la búsqueda y selección efectiva de información ● CT2- Expresarse de forma escrita de forma adecuada al contexto académico y profesional ● CT3- Comprensión de textos académicos y profesionales complejos escritos en inglés en el ámbito técnico.
Competencias específicas: ● CE3- Evaluar y tomar las decisiones más adecuadas en cuanto a la selección y uso de herramientas y tecnologías del mercado en el ámbito de la ciberseguridad y la privacidad. ● CE7- Formular y desarrollar soluciones integrales e innovadoras en el ámbito de la ciberseguridad y privacidad, teniendo en cuenta las dinámicas de transformación y las tendencias tecnológicas

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	50	0
Pruebas objetivas	30	0
Resolución de problemas	30	0
Experimentación con objetos reales o laboratorios virtuales	40	0

Metodologías docentes:

- Aprendizaje autónomo
- Aprender haciendo (Learning by doing)
- Aprendizaje basado en problemas (PBL)
- Aprendizaje indagativo

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	40	70
Actividades de prácticas	30	60

Denominación de la Asignatura

- Seguridad del software

ECTS materia: 6 ECTS	**Carácter:** Optativa
Unidad temporal: Semestral	**Despliegue temporal:** 1r semestre

Lenguas en las que se imparte:
Catalán/Castellano/inglés

Resultados de aprendizaje:

- Comprender dónde se producen y por qué existen vulnerabilidades en los programas

informáticos ● Conocer los tipos y consequències de las vulnerabilidades y de los exploits, y saber protegerse frente a estos ● Seguir las metodologías propias del diseño de aplicaciones seguras ● Aplicar buenas prácticas en el desarrollo de software seguro ● Diseñar y ejecutar tests de seguridad
Contenidos: ● Exploits: bugs; vulnerabilidades; sistemas de explotación ● Herramientas: depuradores, compiladores ● Diseño de aplicaciones seguras: ciclo de vida del desarrollo de software seguro; evaluación de riesgos; modelado de las amenazas; técnicas de seguridad ● Testing y buenas prácticas ● Técnicas de ingeniería inversa
Observaciones:
Competencias 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; ● 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. ● CG1- Analizar y sintetizar las propiedades de seguridad y privacidad de un sistema. ● CG2- Seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas de ciberseguridad en entornos nuevos o poco conocidos.
Competencias transversales: ● CT1- Capacidad de iniciativa, de automotivación, y de aprendizaje autónomo a partir de la búsqueda y selección efectiva de información ● CT3- Comprensión de textos académicos y profesionales complejos escritos en inglés en el ámbito técnico.
Competencias específicas: ● CE2- Analizar y aplicar las técnicas básicas de prevención, protección y detección de ataques a un sistema informático. ● CE3- Evaluar y tomar las decisiones más adecuadas en cuanto a la selección y uso de herramientas y tecnologías del mercado en el ámbito de la ciberseguridad y la privacidad. ● CE6- Identificar, examinar y evaluar los principales riesgos de un dominio informático y

diseñar estrategias para gestionarlos.

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	30	0
Análisis crítico	20	0
Resolución de problemas	20	0
Discusión dirigida	20	0
Simulación	30	0
Experimentación con objetos reales o laboratorios virtuales	30	0

Metodologías docentes:

- Aprender haciendo (Learning by doing)
- Aprendizaje basado en problemas (PBL)
- Aprendizaje autónomo

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	40	60
Actividades de prácticas	40	60

Denominación de la Asignatura

- Arquitecturas y protocolos de seguridad

ECTS materia: 6 ECTS	**Carácter:** Optativa
Unidad temporal: Semestral	**Despliegue temporal:** 2º semestre

Lenguas en las que se imparte:
Catalán/Castellano/inglés

Resultados de aprendizaje:
Al terminar con éxito la asignatura, los estudiantes serán capaces de:

- 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.
- Planificar, configurar y administrar de sistemas de autenticación, autorización y control de acceso
- Diseñar soluciones integrales apropiadas en escenarios complejos con servidores en el cloud que combinen las técnicas y contramedidas conocidas para la prevención, detección y disuasión de ataques.

Contenidos:

- Protocolos seguros de red (e.g. SSH, Radius, WPA)
- Protocolos de autenticación, autorización y control de acceso
- Arquitecturas de Single Sign On
- Riesgos de seguridad de los sistemas cloud y soluciones

Observaciones:

Competencias 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;
- 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.

- CG1- Analizar y sintetizar las propiedades de seguridad y privacidad de un sistema.
- CG2- Seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas de ciberseguridad en entornos nuevos o poco conocidos.
- CG3- Buscar, gestionar y utilizar de manera efectiva la información asociada al proceso de análisis y adaptación de nuevas soluciones tecnológicas.

Competencias transversales:

- CT1- Capacidad de iniciativa, de automotivación, y de aprendizaje autónomo a partir de la búsqueda y selección efectiva de información
- CT3- Comprensión de textos académicos y profesionales complejos escritos en inglés en el ámbito técnico.

Competencias específicas:

- CE2- Analizar y aplicar las técnicas básicas de prevención, protección y detección de ataques a un sistema informático.
- CE3- Evaluar y tomar las decisiones más adecuadas en cuanto a la selección y uso de herramientas y tecnologías del mercado en el ámbito de la ciberseguridad y la privacidad.
- CE6- Identificar, examinar y evaluar los principales riesgos de un dominio informático y diseñar estrategias para gestionarlos.
- CE7- Formular y desarrollar soluciones integrales e innovadoras en el ámbito de la ciberseguridad y privacidad, teniendo en cuenta las dinámicas de transformación y las tendencias tecnológicas

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	40	0
Pruebas objetivas	30	0
Resolución de problemas	20	0
Análisis crítico	20	0
Experimentación con objetos reales o laboratorios virtuales	40	0

Metodologías docentes:

- Aprender haciendo (Learning by doing)
- Aprendizaje autónomo
- Aprendizaje basado en problemas (PBL)
- Aprendizaje indagativo

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	40	70
Actividades prácticas	30	60

Denominación de la Asignatura ● Sistemas de gestión de la seguridad	
ECTS materia: 6 ECTS	**Carácter:** Optativa
Unidad temporal: Semestral	**Despliegue temporal:** 1r semestre
Lenguas en las que se imparte: Catalán/Castellano/inglés	
Resultados de aprendizaje: Al terminar con éxito la asignatura, los estudiantes serán capaces de: ● Comprender los objetivos y utilidades de las normas ISO 27000 ● Identificar y analizar los procesos críticos de una organización, así como el impacto que produciría la interrupción de estos procesos ● Implantar un Sistema de Gestión de la Seguridad de la Información siguiendo las fases del ciclo de Deming y gestionando correctamente los riesgos de la organización ● 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 ● 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	
Contenidos: ● Introducción a la seguridad de la Información: qué es, dimensiones, gestión, normativa legal, estándares ● Análisis de riesgos: ciclo de vida de la seguridad, justificación y estudio del análisis de riesgos, metodologías ● Implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI), familia ISO 27000 ● Planes de continuidad de negocio	
Observaciones:	
Competencias básicas y generales: ● 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.	

- CG1- Analizar y sintetizar las propiedades de seguridad y privacidad de un sistema.
- CG2- Seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas de ciberseguridad en entornos nuevos o poco conocidos.
- CG3- Buscar, gestionar y utilizar de manera efectiva la información asociada al proceso de análisis y adaptación de nuevas soluciones tecnológicas.

Competencias transversales:

- CT1- Capacidad de iniciativa, de automotivación, y de aprendizaje autónomo a partir de la búsqueda y selección efectiva de información
- CT2- Expresarse de forma escrita de forma adecuada al contexto académico y profesional

Competencias específicas:

- CE1- Ejercer profesionalmente de forma responsable y honesta, actuando de acuerdo al código ético y a los aspectos legales actuales en el entorno de la seguridad y privacidad de datos.
- CE3- Evaluar y tomar las decisiones más adecuadas en cuanto a la selección y uso de herramientas y tecnologías del mercado en el ámbito de la ciberseguridad y la privacidad.
- CE6- Identificar, examinar y evaluar los principales riesgos de un dominio informático y diseñar estrategias para gestionarlos.

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	40	0
Presentación y difusión de la información	30	0
Análisis crítico	30	0
Estudio y resolución de un caso	20	0
Pruebas objetivas	20	0
Discusión dirigida	10	0

Metodologías docentes:

- Aprender haciendo (Learning by doing)
- Aprendizaje autónomo
- Estudio de caso

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	100	100

Denominación de la Asignatura
- Auditoría técnica

ECTS materia: 6 ECTS	**Carácter:** Optativa
Unidad temporal: Semestral	**Despliegue temporal:** 2º semestre

Lenguas en las que se imparte:
Catalán/Castellano/inglés

Resultados de aprendizaje:
Al terminar con éxito la asignatura, los estudiantes serán capaces de:
- Distinguir los distintos tipos de auditorías de seguridad aplicables a los Sistemas de Información
- Presentar las técnicas de auditoría más habituales
- Gestionar la certificación de un sistema de gestión de la seguridad de la información, así como comprender, interpretar y explicar las ventajas que aporta la certificación de estos sistemas.
- Elaborar e implementar un plan de auditoría. Saber usar las herramientas habituales para realizar una auditoría técnica de seguridad y comprobar el grado de implantación de los controles de seguridad
- Aplicar las consideraciones legales adquiridas para realizar la gestión de un incidente de seguridad.

Contenidos:
- Introducción a la auditoría informática: componentes, proceso, programa, estandarización de la auditoría, peritaje informático
- Auditoría de certificación ISO 27001
- Auditoría técnica de seguridad: tipos de auditorías, alcance, planificación
- Metodologías

- Técnicas de auditorías

Observaciones:

Competencias 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.

- CG1- Analizar y sintetizar las propiedades de seguridad y privacidad de un sistema.
- CG2- Seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas de ciberseguridad en entornos nuevos o poco conocidos.

Competencias transversales:

- CT1- Capacidad de iniciativa, de automotivación, y de aprendizaje autónomo a partir de la búsqueda y selección efectiva de información
- CT2- Expresarse de forma escrita de forma adecuada al contexto académico y profesional

Competencias específicas:

- CE1- Ejercer profesionalmente de forma responsable y honesta, actuando de acuerdo al código ético y a los aspectos legales actuales en el entorno de la seguridad y privacidad de datos.
- CE3- Evaluar y tomar las decisiones más adecuadas en cuanto a la selección y uso de herramientas y tecnologías del mercado en el ámbito de la ciberseguridad y la privacidad.
- CE5- Aplicar el marco jurídico que afecta a la gestión de la seguridad de sistemas informáticos, teniendo en cuenta la legislación relativa a la protección de de los datos personales, la propiedad intelectual, la ley de los servicios de la sociedad de la información y el comercio electrónico, así como el derecho penal.
- CE6- Identificar, examinar y evaluar los principales riesgos de un dominio informático y

diseñar estrategias para gestionarlos.

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	40	0
Presentación y difusión de la información	30	0
Análisis crítico	30	0
Estudio y resolución de un caso	20	0
Pruebas objetivas	20	0
Discusión dirigida	10	0

Metodologías docentes:

- Aprender haciendo (Learning by doing)
- Aprendizaje autónomo
- Estudio de caso

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	100	100

Denominación de la Asignatura

- Gestión de la seguridad en el cloud

ECTS materia: 6 ECTS	**Carácter:** Optativa
Unidad temporal: Semestral	**Despliegue temporal:** 2º semestre
Lenguas en las que se imparte:	

Catalán/Castellano/inglés
Resultados de aprendizaje: ● Analizar y gestionar los riesgos de seguridad en el cloud ● Establecer políticas de control de accesos e identidades ● Manejar servicios de gestión de claves criptográficas ● Implantar estrategias de detección de vulnerabilidades y gestión de incidentes en el cloud ● Conocer los aspectos legales vinculados a la protección de datos en el cloud ● Establecer acuerdos con proveedores de cloud para asegurar el cumplimiento normativo y la protección de datos
Contenidos: ● Riesgos de seguridad en el cloud ● Políticas de control de accesos, identidades y gestión de claves ● Gestión de vulnerabilidades ● Detección, respuesta y recuperación de incidentes ● Proveedores de cloud: acuerdos de gestión de riesgos, externalización de datos y cómputo ● Cumplimiento normativo en relación a la seguridad y protección de datos
Observaciones:
Competencias 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; ● 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. ● CG3- Buscar, gestionar y utilizar de manera efectiva la información asociada al proceso de análisis y adaptación de nuevas soluciones tecnológicas.
Competencias transversales: ● CT1- Capacidad de iniciativa, de automotivación, y de aprendizaje autónomo a partir de la búsqueda y selección efectiva de información ● CT2- Expresarse de forma escrita de forma adecuada al contexto académico y profesional

Competencias específicas:

- CE1- Ejercer profesionalmente de forma responsable y honesta, actuando de acuerdo al código ético y a los aspectos legales actuales en el entorno de la seguridad y privacidad de datos.
- CE3- Evaluar y tomar las decisiones más adecuadas en cuanto a la selección y uso de herramientas y tecnologías del mercado en el ámbito de la ciberseguridad y la privacidad.
- CE6- Identificar, examinar y evaluar los principales riesgos de un dominio informático y diseñar estrategias para gestionarlos.

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	50	0
Presentación y difusión de la información	20	0
Estudio y resolución de un caso	40	0
Pruebas objetivas	25	0
Discusión dirigida	15	0

Metodologías docentes:

- Aprender haciendo (Learning by doing)
- Trabajo por proyectos
- Aprendizaje autónomo
- Estudio de caso

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	100	100

Módulo 3: Optatividad

Denominación de la Asignatura ● Dirección estratégica de sistemas y tecnologías de la información	
ECTS materia: 6 ECTS	**Carácter:** Optativa
Unidad temporal: Semestral	**Despliegue temporal:** 1r semestre
Lenguas en las que se imparte: Catalán/Castellano/inglés	
Resultados de aprendizaje: ● Examinar el concepto de alineamiento estratégico de los SI/TI y los temas principales de la dirección estratégica de SI/TI, en particular, la evolución del rol de la dirección informática y el papel de la dirección general y el comité de dirección en la definición de las estrategias de sistemas y tecnologías. ● Argumentar los conceptos principales de estrategia de empresa, tal como han sido expuestos por Michael Porter, en su aplicación a la función de gestión de sistemas de información: la cadena de valor, las estrategias competitivas y el atractivo de un mercado; el rol doble de la tecnología (al mismo tiempo fuente de ventaja y riesgo competitivo) y particularmente de Internet. ● Entender el proceso y contenidos de la planificación estratégica de SI/TI y disponer de una aproximación metodológica para ponerla en práctica dentro de la empresa. ● Comprender la evolución y transformación de la función informática en la empresa, los factores que la han propiciado y las formas que adopta, tanto en lo que respecta al negocio como en lo referente a la relación con proveedores y socios. ● Recomendar el diseño y la gestión de la arquitectura y las infraestructuras tecnológicas desde un punto de vista estratégico. ● Defender el concepto de innovación y los modelos de negocio basados en la aplicación de las TIC.	
Contenidos: ● Decisiones estratégicas en sistemas y tecnologías de la información. ● Tecnologías de la información y estrategia de empresa. ● Planificación estratégica de sistemas y tecnologías de la información. ● Transformación de la Función Informática. ● Dirección estratégica de la infraestructura tecnológica y las operaciones. ● Innovación: Modelos de negocio basados en las TIC.	
Observaciones:	

Competencias 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.

- CG3- Buscar, gestionar y utilizar de manera efectiva la información asociada al proceso de análisis y adaptación de nuevas soluciones tecnológicas.

Competencias transversales:

- CT1- Capacidad de iniciativa, de automotivación, y de aprendizaje autónomo a partir de la búsqueda y selección efectiva de información
- CT2- Expresarse de forma escrita de forma adecuada al contexto académico y profesional

Competencias específicas:

- CE3- Evaluar y tomar las decisiones más adecuadas en cuanto a la selección y uso de herramientas y tecnologías del mercado en el ámbito de la ciberseguridad y la privacidad.

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	50	0
Discusión dirigida	10	0
Estudio y resolución de casos	50	0
Realización de un trabajo o proyecto	40	0

Metodologías docentes:

- Aprendizaje autónomo
- Aprender haciendo (Learning by doing)
- Aprendizaje basado en problemas (PBL)
- Trabajo por proyectos

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	100	100

Denominación de la Asignatura
- Técnicas de investigación

ECTS materia: 6 ECTS	**Carácter:** Optativa
Unidad temporal: Semestral	**Despliegue temporal:** 1r semestre

Lenguas en las que se imparte:
Inglés

Resultados de aprendizaje:
Al terminar con éxito la asignatura, los estudiantes serán capaces de:
- Difundir los resultados de una investigación a través de la publicación y presentación de artículos científicos en lengua inglesa
- Planificar, gestionar, dirigir y coordinar proyectos de investigación en el campo de las TIC.
- Ejercer actividades profesionales de acuerdo con el código ético y los aspectos legales vigentes en el entorno de las TIC y la sociedad en red.
- Diseñar y llevar a cabo investigaciones de acuerdo con las normas del conocimiento científico en el campo de las TIC.

Contenidos:
- Redacción, publicación y presentación de artículos científicos
- Propiedad intelectual
- Financiación pública de proyectos de investigación
- Herramientas de apoyo a la investigación

Observaciones:
Esta asignatura está diseñada para los estudiantes que se quieran dedicar a la investigación y se realiza íntegramente en inglés.

Competencias 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.

- CG3- Buscar, gestionar y utilizar de manera efectiva la información asociada al proceso de análisis y adaptación de nuevas soluciones tecnológicas.

Competencias transversales:

- CT2- Expresarse de forma escrita de forma adecuada al contexto académico y profesional
- CT3- Comprensión de textos académicos y profesionales complejos escritos en inglés en el ámbito técnico.

Competencias específicas:

- CE1- Ejercer profesionalmente de forma responsable y honesta, actuando de acuerdo al código ético y a los aspectos legales actuales en el entorno de la seguridad y privacidad de datos.

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	40	0
Presentación y difusión de la información	60	0
Análisis crítico	25	0
Resolución de problemas	25	0

Metodologías docentes:

- Aprender haciendo (Learning by doing)
- Trabajo por proyectos
- Aprendizaje basado en problemas (PBL)
- Aprendizaje indagativo

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	100	100

Denominación de la Asignatura

- Modelos avanzados de minería de datos

ECTS materia: 6 ECTS	**Carácter:** Optativa
Unidad temporal: Semestral	**Despliegue temporal:** 1r semestre

Lenguas en las que se imparte:
Catalán/Castellano/inglés

Resultados de aprendizaje:

- Comprender la diferencia entre métodos supervisados y no supervisados, saber escoger el más adecuado y cómo combinarlos para resolver un problema determinado.
- Conocer los métodos principales para la creación de modelos de clasificación, predicción y regresión.
- Saber evaluar el ajuste de los resultados obtenidos a partir de los modelos construidos.
- Aplicar métodos de combinación de clasificadores para mejorar la eficiencia de los modelos construidos.

Contenidos:

- Validación y evaluación de resultados
- Extracción y selección de atributos
- Métodos no supervisados
    - Agrupamiento jerárquico

- El método k-means y derivados
- Canopy clustering algorithm

- Métodos supervisados
  - Algoritmo K-NN
  - Árboles de decisión
  - Support Vector Machines (SVM)
- Redes neuronales y deep learning
- Combinación de clasificadores

Observaciones:
Esta asignatura requiere que los estudiantes tengan conocimientos de programación (preferiblemente en lenguaje Python), así como conocimientos de minería de datos.

Competencias 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.

- CG3- Buscar, gestionar y utilizar de manera efectiva la información asociada al proceso de análisis y adaptación de nuevas soluciones tecnológicas.

Competencias transversales:

- CT1- Capacidad de iniciativa, de automotivación, y de aprendizaje autónomo a partir de la búsqueda y selección efectiva de información
- CT2- Expresarse de forma escrita de forma adecuada al contexto académico y profesional
- CT3- Comprensión de textos académicos y profesionales complejos escritos en inglés en el ámbito técnico.

Competencias específicas:

- CE4- Desarrollar, integrar, y evaluar técnicas informáticas que permitan aplicar los principios de privacidad y protección de datos desde el diseño y por defecto que exige el Reglamento General de Protección de Datos (RGPD) a los sistemas, servicios y aplicaciones que traten con datos personales.

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	50	0
Resolución de problemas	50	0
Realización de un trabajo o proyecto	50	0

Metodologías docentes:

- Aprendizaje autónomo
- Aprender haciendo (Learning by doing)
- Aprendizaje basado en problemas (PBL)
- Aprendizaje indagativo

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	40	70
Actividades de prácticas	30	60

Denominación de la Asignatura

- Ciberdelitos: estudio de los tipos delictivos

ECTS materia: 6 ECTS	**Carácter:** Optativa
Unidad temporal: Semestral	**Despliegue temporal:** 1r semestre

Lenguas en las que se imparte:
Catalán/Castellano/inglés

Resultados de aprendizaje:

- Identificar las diversas tipologías delictivas relacionadas con la ciberdelincuencia, en especial según la previsión de las mismas en el Código penal español: daños y sabotaje informático, descubrimiento y revelación de secretos, intrusión en sistemas informáticos, defraudaciones y estafa informática, pornografía infantil, embaucamiento o acoso sexual en línea.
- Emplear el marco normativo internacional y en particular europeo que determina la respuesta jurídica a la ciberdelincuencia.
- Conocer el marco jurídico-procesal, en especial las normas introducidas en la legislación procesal española para la persecución de los ciberdelitos.
- Conocer los aspectos normativos, en su dimensión europea y española, relacionados con el uso y la protección de las bases datos.
- Aplicar los mecanismos y estrategias de detección de elementos de prueba de ciberdelitos y ser capaz de construir y presentar las pruebas en el seno de un procedimiento penal.

Contenidos:

- Ciberdelitos; estudio de los tipos delictivos: daños informáticos, acceso ilícito a sistemas de información, intercepción y transmisión de datos informáticos, violación de secretos estafas informáticas, delitos contra la propiedad intelectual e industrial.
- Aspectos procesales de la ciberdelincuencia: estudio de las especialidades introducidas en las reformas de 2015.
- Protección de datos: marco normativo general que regula el tratamiento de la información personal. Estudio del Reglamento 2016/679/UE, principio de responsabilidad proactiva, nuevos derechos (portabilidad y limitación del tratamiento) y obligaciones del responsable del tratamiento; evaluaciones de impacto, consulta previa, la figura del delegado de protección de datos.
- Tratamiento de datos en entornos digitales: marco jurídico de actuación del responsable y del encargado del tratamiento; estatuto del sujeto afectado por el tratamiento.

Observaciones:

Competencias 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.

- CG1- Analizar y sintetizar las propiedades de seguridad y privacidad de un sistema.
- CG2- Seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas de ciberseguridad en entornos nuevos o poco conocidos.

Competencias transversales:

- CT1- Capacidad de iniciativa, de automotivación, y de aprendizaje autónomo a partir de la búsqueda y selección efectiva de información
- CT2- Expresarse de forma escrita de forma adecuada al contexto académico y profesional

Competencias específicas:

- CE1- Ejercer profesionalmente de forma responsable y honesta, actuando de acuerdo al código ético y a los aspectos legales actuales en el entorno de la seguridad y privacidad de datos.

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	50	0
Resolución de problemas	40	0
Pruebas objetivas	20	0
Estudio y resolución de un caso	20	0
Discusión dirigida	20	0

Metodologías docentes:

- Aprendizaje autónomo
- Aprender haciendo (Learning by doing)
- Aprendizaje basado en problemas (PBL)

- Aprendizaje indagativo

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	40	70
Actividades de prácticas	30	60

Denominación de la Asignatura
- Criptografía avanzada

ECTS materia: 6 ECTS	**Carácter:** Optativa
Unidad temporal: Semestral	**Despliegue temporal:** 2º semestre

Lenguas en las que se imparte:
Catalán/Castellano/inglés

Resultados de aprendizaje:
- Reconocer los principales tópicos que forman parte de la Criptografía Avanzada.
- Saber construir un cuerpo finito y saber calcular con sus elementos.
- Saber las técnicas básicas de sumar y operar puntos de una curva elíptica.
- Conocer y saber utilizar los principales criptosistemes, tanto clásicos como avanzados.
- Conocer y saber utilizar los principales criptosistemes, tanto de clave privada como de clave pública.
- Conocer y saber utilizar los principales protocolos (autenticación, distribución de claves, etc.) tanto los basados en los problemas clásicos de factorización y logaritmo discreto, como los basados en el logaritmo elíptico)
- Aplicar los conceptos adquiridos a través de la programación en software simbólico (MAGMA, SAGE, por ejemplo)

Contenidos:
- Computación en cuerpos finitos
- Criptografía cuántica

- Protocolos de gestión y distribución de claves
- Protocolos de autenticación
- Transacciones electrónicas seguras
- Protocolos de transferencia inconsciente
- Esquemas umbral y reparto de secretos
- Votaciones electrónicas
- Sistemas de curvas elípticas
- Pairings en curvas elípticas
- Criptografía basada en la identidad

Observaciones:

Competencias 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;
- 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.

- CG1- Analizar y sintetizar las propiedades de seguridad y privacidad de un sistema.
- CG2- Seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas de ciberseguridad en entornos nuevos o poco conocidos.

Competencias transversales:

- CT2- Expresarse de forma escrita de forma adecuada al contexto académico y profesional

Competencias específicas:

- CE2- Analizar y aplicar las técnicas básicas de prevención, protección y detección de ataques a un sistema informático.
- CE3- Evaluar y tomar las decisiones más adecuadas en cuanto a la selección y uso de herramientas y tecnologías del mercado en el ámbito de la ciberseguridad y la privacidad.
- CE6- Identificar, examinar y evaluar los principales riesgos de un dominio informático y diseñar estrategias para gestionarlos.
- CE8- Analizar la implementación y despliegue de soluciones criptográficas para validar su funcionamiento

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	40	0
Pruebas objetivas	20	0
Resolución de problemas	40	0
Experimentación con objetos reales o laboratorios virtuales	50	0

Metodologías docentes:

- Aprendizaje autónomo
- Aprender haciendo (Learning by doing)
- Aprendizaje basado en problemas (PBL)

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	40	70
Actividades de prácticas	30	60

Denominación de la Asignatura

- Biometría

ECTS materia: 6 ECTS	**Carácter:** Optativa
Unidad temporal: Semestral	**Despliegue temporal:** 2º semestre
Lenguas en las que se imparte: Catalán/Castellano/inglés	
Resultados de aprendizaje:	

● Identificar las características básicas de los sistemas biométricos. ● Clasificar las herramientas para evaluar la bondad de los sistemas biométricos. ● Argumentar el reconocimiento de las personas a través del dedo. ● Argumentar el reconocimiento de las personas a través de la imagen de la cara. ● Argumentar el reconocimiento de las personas a través de la imagen del iris. ● Analizar los métodos para garantizar la seguridad en los sistemas biométricos.
Contenidos: ● La Biometría por la Identificación de las Personas ● Evaluación de los Sistemas Biométricos en Aplicaciones Reales ● Reconocimiento de las Personas por el Dedo ● Reconocimiento de las Personas por la Cara ● Reconocimiento de las Personas por Iris ● Seguridad en los Sistemas Biométricos
Observaciones:
Competencias 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; ● 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. ● CG1- Analizar y sintetizar las propiedades de seguridad y privacidad de un sistema. ● CG3- Buscar, gestionar y utilizar de manera efectiva la información asociada al proceso de análisis y adaptación de nuevas soluciones tecnológicas.
Competencias transversales: ● CT2- Expresarse de forma escrita de forma adecuada al contexto académico y profesional
Competencias específicas: ● CE2- Analizar y aplicar las técnicas básicas de prevención, protección y detección de ataques a un sistema informático. ● CE3- Evaluar y tomar las decisiones más adecuadas en cuanto a la selección y uso de herramientas y tecnologías del mercado en el ámbito de la ciberseguridad y la privacidad. ● CE6- Identificar, examinar y evaluar los principales riesgos de un dominio informático y

diseñar estrategias para gestionarlos.
- CE7- Formular y desarrollar soluciones integrales e innovadoras en el ámbito de la ciberseguridad y privacidad, teniendo en cuenta las dinámicas de transformación y las tendencias tecnológicas

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	40	0
Pruebas objetivas	20	0
Análisis crítico	20	
Resolución de problemas	30	0
Experimentación con objetos reales o laboratorios virtuales	40	0

Metodologías docentes:
- Aprendizaje autónomo
- Aprender haciendo (Learning by doing)
- Aprendizaje basado en problemas (PBL)

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	100	100

Denominación de la Asignatura
- Técnicas de ocultación de la información

ECTS materia: 6 ECTS	**Carácter:** Optativa
Unidad temporal: Semestral	**Despliegue temporal:** 2º semestre

Lenguas en las que se imparte: Catalán/Castellano/inglés	
Resultados de aprendizaje: ● Comprender los conceptos básicos del watermarking y la esteganografía. ● Evaluar las diferentes propiedades de los esquemas de marcado de la información. ● Saber utilizar diferentes mecanismos de marcado de imágenes. ● Conocer las diferentes aplicaciones existentes para los mecanismos de watermarking y esteganografía.	
Contenidos: ● Introducción: Se proporcionan las definiciones básicas y la nomenclatura que se utiliza en el área del marcado de la información, se realiza un repaso histórico de esta disciplina y se enumeran las diferentes aplicaciones que tienen hoy en día las técnicas de marcado de la información. ● Propiedades de los esquemas de marcado de la información: Se describen en detalle las diferentes propiedades que deben tener los sistemas de marcado de la información (imperceptibilidad, capacidad, robustez, seguridad...) en función del objetivo y la aplicación que se les quiera dar. ● Evaluación de los esquemas de marcado de la información: Se presentan las técnicas para medir las propiedades presentadas en el punto anterior para poder evaluar los diferentes sistemas de marcado de imágenes. ● Esquemas de esteganografía: Se analizan diferentes técnicas prácticas de esteganografía para imágenes. ● Esquemas de watermarking para imágenes: Se presentan diferentes técnicas prácticas de watermarking en imágenes. Estas técnicas van desde la inserción de información en el dominio espacial de la imagen como en el dominio transformado.	
Observaciones:	
Competencias 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; ● 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.	

- CG1- Analizar y sintetizar las propiedades de seguridad y privacidad de un sistema.

Competencias transversales:

- CT1- Capacidad de iniciativa, de automotivación, y de aprendizaje autónomo a partir de la búsqueda y selección efectiva de información
- CT2- Expresarse de forma escrita de forma adecuada al contexto académico y profesional
- CT3- Comprensión de textos académicos y profesionales complejos escritos en inglés en el ámbito técnico.

Competencias específicas:

- CE6- Identificar, examinar y evaluar los principales riesgos de un dominio informático y diseñar estrategias para gestionarlos.

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	20	0
Análisis crítico	20	0
Pruebas objetivas	30	0
Resolución de problemas	40	0
Experimentación con objetos reales o laboratorios virtuales	40	0

Metodologías docentes:

- Aprendizaje autónomo
- Aprender haciendo (Learning by doing)
- Aprendizaje basado en problemas (PBL)

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Evaluación continua (EC)	100	100

Módulo 4: Trabajo final

Denominación de la Asignatura ● Trabajo final de máster	
ECTS materia: 12 ECTS	**Carácter:** Obligatoria
Unidad temporal: Semestral	**Despliegue temporal:** 2º semestre
Lenguas en las que se imparte: Catalán/Castellano/inglés	
Resultados de aprendizaje: ● Demostrar comprensión detallada en un ámbito especializado dentro de la ciberseguridad y privacidad. ● Adquirir la capacidad de definir, planificar, ejecutar y evaluar proyectos integrales en el ámbito de la ciberseguridad y privacidad. ● 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 del de la ciberseguridad y privacidad	
Contenidos: En el Trabajo Final de Máster se pondrán en práctica y se profundizará en las competencias generales del máster mediante la elaboración de un trabajo escrito. Asimismo, durante la elaboración de dicho trabajo se intentará fomentar el desarrollo de competencias similares a las de la práctica profesional o científica. Cabe 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. Por último, es importante destacar que en función de la temática del Trabajo Final de Máster, el estudiante profundizará sus conocimientos en las competencias relacionadas.	
Observaciones:	
Competencias 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.

- CG1- Analizar y sintetizar las propiedades de seguridad y privacidad de un sistema.
- CG2- Seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas de ciberseguridad en entornos nuevos o poco conocidos.
- CG3- Buscar, gestionar y utilizar de manera efectiva la información asociada al proceso de análisis y adaptación de nuevas soluciones tecnológicas.

Competencias transversales:
- CT1- Capacidad de iniciativa, de automotivación, y de aprendizaje autónomo a partir de la búsqueda y selección efectiva de información
- CT2- Expresarse de forma escrita de forma adecuada al contexto académico y profesional
- CT3- Comprensión de textos académicos y profesionales complejos escritos en inglés en el ámbito técnico.

Competencias específicas:
- CE1- Ejercer profesionalmente de forma responsable y honesta, actuando de acuerdo al código ético y a los aspectos legales actuales en el entorno de la seguridad y privacidad de datos.
- CE2- Analizar y aplicar las técnicas básicas de prevención, protección y detección de ataques a un sistema informático.
- CE3- Evaluar y tomar las decisiones más adecuadas en cuanto a la selección y uso de herramientas y tecnologías del mercado en el ámbito de la ciberseguridad y la privacidad.
- CE4- Desarrollar, integrar, y evaluar técnicas informáticas que permitan aplicar los principios de privacidad y protección de datos desde el diseño y por defecto que exige el Reglamento General de Protección de Datos (RGPD) a los sistemas, servicios y aplicaciones que traten con datos personales.

- CE5- Aplicar el marco jurídico que afecta a la gestión de la seguridad de sistemas informáticos, teniendo en cuenta la legislación relativa a la protección de de los datos personales, la propiedad intelectual, la ley de los servicios de la sociedad de la información y el comercio electrónico, así como el derecho penal.
- CE6- Identificar, examinar y evaluar los principales riesgos de un dominio informático y diseñar estrategias para gestionarlos.
- CE7- Formular y desarrollar soluciones integrales e innovadoras en el ámbito de la ciberseguridad y privacidad, teniendo en cuenta las dinámicas de transformación y las tendencias tecnológicas
- CE8- Analizar la implementación y despliegue de soluciones criptográficas para validar su funcionamiento
- CE9- Realizar, presentar y defender ante un tribunal universitario un ejercicio original realizado individualmente, consistente en un proyecto integral de Ciberseguridad y privacidad de naturaleza profesional o de investigación, en el que se sinteticen e integren las competencias adquiridas en las enseñanzas.

Actividades formativas (indicar nº de horas y % de Presencialidad de cada una):

Actividades formativas	Horas	Presencialidad
Búsqueda, selección y gestión de la información	100	0
Análisis crítico	40	0
Realización de un trabajo o proyecto	140	0
Presentación y difusión de la información	20	0

Metodologías docentes:

- Aprendizaje autónomo
- Aprender haciendo (Learning by doing)
- Trabajo por proyectos
- Aprendizaje indagativo

Sistemas de evaluación (indicar Ponderación Máxima y Mínima):

Sistemas de evaluación	Ponderación mínima (%)	Ponderación máxima (%)

Evaluación continua (EC)	40	60
Trabajo Final de Máster	40	60

Mapa de competencias del Máster

Módulo	Asignatura	Competencia básica					Competencia general			Competencia transversal			Competencia específica								
		CB6	**CB7**	**CB8**	**CB9**	**CB10**	**CG1**	**CG2**	**CG3**	**CT1**	**CT2**	**CT3**	**CE1**	**CE2**	**CE3**	**CE4**	**CE5**	**CE6**	**CE7**	**CE8**	**CE9**
Fundamentos	Legislación y protección de datos		X	X	X	X	X			X	X		X				X				
	Fundamentos de ciberseguridad	X	X			X	X	X	X	X		X		X	X			X		X	
	Privacidad	X	X			X	X	X	X			X			X	X		X	X		
Especialidad	Seguridad y pentesting de servidores de datos					X	X	X	X	X		X	X	X	X			X			
	Seguridad y pentesting de sistemas					X	X	X	X	X		X	X	X	X			X			
	Análisis forense		X			X	X			X	X	X	X		X						

	Sistemas de blockchain	X	X		X	X	X		X	X	X	X			X				X		
	Seguridad del software		X			X	X	X		X		X		X	X			X			
	Arquitecturas y protocolos de seguridad		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		X		X	X			
	Gestión de la seguridad en el cloud	X	X			X			X	X	X		X		X			X			
Optatividad	Dirección estratégica de sistemas y tecnologías de la información		X		X	X			X	X	X				X						
	Técnicas de investigación		X		X	X			X		X	X	X								
	Modelos avanzados de minería de datos	X	X	X	X	X			X	X	X	X				X					
	Ciberdelitos: estudio de los tipos delictivos	X	X	X	X	X	X	X		X	X		X								
	Criptografía avanzada	X	X			X	X	X			X			X	X			X		X	
	Biometría	X	X			X	X		X		X			X	X			X	X		
	Técnicas de ocultación de la información	X	X			X	X			X	X	X						X			
Trabajo final	Trabajo Final de Máster	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

6. PERSONAL ACADÉMICO

6.1. Profesorado y otros recursos humanos necesarios y disponibles para llevar a cabo el plan de estudios propuesto

La Universitat Oberta de Catalunya dispone de una estructura académica y de una estructura de gestión fija que garantizan el buen funcionamiento de la Universidad.

La estructura académica está formada por el personal académico cuya vinculación con la universidad determina la actividad acadèmica que desarrolla.:

Personal académico con vinculación o contratación laboral:

- Profesorado permanente
- Investigador
- Otro personal académico

Personal académico cuya vinculación o contratación no es laboral:

- Personal docente colaborador

Personal académico con vinculación o contratación laboral:

El profesorado permanente es el contratado a tiempo completo, de manera indefinida con dedicación de exclusividad, salvo autorización expresa. El otro personal académico, presta una dedicación a tiempo parcial, por un período de tiempo determinado y vinculado a un proyecto o programa académico concreto.

Estas figuras académicas (Profesorado permanente y otro personal académico) son responsables de la dirección académica de los programas y las asignaturas y de la calidad del proceso de enseñanza-aprendizaje y cumplimiento de los objetivos de formación. Este profesorado es el responsable de la planificación académica, de la definición de los contenidos y recursos y del proceso de evaluación del estudiante.

La Política de personal académico de la UOC contempla las siguientes posiciones, en adelante categorías y sus funciones asociadas (al no coincidir las categorías del convenio colectivo de la universidad con las presentes en el cuadro resumen de la aplicación del Ministerio, se concreta para cada categoría la que se usará en la aplicación):

Profesorado permanente:

- Profesor lector: Se trata de una posición inicial de profesorado, mantiene una dedicación preferente a las funciones docentes si bien participa de manera progresiva en funciones de planificación docente, innovación y mejora e investigación. Los requisitos mínimos para esta posición son estar en posesión del título de doctor y un mínimo de 2 años de experiencia docente.

- Profesor agregado: Se trata de un profesor doctor, experto en la metodología de aprendizaje de la UOC i con plena capacidad docente e investigadora debidamente acreditada por los procedimientos establecidos en el sistema universitario. Los requisitos mínimos para esta posición son estar en posesión del título de doctor, un mínimo de 6 años de experiencia como profesor y haber obtenido los méritos académicos establecidos en la Política de personal académico.

- Profesor senior: Asume un rol de liderazgo en la planificación y ejecución de la actividad académica, su evaluación y mejora y con una carrera académica consolidada y debidamente acreditada por los procedimientos vigentes en el sistema universitario. Los requisitos mínimos para esta posición son estar en posesión del título de doctor, un mínimo de 10 años de experiencia como profesor y haber obtenido los méritos académicos establecidos en la Política de personal académico.

- Catedrático: Asume el rol de liderazgo en la planificación y ejecución de la actividad académica, su evaluación y mejora y dispone de una ámplia experiencia en el liderazgo de equipos de investigación. Es excelente en investigación y dispone de una carrera académica plenamente consolidada y debidamente acreditada por los procedimientos vigentes en el sistema universitario. Los requisitos mínimos para esta posición son estar en posesión del título de doctor, un mínimo de 10 años de experiencia como profesor y disponer de la acreditación en investigación avanzada de AQU o Catedrático ANECA, así como disponer de los méritos académicos establecidos en la Política de personal académico.

Otros personal académico:

- Profesor asociado: Se corresponde al profesorado que puede ser contratado por la universidad considerando su experiencia profesional o académica para complementar ámbitos de especialización del profesorado permanente. Se valora la experiencia y competencia profesional. La contratación es a tiempo parcial.

- Profesor compartido: Es profesor en otra universidad que mediante acuerdo institucional también presta servicios a la UOC.

- Profesor visitante: Se corresponde al profesorado que, resultado de alianzas de institucionales permite la movilidad para el intercambio de conocimiento y experiencia.

La Política de personal académico reconoce la categoría de ayudante, para aquel profesorado cuya vinculación contractual es de carácter permanente pero no ha consolidado el título de doctor. La Política de personal académico reconoce también la figura de profesor emérito.

Personal académico cuya vinculación o contratación no es laboral

Para el completo desarrollo de los procesos de enseñanza-aprendizaje de los estudiantes en el aula virtual, la Universidad cuenta una red de más de cuatro mil profesores colaboradores y tutores, coordinados en todo momento por el profesorado de la Universidad:

- Profesor colaborador: Asume funciones de acompañamiento docente y evaluación de un grupo de estudiantes (de un máximo de 70) de una asignatura determinada.
- Tutor: Asume funciones de acogida, asesoramiento y orientación académica a los estudiantes. Les ofrece apoyo en la adaptación al entorno de aprendizaje y participa activamente en la prevención del abandono.

6.1.1.Personal académico disponible para el título

Los Estudios de Informática, Multimedia y Telecomunicación están dirigidos por el/la directora/a de estudios, que es el responsable de toda la oferta de los estudios y es miembro de la Comisión Académica. La Comisión de la Titulación, responsable principal del diseño de la titulación, del seguimiento de su implementación y de la evaluación del programa, está presidida por el/la directora/a del máster universitario.

El profesorado participante en el título se detalla a continuación:

Dirección del programa:

Tabla resumen CV					
Profesorado	**Titulación académica**	**Acreditación académica**	**Categoría / nivel contractual**	**Dedicación**	**Experiencia académica y/ o profesional y/o investigad**
Rifà Pous, Helena	Doctora en Telemática e Ingeniería de Telecomunicaciones (UPC)	Acreditación de Investigación (profesor agregado) AQU 2 tramos de docencia 1 tramo de investigación	Profesora Agregada	Parcial 50%	Docencia:Criptografía Seguridad de Redes Grupo de investigación: KISON Directora del Máster en Seguridad de las TIC (UOC, UAB,URV),desde septiembre Profesora de los Estudios de Informática, Multimedia y Telecomunicación de la UOC desde 2007. 2005-2012:profesora ayudante UAB,dpt. de ingeniería de la información y las comunicaciones 2000-2007, responsab le de proyectos en Safelayer.

Profesorado:

Tabla resumen CV					
Profesorado	**Titulación académica**	**Acreditación académica**	**Categoría / nivel contractual**	**Dedicación**	**Experiencia académica y/ o profesional y/o investigad**
Garrigues Olivella, Carles	Doctor en Ingeniería Informática por la Universidad Autónoma de	Acreditado como Profesor Lector por la AQU	Profesor agregado	100%	Desarrollo asistido de aplicaciones, Protección de agentes móviles, Sistemas dist Código móvil, Entornos ubicuos. Investigación en seguridad en redes de sensores y redes de radio cognitiva.

	Barcelona (UAB) Ingeniería Informática por la Universidad Autónoma de Barcelona (UAB)	1 tramo docente 2 tramos investigación			Desde 2008: Investigador del grupo de investigación KISON (K-ryptography and I Security for Open Networks) Desde 2015 Director del Máster Univ. en Desarrollo para móviles de la UOC 2009 - 2015 Director del Máster Univ. en Software Libre de la UOC Desde 2008 Profesor en la UOC 2004 - 2008 Investigador predoctoral en la UAB 2004 - 2008 Docente colaborador en la UAB 2003 - Analista programador
Serra Ruiz, Jordi	Doctor en Sociedad de la Información y el conocimiento	2 tramos docentes.Último tramo docente: 2011	Profesor	100%	Seguridad de la información y seguridad en redes, Software y conocimientos libres 2016-2018: Director del Posgrado de Cisco Profesor ayudante en la UAB entre septiembre de 1997 y julio de 2002. Desde 2002 es profesor de la UOC Del 2015 al 2016 fue mentor de proyectos tecnológicos en Talentum StartUp Tel año 2015 llevó los proyectos Talentum en ElBulliFoundation de Ferran Adrià. Las actividades docentes se centran en el análisis forense, el malware, vulnerabi ciberseguridad... Sus ámbitos de investigación principales incluyen la esteganografía, criptografía, informática, ciberseguridad, análisis forense...
Serra Vicern, Montse	Doctorado en Informática	3 tramos docentes. Último tramo docente: 2016	Profesor agregado	100%	Desde 2001: Profesora en la Universitat Oberta de Catalunya. 1999-2001: Técnica de telecomunicación en Telefónica España. 1997-1999: Profesora Asociada en la Universitat Autònoma de Barcelona. 1996-1997: Becaria en la Universidad Técnica de Wroclaw - Polonia (beca Tempu Unión Europea). Docencia:Fundamentos de computadores, aspectos jurídicos, gestión de la segu Investigación: Ética profesional aplicada a las ingenierías y a los entornos virtuales
Garcia Font, Victor	Doctorado en Tecnología de la información y redes		Profesor	50%	Profesor e investigador de la UOC, desde 2017 Assistant professor UAB , desde 2018 Investigador postdoc URV (enero'18-ago'18) Industrial Phd, UOC, 2014-2017 Senior technical specialist, Centre for Ecological Research and Forest Application Autonomous University of Barcelona, 2006-2013 Junior programmer, Electronic Data system,2005-2006

Perez-Solá, Cristina	Doctorado en Ciencia de Ingeniería	Acreditado como Profesor Lector por la AQU	Profesor	100%	Docencia: Investigación:criptomonedas basadas en el blockchain y en la privacidad, criptog machine learning. Profesora colaboradora de la UOC desde 2012 en temas de criptografía Postdoctoral researcher: Universitat Rovira i Virgili (URV), September 2018 - (now) Postdoctoral researcher: Departament d'Enginyeria de la Informació i les Comunicacions (dEIC), January 2 August 2018 PhD Grantholder (Formación de Profesorado Universitario - FPU), Departament d'Enginyeria de la Informació i les Comunicacions (dEIC), February December 2016 Superior research technician for Project N-KHRONOUS, Departament d'Enginyeria de la Informació i les Comunicacions (dEIC), July 2011 2013 Superior research technician for Project Avanza MyCity (Tècnic superior de supo recerca), Departament d'Enginyeria de la Informació i les Comunicacions (dEIC), Septemb April 2011 Specialist research technician for Project Avanza MyCity (Tècnic especialista de s recerca), Departament d'Enginyeria de la Informació i les Comunicacions (dEIC), April 201 September 2010 Research assistant for Project Avanza MyCity (Becari de Suport a la Recerca), Departament d'Enginyeria de la Informació i les Comunicacions (dEIC), May 200 2010
Megías Giménez, David	Doctorat en enginyeria informàtica	Acreditado como Profesor Lector por la AQU Acreditación de investigación 2011 Investigación avanzada (catedrático AQU-ANECA) 3 tramos de investigación 3 tramos docentes	Catedrático	100%	Profesor ayudante en la UAB entre septiembre de 1994 y octubre de 2001. Desde octubre de 2001, trabaja como profesor de la UOC. Director del IN3 de la UOC, desde 2015 Docencia: software libre y código abierto. Investigación: protección de los derechos de autor (copyright) de contenidos mu software libre (free software) y el software de código abierto (open source) y el procesos industriales. Ha participado en proyectos y convenios de investigación como miembro del eq investigación y también como gestor del proyecto (investigador principal). Tamb experiencia en proyectos europeos, como por ejemplo la European Network of E Cryptology (formando un grupo conjuntamente con la Universidad de Vigo) del s programa marco de la Comisión Europea. Miembro del grupo de investigación KISON
Rodríguez, Jose Ramón	Máster universitario en Aplicaciones multimedia		Profesor asociado	50%	docencia e investigación en Management Information systems and Business Inte Profesor de la UOC desde 2011

					consultor independiente de BI
Romero Tris, Cristina	Doctorado en Ingeniería Informática.		Profesor	50%	2019 - actualidad Profesora UOC 2015 - 2018 Investigador post-doctoral Universitat Oberta de Catalunya (UOC) e de investigación KISON 2011 - 2015 Becario del programa del Ministerio Educación y Cultura de España Formación del Profesorado 2009 - 2010 Becario de investigación financiado por el Departamento de Ingenie Informática y Matemáticas de la Universidad Rovira i Virgili 2010 - 2011 Becario programa de Investigación R+D+I Universidad Rovira i Virgili 2008 - 2009 Contrato investigación en Inteligencia Artificial Universidad Rovira i
Prieto, Josep	Doctorado en Sociedad de la información y el conocimiento	Acreditado como Profesor Lector por la AQU 1 tramo investigación 3 tramos docentes	Profesor agregado	100%	1998 profesor de los Estudios de Informática, Multimedia y Telecomunicación en 2013-2019:Decano de los Estudios de Informática, Multimedia y Telecomunicaci UOC. investigación: prospectiva y aplicaciones tecnológicas en el ámbito de las TIC, ha participado en los proyectos Wireless, Herramientas de aprendizajes en entorno trabajo cooperativo en entornos virtuales y siendo miembro también del grupo investigación KISON (K-ryptography and Information Security for Open Network Actualmente es el responsable tecnológico del proyecto H2020 TeSLA (Adaptive e-assessment System for Learning)
Casas Roma, Jordi	Doctorado en Informática	Evaluación positiva lector (AQU/ANECA) 1 tramo de investigación 1 tramo de docencia	Profesor agregado	100%	Desde 2014: Profesor Universitat Oberta de Catalunya (UOC) Desde 2010: Miembro del grupo de investigación KISON (K-ryptography and Info Security for Open Networks) 2009-2014: Profesor/a ayudante UOC 2004-2009: Docente colaborador en la UOC 2004-2009: Analista programador freelance. 2003-2003: Becario en la Cátedra IBM-La Caixa
Tamarit Sumalla, Josep Mª	Doctorado en Derecho	Acreditado como Profesor Lector por la AQU Evaluación positiva lector (AQU/ANECA) Investigación avanzada(	Catedrático	100%	Catedrático de Universidad en la Universidad de Lleida desde 1999. Direc programa de Criminología en la UOC desde 2010. Coordinador del Grupo consolidado de investigación Sistema de justicia penal desde 2005. Cinco de investigación

		catedrático AQU-Catedrático ANECA) 5 tramos de investigación 5 tramos de docencia			

Tabla resumen *(rellenar la tabla con el profesorado recogido en las tablas anteriores)*:

Universidad	Categoría *	Total %	Doctores %	Horas %
UOC	Profesor Contratado Doctor	33,33%	100%	42,86%
UOC	Profesor Asociado	8,33%	0%	4,76%
UOC	Profesor Agregado	41,67%	100%	38,10%
UOC	Catedrático	16,67%	100%	14,29%

** NOTA: Seleccionar en función de la Categoría.*
Asociado UOC= Profesor Asociado
Profesor ayudante UOC= Ayudante
Profesor UOC= Profesor Contratado Doctor
Profesor Agregado UOC= Profesor Agregado
Catedrático UOC= Catedrático de universidad

Además se aporta la siguiente información agregada del profesorado vinculado con la titulación:

Méritos docentes:

	Menos de 5 años	Entre 5 y 10 años	10 años o más
Años experiencia docente	3	4	5
Tramos docentes acumulados	20		
Profesores con tramos docentes	8		
Profesores con tramos docentes vivos	4		

Méritos de investigación:

Tramos investigación acumulados	13
Profesores con tramos investigación	6

Profesores con tramos de investigación vivos	5

Otros méritos académicos

Finalmente, hay que mencionar que un 50% posee experiencia profesional diferente a la académica o investigadora, sea en el ámbito empresarial o en el de la administración pública.

El/La directora/a de Programa tiene como funciones la coordinación general de la titulación y la garantía de su calidad, lo que implica la coordinación del equipo de profesores responsables de asignatura (PRA) así como del equipo de tutores.

El PRA es responsable del diseño de la asignatura, planificación de la acción docente y de la garantía de la calidad de su enseñanza, y delega en el profesor colaborador la ejecución de la atención docente que recibe el estudiante. El Profesor responsable de asignatura es el responsable de la selección y valoración de los profesores colaboradores.

En el momento del diseño de la asignatura, se define cuál debe ser el perfil adecuado del profesor colaborador en términos de requisitos: titulación académica, años de experiencia académica y/o profesional adecuados al ámbito de especialización de la asignatura, y otros méritos que permitan confirmar la adecuación durante el proceso de selección.

El proceso de selección es público y de libre concurrencia. Todas las ofertas están disponibles en el portal web de la universidad, y en ellas se definen tanto la titulación requerida, así como el tipo de experiencia docente y/o profesional que se debe aportar.

Anualmente, en el marco del proceso de seguimiento de las titulaciones, se valora la adecuación del perfil de los profesores colaboradores en términos de adecuación académica, así como la experiencia profesional y/o docente requerida para el desarrollo de una formación de calidad. Así mismo se revisan los resultados académicos y de satisfacción con la acción docente.

La información relativa al perfil del profesorado colaborador se analiza de forma agregada desde la dirección de programa, y a nivel de asignatura a través del profesor responsable.

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 recursos de aprendizaje, el diseño del plan docente, la planificación de todas las actividades del semestre y la evaluación de los procesos de aprendizaje de los estudiantes, hasta la selección, coordinación y supervisión de los profesores colaboradores, que son quienes llevan a cabo la ejecución de la docencia siguiendo las directrices marcadas por el PRA. Es el PRA quién 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 la UOC.

El PRA coordina a los distintos profesores colaboradores 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. Esta coordinación se lleva a cabo a través de los medios del campus virtual de la UOC a lo largo de todo el semestre, y al inicio y al final de cada semestre, se llevan a cabo reuniones de cada PRA con el equipo de docentes colaboradores que coordina, 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.

En la propuesta de la UOC, el número de profesores responsables de asignatura necesarios está más relacionado con el número de asignaturas y ámbitos distintos de conocimiento del programa, que con el número de estudiantes matriculados. Es el número de profesores colaboradores el que está directamente relacionado con el número de estudiantes matriculados, de acuerdo con las ratios explicadas en el apartado 7 (70 estudiantes por aula en el caso de asignaturas estándar).

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. La definición del perfil adecuado de profesorado colaborador se concreta en términos de requisitos: titulación académica, años de experiencia académica y/o profesional adecuados al ámbito de especialización de la asignatura, y otros méritos que permitan confirmar la adecuación durante el proceso de selección.

Profesores colaboradores

La Universidad cuenta con las figuras de profesores colaboradores y tutores para el desarrollo de la actividad docente en el aula virtual. La relación con estos colaboradores se formaliza mediante un contrato civil de prestación de servicio o bien en el marco de convenios que la Universidad tiene firmados con otras universidades

Como ya se ha mencionado, en función del número de estudiantes matriculados cada semestre, los profesores cuentan con la colaboración de los tutores y de los profesores colaboradores, que prestan la atención individualizada a los estudiantes y despliegan el proceso de evaluación.

El profesor colaborador tiene que actuar como agente facilitador del aprendizaje, por lo que debe ejercer de mediador entre los estudiantes y los diferentes recursos de aprendizaje 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 los estudiantes 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 profesores colaboradores 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.

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.

Se estima que la dedicación del profesorado colaborador es un tercio del profesorado con carácter permanente.

Como hemos apuntado, la necesidad de tutores y profesores colaboradores 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 profesores colaboradores y tutores dando publicidad tanto en medios públicos como en el propio sitio Web de la Universidad.

Se estima que este nuevo programa contará inicialmente con un mínimo de 48 profesores colaboradores y 7 tutores para el desarrollo de la actividad docente.

El detalle de los profesores colaboradores y tutores que participaran en esta propuesta de programa se muestra a continuación:

Nombre colaborador	Centro / Univ / Organización	Rol Profesional	Titulación superior	Tipo colaborador
Estevan de Quesada,Rafael	Ackcent Cybersecurity SL	Responsable	Ingeniero Superior	Profesor colaborador
Hernández Jiménez,Enric	Agencia Notarial de Certificación (ANCERT)	Director/a de Área	Doctorado/da	Profesor colaborador
del Canto Rodrigo,Pau	Agencia Notarial de Certificación S.L.U. (ANCERT)	Responsable	DEA/Suficiencia Investigadora	Profesor colaborador
Muñoz Baracco,Joan Francesc	Ayuntamiento de Mollet del Vallès	Responsable	Licenciado/da	Profesor colaborador
Hernández García,David	Applus Laboratories	Responsable	Doctorado/da	Profesor colaborador
Castillo Pérez,Sergio	Banca Privada	Director/a de Área	Doctorado/da	Profesor colaborador
Guijarro Olivares,Jordi	Consorci Serveis Universitaris de Catalunya (CSUC)	Responsable	Ingeniero	Profesor colaborador
Hernández Gañán,Carlos	Delft University of Technology	Profesor Titulado	Doctorado/da	Profesor colaborador
Sebastián Pérez,Juan Carlos	Departamento de Educación	Profesor	Ingeniero	Profesor colaborador
Sánchez González,Laura	Diputación de Tarragona	Técnico/a	Doctorado/da	Profesor colaborador

Chinea López,Jorge	ECLAP | Escuela de Administración Pública de Castilla y León / INCIBE	Profesor	Doctorado/da	Profesor colaborador
Gorga López,Mario	Enghouse Interactive	Responsable	Ingeniero Superior	Profesor colaborador
Carpintero Rodríguez,Miguel Angel	Generalitat de Catalunya	Profesor	Licenciado/da	Profesor colaborador
Tejero Fernández,Xavier	Ibermática	Responsable	Ingeniero	Profesor colaborador
Rodriguez Moreno,Jose Manuel	Ibermática	Técnico/a	Máster	Profesor colaborador
Caballero González,Carlos	IES POLITÉCNICO JESÚS MARÍN / Junta de Andalucía-Consejería de Educación	Profesor titular	Doctorado/da	Profesor colaborador
Vaño Chic,Josep	Institut Badia del Vallés	Profesor	Ingeniero	Profesor colaborador
Gualda Muñoz,Javier	MCR Solutons Business Software	Responsable	Ingeniero	Profesor colaborador
Doce Reyes,Carlos	MCSec	Director/a General	Ingeniero	Profesor colaborador
Noguera Otero,Francisco Javier	New Relic	Responsable	Ingeniero	Profesor colaborador
García Peña,Gerardo	PriceWaterhouseCoopers	Responsable	Ingeniero	Profesor colaborador
Fernandez Jara,Juan Carlos	Safelayer Secure Communications S.A	Director General	Ingeniero Superior	Profesor colaborador
Puiggalí Allepuz,Jordi	Scytl Secure Electronic Voting	Director/a de Área	Ingeniero	Profesor colaborador
Tortajada Gallego,Arsenio	T-Systems	Técnico/a	Ingeniero	Profesor colaborador
Chulia Cebolla,Ana Maria	Titular Despatx d'Advocats	Responsable	Licenciado/da	Profesor colaborador
Navarro Arribas,Guillermo	UNIVERSITAT AUTONOMA DE BARCELONA	Profesor	Doctorado/da	Profesor colaborador
Herrera Joancomartí,Jordi	Universitat Autònoma de Barcelona	Profesor agregado	Doctorado/da	Profesor colaborador
Martí Escalé,Ramon	Universitat Autònoma de Barcelona	Profesor titular	Doctorado/da	Profesor colaborador
Margalef Burrull,Tomàs Manuel	Universitat Autònoma de Barcelona	Catedrático	Doctorado/da	Profesor colaborador
Isern Deyà,Andreu Pere	Universitat de les Illes Balears /Gedocu IT Consulting SL	Profesor asociado	Doctorado/da	Profesor colaborador
Sebé Feixas,Francesc	Universitat de Lleida	Profesor titular	Doctorado/da	Profesor colaborador

Cores Prado,Fernando	Universitat de Lleida	Profesor agregado	Doctorado/da	Profesor colaborador
Morancho Llena,Enric	Universitat Politècnica de Catalunya	Profesor titular	Doctorado/da	Profesor colaborador
Mateos Bartolomé,Alberto José	Universitat Politècnica de Catalunya	Técnico/a	Ingeniero	Profesor colaborador
Tarrés Puertas,Marta Isabel	Universitat Politècnica de Catalunya	Profesor	Doctorado/da	Profesor colaborador
Esteban Grifoll,Juan Ramon	Universitat Politècnica de Catalunya	Técnico/a	Diplomado/da	Profesor colaborador
Farràs Ventura,Oriol	Universitat Politècnica de Catalunya	Profesor	Doctorado/da	Profesor colaborador
Peig Olivé,Enric	Universitat Pompeu Fabra	Profesor	Doctorado/da	Profesor colaborador
Castellà Roca,Jordi	Universitat Rovira i Virgili	Profesor titular	Doctorado/da	Profesor colaborador
Serratosa Casanelles,Francesc	Universitat Rovira i Virgili	Profesor	Doctorado/da	Profesor colaborador
Viejo Galicia,Luis Alexandre	Universitat Rovira i Virgili	Profesor Lector	Doctorado/da	Profesor colaborador
Duch Gavaldà,Jordi	Universitat Rovira i Virgili	Profesor	Doctorado/da	Profesor colaborador
Sanchez Artigas,Marc	Universitat Rovira i Virgili	Profesor Lector	Doctorado/da	Profesor colaborador
García López,Pedro Antonio	Universitat Rovira i Virgili	Profesor titular	Doctorado/da	Profesor colaborador
Cortès Martínez,Antoni	Universitat Rovira i Virgili	Responsable	Licenciado/da	Profesor colaborador
Arribi Vilela,Jesús	Xunta de Galicia	Funcionario	Doctorado/da	Profesor colaborador
Colobran Huguet,Miguel Angel	Universitat Autònoma de Barcelona	Responsable	Doctorado/da	Profesor colaborador
Rifà Coma,Josep	Universitat Autònoma de Barcelona	Catedrático	Doctorado/da	Profesor colaborador
Murgui Garcia,Juan Jose	Centre Integrat Públic de Formació Professional Mislata	Funcionario	Licenciado/da	Tutor
Cabré Vicens,Joan Josep	Departament Ensenyament Generalittat Catalunya	Funcionario	Licenciado/da	Tutor
Fouz Rodríguez,Carlos Alberto	Generalitat de Catalunya	Funcionario	Máster	Tutor
Fernandez Jara,Juan Carlos	BlueWatcher	Por cuenta propia	Ingeniero Superior	Tutor
Escudero Quesada,Ana Maria	Por cuenta propia	Por cuenta propia	DEA/Suficiencia Investigadora	Tutor
Talaminos Barroso,Alejandro	Grupo de Ingeniería Biomédica (GIB) de la	Por cuenta propia	Ingeniero	Tutor

	Universidad de Sevilla			
Rivera Guevara,Richard Paul	IMDEA Software Institute	Por cuenta propia	Doctorado/da	Tutor

En relación al perfil de estos docentes, cabe destacar que un 56,2% de los profesores colaboradores colaborador son doctores y que el 47% se dedica profesionalmente a la docencia y la investigación en otras instituciones, mientras que el 53% restante proviene del mundo profesional y de la empresa.

La ratio de doctores en este programa, teniendo en cuenta los profesores en plantilla y los profesores colaboradores, se sitúa en un 71%.En el cálculo de profesorado doctor, se ha tenido en cuenta el profesorado colaborador que ha intervenido hasta ahora en el máster a extinguir.

Movilidad de profesorado

En relación con la movilidad, la UOC solicitó en febrero de 2007 la Carta universitaria Erasmus, que la Dirección General de Educación y Cultura de la Comisión Europea le concedió en julio de 2007.

A principios del 2009 la UOC entró a formar parte del programa de movilidad docente, al año siguiente se añadió para el personal de gestión y en el curso 2011/12 se abrió la primera convocatoria para estudiantes.

La Carta Erasmus abre la puerta a la universidad para participar como coordinadora o socia 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 vicerrectorado responsable de investigación, 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.

Previsión de profesorado

Las estimaciones sobre las necesidades de profesorado para la puesta en marcha del Máster universitario en Ciberseguridad y Privacidad permiten prever que no será necesario el incremento de profesorado para poder garantizar la docencia del conjunto de asignaturas del máster.

El sistema de selección, formación y evaluación del profesorado que interviene en las titulaciones sigue un proceso claramente definido en el Sistema de Garantía Interno de la Calidad de la Universidad y que queda recogido en el manual correspondiente. El Vicerrector competente planifica el proceso de selección de profesorado a partir de los objetivos estratégicos y las necesidades de despliegue de los programas. Dicha 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 en función de los perfiles necesarios y los candidatos presentados. El proceso de formación a través de la identificación de necesidades formativas recae en los Estudios y en el Área de Personas, si bien el profesorado dispone de un amplio abanico de recursos y herramientas para el desarrollo y mejora de la actividad docente e investigadora. La evaluación, promoción y reconocimiento recae en la Comisión de Desarrollo Profesional del Profesorado que es nombrada por el Consejo de Gobierno y tiene la responsabilidad de aplicar el procedimiento de evaluación del profesorado con carácter permanente.

6.2. Otros recursos humanos disponibles

Forma parte del equipo de los estudios, además del personal académico, el personal de gestión. En concreto, existen los siguientes perfiles:

- Mánager de programa
- Técnico de gestión académica
- Técnico de soporte a la dirección de estudios

La categoría de estos perfiles profesionales es de técnico, como mínimo **de nivel N3**, según el convenio laboral de la UOC, que recoge las siguientes categorías para el personal de gestión técnica y administrativa:

1) Técnico/a experto/a
2) Técnico/a de nivel 1
3) Técnico/a de nivel 2
4) Técnico/a de nivel 3
5) Técnico/a de nivel 4
6) Administrativo/va

El perfil principalmente implicado en el diseño y el apoyo a la garantía de la calidad de los programas es el Mánager del programa, como figura de apoyo a la programación académica de la Universidad que desde su responsabilidad de gestión, contribuye al alcance de los objetivos académicos en los procesos de aseguramiento de la calidad de los programas, en 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 Mánagers de programa de acuerdo con la Dirección de Operaciones.

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 Universidad, en torno a la dirección de operaciones a través de los mánagers de programa, 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 de aprendizaje, seguimiento de incidencias y gestión de trámites de estudiantes.

El Máster universitario en Ciberseguridad y Privacidad cuenta con el apoyo directo de un total de 3 personas del equipo de gestión: una mánager de programa, un técnico de gestión académica y una técnica de apoyo a la dirección de los estudios.

Personal de gestión directamente asociado a la titulación			
Posición	**Número personas**	**Categoría según convenio laboral UOC**	**Nivel de titulación/ Experiencia en gestión universitaria**
Mánager de Programa	1	Técnico nivel 1	Licenciatura en Economía / 17 años de experiencia en gestión universitaria.
Técnico de gestión académica	1	Técnico nivel 3	4 años de experiencia en gestión universitaria. Técnico superior, rama administrativa y comercial.
Técnica de apoyo a la dirección de los estudios	1	Técnico nivel 3	Curso de Orientación Universitaria (COU) 3 años de experiencia en gestión universitaria.

Aparte de la adscripción concreta de personas a los Grados, la UOC tiene a disposición de la estructura docente una estructura de gestión que permite dar respuesta a la gestión y organización administrativa de los diferentes programas. Este planteamiento hace que no haya una adscripción a un programa concreto, sino que se dé respuesta a las diferentes necesidades de forma centralizada en diferentes equipos. Por lo tanto, la gestión se realiza tanto en relación directa con los programas desde diferentes equipos de gestión –como los de Servicios Académicos, Área de Biblioteca y recursos de aprendizaje, Área de Planificación y calidad, 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 identificados para dar respuesta a las necesidades del Grado son:

El **Área de Servicios Académicos** es el área responsable de posibilitar la gestión docente de la Universidad. Apoya los procesos de gestión vinculados a la docencia y facilita soluciones técnicas para la correcta implementación. Gestiona, además, el entorno virtual y los encargos

realizados a los profesores colaboradores, y facilita el acceso a los recursos en el aula para que la docencia y su evaluación sean posibles.

Gestiona los calendarios y las hojas personales de exámenes y pruebas finales de evaluación 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.

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 Grado y prácticas, y los traslados de expediente solicitados por el estudiante. Asimismo se ocupa de gestionar la tramitación de la evaluación de estudios previos, desde las solicitudes hasta la resolución y sus posibles alegaciones.

Además 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 recursos de aprendizaje. 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. También lo es del desarrollo de los convenios interuniversitarios, de movilidad y de prácticas.

Área de Biblioteca y recursos de aprendizaje

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 funcionamiento de la Biblioteca se ha concebido para que pueda obtenerse lo que se necesita de forma inmediata y desde cualquier lugar con acceso a la red de Internet. 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 (información institucional y una visita virtual a la biblioteca), lo siguiente:

- El catálogo. Da acceso al fondo bibliográfico de la Universidad, tanto a la bibliografía recomendada como al fondo especializado en sociedad de la información, y a otros catálogos universitarios nacionales e internacionales.
- La colección digital. Permite acceder a toda la información en formato electrónico, bases de datos, revistas, enciclopedias y diccionarios en línea, libros electrónicos, portales temáticos, etc., organizados tanto por tipo de recurso como por las áreas temáticas que se imparten en la Universidad.
- Los servicios. Proporcionan acceso directo al préstamo, encargo de búsqueda documental y otros servicios de información a medida, como el servicio de noticias, la distribución electrónica de sumarios y el servicio de obtención de documentos.

El **Área de Planificación y Calidad** está implicada en los procesos de programación académica, de verificación, seguimiento, modificación y evaluación (acreditación) de los programas.

También recae en esta unidad el diseño y evaluación de los sistemas internos de garantía de la calidad. Es responsable de los datos oficiales e indicadores docentes de la universidad, y del servicio de encuestas a todos los grupos de interés.

Mecanismos de que se dispone para asegurar la igualdad entre hombres y mujeres y la no-discriminación de personas con discapacidad

La Unidad de Igualdad de la UOC tiene el encargo del Rectorado de impulsar medidas con el objetivo de que toda la comunidad universitaria aprenda a reconocer las diferencias de género, a valorarlas y a trabajar para transformar las prácticas organizativas, docentes y de investigación que impiden que esta diversidad se manifieste.

La UOC dispone desde 2007 de un plan de igualdad. El Plan se ha ido revisando y el Consejo de Gobierno aprobó el pasado 20 de julio de 2015 el nuevo Plan para el período 2015-2019. El nuevo plan parte de un diagnóstico que refleja la situación actual en la universidad y establece

el conjunto de acciones que deben llevarse a cabo para la consecución de los objetivos marcados.

Ver el Plan de Igualdad de la UOC:
http://www.uoc.edu/portal/_resources/ES/documents/la_universitat/igualtat/plan_igualdad_2015-2019_es.pdf

La investigación en Igualdad

El programa de investigación Género y TIC analiza el rol del género en la sociedad de la información y comunicación desde una perspectiva internacional.
Las principales líneas de investigación son:

- El análisis comparativo de las políticas de igualdad de género en Ciencia y Tecnología en Europa.
- El análisis comparativo de trayectorias de vida de las mujeres en las TIC.
- La movilidad internacional del personal altamente cualificado en el ámbito de la Ciencia y la Tecnología en perspectiva de género.
- La situación de la mujer en los estudios universitarios TIC.
- La situación de la mujer en la investigación y empleo TIC.
- El género y la elección de estudios TIC en secundaria.
- El género y su relación con las TIC y la creatividad.

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 premio fem.Talent. Promoción de la Igualdad 2015. Participa en diversos foros donde se comparten prácticas sobre igualdad y conciliación.

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

La UOC tiene como base un modelo de enseñanza a distancia centrado en el estudiante. Este modelo 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 dos espacios de comunicación básicos: el tablón del profesor y el foro. 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.

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 a través de los buzones personales de cada estudiante, los buzones grupales y la dinamización de profesores colaboradores en el aula. La ratio de estudiantes por aula virtual en las asignaturas estándar es de un máximo de 70 estudiantes.

- En las asignaturas con especial dedicación priman los elementos de individualización sobre los grupales, de manera que cada estudiante, o grupo reducido de estudiantes, sigue un itinerario de aprendizaje diferenciado. La ratio de estudiantes en las asignaturas con especial dedicación es de un máximo de 50 estudiantes por aula virtual.

- En las asignaturas de Trabajo de fin de Máster (TFM) es preciso realizar un seguimiento individualizado y personalizado. La ratio de estudiantes por aula en estas asignaturas es de entre 10 y 15 estudiantes como máximo. Aun así, en la mayoría de los casos la ratio de estudiantes suele ser inferior a 10 estudiantes.

Biblioteca y Recursos de aprendizaje

Desde su inicio, la UOC proporciona a sus estudiantes los recursos de aprendizaje vinculados a cada una de sus asignaturas para la realización de su actividad docente.

El origen de estos recursos de aprendizaje es múltiple. Pueden ser recursos de aprendizaje que la propia UOC encarga y elabora o pueden ser recursos existentes en la red o ya publicados por terceros.

El encargo y elaboración de los recursos de aprendizaje propios es una característica del modelo de aprendizaje de la UOC. En estos momentos, la UOC tiene un volumen considerable de recursos de aprendizaje elaborados por expertos y editados por profesionales que se encargan de hacer tratamiento didáctico, corrección y/o traducción, edición y maquetación.

La edición del contenido docente UOC se hace en XML de forma que el contenido tiene múltiples versiones: web, pdf, audio o dispositivo electrónico.

Cada año la UOC hace una inversión en nuevos contenidos y en la renovación de aquellos que han quedado obsoletos.

Por otro lado, los usuarios de la UOC cuentan con una Biblioteca Virtual, tal como se explica en el apartado 6 de esta memoria, que tiene como principal objetivo proporcionar a estudiantes, docentes e investigadores acceso a la documentación e información necesaria para el desarrollo de su actividad.

La Biblioteca Virtual de la UOC es accesible a través del portal web para toda la comunidad universitaria e incluso para usuarios externos en el caso de algunos servicios y colecciones. Asimismo, se accede a ella directamente desde las aulas del Campus Virtual por medio del espacio “Recursos” que reúne y proporciona una selección rigurosa de recursos, preparada conjuntamente entre el profesorado y el equipo de la Biblioteca. Este espacio de recursos está presente en todas las asignaturas, facilita a los estudiantes el seguimiento de las actividades propuestas y les permite tener a su alcance fuentes de información y recursos actualizados para cada ámbito. Los recursos que se incluyen en el aula son de tipología diversa: contenidos creados *adhoc* (anteriormente descritos) 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 contenidos docentes de las aulas son revisados cada semestre por el profesor responsable con el apoyo técnico del equipo de Biblioteca, quienes se responsabilizan de gestionar el proceso de generación de contenidos docentes, ya sea mediante la contratación y creación de obras UOC, como mediante la gestión de derechos de autor de material ya publicado. Este material se complementa con la bibliografía recomendada y otras fuentes de información que se actualiza semestre a semestre.

La red territorial

La UOC cuenta con una red territorial formada por sedes y puntos de información.

Esta red representa el vínculo y el compromiso entre la Universidad y el territorio. Su misión es difundir el conocimiento que genera la Universidad, dar apoyo y dinamizar la comunidad universitaria, contribuyendo a la transformación de la sociedad.

Los objetivos de esta red son:

- Potenciar la visibilidad y la notoriedad de la universidad.
- Promover y potenciar las relaciones con el entorno local, actuando como dinamizador del territorio.
- Acercar y adecuar los servicios y recursos que faciliten la formación virtual.
- Canalizar y atender las necesidades de la comunidad universitaria.

La información actualizada sobre las sedes y puntos de información en activo se encuentra en el siguiente enlace: http://www.uoc.edu/portal/es/universitat/contacte-seus/on-som/seus.html

Los servicios que ofrecen las sedes son:

- Asesoramiento personalizado de la oferta formativa de la Universidad.
- Apoyo a la gestión académica, posibilidad de entrega y recogida de documentación, entrega de títulos y resolución de dudas académicas.
- Servicio de retorno y préstamo bibliográfico.
- Centro de recursos, con la puesta a disposición de conexión a internet, equipamiento audiovisual, salas de estudio y salas de reuniones.

- Participar en los órganos de representación de los estudiantes en el territorio a través de las comisiones de sede.
- Participar en las actividades que se organizan regularmente, como talleres y ciclos de conferencias http://symposium.uoc.edu/
- Asistir a les Jornadas de acogida, actividades dirigidas a estudiantes de nuevo acceso para facilitar la incorporación a la Universidad. En estas jornadas se ayuda al estudiante a identificar los aspectos más relevantes de su nueva etapa formativa.

Los servicios que ofrecen los puntos de información 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.

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 una, escogidos por votación entre los propios estudiantes. Las funciones de las comisiones de sede (que preside el director de la sede correspondiente) son proponer mejoras de los servicios que se ofrecen y proponer actividades a realizar.
- Buzón de sugerencias en cada sede.
- Encuesta a los estudiantes usuarios de las sedes.
- Detección de las necesidades de los estudiantes directamente a través de los comentarios que envían al personal de atención de las sedes.

Inversiones

Por la propia naturaleza de la Universidad, no existen inversiones específicas para los programas.

Las inversiones en equipamientos de la Universidad son de carácter general y se distribuyen en inversiones en las oficinas de gestión, en las inversiones en las sedes y puntos de información de la red territorial 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.

Tecnología

El Campus Virtual es el espacio donde se desarrolla toda la actividad docente y un espacio de comunicación y relación entre los usuarios. Permite a docentes y estudiantes enseñar y aprender mediante el uso de más de 20 herramientas distintas como wikis, blogs, foros, videoconferencia, vídeos, recursos de aprendizaje, buscadores, etc. Es un entorno abierto que permite añadir nuevas herramientas y también un sistema de gestión que permite gestionar la creación de las aulas, la asignación de usuarios y la copia de información semestre a semestre de forma automática. El Campus Virtual ha garantizado el acceso de los usuarios a pesar del incremento anual constante.

La UOC realiza encuestas de uso y satisfacción, y análisis periódicos de las necesidades de los usuarios. Las mejoras y desarrollos se fundamentan en una metodología de diseño centrado en el usuario asegurando así la usabilidad y adecuación a las necesidades. Dispone de un comité de accesibilidad que centraliza y gestiona las peticiones de accesibilidad de los alumnos con discapacidad.

Antes de que un servicio esté disponible por el usuario, se sigue un proceso de control con el objetivo de garantizar que su funcionamiento sea el adecuado. Para ello se dispone de un entorno de prueba y un entorno de pre-producción, que permiten realizar test funcionales, de integridad y de carga sin condicionar el entorno de producción.

El Campus Virtual se fundamenta en estándares tecnológicos internacionales y en una arquitectura orientada a servicios. La consultora Gartner ha publicado en el año 2011 un estudio de caso para instituciones de educación virtual basado en el modelo tecnológico del Campus Virtual de la UOC, destacándolo como ejemplo y modelo a seguir [Gartner, 28 March 2011, Case Study: Approaching the Learning Stack. The Third-Generation LMS at Universitat Oberta de Catalunya].

La UOC dispone de dos salas de máquinas propias. Una principal que alberga los entornos de producción, y otra más pequeña que es donde residen los entornos de contingencia y preproducción. Ambas salas se encuentran protegidas por distintos sensores, que pueden enviar alarmas a través de la red. Existen sistemas de monitorización y vigilancia 24x7 que permiten aplicar procedimientos para la recuperación de un servicio en el mínimo tiempo posible. La infraestructura se basa en sistemas redundados de alta disponibilidad donde los posibles puntos de fallo se duplican y de manera automática entra en funcionamiento un elemento de reserva de

modo que el servicio no se ve afectado. Los niveles de servicio se sitúan por encima del 99%, estándar de calidad de servicio en Internet.

Los sistemas de almacenamiento están duplicados y se realizan copias de seguridad de todos los datos. Existe una política de acceso a los datos y protocolos de seguridad. La institución tiene un responsable de seguridad de los datos. Se contratan periódicamente auditorias de seguridad y existe guías de desarrollo seguro que se aplica en los desarrollos.

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.

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 recursos de 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.

El 16 de diciembre de 2015 se firmó un nuevo Convenio Programa entre el Departamento de Economía y Conocimiento y la fundación Universitat Oberta de Catalunya para la financiación de la UOC para el período 2015-2018.

Las necesidades de recursos de aprendizaje 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 de cada titulación tiene en cuenta la estructura de gasto variable directamente asociado en cada curso y que se corresponde con los siguientes conceptos:

- tutoría y acción docente del profesorado colaborador, cuya necesidad viene determinada por el número real de matriculados,
- acceso a los recursos de aprendizaje (gastos no asociados a la inversión), y
- 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 la titulación se ha estimado de acuerdo con la información proporcionada por parte del Área de marketing de la Universidad y sus valores permiten determinar el ingreso estimado derivado de los derechos de matrícula.

Además se han estimado las inversiones para la elaboración de los nuevos recursos docentes para las asignaturas que deberán desplegarse.

	EVOLUCIÓN PREVISTA CUENTA DE EXPLOTACIÓN			
MU en Ciberseguridad y Privacidad	Curso 2020-2021	Curso 2021-2022	Curso 2022-2023	Curo 2023-2024
INGRESOS	**662.980,21**	**1.161.955,28**	**1.530.623,97**	**1.796.834,56**
Matrículas	484.633,78	880.748,06	1.179.386,52	1.397.242,83
Financiamiento público *	142.714,58	216.451,74	264.525,09	296.861,87
Otros ingresos *	35.631,86	64.755,48	86.712,35	102.729,86
GASTOS	**552.289,90**	**999.688,58**	**1.328.181,59**	**1.577.501,32**
Gastos de Personal	87.675,12	87.675,12	87.675,12	87.675,12
Gastos de Funcionamiento	176.453,79	320.677,89	429.411,31	508.732,18
Gastos de estructura y servicios *	253.960,98	557.135,57	776.895,16	946.894,02
Amortizaciones	34.200,00	34.200,00	34.200,00	34.200,00
RESULTADO	**110.690,32**	**162.266,70**	**202.442,37**	**219.333,24**

8. RESULTADOS PREVISTOS

8.1. Valores cuantitativos estimados para los indicadores y su justificación

Para la estimación de los valores de tasas y resultados académicos y de satisfacción, la Universidad se ha basado en la experiencia previa de los Másteres universitarios desplegados hasta el momento.

Tasa de graduación

Debido a las características específicas de los estudiantes de la UOC (número de créditos matriculados por curso significativamente inferior al número de créditos teóricos por curso) la tasa de graduación además de en T+1, también la calculamos en T+2, T+3,… ya que aporta más información sobre la evolución de la graduación de las diferentes cohortes.

	Cohorte 2010-11	Cohorte 2011-12	Cohorte 2012-13	Cohorte 2013-14	Cohorte 2014-15	Cohorte 2015-16	Cohorte 2016-17
Tasa graduación en T+1	**25,4%**	**32,4%**	**25,4%**	**28,0%**	**31,9%**	**35,5%**	**41,3%**
Tasa graduación en T+2	56,7%	44,9%	42,4%	48,4%	50,1%	54,5%	57,1%
Tasa graduación en T+3	59,8%	52,3%	50,5%	56,2%	58,0%	61,6%	-
Tasa graduación en T+4	61,4%	57,6%	54,6%	61,8%	63,6%	-	-

La previsión para la tasa de graduación en T+1 es que siga siendo superior al **25%.**

Tasa de abandono

Para la estimación de esta tasa, de nuevo se han considerado los resultados obtenidos por los Másteres universitarios de la UOC. Teniendo en cuenta que una cohorte no puede tener abandono hasta el 3r curso, la tasa de abandono se calcula en T+2. Los valores obtenidos son

los siguientes:

	Cohorte 2010-11	Cohorte 2011-12	Cohorte 2012-13	Cohorte 2013-14	Cohorte 2014-15	Cohorte 2015-16
Abandono en T+2	19,1%	21,9%	21,4%	20,6%	20,9%	17,0%

Se propone que la tasa de abandono en T+2 sea inferior al 25%

Tasa de eficiencia
Para la estimación de esta tasa se han tenido de nuevo en cuenta los resultados obtenidos por los Másteres universitarios de la UOC; superiores siempre al 90%.

Si tenemos en cuenta que esta tasa está muy relacionada con las tasas de éxito y rendimiento, y estas también se han mantenido estables en los últimos cuatro años, la previsión es que la tasa de eficiencia siga siendo para los programas de Máster **superior al 90%.**

Además de las tasas exigidas, la Universidad considera necesario establecer objetivos de rendimiento académico para cada curso; los indicadores para la valoración del Máster de consecución de estos objetivos son los siguientes.

Tasa de éxito
La tasa de éxito corresponde al número de créditos superados / número de créditos presentados. En esta tasa, en los actuales Másteres oficiales, los resultados obtenidos son los siguientes:

	2008-09	2009-10	2010-11	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17	2017-18
Tasa éxito (%)	93,6	94,9	94,8	92,9	95,5	96,5	96,5	96,6	96,6	95,9

La tasa de éxito se ha mantenido estable en los últimos cuatro años y la previsión para todos los programas de Máster es que siga siendo superior al 90%.

Tasa de rendimiento
Esta tasa corresponde al número de créditos superados / número de créditos matriculados; en los Másteres universitarios de la UOC tiene los siguientes valores:

	2008-09	2009-10	2010-11	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17	2017-18
Tasa rendimiento (%)	78,6	80,5	81,7	81,4	84,9	85,4	86,5	87,5	88,2	87,3

La tasa de rendimiento se ha mantenido estable, aunque con un ligero descenso en los últimos años. La previsión es que la tasa se mantenga para todos los Másteres de la UOC por encima del 70%.
Además, debe considerarse la medida de la satisfacción del estudiante, que se obtendrá, tal como se explicita en el apartado relativo a los sistemas internos de garantía de la calidad, por medio de las encuestas de satisfacción que se realizan cada curso.

Tasa de satisfacción
Esta tasa, que corresponde a la media de las respuestas a la pregunta de satisfacción general del curso en una escala de 1 a 5 (siendo 5 una valoración muy positiva y 1 muy negativa), en las titulaciones de la UOC, de acuerdo con los datos obtenidos, tiene los siguientes valores:

2008-09	2009-10	2010-11	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17
4	4,1	4,1	4,1	4,0	4,0	4,0	3,9	3,9

La tasa de satisfacción se ha mantenido estable alrededor del 4, se valorarán como resultados satisfactorios medias de satisfacción superiores a 4 entre valores de 1 a 5.

Todos los datos estimados se revisarán por medio de los resultados semestrales obtenidos a partir del despliegue de la titulación y se revisarán de acuerdo con ellos. Esta revisión permitirá ir ajustando tanto los resultados reales como la estimación de los objetivos que hay que alcanzar como resultados satisfactorios para este Máster.

8.2. Progreso y resultados de aprendizaje

Durante el desarrollo del semestre, por medio del REC (registro de evaluación continua) y otros recursos del aula, el profesorado y el personal de gestión vinculado a la actividad docente pueden consultar los resultados de los estudiantes en las pruebas de evaluación continua y ver el funcionamiento y la evolución de cada asignatura durante el periodo docente. Esta información permite hacer acciones durante el semestre para reforzar y mejorar el rendimiento de los estudiantes y llevar a cabo acciones de mejora para asegurar el progreso y la consecución de

los resultados de aprendizaje.

Cada final de semestre y de curso, se facilitan con el máximo detalle los resultados por medio de los sistemas de información de la Universidad. Los indicadores quedan recogidos en su almacén de datos (Datawarehouse), que es la fuente básica de información de los resultados de valoración de la docencia para el profesorado. La información se recoge para todos los niveles (programa, asignatura y aula) y, por tanto, va dirigida a diferentes perfiles (director de estudios, director académico de programa y profesor responsable de asignatura), este nivel de detalle permite identificar el nivel de consecución tanto a nivel de asignatura como de titulación.

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

- Gestión académica.
- Proceso PS11 de recogida de la percepción de los grupos de interés, del Sistema de garantía interna de la calidad.

Los resultados de estos procesos se cargan semestralmente y anualmente en el almacén de datos (Datawarehouse denominado DAU) de la Universidad. La validación de estos procesos y la idoneidad de los indicadores es una función coordinada por el Área de Planificación y Calidad, que periódicamente se reúne con los responsables académicos de los estudios para asegurar el uso y la garantía de los indicadores.

Los responsables del seguimiento y la valoración de los resultados de cada asignatura son el profesor responsable de la 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 son accesibles con las herramientas del profesor en formato digital.

El director académico del programa, en el marco de la Comisión de Titulación, y de acuerdo con el proceso PO07_Desplegar, revisar y mejorar del Sistema de garantía interna de la calidad, valorará los resultados globales de la titulación. Esta valoración incluye la comparación con la información de previsión de resultados, la comparación entre otros másteres de la universidad de la misma rama de conocimiento y el análisis detallado de cada una de las asignaturas aportado por cada profesor responsable de asignatura. Las valoraciones hechas por la Comisión y las posibles acciones de mejora que hay que desarrollar deberán ser recogidas por el director académico del programa y validadas por su director de estudios.

Los principales resultados que se valoran en la Comisión de Titulación semestralmente corresponden a las siguientes variables:

- Rendimiento: se valoran los ítems de seguimiento de la evaluación continua, tasa de rendimiento y tasa de éxito, con seguimiento especial para las asignaturas de trabajo final y prácticas.
- Continuidad: se valora el abandono principalmente a partir de la rematrícula o las anulaciones voluntarias de primer semestre.
- Satisfacción de los estudiantes: se valoran los ítems correspondientes a la acción de los profesores colaboradores, la planificación, los recursos de aprendizaje y el sistema de evaluación.

Al final de cada curso, además de los resultados expresados, se recogen los correspondientes al balance académico de curso, que presenta el vicerrector responsable de calidad a la Comisión Académica y a la Comisión de Programas. Estos resultados y indicadores se han definido de acuerdo con el proceso PE05_Definir los indicadores del SGIC:

- Rendimiento: se valoran los mismos ítems.
- Continuidad: se valoran los mismos ítems y, además, la tasa de abandono.
- Satisfacción de los estudiantes: se valoran los mismos ítems y, además, la satisfacción con la UOC, el programa, su aplicabilidad y los servicios.
- Satisfacción del profesorado participante en el título en relación a: nivel previo de los estudiantes matriculados en la asignatura, metodología y recursos utilizados, mecanismos de coordinación, apoyo de la institución para el seguimiento y mejora de las titulaciones;
- Graduación: tasa de graduación y de eficiencia;
- Inserción o mejora profesional: a partir de los estudios propios elaborados por la Universidad cada dos 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 está disponible para todos los tipos de asignatura, para los trabajos de final de Grado y también para las prácticas. En estos casos es pertinente valorar las memorias y los trabajos realizados para evaluar la adquisición del conjunto de competencias previstas.

El análisis de los resultados se lleva a cabo en el marco de los procesos PO07 y PO14, descritos en el Sistema de Garantía Interna de la Calidad.

9. SISTEMA DE GARANTÍA DE CALIDAD DEL TÍTULO

https://www.uoc.edu/portal/_resources/CA/documents/qualitat/politica-qualitat/Manual_SGIQ__v.1__ES.pdf

10. CALENDARIO DE IMPLANTACIÓN

10.1. Cronograma de implantación de la titulación

El cronograma de implantación de la titulación no muestra cuál ha de ser el itinerario de un estudiante para seguir el máster, sino que señala el semestre en que por vez primera se ofrecerán las distintas asignaturas. A partir de esta primera oferta, las asignaturas se impartirán cada curso.

Curso lectivo 2020-2021	
Semestre 1 Septiembre 2020	Semestre 2 Febrero 2021
• Legislación y protección de datos (6 ECTS)	• Seguridad y pentesting de sistemas (6 ECTS)
• Fundamentos de ciberseguridad (6 ECTS)	• Análisis forense (6 ECTS)
• Privacidad (6 ECTS)	• Arquitecturas y protocolos de seguridad (6 ECTS)
• Seguridad y pentesting de servidores de datos (6 ECTS)	• Gestión de la seguridad en el cloud (6 ECTS)
• Seguridad del software (6 ECTS)	• Auditoría técnica (6 ECTS)
• Sistemas de blockchain (6 ECTS)	• Criptografía avanzada (6 ECTS)
• Sistemas de gestión de la seguridad de la información (6 ECTS)	• Técnicas de ocultación de la información (6 ECTS)
• Dirección estratégica de sistemas y tecnologías de la información (6 ECTS)	• Biometría (6 ECTS)
• Técnicas de investigación (6 ECTS)	

• Modelos avanzados de minería de datos (6 ECTS)	
• Ciberdelitos: estudio de los tipos delictivos (6 ECTS)	
• Trabajo final de máster (12 ECTS)	
78 ECTS	**48 ECTS**

10.2. Procedimiento de adaptación, en su caso, de los estudiantes de los estudios existentes al nuevo plan de estudios *

La implantación de éste plan de estudios supone la extinción del plan Seguridad de las Tecnologías de la Información y de las Comunicaciones con código de Registro: 4312898, la adaptación al nuevo plan de estudios se llevará a cabo según la siguiente tabla de equivalencias.

Tabla de equivalencias para la adaptación	
Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones	Máster Universitario en Ciberseguridad y Privacidad
• Identidad digital (6 ECTS)	• Privacidad (6 ECTS)
• Vulnerabilidades (6 ECTS)	• Fundamentos de ciberseguridad (6 ECTS)
• Legislación y regulación (6 ECTS)	• Legislación y protección de datos (6 ECTS)
• Seguridad en redes (6 ECTS)	• Arquitecturas y protocolos de seguridad (6 ECTS)
• Seguridad en sistemas operativos (6 ECTS)	• Seguridad y pentesting de sistemas (6 ECTS)
• Seguridad en bases de datos (6 ECTS)	• Seguridad y pentesting de servidores de datos (6 ECTS)
• Programación de código seguro (6 ECTS)	• Seguridad del programario (6 ECTS)

• Biometría (6 ECTS)	• Biometría (6 ECTS)
• Sistemas de gestión de la seguridad (6 ECTS)	• Sistemas de gestión de la seguridad (6 ECTS)
• Auditoría técnica (6 ECTS)	• Auditoría técnica (6 ECTS)
• Análisis forense (6 ECTS)	• Análisis forense (6 ECTS)
• Técnicas de investigación (6 ECTS)	• Técnicas de investigación (6 ECTS)
• Criptografía avanzada (6 ECTS)	• Criptografía avanzada (6 ECTS)
• Técnicas de marcado de la información (6 ECTS)	• Técnicas de ocultación de la información (6 ECTS)
• Dirección estratégica de sistemas y tecnologías de la información (6 ECTS)	• Dirección estratégica de sistemas y tecnologías de la información (6 ECTS)

Las asignaturas del Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones que no tengan un equivalente en el Máster Universitario en Ciberseguridad y Privacidad, seguirán ofreciéndose durante el tiempo que marque la normativa de extinción de la UOC.
Son las asignaturas siguientes:

- Seminarios de investigación
- Seminarios en empresa
- Metodologías de investigación
- Trabajo final de máster

10.3. Enseñanzas que se extinguen por la implantación del correspondiente título propuesto

La implantación del máster en Ciberseguridad y Privacidad de la UOC supone la extinción del Seguridad de las Tecnologías de la Información y de las Comunicaciones (título oficial) con código RUCT 4312898 que se venía impartiendo en esta Universidad.

Anexo I - Titulación propia “Diploma de Posgrado en Gestión y Auditoría de la Seguridad”

El Diploma de Posgrado en Gestión y Auditoría de la Seguridad es una titulación propia de **30 créditos ECTS** que se extinguió con la implantación del Máster universitario en Ciberseguridad y Privacidad.

Plan de Estudios

Este posgrado ofrece una formación técnica especializada en el ámbito de la gestión de la seguridad informática, que garantiza la adquisición de las habilidades necesarias para asegurar el cumplimiento de la normativa legal vinculada a la prevención de los riesgos informáticos y a la protección de datos personales y privados, para crear y gestionar unas buenas prácticas y políticas de seguridad empresariales y para comprobar la correcta gestión e implantación de aquellas prácticas llevadas a cabo por las organizaciones en relación a estas cuestiones.

Objetivos

El objetivo principal del posgrado de Gestión y Auditoría de la Seguridad es ofrecer una formación técnica y especializada en el ámbito de la gestión de la seguridad informática. La enseñanza combina la adquisición de una base teórica sólida de conocimientos con una formación práctica basada en el estudio de casos reales. Una vez completado el programa, el estudiante será capaz de evaluar, administrar y controlar los riesgos de seguridad de una compañía. Podrá asumir la responsabilidad de analizar los riesgos de la organización, comunicar dichos riesgos, aplicar las soluciones necesarias para reducir las amenazas de la organización, promover la transparencia y cumplir con las regulaciones.

Competencias

- 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.
- Poseer y comprender conocimientos de las estructuras normalizadoras, evaluadoras, certificadoras, y las normas correspondientes que regulan los ámbitos de la seguridad
- Capacidad para identificar y analizar los procesos críticos de una organización y también el impacto que produciría la irrupción de estos procesos.
- Capacidad para elaborar un plan de seguridad, teniendo en cuenta 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.

- Capacidad para desarrollar un plan de continuidad y conocer sus fases y el personal que debe implicarse para desarrollarlo. Conocer las normas y los estándares de referencia relacionados con la continuidad del negocio.
- Capacidad para implantar un Sistema de Gestión de Seguridad de la Información (SGSI) siguiendo las fases del ciclo Deming
- Capacidad para gestionar la certificación de un SGSI y de comprender, interpretar y explicar las ventajas que aporta la certificación de dichos sistemas.
- Capacidad para elaborar e implantar un plan de auditoría. Uso de las herramientas habituales para hacer una auditoría técnica de seguridad.
- Capacidad para realizar un análisis forense de cualquier sistema informático (ordenador, móviles, encaminadores, etc.) y presentarla en una sede judicial.
- Capacidad para aplicar las consideraciones legales adquiridas para la gestión de un incidente de seguridad.
- Capacidad para realizar, presentar y defender ante un tribunal un ejercicio en el cual se sinteticen las competencias adquiridas en el posgrado.

Perfil profesional

- Consultor de seguridad / experto en normativas: profesional que estudia el mercado informático en relación con nuevos productos, tendencias y servicios del ámbito de la seguridad informática. Hace análisis de riesgos y elabora planes de continuidad y políticas de seguridad de los sistemas de información de la organización, y colabora con el responsable de sistemas en tareas de evaluación, planificación y coordinación de nuevas implantaciones.
  También es el responsable de la documentación de políticas, de procedimientos y de estándares de seguridad y, a su vez, del cumplimiento de los estándares internacionales y de las regulaciones que se apliquen a la organización. Es un experto en materia de protección de datos y gestión de la información.
- Implantador de sistemas de gestión de la seguridad de la información (SGSI): es el responsable de desplegar los SGSI, cumpliendo las normativas vigentes.
- Auditor de seguridad de sistemas de información: es el responsable de verificar el correcto funcionamiento de las medidas de seguridad y también el cumplimiento de las normas y leyes correspondientes. Entre sus responsabilidades están crear controles e indicadores para el mantenimiento del nivel de protección adecuado, revisandolos periódicamente, evaluando la efectividad de los controles, evaluar el cumplimiento de las normas de seguridad, analizar las intrusiones en el sistema informático y desarrollar un análisis forense (segundo nivel de respuesta ante incidentes), y colaborar con los consultores de seguridad para elaborar políticas y planes de contingencia.

Programa académico

El posgrado tiene una duración de un curso académico y se estructura en dos semestres:

- 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.

- 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-.
- 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.

- Proyecto de gestión y auditoría de la seguridad (6 ECTS): Proyecto de final de posgrado

Sistema de evaluación

El sistema de evaluación del Diploma de Posgrado en Gestión y Auditoría de Seguridad es la evaluación continua (EC). La EC consiste en la realización y superación de una serie de pruebas de evaluación continua (PEC) establecidas en el plan docente, de acuerdo con el número y el calendario que se concreta. La EC de cada asignatura se ajusta a los objetivos, competencias, contenidos y carga docente de cada asignatura. El plan docente establece los criterios mínimos y el calendario de entrega para seguir y superar la EC. En todo caso, para considerar que se ha seguido la EC debe haber hecho y entregado como mínimo el 50% de las PEC. El no seguimiento de la EC se califica con una N (equivalente al no presentado).

Anexo II - Titulación propia “Diploma de Posgrado en Seguridad en Redes y Sistemas”

El Diploma de Posgrado en Seguridad en Redes y Sistemas es una titulación propia de **30 créditos ECTS** que se extinguió con la implantación del Máster universitario en Ciberseguridad y Privacidad.

Plan de Estudios

Este posgrado proporciona amplios conocimientos sobre la seguridad en redes informáticas y sistemas corporativos. Se estudian los problemas y las soluciones empleadas para resolver el cibercrimen, se examinan en profundidad los riesgos de ciberseguridad en las redes fijas e inalámbricas, y se analizan los mecanismos de protección particulares de cada sistema operativo

Objetivos

La enseñanza combina la adquisición de una base teórica sólida de conocimientos con una formación práctica y basada en el estudio de casos reales. Tras completar el programa, el estudiante será capaz de diseñar e implementar estrategias que puedan garantizar la seguridad de los recursos informáticos de una empresa, a través de políticas de prevención, protección y prevención de ataques.

Competencias

- Conocer las técnicas de explotación de vulnerabilidades de una red y los puntos débiles de un sistema.
- Capacidad para identificar, evaluar y gestionar los principales riesgos de un dominio informático, tanto tecnológicos como procedentes de la ingeniería social.
- Capacidad para usar técnicas y contramedidas básicas de seguridad para la prevención de ataques derivados de la ingeniería social.
- Conocimiento y utilización de herramientas para la administración y la protección de redes cableadas e inalámbricas, y la gestión de alertas de seguridad.
- Capacidad para concebir, desplegar, organizar y gestionar redes de comunicaciones en contextos residenciales, empresariales o institucionales, responsabilizándose de la seguridad del sistema y de la protección de los datos de los usuarios.
- Conocer las técnicas principales de seguridad en los sistemas operativos.

- Capacidad para configurar y administrar una base de datos físicamente y lógicamente, para asegurar la integridad, la disponibilidad y la confidencialidad de la información almacenada.
- Capacidad para realizar una configuración experta de un servidor GNU/Linux o Windows.
- Capacidad para diseñar soluciones integrales apropiadas en escenarios complejos que combinen las técnicas y contramedidas conocidas para la prevención, la detección y la disuasión de ataques.
- Capacidad para realizar, presentar y defender ante un tribunal un ejercicio en el cual se sinteticen las competencias adquiridas en el posgrado.

Perfil profesional

El objetivo del programa es capacitar a los estudiantes para que adquieran las competencias para ejercer los perfiles profesionales siguientes:

- Director de sistemas informáticos: dirige, supervisa y propone procesos operativos mediante sistemas informáticos. Ejecuta las políticas y los planes informáticos y tecnológicos de la institución.
- Consultor de seguridad de sistemas de la información: en el ámbito de una organización, es el responsable de identificar los riesgos vinculados a la ocupación de los servicios informáticos y de proponer soluciones para dotarlos de un buen nivel de seguridad. Apoya a la aplicación de soluciones y define los procedimientos organizativos que puedan ser plenamente eficaces con relación al sistema de seguridad. Desarrolla procedimientos y métodos de seguridad. Identifica, selecciona, especifica y planifica los mecanismos de seguridad. Divulga las políticas de seguridad, involucrando a todos los miembros de la organización.
- Ingeniero de comunicación de voz y datos: diseña arquitecturas de redes de datos seguros (internet, redes de datos privados, etc.) y diseña redes inalámbricas seguras (Wifi, WiMAX, GSM, UMTS, etc.).
- Administrador de redes y sistemas: lleva a cabo las acciones congruentes con la estrategia definida por el oficial de seguridad. Entre las responsabilidades que asume está la implementación, la configuración y la operativa de los controles de seguridad informática (cortafuegos, IPS/IDS, filtros contra programas maliciosos o antimalware, etc.); la monitorización de indicadores de controles de seguridad; proveer un primer nivel de respuesta ante incidentes (típicamente por medio de acciones en los controles de seguridad que operan); apoyar a usuarios; gestionar el alta, la baja y la modificación de accesos a sistemas y aplicaciones, y gestionar los parches de seguridad informática (pruebas e instalación).
- Administrador de bases de datos: gestiona las bases de datos corporativas.

- Auditores técnicos de seguridad: especialistas en monitorización, análisis del tránsito de redes y detección de intrusiones.

Programa académico

El posgrado tiene una duración de un curso académico y se estructura en dos semestres:

- Vulnerabilidades de seguridad (6 ECTS)
  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.

- 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

- 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.

- Proyecto de Seguridad en Redes y Sistemas (6 ECTS): Proyecto final de Posgrado

Sistema de evaluación

El sistema de evaluación del Diploma de Posgrado en Seguridad en Redes y Sistemas es la evaluación continua (EC). La EC consiste en la realización y superación de una serie de pruebas de evaluación continua (PEC) establecidas en el plan docente, de acuerdo con el número y el calendario que se concreta. La EC de cada asignatura se ajusta a los objetivos, competencias, contenidos y carga docente de cada asignatura. El plan docente establece los criterios mínimos y el calendario de entrega para seguir y superar la EC. En todo caso, para considerar que se ha seguido la EC debe haber hecho y entregado como mínimo el 50% de las PEC. El no seguimiento de la EC se califica con una N (equivalente al no presentado).

Anexo III - Titulación propia "Diploma de Posgrado en Seguridad en Servicios y Aplicaciones"

El Diploma de Posgrado en Seguridad en Servicios y Aplicaciones es una titulación propia de **30 créditos ECTS** que se extinguió con la implantación del Máster universitario en Ciberseguridad y Privacidad.

Plan de Estudios

El posgrado en Seguridad en Servicios y Aplicaciones permite a los estudiantes orientar su carrera profesional en la consultoría de construcción de servicios y aplicaciones seguras. Algunos de los aspectos clave que los estudiantes del posgrado conocen en profundidad desde un punto de vista teórico y práctico al finalizar sus estudios son el control de acceso a las aplicaciones, la integración de servicios seguros a través de la federación de identidades, la programación de código seguro o el uso de sistemas de pago en línea para el comercio electrónico.

Objetivos

El Posgrado proporciona una formación técnica especializada en el ámbito del desarrollo de servicios y aplicaciones de seguridad. El programa combina la adquisición de una base teórica sólida de conocimientos, con una formación práctica y basada en el estudio de casos reales. Al finalizar el programa, el estudiante será capaz de liderar el diseño de programas para medianas y grandes corporaciones con unos requisitos de seguridad específicos.

Competencias

- Conocer las arquitecturas más importantes de AAA (autenticación, autorización, contabilidad), así como los sistemas de federación de identidades y autenticación mútua (SSO - *single sign on*)

- Capacidad para identificar las vulnerabilidades de privacidades de los sistemas (especialmente en aplicaciones web) y capacidad para protegerlos.
- Capacidad para analizar, diseñar y desarrollar aplicaciones y servicios web seguros.
- Tener conocimientos de los sistemas que forman parte de una arquitectura de comercio electrónico y capacidad para poder desplegar una.
- Capacidad para comprender y analizar los sistemas de facturación electrónica, de pago y de micropago.
- Comprender las técnicas de reconocimiento de las personas a través de características físicas: cara, huellas dactilares, orejas, iris, manos, forma de caminar, voz, etc.
- Capacidad para diseñar aplicaciones reales con acceso biométrico. Conocer el software y hardware actual para desarrollar aplicaciones.
- Capacidad para realizar, presentar y defender ante un tribunal un ejercicio en el cual se sinteticen las competencias adquiridas en el posgrado.

Perfil profesional

- Responsable de proyectos de seguridad TIC: profesional responsable del diseño, desarrollo y adecuación de controles de seguridad informática (típicamente controles de programario).
- Experto en el desarrollo de aplicaciones y servicios web seguros: responsable del diseño y programación de controles de seguridad (controles de acceso, funciones criptográficas, filtros, bitácoras de seguridad de aplicaciones, etc.), análisis de aplicaciones robustas a vulnerabilidades de seguridad, preparación de librerías con funciones de seguridad para su uso por parte del área de desarrollo de sistemas, soporte de seguridad para el área de desarrollo de sistemas, consultoría de desarrollos seguros (integración de seguridad en aplicaciones desarrolladas por sistemas).
- Especialista en sistemas de registro web y control de acceso: analista/programador de servicios de registro y federación de identidades.
- Consultor de proyectos de administración electrónica: responsable del análisis, diseño y programación de proyectos de la administración electrónica.
- Consultor de comercio y banca electrónica: responsable del análisis, diseño y programación de proyectos de banca y transacciones comerciales electrónicas.
- Especialista en servicios de privacidad y anonimato.

Programa académico

El posgrado tiene una duración de un curso académico y se estructura en dos semestres:

- 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.

- 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 electrónico. 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.

- Proyecto en Seguridad en Servicios y Aplicaciones (6 ECTS): Proyecto Final de Posgrado

Sistema de evaluación

El sistema de evaluación del Diploma de Posgrado en Seguridad en Servicios y Aplicaciones es la evaluación continua (EC). La EC consiste en la realización y superación de una serie de pruebas de evaluación continua (PEC) establecidas en el plan docente, de acuerdo con el número y el calendario que se concreta. La EC de cada asignatura se ajusta a los objetivos, competencias, contenidos y carga docente de cada asignatura. El plan docente establece los criterios mínimos y el calendario de entrega para seguir y superar la EC. En todo caso, para considerar que se ha seguido la EC debe haber hecho y entregado como mínimo el 50% de las PEC. El no seguimiento de la EC se califica con una N (equivalente al no presentado).