

MEMORIA PARA LA SOLICITUD DE VERIFICACIÓN DE TÍTULOS OFICIALES

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

Universidade de Vigo



UNIVERSIDADE DA CORUÑA

1. DESCRIPCIÓN DEL TÍTULO

Responsable del título (Coordinador/a)

1º Apellido	Fernández
2º Apellido	Vilas
Nombre	Ana
Categoría profesional	Profesora titular de universidad
NIF	35307306Y

Universidad solicitante

Nombre de la Universidad	Universidade de Vigo
CIF	Q8.650.002B
Centro responsable del título	Escola de Enxeñaría de Telecomunicación

Datos básicos del título

Denominación del título	Máster en Ciberseguridad
Centro/s donde se imparte el título	Escola de Enxeñaría de Telecomunicación (UVigo) Facultade de Informática (UdC)
Título conjunto (Sí/No)	Sí
Universidades participantes (indicar universidad coordinadora)	Universidade de Vigo (coordinadora) Universidade da Coruña
Rama de conocimiento	Ingeniería y Arquitectura
Código ISCED (incluir 1 obligatorio, máximo 2)	480 (Informática), 520 (Ingeniería y profesiones afines)
Indicar si habilita para profesión regulada	Non

Datos asociados al centro (indicar esta información para cada uno de los centros)

Modalidad de enseñanza (presencial, semipresencial, no presencial)	Presencial
Número de plazas máximas de nuevo ingreso ofertadas en el primer curso de implantación por modalidad de enseñanza	40 (20 en cada una de las universidades participantes)
Número de plazas máximas de nuevo ingreso ofertadas en el segundo curso de implantación por modalidad de enseñanza	40 (20 en cada una de las universidades participantes)
Lenguas empleadas en el proceso formativo (sólo de las materias obligatorias)	Español, gallego, inglés
Número de ECTS del título	90

Universidad de Vigo

	Tiempo completo		Tiempo parcial	
	ECTS matrícula mínima	ECTS matrícula máxima	ECTS matrícula mínima	ECTS matrícula máxima
1er curso	48	60	18	47
Resto cursos	48	78	18	47

Universidad de la Coruña

	Tiempo completo		Tiempo parcial	
	ECTS matrícula mínima	ECTS matrícula máxima	ECTS matrícula mínima	ECTS matrícula máxima
1er curso	60	60	24	48
Resto cursos	48	78	24	48

El número de créditos mínimo y máximo en cada curso académico viene determinado por las normativas de permanencia de las universidades participantes (Universidades de Vigo y de A Coruña).

Especialidades: no existen especialidades

Enlaces a las normativas de permanencia:

- Universidade de Vigo:
 - https://www.xunta.gal/dog/Publicados/2017/20170630/AnuncioU500-210617-0001_es.html
- Universidade da Coruña:
 - https://www.udc.es/export/sites/udc/normativa/_galeria_down/academica/dedicacion_estudo_permanencia.pdf

2. JUSTIFICACIÓN DEL TÍTULO PROPUESTO

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

2.1.1. Introducción

El presente tecnológico actual está marcado por el desarrollo de las nuevas tecnologías y la capacidad disruptiva de las tecnologías exponenciales (*cloud*, robótica, inteligencia artificial, Internet de las cosas, *analytics*, ...). Las grandes empresas e instituciones generan un volumen de negocio y datos cada vez más importante en canales digitales para la relación con sus clientes, y el mundo acaba de superar, sin duda, la cuarta revolución industrial, de la que nuestra Comunidad Autónoma no puede ni debe quedar fuera. La confianza en el nuevo entorno digital es una de las cuestiones que más preocupa a los agentes implicados (empresas, gobiernos y ciudadanos), ya que este nuevo entorno cambió los riesgos a los que se ven expuestas las personas que se relacionan entre sí en un mundo hiperconectado y que hizo proliferar nuevos modos de explotar la información... pero también de delinquir con ella.

Para hacer frente a estos nuevos riesgos, son necesarios profesionales especializados en la ciberseguridad, entendida como seguridad de los sistemas de información pero también en los programas informáticos y en los procesos industriales. Para hacernos una idea, en los EE.UU. la demanda de puestos de trabajo en Ciberseguridad creció un 91% en el período 2010-2014, mientras que el global de las TIC (Tecnologías de la Información y las Comunicaciones) en el mismo período fue de un 28%, tres veces inferior.

La institución (ISC)² estima que en 2021 habrá más de 1,5 millones de puestos especialistas en este campo que no podrán ser cubiertos. Este es el presente que está transformando el panorama profesional a una velocidad muy superior a la que las escuelas tecnológicas pueden formar a los profesionales TIC en los retos del futuro. Es, por tanto, una obligación de las instituciones académicas, de las universidades y, especialmente, de las escuelas y facultades TIC, poner en marcha programas formativos que ayuden a cubrir la demanda de profesionales cualificados que exista en el futuro y, al tiempo, generar oportunidades de empleabilidad y de desarrollo de talento que tengan una repercusión muy positiva en su entorno de influencia, especialmente ayudando a reforzar las capacidades del tejido empresarial y el sector público, en este caso, de la Comunidad Autónoma de Galicia, el Reino de España y la Unión Europea.

Estamos en el momento ideal para la puesta en marcha de la titulación: hay una necesidad empresarial e industrial, mostrada en diferentes eventos y situaciones; una demanda por parte de los estudiantes de nuestros centros TIC; profesorado capacitado y motivado para poner en marcha esta titulación; y un cambio en el paradigma industrial, la conocida Industria 4.0, que precisa de una fuerte inversión en seguridad de la información y de los procesos. Todo esto se suma a la confluencia en el mismo proyecto de los centros que forman a los especialistas en redes, comunicaciones, software y sistemas de información.

La propuesta de Máster Interuniversitario en Ciberseguridad, impartido entre las Universidades de A Coruña y Vigo, implica a dos centros (Facultade de Informática de A

Coruña, Escuela de Ingeniería de Telecomunicación de Vigo) y complementa las titulaciones TIC de ambas instituciones: Grado en Ingeniería de Tecnologías de Telecomunicación, en la UVIGO, y Grado en Ingeniería Informática en la UDC. Además, potencia las apuestas tecnológicas de la Universidade de Vigo (Vigo Tecnolóxico y Campus da Auga) y de la Universidade da Coruña (Campus Innova TIC).

El Máster aprovecha, además, las sinergias creadas en el ámbito de la Cátedra Deloitte de Ciberseguridad, creada en la Universidade de Vigo en 2016, constituyendo una titulación singular en el Sistema Universitario Gallego (SUG) por su implicación con las titulaciones TIC y su orientación al mundo empresarial.

Al servicio de este ambiente institucional, social y económico-empresarial, el Máster Interuniversitario en Ciberseguridad se concibe como un título con una marcada vocación profesional, pensado con la misión de formar especialistas que la empresa gallega, nacional e internacional pueda incorporar en cualquiera de sus procesos para suplir las carencias a las que actualmente se enfrentan en el campo de la seguridad digital y la protección de la información, y dirigido fundamentalmente a las personas que quieran adquirir formación especializada pero de carácter aplicado en estas disciplinas. El diseño del currículum que más adelante expone esta memoria responde, pues, a esta orientación profesional de las enseñanzas, en la creencia que con ello se satisfacen más plenamente las necesidades e intereses de las universidades del SUG, las empresas y los estudiantes potenciales.

2.1.2. Experiencia y potencial de los centros implicados

Como se indica en la introducción, esta memoria sustenta un máster interuniversitario con participación de un centro de la Universidad de Vigo y otro de la Universidade da Coruña. En los apartados siguientes se detalla la trayectoria previa de los centros.

2.1.2.1. Escuela de Ingeniería de Telecomunicación, Universidad de Vigo

Los estudios universitarios de **Ingeniería de Telecomunicación** en Galicia nacen en el año **1985** con la creación de la Escuela Técnica Superior de Ingenieros de Telecomunicación (ETSE), actualmente Escuela de Ingeniería de Telecomunicación, en el campus de Vigo, adscrito por entonces a la Universidad de Santiago de Compostela. El plan de estudios inicial de dicha titulación contenía dos posibles especialidades, llamadas Comunicaciones y Telemática. En el momento de su implantación en el campus de Vigo, la titulación de Ingeniería de Telecomunicación sólo se impartía en las Universidades Politécnicas de Madrid y Cataluña, por lo que la afluencia de alumnos de otras comunidades autónomas españolas fue muy amplia.

Durante los primeros años, la titulación compartió sede con la Escuela Técnica Superior de Ingenieros Industriales, hasta que el curso 1990/91 se inicia en el edificio en que radica actualmente la Escuela.

En el año 1990, la Xunta de Galicia aprueba la segregación de las Universidades de Vigo y A Coruña, asumiendo los campus de Vigo, Pontevedra y Ourense, y de A Coruña y Ferrol, respectivamente, que hasta entonces formaban parte de la Universidad de Santiago de Compostela. Es así como la ETSE Telecomunicación cesa en su vinculación con la Universidad compostelana para depender de la recién creada Universidad de Vigo.

En el curso **1994/95** entra en vigor un nuevo plan de estudios de la titulación de Ingeniero de Telecomunicación (BOE 23 de noviembre de 1994). En este plan de estudios, que se extingue en septiembre de 2017, presenta tres especialidades: **Electrónica, Telemática y Comunicaciones**. Esta última especialidad incluye, además, dos intensificaciones: Radio y

Procesado de Señal.

En el curso **2003/04**, la oferta de titulaciones de la ETSE de Telecomunicación se amplía con la implantación de las correspondientes a **Ingeniería Técnica de Telecomunicación**, especialidad en Sistemas de Telecomunicación (BOE 9 marzo 2004), e Ingeniería Técnica de Telecomunicación, especialidad en Sonido e Imagen (BOE 9 marzo 2004). Ambos planes de estudio se extinguen con el Grado en Ingeniería de Tecnologías de Telecomunicación.

En el año 2006 se inaugura la segunda fase de construcción del edificio sede de la Escuela, lo que permite disponer de 20 nuevas aulas y laboratorios, así como la reordenación de los antiguos espacios, permitiendo la expansión física, tanto en despachos para profesores como en laboratorios para investigadores, de los grupos de investigación de los cuatro departamentos con sede en el edificio de la Escuela: Teoría de la Señal y Comunicaciones, Ingeniería Telemática, y Matemática Aplicada I y II.

Cuando comienza el proceso de adaptación al Espacio Europeo de Educación Superior, las titulaciones de Ingeniería e Ingeniería Técnica de Telecomunicación se encuentran plenamente consolidadas en el Sistema Universitario de Galicia y cumplen plenamente los requisitos de viabilidad que, en su documento "Liñas xerais para a implantación dos Estudos de Grao e Posgrao no Sistema Universitario de Galicia", aprobado el 5 de noviembre de 2007, marca el Consello Galego de Universidades para las titulaciones que se transformarán y podrán implantarse como nuevos títulos de Grado en el curso 2009/2010.

En el curso **2010/11** comenzó la impartición de la titulación de **Grado en Ingeniería de Tecnologías de Telecomunicación**, con cuatro menciones (Sistemas Electrónicos, Sistemas de Telecomunicación, Sonido e Imagen, y Telemática). Este Grado proporciona atribuciones profesionales de Ingeniero Técnico de Telecomunicación, en cada una de las cuatro ramas de esta profesión, dependiendo de la mención seleccionada, en tercer curso, por el alumno. En el curso **2014/15** comienza a impartirse el **Máster en Ingeniería de Telecomunicación** que proporciona a los graduados la obtención de las atribuciones profesionales de Ingeniero de Telecomunicación, y a la Escuela mantener un título (habilitante para dicha profesión) que lleva impartiendo desde su constitución.

La Escuela de Ingeniería de Telecomunicación tiene, por tanto, una experiencia de 32 años en la formación de Ingenieros de Telecomunicación. En el curso 1989/90 se graduaron los primeros alumnos de la titulación de Ingeniería de Telecomunicación de este Centro, y desde entonces, y hasta el momento de redactar esta memoria, se han incorporado al mercado laboral casi 3000 egresados de esta titulación.

Además de estas titulaciones de primer y segundo ciclos, en la Escuela se imparte el **Máster en Matemática Industrial, interuniversitario**, coordinado con las Universidades de Santiago de Compostela (que lleva la coordinación), A Coruña, Politécnica de Madrid y Carlos III de Madrid. El éxito de funcionamiento, coordinación y empleabilidad de este máster con programa de doctorado asociado resulta una buena medida de las posibilidades de la propuesta de esta memoria: tenemos capacidad técnica para impartir un máster deslocalizado en cuanto a sedes, la experiencia de hacerlo y la seguridad de poder hacerlo con éxito.

En lo que respecta a la formación doctoral, los dos departamentos mayoritarios en las titulaciones de Telecomunicación que tienen sede en la Escuela, Ingeniería Telemática y Teoría de la Señal y Comunicaciones, con el apoyo del Centro de Investigación AtlantTIC, ofrecen conjuntamente un programa de doctorado conocido como **DocTIC**, Doctorado en

Tecnologías de la Información y las Comunicaciones, que pretende generar investigación de calidad con impacto internacional y proporcionar a la industria profesionales con conocimientos avanzados que mejoren su competitividad a nivel global.

Más relacionado con la Ciberseguridad, en los últimos años se han llevado a cabo diversas iniciativas al respecto, en buena medida a raíz de solicitudes por parte del tejido industrial gallego y también por parte de nuestro propio alumnado, organizado un Club de Ciberseguridad. Entre las más destacadas está un **Curso Complementario de Introducción a la Ciberseguridad**, impartido en su totalidad por profesionales de diferentes empresas gallegas (salvo dos ponentes de otros puntos de la geografía española) del ámbito, con ediciones en 2016 y 2017. El otro hito fundamental es la creación, en diciembre de 2016, de la **Cátedra Deloitte de Ciberseguridad** con sede en la Escuela pero con actividades previstas tanto en los campus de Vigo como de Ourense. Esta Cátedra servirá como elemento difusor del interés e importancia de la seguridad pero también como catalizador de vocaciones hacia esta disciplina.

A lo largo de todos estos años, la Escuela de Ingeniería de Telecomunicación ha podido incorporar a su plantilla docente un número importante de profesores egresados de sus titulaciones de ciclo largo. Durante muchos cursos, hasta un 25% del total de profesores, contratados bajo la figura de profesorado asociado a tiempo parcial, compaginaban la docencia con su trabajo como profesionales del sector (técnicos de empresas de telecomunicación, consultores, analistas, responsables de proyectos), cuya visión de las necesidades del mundo de la empresa aporta un gran valor a la formación del alumno. Aunque este tipo de profesorado se ha visto reducido en número debido a los ajustes de plantilla docente de los últimos años, la conexión con la empresa de muchos de los docentes e investigadores actuales es constante y reflejo de esto es el elevado número de proyectos y contratos suscritos, pudiendo aportar una formación adecuada a las necesidades observadas.

Si a ello se añade que el 99% del profesorado posee el título de doctor, se puede afirmar sin género de dudas que la Escuela de Ingeniería de Telecomunicación dispone de una equilibrada y excelente plantilla de profesorado con amplia y acreditada experiencia en la formación de ingenieros de telecomunicación en los tres ciclos universitarios.

2.1.2.2. Facultad de Informática, Universidade da Coruña

Esta facultad empezó su andadura en el año 1986, entonces dependiente de la USC. La creación, por la Ley 11/1989 del 20 de julio de ordenación del sistema universitario de Galicia, de la Universidade da Coruña, amparó su integración en esta nueva universidad. Poco después, en 1993, alcanzó su ubicación actual en un edificio del Campus de Elviña, a las puertas de A Coruña.

En la actualidad se puede cursar en la FIC

- Grado en Ingeniería Informática, siendo actualmente el único centro de Galicia en el que se pueden estudiar las 5 especialidades recogidas en las recomendaciones del Consejo de Universidades para la titulación.
- Cinco másteres:
 - el Máster Universitario en Ingeniería Informática, que cuenta con la colaboración directa de profesionales de empresas punteras del sector TIC en Galicia y permite la colegiación en el Colegio Profesional de Ingeniería en Informática,
 - el Máster Universitario en Bioinformática para Ciencias de la Salud, que tiene

como objetivo la formación de investigadores y profesionales en el ámbito de la Bioinformática y la Bioingeniería con especial énfasis en su vertiente biomédica,

- el Máster Universitario en Geoinformática, interuniversitario con la Universidad de Vigo,
- el Máster Universitario en Matemática Industrial, interuniversitario entre las tres universidades gallegas, Universidad Carlos III y Universidad Politécnica de Madrid, y
- el Máster Universitario en Técnicas Estadísticas, interuniversitarios entre las tres universidades gallegas.

El compromiso de la Facultad con la calidad tanto docente como investigadora es indudable, y reposa, en buena parte, en la actividad desarrollada por los grupos de investigación constituidos en el centro y en una fuerte relación con las empresas de nuestro entorno y con centros tecnológicos como el CITIC, que recientemente ha sido reconocido por la Consellería de Cultura, Educación y Ordenación Universitaria como Centro Singular de Investigación de Galicia para el período 2016-2019. El CITIC es el único centro TIC en Galicia reconocido con este distintivo. Esta relación favorece la realización de prácticas en empresas (curriculares y extracurriculares) y permite la organización continuada de charlas de contrastados profesionales informáticos, muchos de ellos egresados de nuestro centro.

Asimismo, se potencian los programas de movilidad, que se vieron muy favorecidos con la introducción de una línea de docencia en inglés en el curso 2015/16. Estos programas de movilidad incluyen tanto acciones en el marco general de la convocatoria europea Erasmus como acciones bilaterales, como la que se mantiene con la University of South Wales, que posibilita a los alumnos que la eligen completar su ciclo con una doble titulación, española y galesa.

2.1.3. Interés para la Sociedad, demanda potencial y relación con el entorno socioeconómico

Según los estudios de inserción de empleo de los egresados de los centros implicados, un porcentaje importante se emplea en empresas o administraciones públicas que desarrollan su actividad en la propia comunidad autónoma gallega. La situación del mercado de las Telecomunicaciones y la Informática en Galicia puede considerarse peculiar dentro de la realidad económica de la propia comunidad, ya que cuenta con un número importante de empresas de mayor o menor envergadura en el sector de interés. Por citar algunas, encontramos desde fabricantes de equipos de comunicaciones (Televés, Egatel) a operadores (propios como R o delegaciones de compañías de ámbito nacional o internacional: Telefónica, Orange, Vodafone –con peso ampliado en la comunidad tras la compra de Tele2-Comunitel, empresa con sede en Vigo–), pasando por fabricantes de electrónica de consumo (Blu:sens). Además, y esto es de especial interés para esta propuesta, existe un número creciente de empresas medianas o pequeñas que proporcionan servicios de asesoramiento, auditoría o gestión de las áreas de seguridad de sistemas, equipos y software para otras empresas o instituciones en la propia Galicia, en el resto de España o, incluso, corporaciones extranjeras, dado que nos centramos en un ámbito en el que la actividad remota no sólo es posible sino que es muy habitual. Un buen número de estas empresas han colaborado con la Escuela y Facultad proponentes en diversos ámbitos, tanto en áreas de I+D como en formación mediante prácticas; y deben ser vivero de las prácticas obligatorias en empresa propuestas en el presente plan.

Los grandes centros de desarrollo económico estatales, como son Madrid y Barcelona, atraen también un número considerable de egresados. Es de destacar el carácter emigrante del egresado en busca de su primer empleo, y también la tendencia a volver a Galicia una vez

que su carrera profesional ha desarrollado sus primeros impulsos: el 60% de los egresados que trabaja fuera de la comunidad desea volver.

No obstante, y acorde con los principios que inspiran el proceso de construcción del Espacio Europeo de Educación Superior, que centra su objetivo en el proceso de aprendizaje del estudiante en un contexto que se extiende a lo largo de toda su vida laboral, el objetivo no podía centrarse exclusivamente en la formación de un titulado con un alto nivel de empleabilidad inicial. Por el contrario, el esfuerzo debía dirigirse hacia el diseño de unas competencias que permitan al alumno desarrollar con éxito su potencial en una carrera profesional que le lleve hacia puestos de alta responsabilidad.

En esta línea de objetivos a alcanzar, el desarrollo de la elaboración de la presente memoria contó con las opiniones de egresados de los centros, profesionales de la Ciberseguridad, representantes de los Colegios Profesionales del ramo, y de académicos de otras Universidades, con el objetivo de que aportaran a los trabajos de la comisión la necesaria perspectiva externa y redujeran el riesgo de desarrollar una propuesta excesivamente académica y alejada de las necesidades reales del mercado.

2.2. Referentes externos a la Universidad

2.2.1. Universidades nacionales y extranjeras

En la Universidad española existen diversas iniciativas relacionadas con la Ciberseguridad, desde títulos propios (el curso complementario de la Universidad de Vigo es un ejemplo cercano, pero también el catálogo de másteres no oficiales) hasta másteres verificados por ANECA o las agencias autonómicas acreditadas. De entre ellos, destacan:

- Máster universitario en seguridad de las tecnologías de la información y de las comunicaciones, Universidad Autónoma de Barcelona (interuniversitario UAB, UoC, URV)
- Máster universitario en ciberseguridad, Universidad Carlos III de Madrid
- Máster en técnicas de seguridad informática. Ciberseguridad. Universidad de Barcelona
- Máster universitario en seguridad informática (ciberseguridad). Universidad de Cádiz
- Máster universitario en seguridad informática. Universidad de Jaén
- Máster universitario en investigación en ciberseguridad. Universidad de León. Se ofrece también online.
- Máster universitario en ciberseguridad. Universidad Politécnica de Madrid
- Máster Universitari en seguretat informàtica i la intel·ligència artificial. Universitat de les Illes Balears
- Máster universitario en seguridad informática e inteligencia artificial. Universitat Rovira i Virgili
- Máster universitario en ingeniería de seguridad de la información y las comunicaciones. Universidad Alfonso X El sabio
- Máster en ciberseguridad UCAV-DELOITTE. Universidad Católica de Ávila. Título propio
- Máster universitario en seguridad de tecnologías de la información y de las comunicaciones. Universidad Europea de Madrid
- Máster universitario en seguridad de las tecnologías de la información y de las comunicaciones. Universitat Oberta de Catalunya (interuniversitario UoC, UAB, URV)

En Universidades extranjeras, se ha constatado la inexistencia de titulaciones de

Ciberseguridad, como tales, entre las de máximo prestigio en Estados Unidos, sustituidas por un catálogo de asignaturas en este ámbito en titulaciones de Computer Science en los niveles de Bachelor y Master. Sin embargo, un buen número de centros de gran prestigio en Estados Unidos, Reino Unido y resto de Europa disponen de titulaciones de Máster en Ciberseguridad, entre las que se pueden enumerar:

- M.Sc. in cybersecurity. Webster university
- Master in cybersecurity. University of Central Missouri
- Network security and pentesting MSc. Middlesex University London
- Master's degree programme in information security and cryptography. University of Turku
- MSc computer forensics and cybersecurity. University of Greenwich
- Msc in Cybersecurity and Forensics. University of Westminster
- MSc in Cybersecurity. Manchester Metropolitan University
- MSc Information Security and Biometrics. University of Kent
- MSc Cyber Security. Northumbria University
- MSc Cybersecurity Engineering. The University of Warwick
- MSc in Information Security & Privacy. University of Cardiff
- Master of Science in Cybersecurity in Computer Science. George Washington University
- MSc Advanced Security and Digital Forensics. Edinburgh University
- Master of Science in Computer Communication and Information Sciences - Security and Mobile Computing. Aalto University
- MSc Forensic Computing. Coventry University
- MSc System and Network engineering: Security. Amsterdam University
- MSc in Cybersecurity. University of Dallas
- MSc Network & Information Security. Kingston University, London
- Master of Science Cybersecurity Engineering. University of Southern California
- Cybersecurity Technology Master's Degree. University of Maryland
- Master in Cybersecurity. Universiteit Leiden
- Master of Information and Cybersecurity. University of Berkeley
- Master of Science in Security Informatics. Johns Hopkins University
- Master of Science in Information Security. Carnegie Mellon University
- Information Security MSc. University College London
- Computing & Security MSc. King's College London
- Master of Information Security Technology. University of Eindhoven
- MS Cybersécurité et cyberdéfense. Paritech Telecom
- Master in Cybersecurity. Université Catholique de Louvain
- Information Security Master. ETH Zurich

2.2.2. Informes de organismos oficiales

A nivel nacional, el Instituto Nacional de Ciberseguridad, INCIBE, con sede en León, publica un informe sobre la formación en el ámbito. Este informe se ha usado como referencia para la elaboración de la propuesta. El informe en cuestión lleva por título "Punto de partida al Modelo de gestión y seguimiento del TALENTO en ciberseguridad en España" y data de 2016.

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

2.3.1. Descripción de los procedimientos de consulta internos

La Junta de Centro de la Escuela de Ingeniería de Telecomunicación de la Universidad de Vigo expresó al Vicerrectorado de Organización Académica, Profesorado y Titulaciones su intención de formal de implantar una titulación de Máster en Ciberseguridad, en sesión ordinaria el día 15 de febrero de 2017. Con la misma fecha, la Junta de Centro de la Escuela Superior de Ingeniería Informática de la Universidad de Vigo aprobó una declaración de interés prácticamente igual en su contenido, fruto de la coordinación previa en su redacción.

El 17 de marzo de 2017, el Consejo de Gobierno de la Universidad de Vigo aprobó la declaración de interés para implantar, en el curso 2018/19, un nuevo título de Máster en Ciberseguridad.

En cada uno de los centros se creó un pequeño grupo de trabajo con la misión de elaborar la memoria de la titulación.

En el de la Escuela de Ingeniería de Telecomunicación participaron el Director y el Subdirector de Organización Académica, el Director del Departamento de Ingeniería Telemática, el Subdirector de Relaciones Internacionales (participante en un plan de formación en Ciberdefensa para la OTAN) y un representante de los alumnos; y fueron invitados a participar el Director del Centro Universitario de la Defensa (con sede en la Escuela Naval Militar y adscrito a la Universidad de Vigo) y el Director de la Escuela Superior de Ingeniería Informática, del campus de Ourense.

El 17 de abril de 2017, tras una ronda de conversaciones telefónicas en las semanas previas, se reunieron en Santiago de Compostela los directores y decano de los centros implicados en esta propuesta, acordando sentar las bases para elaborar una memoria interuniversitaria y crear una pequeña comisión de seis miembros (dos de la Facultad de Informática, dos de la Escuela Superior de Ingeniería Informática y dos de la Escuela de Ingeniería de Telecomunicación) que se encargará de determinar un esquema base de la titulación y de definir competencias y asignaturas.

El 4 de mayo de 2017, la comisión interuniversitaria se reunió presencialmente en Santiago de Compostela para acordar la definición general del plan de estudios, los procedimientos de coordinación y los aspectos básicos de la docencia.

A esta reunión presencial se sucedieron múltiples reuniones on-line, así como trabajo distribuido sobre documentos compartidos en plataformas como Google Drive.

En paralelo, las direcciones y decanato de los centros mantuvieron reuniones telefónicas para concretar otros aspectos de la memoria no estrictamente relacionados con el plan de estudios, avanzando así en la redacción de los otros puntos de la memoria.

El 24 de mayo de 2017, durante el evento “Xuntanza da Rede Galega de Ciberseguridade”, se presentó la propuesta de plan de estudios a los profesionales de la Ciberseguridad que forman parte de dicho grupo, prácticamente todos los que se dedican a este ámbito en Galicia. A partir de los interesantes comentarios recibidos, se siguió trabajando en la redacción de la memoria.

El 23 de junio de 2017 la Junta de Centro de la Escuela Superior de Ingeniería Informática acordó no seguir participando en la titulación.

Los procesos de revisión y consulta en las universidades participantes se resumen en los

siguientes eventos:

- Aprobación por las juntas de centro de la primera versión de la memoria, 12 de mayo de 2017 en los centros de la Universidade de Vigo (Escuela de Ingeniería de Telecomunicación y Escuela Superior de Ingeniería Informática) y 27 de mayo en la Universidade de A Coruña (Facultad de Informática). Exposición pública de la memoria ante la Comunidad universitaria y apertura de un plazo de alegaciones a la propuesta. Tras la recepción de alegaciones, se compiló una nueva versión de la memoria.
- Validación en la Comisión de Calidad de la Escuela de Ingeniería de Telecomunicación, el 27 de junio de 2017.
- Aprobación en las juntas de centro de la memoria final:
 - o Facultad de Informática, el 28 de junio de 2017
 - o Escuela de Ingeniería de Telecomunicación, el 29 de junio de 2017.
- Recepción del informe provisional de verificación, el 9 de febrero de 2018.
- Aprobación en las Juntas de Centro/CAMC de las alegaciones y la memoria final
 - o Escuela de Ingeniería de Telecomunicación, el 9 de marzo de 2018
 - o Facultad de Informática

2.3.2. Descripción de los procedimientos de consulta externos

Con el objetivo de adecuar las competencias y contenidos del plan de estudios a las necesidades del mercado laboral y tratar de garantizar el mayor nivel de empleabilidad posible de los egresados, se utilizaron dos mecanismos:

- Se estudiaron con detenimiento las propuestas formuladas por expertos profesionales en el ámbito de la Ciberseguridad, en concreto la formulada directamente a la Escuela de Ingeniería de Telecomunicación por Rubén Frieiro, socio de Deloitte España, y por Roberto Baratta, responsable de Seguridad de Abanca.
- Se trabajó en la confrontación del programa de estudios de Máster con los diseñados o en fase de diseño por parte de otros centros universitarios.

Durante la elaboración de la memoria se contó con la opinión de los profesionales agrupados en la autodenominada Rede Galega de Ciberseguridade (RGC). En dicho grupo participan una buena parte de las personas que se dedican a la seguridad de información, sistemas y software en Galicia, y se usaron sus foros para recabar opiniones sobre el proceso. Concretamente, se aprovechó la primera reunión presencial de esta Red, en Santiago de Compostela el día 24 de mayo de 2017, para presentar el proyecto de plan de estudios, recibiendo una muy positiva retroalimentación entre los asistentes. La opinión generalizada es que la propuesta encaja con precisión en las necesidades del tejido empresarial del ámbito de la Ciberseguridad en Galicia. Durante esta presentación se pidieron opiniones y propuestas a los asistentes, así como la inclusión del programa de Máster como tema de debate en el foro de LinkedIn de la Red, algo que se hizo efectivo a principio de junio de 2017, de modo que todos los miembros de la Red pudieron analizar el esquema del plan de estudios y aquellos que quisieron pudieron aportar sus ideas .

Así, *motu proprio* o a través de esta iniciativa de apertura a la RGC, participaron en la presente propuesta de plan de estudios los siguientes profesionales del ámbito:

- Rubén Frieiro, socio de Seguridad de Deloitte España, que colaboró muy activamente en la redacción de la declaración de intenciones, propuso (junto con Roberto Baratta) un plan de estudios que sirvió como documento de partida para las deliberaciones y aportó opiniones sobre el finalmente presentado.
- Roberto Baratta, director de Seguridad de Abanca (y actualmente del grupo Banesco, al que pertenece Abanca, a nivel global), que fue uno de los más fervientes impulsores de la implantación en el SUG de una titulación de máster en Ciberseguridad, participó en

múltiples reuniones e iniciativas previas para la puesta en marcha y propuso un primer borrador de plan de estudios.

- Susana Rey Baldomir, responsable de Seguridad en R, que participó en la redacción de la declaración de interés que lanzó esta propuesta y en la organización de diferentes acciones formativas, como los dos cursos complementarios de Introducción a la Ciberseguridad celebrados en UVIGO, en cuyo diseño se intuyen los contenidos que se desarrollan en este plan de estudios de Máster.
- Iago Fortes Caramés, director gerente de Inprosec, aportó sus comentarios al programa de estudios durante su elaboración.
- Natalia Costas, de CESGA, mostró su interés por los contenidos a la hora de opinar sobre el diseño del plan.
- Jorge Cerqueiro, decano del Colegio Oficial de Ingenieros Técnicos Industriales de Vigo (COITIVIGO), mostró desde el primer momento el interés de su colectivo por la existencia de alguna asignatura orientada hacia la seguridad de sistemas industriales, dada la especial relevancia de las máquinas programadas, robotizadas o automatizadas en las plantas de producción industrial y su vulnerabilidad ante ataques externos, en muchos casos por desconocimiento y/o infravaloración por parte de los especialistas en el ámbito mecánico.
- Belén Pérez Rodríguez, miembro del Grupo de Ciberseguridad Industrial de COITIVIGO, indicó la conveniencia de formar a los titulados de modo que tengan habilidades sociales para comunicarse con profesionales de ámbitos industriales, que no tienen formación en redes, servicios y software, pero que pueden dirigir instalaciones vulnerables a los ciberataques.
- Diego Pérez, de la Asociación Gallega de Graduados e Ingenieros Técnicos de Telecomunicación (AGGETT) expresó, asimismo, el interés de su colectivo por el programa de formación y su apoyo a una iniciativa que permitirá completar la formación de estos profesionales.
- José Luis Rivas López, *managing director* en SECITOR, indicó la importancia de disponer de asignaturas con tiempo suficiente para adquirir praxis además de conocimiento, aunque fuera a costa de reducir la duración de las prácticas en empresas o el trabajo de fin de máster.
- Juan Brión, Director Tecnológico en Green TIC, manifestó que sería interesante presentar y formar al alumnado en las principales tendencias y problemáticas que se dan en la actualidad en el ámbito de la seguridad en el sector TIC, así como realizar laboratorios y prácticas con equipamiento real (Hardware y/o Virtual Appliance), de forma que el alumnado conozca su funcionamiento y pueda servirle de punto de partida para un posterior desarrollo profesional.

Por otra parte, el contacto permanente con el Colegio Profesional de Ingeniería Informática y con el COETG, la demarcación del Colegio Oficial de Ingenieros de Telecomunicación en Galicia, también proporciona una información actualizada sobre el estado del mercado laboral y las necesidades de las empresas del ámbito en el entorno más cercano.

3. COMPETENCIAS

Competencias básicas

Relación de competencias básicas (reguladas por el RD 861/2010)	
Competencia básica 1 (CB1)	Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación
Competencia básica 2 (CB2)	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
Competencia básica 3 (CB3)	Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar 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
Competencia básica 4 (CB4)	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
Competencia básica 5 (CB5)	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

Competencias generales

Relación de competencias generales que el alumnado debe adquirir durante sus estudios	
Competencia general 1 (CG1)	Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación
Competencia general 2 (CG2)	Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones
Competencia general 3 (CG3)	Capacidad para el razonamiento crítico y la evaluación crítica de cualquier sistema de protección de la información, cualquier sistema de seguridad de la información, de la seguridad de las redes y/o los sistemas

	de comunicaciones
Competencia general 4 (CG4)	Compromiso ético. Capacidad para diseñar e implantar soluciones técnicas y de gestión con criterios éticos de responsabilidad y deontología profesional en el ámbito de la seguridad de la información, las redes y/o los sistemas de comunicaciones
Competencia general 5 (CG5)	Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos
Competencia general 6 (CG6)	Destreza para investigar. Capacidad para innovar y contribuir al avance de los principios, las técnicas y los procesos referidos a su ámbito profesional, diseñando nuevos algoritmos, dispositivos, técnicas o modelos útiles para la protección de los activos digitales públicos, privados o comerciales

Competencias específicas

Relación de competencias específicas que el alumnado debe adquirir durante sus estudios	
Competencia específica 1 (CE1)	Conocer, comprender y aplicar los métodos de criptografía y criptoanálisis, los fundamentos de identidad digital y los protocolos de comunicaciones seguras
Competencia específica 2 (CE2)	Conocer en profundidad las técnicas de ciberataque y ciberdefensa
Competencia específica 3 (CE3)	Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información
Competencia específica 4 (CE4)	Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información
Competencia específica 5 (CE5)	Diseñar, implantar y mantener un sistema de gestión de la seguridad de la información utilizando metodologías de referencia
Competencia específica 6 (CE6)	Desarrollar y aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad
Competencia específica 7 (CE7)	Tener capacidad para realizar la auditoría de seguridad de sistemas e instalaciones, el análisis de riesgos derivados de debilidades de ciberseguridad y desarrollar el proceso de certificación de sistemas seguros

Competencia específica 8 (CE8)	Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad
Competencia específica 9 (CE9)	Tener capacidad para elaborar de planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados
Competencia específica 10 (CE10)	Conocer los fundamentos matemáticos de las técnicas criptográficas y comprender su evolución y tendencias futuras
Competencia específica 11 (CE11)	Reunir e interpretar datos relevantes dentro del área de la seguridad informática y de las comunicaciones
Competencia específica 12 (CE12)	Conocer el papel de la ciberseguridad en el diseño de las nuevas industrias, así como las particularidades, restricciones y limitaciones que se han de acometer para obtener una infraestructura industrial segura
Competencia específica 13 (CE13)	Tener capacidad de análisis, detección y eliminación de vulnerabilidades, y del malware susceptible de utilizarlas, en sistemas y redes
Competencia específica 14 (CE14)	Tener capacidad para desarrollar un plan de continuidad de negocio siguiendo normas y estándares de referencia
Competencia específica 15 (CE15)	Tener capacidad de identificar el valor, tanto económico como de otra índole, de la información de la institución, sus procesos críticos y el impacto que produciría la interrupción de estos; y, también, las necesidades internas y externas que permitirán estar preparados ante ataques de seguridad
Competencia específica 16 (CE16)	Tener capacidad para vislumbrar y enfocar el esfuerzo de negocio en temáticas relacionadas con la ciberseguridad, y con una monetización viable
Competencia específica 17 (CE17)	Tener capacidad de planificar en el tiempo los periodos de detección de incidentes o desastres, y su recuperación
Competencia específica 18 (CE18)	Interpretar de una forma adecuada las fuentes de información en el ámbito del derecho penal informático (leyes, jurisprudencia y doctrina) de ámbito nacional e internacional
Competencia específica 19 (CE19)	Saber identificar los perfiles de personal necesarios para una institución en función de sus características y su sector
Competencia específica 20 (CE20)	Conocimiento de las empresas orientadas específicamente al sector de seguridad de nuestro entorno

Competencias transversales

Relación de competencias transversales que el alumnado debe adquirir durante sus estudios.	
Competencia transversal 1 (CT1)	Tener capacidad para comprender el significado y aplicación de la perspectiva de género en los distintos ámbitos de conocimiento y en la práctica profesional con el objetivo de alcanzar una sociedad más justa e igualitaria
Competencia transversal 2 (CT2)	Tener capacidad para comunicarse oralmente y por escrito en lengua gallega
Competencia transversal 3 (CT3)	Incorporar en el ejercicio profesional criterios de sostenibilidad y compromiso ambiental. Incorporar a los proyectos el uso equitativo, responsable y eficiente de los recursos
Competencia transversal 4 (CT4)	Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad
Competencia transversal 5 (CT5)	Tener capacidad para comunicarse oralmente y por escrito en inglés

4. ACCESO Y ADMISIÓN DE ESTUDIANTES

4.1. Sistemas de información previa a la matriculación y procedimientos de acogida y orientación del alumnado de nuevo ingreso para facilitar su incorporación a la Universidad y a las enseñanzas.

El Real Decreto 1393/2007 de 29 de octubre, que establece la ordenación de las enseñanzas universitarias oficiales, especifica la obligación de las universidades españolas de disponer de sistemas accesibles de información y procedimientos de acogida y orientación de los estudiantes de nuevo ingreso. Atendiendo a este requerimiento, las universidades participantes en esta propuesta disponen de diferentes medios.

La Universidad de Vigo ofrece información y orientación al alumnado de nuevo ingreso en su página web dentro de los siguientes apartados: *Estudios y Titulaciones*, *Centros*, *Administración y Servicios*, y *Biblioteca*. Además, la Universidad de Vigo pone a disposición de los futuros alumnos los siguientes documentos:

1. Guía rápida del estudiante. Se pone a disposición del alumnado de nuevo ingreso la información orientativa que facilita el conocimiento de la institución. En ella se incluye información general sobre el sistemas universitario, estudios oficiales, calendario escolar, programas de movilidad, becas y ayudas al estudio, oferta académica, transporte a los campus universitarios, alojamientos, etc. También incluye un apartado específico para el alumnado de nuevo ingreso en el que se le orienta sobre su proceso de matriculación.
2. Guía del estudiante extranjero. Con información práctica para los estudiantes extranjeros que deseen cursar estudios en la Universidad de Vigo en el marco de un programa de intercambio o de un convenio de cooperación internacional, o bien como estudiantes visitantes extranjeros, durante un cuatrimestre o un curso académico completo.
3. Otras publicaciones centradas en aspectos propios de la vida universitaria como el empleo, la movilidad, las actividades de extensión cultural, etc. Enfocadas para que el alumno conozca las posibilidades extracurriculares que ofrece la Universidad.

La Universidad de Vigo participa en diversas ferias educativas y realiza diferentes campañas de difusión de su oferta académica en medios de comunicación y en redes sociales. En estas acciones colaboran los servicios centrales de estudiantes, relaciones internacionales y el área de posgrado. Además, también se articulan desde el Vicerrectorado con competencias en este ámbito, actualmente el de Estudiantes y el de Extensión Universitaria y Relaciones Institucionales otras acciones, como la organización de jornadas con orientadores, o las visitas guiadas a los Campus de la Universidad.

Por parte de la Universidade da Coruña (UDC), el [Servicio de Asesoramiento y Promoción del Estudiante \(SAPE\)](http://www.udc.es/sape/)¹ y la [Guía del Estudiantado](http://www.udc.es/estudiantes/guia_estudiante/),² difunden información acerca de la oferta de la universidad, el proceso de matrícula y en general orientan en cuanto les resulta de interés a los posibles alumnos. En las dos universidades, los centros y departamentos exponen carteles informativos con los plazos de admisión y matrícula.

Los estudiantes podrán encontrar la información concreta sobre los estudios de máster en

¹ <http://www.udc.es/sape/>

² http://www.udc.es/estudiantes/guia_estudiante/

los siguientes enlaces de la página web de la UDC: <http://estudios.udc.es/es/degrees> y <http://estudios.udc.es/es/study/start/473V01>.

La información relativa a la admisión y matrícula en los másteres se puede obtener a través de la página web de la UDC: <http://estudios.udc.es/es/study/admission/473V01>, la cual se mantiene constantemente actualizada.

Los estudiantes del último año de licenciaturas/diplomaturas/grados reciben información de la oferta de títulos de máster durante el verano del año en que culminan esos estudios. Pero más específicamente, los coordinadores en cada una de las universidades organizará una sesión informativa en sus centros en el mes de mayo, destinada especialmente (aunque no exclusivamente) a los estudiantes de último curso de grado que puedan estar interesados en continuar sus estudios en este máster.

Las dos universidades realizan, al inicio de cada curso académico, jornadas de acogida organizadas por los Vicerrectorados con competencias en asuntos estudiantiles. Estas jornadas tienen por objeto presentar a los nuevos estudiantes las posibilidades, recursos y servicios que les ofrece la Universidad. Los centros implicados en este máster, por su parte, recibirán en una jornada de acogida a los nuevos estudiantes el primer día de clase. En ella se les ofrecerá una presentación del equipo docente, las aulas, la biblioteca, los servicios administrativos y la organización académica del centro.

Además de estos canales de difusión, el máster dispondrá en todo momento de una página web con información detallada del máster siguiendo los criterios y recomendaciones de la ANECA. Este portal web mantendrá la información completa sobre el programa, el profesorado, la metodología docente, los procesos administrativos, el calendario, los procesos de sugerencias y reclamaciones, los eventos relacionados o la información sobre empleo y becas.

Vías de acceso

Se podrá acceder al Máster estando en posesión de un título universitario expedido por el Estado español u otro equivalente otorgado por cualquier Estado miembro del EEES que faculte para el acceso a enseñanzas de Máster. También podrán acceder quienes posean un título extranjero expedido por una institución de educación superior de un país ajeno al EEES, siempre que ese título haya sido homologado a un título español que habilite para acceder a los estudios de Máster o que, sin estar homologado, haya sido comprobado como equivalente al nivel de formación de los estudios de grado en España y que faculte, en su país de origen, para el acceso a los estudios de Máster. El acceso por esta vía no implicará, en ningún caso, la homologación del título previo de que esté en posesión el interesado, ni su reconocimiento a otros efectos que de cursar las enseñanzas de Máster

Canales de difusión

Los futuros alumnos pueden obtener información detallada del Máster y/o del proceso de preinscripción y matrícula por los siguientes medios:

- Página web de los centros:
 - Escuela de Ingeniería de Telecomunicación: <http://www.teleco.uvigo.es>
 - Facultad de Informática: <http://www.fic.udc.es>
- Página web del vicerrectorado directamente responsable en cada una de las universidades participantes:
 - Universidade da Coruña http://www.udc.es/gobierno/equipo_reitoral/voaid/
 - Universidad de Vigo <http://profesorado.uvigo.es>
- Páginas web de las instituciones:

- Universidad de Vigo: <http://www.uvigo.es>
 - i. En el apartado “*Estudios y Titulaciones*” figura la información básica de la oferta por curso académico de los títulos de Máster de la Universidad de Vigo.
 - ii. Además, en la página principal de la Universidad de Vigo figura un enlace actualizado (en el momento de redactar esta memoria, con la etiqueta “matrícula del curso 16/17”) en relación al procedimiento administrativo de preinscripción y matrícula en estudios de máster para el curso académico correspondiente.
- Universidade da Coruña: <http://www.udc.es>
 - i. En la web institucional <http://estudios.udc.es/es/degrees> figura la información básica de la oferta por curso académico de los títulos de grado y máster de la Universidade da Coruña.
 - ii. Además, durante el período de matrícula, en la página principal de la Universidade da Coruña figura un enlace actualizado en relación al procedimiento administrativo de preinscripción y matrícula en estudios de máster para el curso académico correspondiente.

Además, en los centros de impartición del máster se realizan acciones concretas.

En la Escuela de Ingeniería de Telecomunicación (UVigo) se desarrollan otras líneas de acción que apoyan la acogida y orientación de los estudiantes de nuevo ingreso en su incorporación a la Universidad y a la titulación, tales como:

- Páginas web del centro. Constituyen un medio de orientación complementario en la vida académica del estudiante. De forma general, en ella el/la estudiante podrá encontrar información básica sobre el plan de estudios de la titulación, los horarios de clase, el calendario de exámenes, la guía de la titulación, el acceso a los servicios comunes del centro (secretaría, biblioteca, aula de informática, etc.) que se actualiza regularmente.
- Presentaciones informativas en las que se presenta a los/las graduados/as de la Escuela la oferta de continuación de estudios en las titulaciones de Máster impartidas en la Escuela.
- Envío de folletos informativos a otros centros de las universidades participantes, explicando a sus graduados los contenidos y las características de la titulación.

También en la Facultade de Informática de la UDC se realizan una serie de acciones complementarias para acoger y orientar al alumnado de nuevo ingreso, como:

- Página web del Centro: donde encontrará una información totalmente análoga a lo ya descrito en los centros anteriores.
- Servicios en redes sociales (Facebook y Twitter): complementan la información de la web de la Escuela con un enfoque más social, y en el que tanto la Dirección del Centro como los coordinadores de las titulaciones pueden atender las consultas que sean formuladas.
- Charlas informativas con el alumnado del último curso, orientadas a la continuación de estudios de Máster ofertadas por el Centro.

Perfil de ingreso recomendado

Este Máster está orientado principalmente a titulados/as en el ámbito de las tecnologías de la información y las comunicaciones, además de a profesionales que ya hayan trabajado en este campo y busquen especializarse en ciberseguridad. Son asimismo admisibles candidatos/as con formación STEM (*Science, Technology, Engineering, Mathematics*) no específica en tecnologías de la información y comunicaciones. Desde el punto de vista de los conocimientos, las habilidades y las aptitudes personales, el perfil de ingreso recomendado para el Máster Universitario en Ciberseguridad debe consistir en:

- Sólida formación científica y técnica básica: conocimientos de informática y matemáticas
- Capacidad de estudio y voluntad de trabajo
- Capacidad para la abstracción, el razonamiento analítico y el espíritu crítico
- Capacidad de síntesis y análisis
- Habilidad para la comunicación oral y escrita
- Interés amplio por las tecnologías de la información y las comunicaciones
- Capacidad para el aprendizaje autónomo, e interés por la actualización de conocimientos.
- Capacidad para trabajar en situaciones de escasez de información y bajo presión, teniendo capacidad de innovación, creatividad y generación de nuevas ideas.
- Capacidad para trabajar de forma colaborativa, integrado en equipos, organizando, planificando, tomando decisiones, negociando y resolviendo conflictos, relacionándose, y criticando y haciendo autocrítica.

Es altamente recomendable, aunque no exigible, un nivel de idioma B2 en inglés. A aquellos alumnos admitidos que no posean o no puedan acreditar un nivel de inglés equivalente a B2, las Universidades ofrecerán formación complementaria en el idioma a través de sus Centros de Lenguas, que cuentan con la potestad de expedir las acreditaciones necesarias (ACLES), de modo que puedan seguir con aprovechamiento las asignaturas del plan de estudios que se impartan parcial o totalmente en inglés. La formación del Centro de Lenguas estará también a disposición de los estudiantes que deseen realizar el trabajo de fin de máster en inglés, a los que sí se exigirá una certificación de nivel B2 en este idioma .

4.2. Requisitos de acceso y criterios de admisión

Acceso

Tal y como se recoge en el Real Decreto 1393/2007, que establece la ordenación de las enseñanzas universitarias oficiales, para acceder a las enseñanzas oficiales de Máster Universitario las y los aspirantes deberán de cumplir alguno de los siguientes requisitos:

- a) Estar en posesión de un título universitario oficial español (graduada o graduado universitario, licenciada o licenciado, arquitecta o arquitecto, ingeniera o ingeniero, arquitecta técnica o arquitecto técnico, ingeniera técnico o ingeniero técnico, diplomada o diplomado) u otro expedido por una institución de educación superior perteneciente a otro Estado integrante del Espacio Europeo de Educación Superior que faculte en el mismo para el acceso a enseñanzas de Máster.
- b) Las y los aspirantes con titulación extranjera expedida en una institución de educación superior no perteneciente a un Estado del Espacio Europeo de Educación

Superior podrán acceder a los estudios de Máster si cumple alguno de los siguientes requisitos:

- a. Estar en posesión de un título expedido por un sistema universitario extranjero que esté homologado a un título español que habilite para el acceso a los estudios de posgrado.
- b. Poseer un título expedido por un sistema universitario extranjero, ajeno al EEES, y sin homologación, con la comprobación previa de que el título expedido por el sistema universitario extranjero acredita un nivel de formación equivalente al correspondiente título español de grado y que faculta para el acceso a los estudios de posgrado en el país en el que se expide el título.

El acceso por esta vía no implicará, en ningún caso, la homologación del título previo de que esté en posesión el interesado, ni su reconocimiento a otros efectos que el de cursar las enseñanzas de Máster.

Admisión

El RD 1393/2007 de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales, modificado por el RD 861/2010 establece, en su artículo 17, que los estudiantes podrán ser admitidos a un Máster conforme a los requisitos específicos y criterios de valoración de méritos que, en su caso, sean propios del título de Máster Universitario o establezca la Universidad. La normativa de la Universidad de Vigo dispone, a través de su Reglamento de los estudios oficiales de posgrado, aprobado en Consello de Gobierno en su sesión del 14 de marzo de 2007, y modificado el 16 de abril de 2010, que el órgano competente en relación con el procedimiento de admisión en los títulos de Máster es la Comisión Académica de Máster.

En el caso de la Universidade da Coruña, la [normativa](#)³ por la que se regula las enseñanzas oficiales de grado y máster universitario en la UDC fue aprobada por el Consejo de Gobierno en su sesión de 27 de junio de 2012 y modificado por el mismo órgano en las sesiones del 19 de diciembre de 2013 y 29 de septiembre de 2015. Y cada año se menciona en la [Normativa de Gestión Académica de la Universidade da Coruña](#).⁴

Los criterios específicos de admisión al Máster serán, por orden de prevalencia, la titulación de acceso de los solicitantes, el expediente académico y la experiencia profesional. Tendrán preferencia en la admisión quienes posean un título de grado relacionado directamente con las tecnologías de la información y las comunicaciones por cualquier universidad del EEES, seguidos por quienes posean un título de grado en disciplinas científicas básicas (Matemáticas, Física o estudios afines), y estos tendrán preferencia sobre cualquier otro título académico. La experiencia profesional previa en el ámbito de la seguridad informática podrá ser utilizada por la comisión Académica del Máster como criterio adicional para decidir las admisiones, así como también, si lo considera necesario, la entrevista personal con las personas solicitantes para calibrar debidamente su aptitud y motivación. No se establecen complementos formativos de ninguna clase para las personas que no se adecuen significativamente a los criterios de admisión anteriores. El baremo de puntuación para la admisión es el siguiente:

- Estudios de acceso y expediente académico: 7 puntos
- Otros: 3 puntos
 - o Experiencia profesional: 0 a 2 puntos

³ http://www.udc.gal/export/sites/udc/normativa/_galeria_down/titulos/normativa_grao_mestrado.pdf

⁴ http://www.udc.gal/export/sites/udc/matricula/_galeria_down/NXA20162017.pdf

o Motivación, interés, entrevista personal: 1 a 2 puntos

Las titulaciones de acceso se ordenarán según la siguiente prelación:

1. Máster Universitario en Informática y Máster Universitario en Ingeniería de Telecomunicación o sus equivalentes LRU (Ingeniería de Telecomunicación y Licenciatura o Ingeniería en Informática).
2. Grado en Ingeniería Informática y Grado con atribuciones profesionales en Ingeniería Técnica de Telecomunicación, en la rama Telemática, o sus equivalentes LRU.
3. Grado con atribuciones profesionales en Ingeniería Técnica de Telecomunicación, en otras ramas y grados "blancos" en Telecomunicación o sus equivalentes LRU.
4. Otras titulaciones de Ingeniería, Matemáticas o Física.
5. Otras titulaciones en función de la decisión de la Comisión Académica del Máster en Ciberseguridad (CAMC) (véase el siguiente párrafo).

El órgano competente en el proceso de admisión será la CAMC, interuniversitaria, que estará presidida por un/a coordinador/a y formada por un total de 7 miembros de los que uno/a será un secretario/a y otro un representante del Sistema de Garantía Calidad. La CAMC será el órgano de decisión para todas las cuestiones referentes a la organización de la titulación, estando su capacidad de decisión supeditada al marco jurídico y normativo general de las universidades participantes y del Estado español.

La CAMC estará integrada por:

1. Presidente/a: la persona que coordina el Máster.
2. Secretario/a: la persona que coordina el máster en la Facultad de Informática de la Universidade da Coruña
3. Persona responsable de la Calidad en el centro coordinador.
4. Una persona designada por cada una de las Juntas de los centros participantes en el Máster
5. Un representante del alumnado
6. Un representante de la secretaría académica del centro coordinador

Cada centro nombrará una Comisión Académica de Máster local, encargada de la gestión del título en el ámbito del propio centro.

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

Los/las estudiantes del Máster en Ciberseguridad tendrán derecho a recibir tutela curricular mientras duren sus estudios con el fin de supervisar y facilitar su desempeño académico, orientarles en la configuración personal de su currículum y ofrecerles información particular sobre el futuro desarrollo profesional en cada disciplina de su interés. Para el ejercicio de esta tutela curricular se cuenta con los siguientes instrumentos:

1. Plan de acción tutorial:
 - La Universidade de Vigo, y en particular la Escuela de Ingeniería de Telecomunicación, es pionera en la implantación de un Plan de acción Tutorial ([MEET⁵](http://teleco.uvigo.es/index.php/es/alumnado/alumnado-actual/plan-de-accion-tutorial/meet-teleco-alu)) en los estudios de grado, por el cual un conjunto de mentores (docentes y alumnos de cursos avanzados que han recibido formación específica al

⁵ <http://teleco.uvigo.es/index.php/es/alumnado/alumnado-actual/plan-de-accion-tutorial/meet-teleco-alu>

respecto) aconsejan académicamente y en otros órdenes de desarrollo personal a los/las estudiantes de nuevo ingreso.

- En la UDC el plan de acción tutorial a nivel de máster está dirigido por los coordinadores de la titulación en la universidad.

2. Servicios institucionales: la OFOE (Oficina de Orientación al Empleo) y la ORI (Oficina de Relaciones Internacionales) ofrecen servicios especializados en la realización de prácticas en empresas, la búsqueda de empleo y la movilidad estudiantil.

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

Siendo un máster interuniversitario, en cada universidad participante se aplican sus normas de gestión académica, incluidas las que tienen que ver con transferencia y reconocimiento de créditos.

En cumplimiento con lo dispuesto en el artículo 6 del Real Decreto 1393/2007, del 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias, el Consello de Goberno de la Universidad de Vigo, en su sesión del 23 de junio de 2008, aprobó la [normativa de transferencia y reconocimiento de créditos](#)⁶ para titulaciones adaptadas al Espacio Europeo de Educación Superior (EEES).

Por su parte, la Universidade da Coruña, aprobó en la sesión de su Consejo de Gobierno que tuvo lugar el 30 de junio de 2011, la [Normativa de reconocimiento y transferencia de créditos](#)⁷ para titulaciones adaptadas al Espacio Europeo de Educación Superior (EEES), mediante la que se desarrolla el RD 1393/2007, de 29 de octubre, modificado por el RD 861/2010, de 2 de julio, por el que se establece la ordenación de las enseñanzas universitarias oficiales. En cualquier caso, en la convocatoria de matrícula de cada curso académico se recoge el procedimiento a seguir y los plazos fijados para el curso académico en vigor.

Con carácter general, el procedimiento para el reconocimiento de créditos se iniciará a petición de la o el interesado, quien presentará una solicitud en la secretaría de alumnado del centro de adscripción de la titulación, dirigida a la Comisión Académica del Máster, dentro de los plazos previstos al efecto. El reconocimiento también se podrá realizar de oficio por la administración en aquellos supuestos recogidos en la normativa.

Tal y como se recoge en la normativa, el reconocimiento de créditos en las enseñanzas de Máster deben respetar las siguientes reglas:

- Serán competencias reconocibles por materias, módulos y complementos formativos del programa de los estudios de Máster cualquier estudio universitario, perfil académico o profesional coincidentes con las competencias y conocimientos que se imparten en el máster así determinado mediante la correspondiente resolución rectoral, de conformidad con los órganos académicos de estos estudios.
- Los módulos, materias y complementos de formación reconocidos por resolución rectoral se consideran superados a todos los efectos y figurarán en el expediente del alumnado.
- Solo se podrán reconocer estudios universitarios oficiales correspondientes a los segundos ciclos de enseñanzas conducentes a las titulaciones de Licenciado,

⁶ http://secxeral.uvigo.es/opencms/export/sites/secxeral/secxeral_gl/_galeria_descargas/normativa_transferencia.pdf

⁷ https://www.udc.es/export/sites/udc/normativa/_galeria_down/academica/rec_transferencia_creditos.pdf

Ingeniero y Arquitecto.

- El número de créditos que podrá ser reconocido a partir de la experiencia profesional o laboral y de estudios universitarios no oficiales, no superará el 15 por ciento del total de los créditos que constituyan el plan de estudios (incluyendo el Trabajo Fin de Máster), con las excepciones que se establecen en el Real Decreto 1393/2007, modificado por el Real Decreto 861/2010, para el reconocimiento de títulos propios. Este reconocimiento no incorporará calificación por lo que no computará a efectos de baremo del expediente.
- En ningún caso serán objeto de reconocimiento los créditos correspondientes al Trabajo Fin de Máster.

No obstante, para cada curso académico se publica un Procedimiento de transferencia y reconocimiento de créditos para titulaciones adaptadas al EEES, en el que se concretan las instrucciones en cuanto a criterios de aplicación, plazos y procedimientos.

Experiencia laboral o profesional

En la titulación de Máster en Ciberseguridad se reconocerán créditos optativos por experiencia laboral o profesional previa, hasta un máximo de 10 ECTS y en módulos de 2,5 ECTS. Como criterio general, el reconocimiento de créditos se hará en función de la duración de la experiencia laboral o profesional acreditada, siempre que se haya desarrollado en empresas, instituciones o actividades propias del ámbito de la ciberseguridad con posterioridad a la obtención del título con el que se accede al máster. Se reconocerán 2,5 ECTS por cada seis meses de experiencia profesional, con un máximo acumulable de 10 ECTS.

Títulos propios

De cara al reconocimiento de créditos cursados en títulos propios, sólo se considerarán los cursados en aquellas titulaciones de máster adaptadas al EEES impartidas en los centros participantes en esta propuesta. Ante la solicitud individual de cada alumno/a, la Comisión Académica del Máster estudiará caso por caso las competencias y contenidos formativos de las asignaturas objeto de reconocimiento y decidirá la conveniencia del reconocimiento solicitado. Se mantendrá una tabla de equivalencias para las asignaturas reconocidas.

En particular, para los reconocimientos por títulos propios de las universidades participantes se establece un mínimo de cero y un máximo de 15 ECTS, excluidos los créditos de prácticas en empresas y de trabajo de fin de máster. Corresponderá a la Comisión Académica de Máster decidir en cada caso qué materias son reconocibles en función de cada caso. El máximo de 15 ECTS representa el 25% del total de créditos necesarios para obtener el título, excluidos los de prácticas en empresa y trabajo de fin de máster, o lo que es igual, 1/6 del total de créditos de la titulación.

Enseñanzas superiores oficiales no universitarias

No se reconocerán créditos cursados en enseñanzas superiores oficiales no universitarias. El órgano en que reside la decisión de todos estos reconocimientos será la Comisión Académica del Máster.

Normativa de transferencia y reconocimiento de créditos por Universidad

A continuación se incluye las Normativas de Transferencia y Reconocimiento de créditos para titulaciones adaptadas al Espacio Europeo de Educación Superior de la Universidad de Vigo y la Universidad de A Coruña:

- NORMATIVA DE TRANSFERENCIA Y RECONOCIMIENTO DE CRÉDITOS – UNIVERSIDAD DE VIGO (Aprobada por el Consello de Goberno de la Universidad de Vigo, en su sesión del 23 de julio de 2008)

EXPOSICIÓN DE MOTIVOS

El Real Decreto 13/93, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales determina que las universidades elaborarán y harán pública su normativa sobre el sistema de reconocimiento y transferencia de créditos; así mismo se definen, estos conceptos y sus principales efectos en el contexto de las nuevas enseñanzas universitarias oficiales.

En cumplimiento de lo dispuesto por el artículo 6 del Real Decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales el Consello de Goberno de la Universidad de Vigo en su sesión de 23 de julio de 2008 acordó aprobar la presente normativa de transferencia y reconocimiento de créditos.

Artículo 1.- De la transferencia de créditos

1.1.- La transferencia de créditos consiste en la inclusión en los documentos académicos oficiales acreditativos de las enseñanzas seguidas por cada estudiante de la totalidad de los créditos que el/ella hayan obtenido en enseñanzas oficiales cursadas con anterioridad, en la misma o en otra universidad, que no conduzcan a la obtención de un título.

1.2. - La Universidad de Vigo transferirá al expediente académico de su estudiantado, previa petición del interesado/a, todos los créditos obtenidos en enseñanzas oficiales cursadas en esta universidad o en otra universidad del EEES.

Artículo 2.- Del reconocimiento de créditos

2.1.- El reconocimiento de créditos consiste en la aceptación por la universidad de los créditos que, siendo obtenidos en enseñanzas oficiales, en la misma o en otra universidad, son computados en otras enseñanzas distintas para los efectos de la obtención de un título oficial.

2.2.- Los criterios generales de reconocimiento son aquellos que fije el Gobierno y, en su caso, concrete la Universidad de Vigo.

Cada titulación podrá establecer los criterios específicos adecuados a cada una de ellas y que serán recogidos en una Resolución Rectoral. Estos criterios serán públicos y vincularán las resoluciones que se adopten.

2.3.- El reconocimiento de créditos en las enseñanzas universitarias oficiales de Grado deberán de respetar las siguientes reglas básicas:

- a) Siempre que la titulación de destino pertenezca a la misma rama que la de origen, serán objeto de reconocimiento los créditos correspondientes a materias de formación básica de dicha rama.
- b) Serán también objeto de reconocimiento los créditos correspondientes a aquellas otras materias de formación básica cursada pertenecientes a la rama de destino.
- c) El resto de créditos serán reconocidos por la universidad teniendo en cuenta la adecuación entre las competencias y los conocimientos asociados a las restantes materias cursadas por el/la estudiante y los previstos en el plan de estudios o bien que tengan carácter transversal.

2.4.- El reconocimiento de créditos en las enseñanzas universitarias de máster oficiales deberá de respetar las siguientes reglas:

- a) Serán competencias reconocibles por asignaturas, módulos y complementos formativos del programa de estudios de máster cualquier estudio universitario, perfil académico o profesional coincidentes con las competencias y conocimientos que se imparten en el máster así

determinado mediante la correspondiente Resolución Rectoral, de conformidad con los órganos académicos de estos estudios.

- b) Los módulos, asignaturas y complementos de formación reconocidos por Resolución Rectoral se consideran superados a todos los efectos y figurarán en el expediente del alumnado.
- c) Sólo se podrán reconocer estudios correspondientes a los segundos ciclos de enseñanzas conducentes a las titulaciones de Licenciado, Ingeniero y Arquitecto.

Artículo 3. Unidad de reconocimiento

La unidad de reconocimiento será el crédito, sin perjuicio de que se puedan reconocer asignaturas o módulos completos. En el expediente figurarán como créditos reconocidos y se tendrán en cuenta a los efectos de considerar realizados los créditos de la titulación.

Artículo 4. Sistema de reconocimiento

4.1.- Para determinar el reconocimiento de créditos correspondientes a asignaturas no recogidas en los artículos 2.3a), 2.3b) y 2.4) se tendrán en cuenta los estudios cursados y su correspondencia con los objetivos y competencias que establece el plan de estudios para cada módulo o asignatura. La universidad acreditará mediante el acto de reconocimiento que el/la alumno/a tiene acreditadas las competencias de la titulación y el cumplimiento de parte de los objetivos de la misma en los términos definidos en el EEES.

4.2.- Para estos efectos cada Centro/Titulación podrá establecer tablas de equivalencia entre estudios cursados en otras universidades y aquellos que puedan ser reconocidos en el plan de estudios de su propia universidad. En estas tablas se especificarán los créditos que se reconoce, y de ser el caso, las asignaturas o módulos equivalentes o partes de asignaturas y módulos y los requisitos necesarios para establecer su superación completa.

Igualmente se establecerán tablas de equivalencia entre las titulaciones anteriores al Real Decreto 1393/2007, de 29 de octubre, y las titulaciones adaptadas a esta normativa.

Estas tablas se aprobarán por Resolución rectoral y se harán públicas para su conocimiento general.

4.3.- La universidad podrá reconocer directamente o mediante convenios, titulaciones extranjeras que den acceso a titulaciones oficiales de la Universidad de Vigo o establecer en esos convenios el reconocimiento parcial de estudios extranjeros.

La Universidad de Vigo dará adecuada difusión de estos convenios.

4.4.- Al /a la alumno/a se le comunicarán los créditos reconocidos y el número de créditos necesarios para la obtención del título, según las competencias acreditadas y según los estudios de procedencia del alumnado. También podrá especificarse la necesidad de realizar créditos de formación adicional con carácter previo al reconocimiento completo de módulos, materias o ciclos.

Artículo 5.- De la solicitud del reconocimiento de créditos

5.1.- El reconocimiento de créditos se realizará de acuerdo con el procedimiento que establezca el Vicerrectorado de Titulaciones y Convergencia Europea.

5.2.- El plazo para la presentación de la solicitud del reconocimiento de créditos se establecerá en el procedimiento que establezca el Vicerrectorado de Titulaciones y Convergencia Europea.

5.3.- Los expedientes de solicitud de reconocimientos de créditos serán resueltos por el Rector, quien delega en los Decanos/Directores, e informados por la comisión de evaluación del centro/titulación. En los casos de créditos de asignaturas de formación básica o la existencia de tablas de reconocimiento, el área académica del centro/titulación resolverá directamente la petición.

Artículo 6.- Suplemento Europeo al Título

Todos los créditos obtenidos por el/la estudiante en enseñanzas oficiales cursados en cualquier universidad, tanto los transferidos, los reconocidos como los superados para la obtención del correspondiente título, serán incluidos en el expediente académico y reflejados en el Suplemento Europeo al Título.

Artículo 7.- Reconocimiento de estudios anteriores al Real Decreto 1393/2007, de 29 de octubre

El procedimiento y criterios para el reconocimiento parcial de estudios de titulaciones de Diplomado/a, Licenciado/a Ingeniero/a o equivalentes para proporcionar efectos en titulaciones adaptadas al EEES serán los establecidos en esta normativa.

Artículo 8.- Reconocimiento de otros estudios o actividades profesionales

Conforme a los criterios y directrices que fije el Gobierno y el procedimiento que fije la Universidad se podrán reconocer como equivalentes a los estudios universitarios a la experiencia laboral acreditada, a las enseñanzas artísticas superiores, a formación profesional de grado superior, a las enseñanzas profesionales de artes plásticas y diseño de grado superior, a las enseñanzas deportivas de grado superior y aquellas otras equivalentes que establezca el Gobierno o la Comunidad Autónoma.

Artículo 9. Reconocimiento al amparo del artículo 46.2.i de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades

Los/as estudiantes podrán obtener reconocimiento académico en créditos por la participación en actividades universitarias culturales, deportivas, de representación estudiantil, solidarias y de cooperación hasta un máximo de seis créditos del total del plan de estudios cursado.

DISPOSICIÓN ADICIONAL

La facultad de interpretación de la presente normativa es competencia exclusiva del Vicerrectorado de Titulaciones y Convergencia Europea

En lo no regulado en esta norma se atenderá a lo dispuesto en las normas de gestión académica .

DISPOSICIONES TRANSITORIAS

1.- La validación de estudios para titulaciones no adaptadas al EEES continuará rigiéndose por la normativa de dichos estudios.

2.- La validación de estudios en los Programas Oficiales de Posgrado desarrollados al amparo del Real Decreto 56/2005, de 21 de enero, y modificado por el Real Decreto 1509/2205, de 16 de diciembre se regulará por la presente normativa y por su regulación específica.

DISPOSICIÓN FINAL

La presente normativa entrará en vigor al día siguiente de su aprobación por el Consello de Gobierno de la Universidad de Vigo.

- NORMATIVA DE RECONOCIMIENTO Y TRANSFERENCIA DE CRÉDITOS PARA TITULACIONES ADAPTADAS AL ESPACIO EUROPEO DE EDUCACIÓN SUPERIOR (EEES) MEDIANTE LA QUE SE DESARROLLA EL RD 1393/2007, DEL 29 DE OCTUBRE, MODIFICADO POR EL RD 861/2010, DEL 2 DE JULIO, POR EL QUE SE ESTABLECE LA ORDENACIÓN DE LAS ENSEÑANZAS UNIVERSITARIAS OFICIALES - UNIVERSIDAD DE A CORUÑA (Aprobada por Consello de Gobierno del 30/06/2011; Modificada por RR 25/05/2012; Modificada por RD 43/2015 (02/02/2015); Texto consolidado)

PREÁMBULO

La Ley Orgánica 4/2007, del 12 de abril, que modifica la Ley orgánica 6/2001, de 21 de diciembre, de universidades (BOE 13 de abril) le da nueva redacción al artículo 36 de la LOU, para pasar a titularse Validación o adaptación de estudios, validación de experiencia, equivalencia de títulos y homologación de títulos extranjeros. En la nueva configuración de la LOU se sigue manteniendo la existencia de criterios a los que se deben ajustar las universidades, pero en este caso estos criterios van a ser fijados por el Gobierno, a diferencia del sistema actual, en que la competencia le corresponde al Consejo de Coordinación Universitaria.

La LOU introduce también cómo importante novedad la posibilidad de validar, para efectos académicos, la experiencia laboral o profesional, siguiendo los criterios y las recomendaciones de las declaraciones europeas para 'dar adecuada respuesta a sus necesidades de formación a lo largo de toda la vida y abrirse a quien, a cualquier edad, deseen acceder a su oferta cultural o educativa', como señala su exposición de motivos.

En desarrollo de la LOU en el Real Decreto 1393/2007, del 29 de octubre, que establece la ordenación de las enseñanzas universitarias oficiales, modificado por el RD 861/2010, del 2 de julio, aparece un nuevo sistema denominado reconocimiento y transferencia de créditos. Este Real Decreto en su introducción y en el artículo 6, en el artículo 12.8, en el artículo 13 y en la disposición adicional cuarta desarrolla estos conceptos. Así mismo dice que, con el objeto de hacer efectiva la movilidad de los estudiantes, las universidades elaborarán y publicarán su normativa de reconocimiento y transferencia de créditos, sujeto a los criterios generales del dicho Real Decreto.

En la memoria para solicitar la verificación de títulos oficiales (anexo I del Real Decreto 1393/2007) deberá constar el sistema existente en la Universidad de A Coruña (UDC) de transferencia y reconocimiento de créditos.

Por todo el anterior, es necesario regular el procedimiento que se debe seguir en la UDC.

La definición del modelo de reconocimiento no solo es de importancia capital para los alumnos que desean acceder a cada titulación, sino que tiene sus raíces en la propia definición de la titulación, que debe tener en cuenta los posibles accesos desde otras titulaciones tanto españolas como extranjeras.

La propuesta de regulación tiene las siguientes bases:

- Un sistema de reconocimiento basado en créditos (no en disciplinas) y en la acreditación de competencias.
- La posibilidad de establecer, con carácter previo a solicitud de los alumnos, tablas de reconocimiento globales entre titulaciones, que permitan una rápida resolución de las peticiones sin necesidad de informes técnicos para cada solicitud y disciplinas.
- La posibilidad de especificar estudios extranjeros susceptibles de obtener reconocimiento, toda vez que se acceda a los estudios de grado, máster o doctorado.
- La posibilidad de reconocer otros estudios y competencias profesionales acreditadas.

Artículo 1: Reconocimiento y transferencia de créditos

La unidad de reconocimiento y de transferencia serán los créditos, que integran disciplinas, materias o módulos completos. En el expediente del alumno figurarán como créditos reconocidos o transferidos. Los créditos reconocidos se tendrán en cuenta para los efectos de considerar realizados los créditos de la titulación.

El reconocimiento de créditos supone la aceptación por la UDC de los créditos que, de ser obtenidos en enseñanzas oficiales, en la UDC o en otra universidad, son computados en otras enseñanzas distintas para los efectos de la obtención de un título oficial. Así mismo, podrán ser objeto de reconocimiento los créditos cursados en otras enseñanzas superiores oficiales o en enseñanzas universitarias conducentes a la obtención de otros títulos a la que se refiere el artículo 34.1 de la Ley orgánica 6/2001, del 21 de diciembre, de universidades.

La experiencia laboral y profesional acreditada podrá también ser reconocida en forma de créditos que computarán para los efectos de la obtención de un título oficial, siempre que esta experiencia esté relacionada con las competencias inherentes al referido título.

En todo caso no podrán ser objeto de reconocimiento los créditos correspondientes a los trabajos de

fin de grado y máster.

El número de créditos que sean objeto de reconocimiento a partir de experiencia profesional o laboral y de enseñanzas universitarias no oficiales no podrá ser superior, en su conjunto, al 15 por ciento del total de créditos que constituyen el plan de estudios. El reconocimiento de estos créditos no incorporará su calificación por lo que no computarán para los efectos de baremación del expediente.

No obstante lo anterior, los créditos procedentes de títulos propios podrán, excepcionalmente, ser objeto de reconocimiento en un porcentaje superior al señalado en el párrafo anterior o, si es el caso, ser objeto de reconocimientos en su totalidad siempre que el correspondiente título propio se extinguiera y fuera substituido por un título oficial.

Para estos efectos, la memoria de verificación del nuevo plan de estudios cumplirá los requisitos que están establecidos en los apartados 4 y 5 del artículo 6 del RD 1393/2007, modificado por el RD 861/2010, del 2 de julio.

La transferencia de créditos supone que, en los documentos académicos oficiales acreditativos de las enseñanzas seguidas por cada estudiante, se incluirá la totalidad de los créditos obtenidos en enseñanzas oficiales cursadas con anterioridad, en la UDC o en otra universidad y que no conducirán a la obtención de un título oficial.

Todos los créditos que obtenga el estudiante en enseñanzas oficiales cursadas en cualquier universidad: los que supere para la obtención del correspondiente título, los reconocidos y los transferidos, serán incluidos en su expediente académico y reflejados en el Suplemento Europeo al Título.

Artículo 2: criterios de reconocimiento de créditos.

Los criterios generales de reconocimiento de créditos son aquellos que fije el Gobierno. La UDC, mediante esta normativa y las resoluciones rectorales que la desarrollen, establecerá el sistema para el reconocimiento de estos créditos. Las titulaciones podrán proponer criterios específicos adecuados a cada titulación que serán aprobados por resolución rectoral. En todo caso deberán respetarse las siguientes reglas básicas para las enseñanzas de grado:

- a) Siempre que la titulación a la que se pretende acceder pertenezca a la misma rama de conocimiento serán objeto de reconocimiento, por lo menos, el 15 por ciento de la totalidad de los créditos del título correspondientes a las materias de formación básica de dicha rama.
- b) Serán también objeto de reconocimiento los créditos obtenidos en aquellas otras materias de formación básica pertenecientes a la rama de conocimiento del título al que se pretende acceder.
- c) El resto de los créditos: los cursados en otras enseñanzas superiores oficiales o en enseñanzas universitarias conducentes a la obtención de otros títulos, a la que se refiere el artículo 34.1 de la Ley orgánica 6/2001, de 21 de diciembre, de universidades, podrán ser reconocidos por la UDC teniendo en cuenta la adecuación entre las competencias y los conocimientos adquiridos, bien en otras materias o enseñanzas cursadas por el estudiante o bien asociados a una experiencia profesional previa y los previstos en el plan de estudios o que tengan carácter transversal.
- d) El reconocimiento de créditos por la participación en actividades universitarias culturales, deportivas, de representación estudiantil, solidarias y de cooperación, a que hace mención el artículo 12.8 del Real decreto 1393/2007 seguirá el procedimiento establecido por el acuerdo del Consejo de Gobierno del 13 de noviembre de 2008.

Artículo 3: sistema y procedimiento para el reconocimiento y la transferencia de créditos.

3.1. Para determinar el reconocimiento de créditos correspondientes a materias no recogidas en los apartados a) y b) del artículo 2 se tendrán en cuenta los estudios cursados, la experiencia laboral y profesional acreditada y su correspondencia con los objetivos y competencias que establece el plan de estudios para cada módulo, materia o disciplina. La universidad dará validez, mediante el acto de reconocimiento, a que el alumno tiene acreditadas competencias de la titulación y el cumplimiento de parte de los objetivos de esta en los términos definidos en el EEES.

3.2. Para estos efectos, cada centro establecerá tablas de equivalencia entre estudios cursados en otras universidades y aquellos que le podrán ser reconocidos en el plan de estudios de la propia

universidad. En estas tablas se especificarán los créditos que se reconocen y, de ser el caso, las disciplinas, las materias o los módulos equivalentes. Si el reconocimiento no es total, se indicarán los requisitos necesarios para establecer su superación completa.

Igualmente se establecerán tablas de equivalencia entre titulaciones correspondientes a ordenaciones de enseñanzas anteriores al Real decreto 1393/2007 y las titulaciones correspondientes a esta nueva ordenación.

Las tablas de equivalencia entre titulaciones, que podrán ser aprobadas de forma parcial o en su totalidad, según el caso, se aprobarán por resolución rectoral por propuesta de la Junta de Centro o comisión en que delegue. Se deberá tener en cuenta que en el caso de ser aprobadas de forma parcial podrán seguir siendo desarrolladas para cada caso concreto; pero cualquier modificación deberá ser aprobada por resolución rectoral siguiendo el procedimiento establecido de forma general.

Para el reconocimiento de créditos cursados en otras enseñanzas superiores oficiales, o en enseñanzas universitarias conducentes a la obtención de otros títulos y por una experiencia laboral o profesional acreditada, se atenderá a lo que establezca cada memoria verificada de su respectivo plan de estudios o, si es el caso, a las normas aprobadas por la Comunidad Autónoma o por la Universidad.

3.3. La UDC podrá reconocer directamente o mediante convenios, titulaciones extranjeras que den acceso a titulaciones oficiales de la UDC o establecer en esos convenios el reconocimiento en parte de estudios extranjeros. La UDC dará adecuada difusión de estos convenios.

3.4. Al alumno se le comunicarán los créditos reconocidos y las disciplina/s o materia/s a que correspondan, si es el caso, así como el número de créditos necesarios y las disciplina/s o materia/s que le restan para la obtención del título, según las competencias acreditadas y según los estudios de origen del alumnado. También se podrá especificar la necesidad de realizar créditos de formación adicional con carácter previo al reconocimiento completo de módulos, materias o disciplinas. Los créditos reconocidos se consignarán en el expediente junto con la calificación obtenida en el origen.

Esta calificación de origen podrá incorporarse a una disciplina/materia o disciplinas/materias de destino en el expediente del alumno; además también podrá optarse por consignar el término “reconocida” en aquella materia/s o disciplina/s en los casos que así corresponda, bien por no existir calificación de origen, bien por tratarse de un reconocimiento de créditos asociados a materias o disciplinas sin relación entre las competencias inherentes a estas, así como en otros casos que quedan a criterio de los órganos competentes en la resolución de estos procedimientos.

Cuando se reconozcan créditos correspondientes a varias materias con notas numéricas por créditos correspondientes a una materia, se le consignará a la materia reconocida la nota numérica resultante de aplicar la fórmula prevista en el apartado 3 del artículo 5 del Real Decreto 1125/2003: “suma de los créditos obtenidos por el alumno multiplicados cada uno de ellos por el valor de las calificaciones que correspondan, y dividida por el número de créditos totales obtenidos por el alumno”.

3.5. El procedimiento se iniciará por instancia de parte, salvo lo previsto en el párrafo 3.3, en el centro en que el alumno va a iniciar o continuar los estudios en que pretende reconocer créditos, mediante la presentación de una instancia, dirigida al decano/la, director/la del centro, en que figurarán sus datos personales, así como los estudios de que procede y aquellos que desea reconocer.

3.6. Se desconcentrará en los decanos/las, directores/las de centro las siguientes competencias:

a) El reconocimiento de los créditos de materias recogidas en los apartados a) y b) del artículo 2 de esta normativa o aquellos otros que consten en las tablas de equivalencia. La solicitud, una vez revisada por la Administración del centro, se resolverá en el plazo establecido en la Normativa de gestión académica correspondiente a cada curso.

b) En el resto de los casos el decano/la, director/la, tras la revisión de la solicitud por la Administración del centro y con el informe vinculante de la Junta de Centro (o de la Comisión en que tenga delegadas esas competencias), resolverá las solicitudes en el plazo establecido en la Normativa gestión académica correspondiente a cada curso.

3.7. En lo que corresponde a la transferencia de créditos, todos los créditos obtenidos en enseñanzas oficiales cursadas en la UDC o en otra universidad del EEES serán objeto de incorporación al expediente del alumno, tras la petición de este, mediante la presentación de una instancia dirigida al

decano/la o director/la del centro, en que figurarán sus datos personales, así como los estudios de que procede y aquellos que desea transferir. La solicitud de transferencia de créditos se resolverá por el mismo procedimiento establecido en la letra b) del apartado anterior.

3.8. La instancia a que se refieren los puntos 3.5 y 3.7 vendrá acompañada de la documentación que proceda, según los siguientes casos:

Estudios cursados en centros universitarios españoles o en otros centros que impartan enseñanzas superiores oficiales:

Para estudios universitarios:

- Certificación académica oficial, en que consten las materias/disciplinas aprobadas y las calificaciones obtenidas en cada una de ellas, así como el plan de estudios realizado. Así mismo deberá figurar el número de créditos correspondiente a cada materia/disciplina o en su defecto deberá presentarse una fotocopia del plan de estudios cursado, debidamente firmada y sellada por el centro de que proceda el alumno.

Para estudios correspondientes a enseñanzas superiores oficiales:

- Certificación académica oficial, en que consten las materias/disciplinas aprobadas y las calificaciones obtenidas en cada una de ellas, así como el plan de estudios realizado.

Estudios cursados en centros extranjeros:

- Certificación acreditativa del nivel y clase de estudios que se pretende reconocer.
- Así mismo, deberá figurar el número de créditos correspondiente a cada materia/disciplina o en su defecto deberá presentarse una fotocopia del plan de estudios cursado, debidamente firmada y sellada por el centro de que proceda el alumno.
- DNI o pasaporte.
- Todos los documentos deberán ser oficiales, traducidos al gallego o castellano, expedidos por las autoridades competentes y legalizados por vía diplomática si fuese el caso (será suficiente con que conste la “Apostilla de la Haya” en aquellos casos pertenecientes a países que tengan suscrito el correspondiente convenio).

3.9. Contra las resoluciones de reconocimiento o transferencia de créditos previstas en los puntos anteriores se podrá interponer un recurso de alzada ante el rector en el plazo de un mes, que contará a partir de que se efectúe su notificación, quien resolverá tras el informe de la Comisión de Plan de Estudios delegada del Consejo de Gobierno de la UDC, que tendrá carácter vinculante.

Experiencia laboral o profesional acreditada:

- Deberá estar relacionada con las competencias inherentes a cada título. Se acreditará conforme al procedimiento previsto en cada memoria verificada correspondiente a cada plan de estudios y mediante la entrega de la documentación que se requiera.

Artículo 4: reconocimiento de otros estudios

4.1. El procedimiento y los criterios para lo reconocimiento parcial de estudios correspondientes a ordenaciones académicas anteriores a la establecida en el Real decreto 1393/2007 (diplomado, licenciado, arquitecto, ingeniero o equivalentes) en titulaciones adaptadas al EEES se seguirá lo que establece esta normativa.

Artículo 5: Precios por servicios académicos

Por el reconocimiento de créditos de estudios realizados se abonarán, si fuera el caso, los precios que para cada curso académico sean fijados por el correspondiente Decreto de la Xunta de Galicia. Los precios se harán efectivos en los centros en que el alumno vaya a iniciar o continuar los estudios según el procedimiento vigente en materia de pago de precios por servicios académicos universitarios, en el plazo máximo de diez días que cuentan a partir de la recepción de la notificación de la correspondiente resolución.

DISPOSICIÓN ADICIONAL

Se faculta al rector o a el/la vicerrector/la en quien delegue para el desarrollo de esta normativa.

DISPOSICIÓN TRANSITORIA

La validación de estudios y la adaptación de planes estudios para titulaciones no adaptadas al EEES seguirán rigiéndose por la normativa de estos estudios.

DISPOSICIÓN DEROGATORIA

Queda derogada la Normativa de reconocimiento y transferencia de créditos para titulaciones adaptadas al espacio europeo de educación superior (EES) aprobada por el Consejo de Gobierno de la UDC en su sesión del 22 de mayo de 2008.

DISPOSICIÓN FINAL

La presente normativa entrará en vigor al día siguiente de su aprobación por el Consello de Gobierno de la Universidad.

4.5. Curso de adaptación para titulados

Se trata de un título nuevo, inexistente en el SUG, por lo que no procede un curso de adaptación.

5. PLANIFICACIÓN E LA ENSEÑANZA

5.1. Distribución del plan de estudios en créditos ECTS por tipo de materia. Esquema general del plan de estudios:

Tipo de materia/asignatura	Créditos a cursar	Créditos ofertados
Obligatorias	51	51
Optativas	9	15
Prácticas externas (si son OB)	15	15
Trabajo fin de Máster	15	15
Total	90	96

Explicación general de la planificación del plan de estudios

La estructura de las enseñanzas se ha articulado de acuerdo a los objetivos del Máster y las competencias que deberán adquirir los/las estudiantes en el transcurso del mismo. En las páginas siguientes se explican las líneas generales del plan de estudios propuesto. Para una gestión más eficiente las asignaturas se han agrupado por módulos, y la distribución por módulos es la siguiente:

- Módulo de Gestión y Legislación en Cibereguridad, de carácter obligatorio. Este módulo consta de 9 ECTS, repartidos en dos asignaturas de 6 y 3 ECTS, respectivamente.
- Módulo de Fundamentos de Ciberseguridad, de carácter obligatorio, compuesto por cuatro materias de 6 ECTS cada una.
- Módulo de Técnicas de Ciberseguridad. El módulo consta de cuatro materias, tres de ellas de 5 ECTS y una de 3 ECTS. El propósito de estas materias es completar la formación de los alumnos aplicando los conocimientos del módulo de Fundamentos a la protección de sistemas.
- Módulo de Formación Complementaria, de carácter obligatorio, pero formado por asignaturas optativas de 3 ECTS cada una.
- Módulo de Prácticas en Empresa y trabajo de fin de Máster, obligatorio, de 30 ECTS. Dentro de este módulo se contempla el reconocimiento de experiencia profesional. Corresponden 15 ECTS a la asignatura Prácticas en Empresa y otros 15 ECTS al Trabajo de Fin de Máster.

El cuadro siguiente resume los módulos y materias de que consta el plan de estudios.

A. Plan de Estudios

Módulo	Asignaturas	ECTS	Carácter	Cuatrimestre	Curso
Gestión y legislación en ciberseguridad	Conceptos y leyes en ciberseguridad	3	Obligatorio	2	1
	Gestión de la seguridad de la información	6	Obligatorio	1	1
Fundamentos de ciberseguridad	Seguridad de la información	6	Obligatorio	1	1
	Seguridad en comunicaciones	6	Obligatorio	1	1
	Seguridad de aplicaciones	6	Obligatorio	1	1
	Redes seguras	6	Obligatorio	1	1
Técnicas de ciberseguridad	Fortificación de sistemas operativos	5	Obligatorio	2	1
	Tests de intrusión	5	Obligatorio	2	1
	Análisis de <i>malware</i>	5	Obligatorio	2	1
	Seguridad como negocio	3	Obligatorio	2	1
Formación complementaria	Seguridad en dispositivos móviles	3	Optativo	2	1
	Análisis forense de equipos	3	Optativo	2	1
	Seguridad ubicua	3	Optativo	2	1
	Gestión de incidentes	3	Optativo	2	1
	Ciberseguridad en entornos industriales	3	Optativo	2	1
Prácticas en empresa y trabajo de fin de máster	Prácticas en empresa	15	Prácticas externas	1	2
	Trabajo de fin de máster	15	Trabajo de fin de máster	1	2

Con esta estructura y estas asignaturas se obtendría el título de Máster en Ciberseguridad con 90 ECTS. Para completar la titulación, un/a alumno/a habrá de cursar todos los módulos obligatorios y 3 materias (9 ECTS) a elegir libremente de entre las del módulo de Formación Complementaria. El plan de estudios no contempla especialidades pero, como se ve, reserva 9 ECTS para que los/las estudiantes particularicen su formación en aquellas áreas específicas que resulten de su mayor interés.

Todos los módulos tienen una carga de créditos múltiplo de 3, lo que facilita el equilibrio entre módulos y cuatrimestres y la organización temporal de los estudios. Los resultados obtenidos por el alumno en cada materia del plan de estudios se calificarán en una escala numérica de 0 a 10 puntos.

La distribución cuatrimestral/semestral de módulos y materias se expone en el siguiente esquema y en el cuadro que después lo acompaña.

Cuatrimestre 1	Cuatrimestre 2
Módulo de gestión y legislación en ciberseguridad (6 ECTS)	Módulo de técnicas de ciberseguridad (18 ECTS)
Módulo de fundamentos de ciberseguridad (24 ECTS)	Módulo de gestión y legislación en ciberseguridad (3 ECTS)
	Módulo de formación complementaria (9 ECTS)

Cuatrimestre 3
Módulo de prácticas en empresa (15 ECTS)
Módulo de trabajo de fin de máster (15 ECTS)

La formación presencial, por tanto, se concentra en el primer año del programa, mientras que el tercer cuatrimestre se dedica en exclusiva a las prácticas en empresa y a la realización del trabajo fin de máster. Con ello se persigue facilitar el paso de los/las titulados/as al mercado laboral y su dedicación preferente en la última etapa formativa al trabajo de fin de máster.

En las fichas de cada asignatura se expondrán los requisitos necesarios, de existir, para cursarla, así como los idiomas de impartición. Para aquellas materias que se impartan total o parcialmente en inglés:

1. Estarán capacitados de forma automática todos los miembros del PDI que acrediten un nivel de inglés igual o equivalente al B2 del MCERL o bien que acrediten haber impartido docencia en inglés en una institución de educación superior durante por lo menos dos cursos académicos consecutivos o tres alternos.

2. El PDI que no disponga de estas acreditaciones, debe realizar una prueba en el Centro de Lenguas que acredita unas competencias mínimas para la docencia en inglés (HELA: *Higher Education Lecturing Accreditation*).

En cualquier caso, son de aplicación las normas de permanencia vigentes en la Universidad de Vigo y en la Universidade da Coruña en lo que se refiere a los estudios de máster.

B. Itinerario a tiempo parcial

Los estudiantes a tiempo parcial deberán completar un programa de estudios en tres años académicos, según establece el plan que se detalla a continuación.

Primer año – primer cuatrimestre: se cursarán 18 ECTS de las materias *Gestión de la seguridad de la información* (6 ECTS), *Seguridad de la información* (6 ECTS) y *Seguridad en comunicaciones* (6 ECTS).

Primer año – segundo cuatrimestre: se cursarán 13 ECTS compuestos por las materias *Fortificación de sistemas operativos* (5 ECTS), *Conceptos y leyes en la ciberseguridad* (3 ECTS) y *análisis de malware* (5 ECTS).

Segundo año – primer cuatrimestre: se cursarán los 12 ECTS de las materias *Seguridad de aplicaciones* (6 ECTS) y *Redes seguras* (6 ECTS).

Segundo año – segundo cuatrimestre: se cursarán los 17 ECTS de las materias *Tests de intrusión* (5 ECTS), *Seguridad como negocio* (3 ECTS) y tres materias optativas (en total, 9 ECTS).

Tercer año – primer cuatrimestre: *Prácticas en empresa* (15 ECTS)

Tercer año – segundo cuatrimestre: *Trabajo de fin de máster* (15 ECTS)

C. Procedimientos de coordinación docente vertical y horizontal del plan de estudios

Las labores de coordinación horizontal y vertical serán realizadas por el/la coordinador/a del Máster, por la Comisión Académica del Máster y por los coordinadores de módulo y especialidad (figuras que nombrará anualmente la Comisión Académica). La persona coordinadora del Máster y la Comisión Académica se encargan de que no haya solapamientos entre las asignaturas. Las personas que coordinan los módulos se encargan básicamente de la organización secuencial del contenido de las asignaturas de su módulo y de organizar las actividades docentes en conexión con todos los docentes que participan en ella (coordinación horizontal). Para ello, se reúnen con los profesores de cada asignatura para decidir cómo se va a impartir, para recabar el material necesario, para recopilar los trabajos a realizar durante la evaluación continua y las preguntas para el examen final. Una vez finalizada la asignatura, los coordinadores informan al coordinador/a del Máster y le comunican las posibles incidencias que hayan tenido lugar. Las labores de coordinación vertical (organización entre materias de distintos módulos) corresponden a la Comisión Académica, como órgano de supervisión común de todas las actividades del Máster, y a las personas coordinadoras de los módulos implicados. Puesto que la estructura define 5 módulos, la coordinación vertical resulta efectiva y ágil. Las funciones de coordinación de los distintos módulos estarán convenientemente repartidas entre todos los centros que tomen parte en la docencia del Máster, no siendo imprescindible para la coordinación que las reuniones sean siempre presenciales. Por último, las decisiones de organización práctica del Máster (horarios de aulas, laboratorios, calendarios de exámenes y otras pruebas, conferencias, etc.) se trasladarán a la persona responsable de esta área (jefaturas de estudios) en cada uno de los

centros donde se desarrolle la docencia, para poder programarlas debidamente sin interferencia en la vida académica general de estos centros.

Al finalizar cada curso, la Comisión Académica del Máster se reunirá con los coordinadores de módulo para analizar el desarrollo del curso y determinar el grado de cumplimiento de los objetivos. Se analizarán los métodos empleados y los resultados alcanzados, se valorará la necesidad de realizar modificaciones en la organización académica, los sistemas de evaluación utilizados, el profesorado del máster, etc. En base a esta información se fijarán los objetivos para la siguiente edición del máster y las actividades a realizar que conformarán el plan de mejora.

LISTADO DE ASIGNATURAS POR COMPETENCIA

LISTADO DE COMPETENCIAS	Módulo de gestión y legislación	Módulo de fundamentos de ciberseguridad	Módulo de técnicas de ciberseguridad	Módulo de formación complementaria	Módulos de prácticas externas y TFM
	ASIGNATURAS				
CB1			AM, SN	AFE, CEI	PE, TFM
CB2	GSI	SI, SC, SA, RS	FSO, TI	SDM, AFE, SU, GI, CEI	PE, TFM
CB3	CLS, GSI			SDM, AFE, SU, GI, CEI	PE, TFM
CB4		SI, SC, RS	TI, SN	SDM, SU	PE, TFM
CB5		SI, SC, RS	FSO, TI	GI	PE, TFM
CG1	GSI	SC, RS	FSO, TI, AM	SDM, GI	PE, TFM
CG2	GSI	SA	FSO, TI	SDM, AFE, SU	PE, TFM
CG3		SC, RS	SN	CEI	PE, TFM
CG4			TI		PE, TFM
CG5		SC	FSO	SDM, SU, GI	PE, TFM
CG6			SN		PE, TFM
CE1		SI, SC			PE, TFM
CE2		SC, SA, RS	TI		PE, TFM
CE3	CLS			GI	PE, TFM
CE4		SI, SC, RS	FSO, TI	SDM, SU, CEI	PE, TFM

CE5	GSI				PE, TFM
CE6				SDM, AFE	PE, TFM
CE7	GSI	SA	TI	CEI	PE, TFM
CE8		SC, RS	FSO, AM		PE, TFM
CE9			SN	SDM, SU, GI	PE, TFM
CE10		SI			PE, TFM
CE11			AM, SN		PE, TFM
CE12		RS			PE, TFM
CE13	GSI	SA	AM		PE, TFM
CE14				GI	PE, TFM
CE15			SN	SDM, GI, CEI	PE, TFM
CE16			SN		PE, TFM
CE17				GI	PE, TFM
CE18	CLS				PE, TFM
CE19			SN		PE, TFM
CE20			SN		PE, TFM
CT1	CLS				PE, TFM
CT2					PE, TFM
CT3					PE, TFM
CT4					PE, TFM

CT5	GSI	SI	SN		PE, TFM
-----	-----	----	----	--	---------

LISTADO DE ASIGNATURAS POR COMPETENCIA

Máster en ciberseguridad	Competencias básicas					Competencias generales						Competencias específicas																				Competencias transversales						
Asignatura	CB1	CB2	CB3	CB4	CB5	CG1	CG2	CG3	CG4	CG5	CG6	CE1	CE2	CE3	CE4	CE5	CE6	CE7	CE8	CE9	CE10	CE11	CE12	CE13	CE14	CE15	CE16	CE17	CE18	CE19	CE20	CT1	CT2	CT3	CT4	CT5		
Conceptos y leyes en la ciberseguridad			X											X															X			X						
Gestión de seguridad de la información		X	X			X	X									X		X						X												X	X	
Seguridad de la información		X		X	X							X			X						X															X		
Seguridad en comunicaciones		X		X	X	X		X		X		X	X		X				X																	X		
Seguridad en aplicaciones		X						X					X					X						X												X		
Redes seguras		X		X	X	X		X					X		X				X				X													X		
Fortificación de sistemas operativos		X			X	X	X			X					X				X																	X		
Test de intrusión		X		X	X	X	X		X				X		X				X																		X	
Análisis de malware	X					X													X			X		X														
Seguridad como negocio	X			X				X			X									X		X					X	X			X	X				X	X	
Seguridad en dispositivos móviles		X	X	X		X	X			X					X		X			X							X									X		
Análisis forense de equipos	X	X	X				X										X																				X	
Seguridad ubicua		X	X	X			X			X					X					X																X		
Gestión de incidentes		X	X		X	X				X				X						X						X	X		X							X		
Ciberseguridad en entornos industriales	X						X	X							X				X					X			X									X		
Prácticas en empresa	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
Trabajo de fin de máster	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	

5.2. Movilidad: Planificación y gestión de la movilidad de los estudiantes propios y de acogida

PROCEDIMIENTO DE COORDINACIÓN DEL MÁSTER:

La gestión de las acciones de movilidad propia o ajena de los estudiantes será responsabilidad de la Comisión Académica del Máster y, en su caso, de la persona que esta designe, si lo considera oportuno, para la coordinación de todas las situaciones derivadas del envío y acogida de estudiantes, el establecimiento de convenios de colaboración y la definición de contratos de estudio y MoU (*Memorandums of Understanding*) entre las instituciones. Puesto que el máster es interuniversitario, la formulación y firma de los convenios habrá de preverse a tres bandas (la institución homóloga y las Universidades de Vigo y La Coruña, conjuntamente) . La persona que coordina la titulación será, a instancias de la comisión Académica, la persona representante ante todas las instituciones durante los procesos de colaboración.

ACCIONES DE MOVILIDAD:

En la Universidad de Vigo, la Escuela de Ingeniería de Telecomunicación mantiene una larga tradición de intercambio de estudiantes apoyados en los programas Erasmus/ISEP/SICUE, que gestiona a través de su Subdirección de Relaciones Externas en colaboración con la Oficina de Relaciones Internacionales de la Universidad. Grosso modo, sobre esta subdirección descansa la responsabilidad y el control académico de los alumnos locales que se van y de los extranjeros que acogemos. La gestión y supervisión de los alumnos que enviamos a otras universidades comienza por el proceso de selección de los candidatos, donde priman tanto su expediente académico como su dominio de la lengua remota si el país anfitrión no es de habla hispana. Seguidamente, y de forma individualiza, se analiza y diseña el contrato de estudios que nuestros alumnos realizarán en la universidad destino, comprobando la idoneidad de las equivalencias entre materias (contenidos) y la cantidad y la distribución de la carga de trabajo según el número de meses de estancia. Finalmente, aunque no menos importante, la Escuela también vela y presta apoyo continuado a nuestros alumnos una vez que se encuentran en su destino, tanto en los temas académicos (modificaciones de los contratos de estudio originales, etc.) como en los meramente administrativos, siendo muchas veces el medio de comunicación más rápido y sencillo para ellos ---por no estar físicamente con nosotros--- con la propia ORI.

En el Máster en Ciberseguridad, en concreto, se prevén como acciones de fomento de la movilidad de estudiantes las siguientes:

- Difusión y promoción de las oportunidades de movilidad estudiantil en el ámbito de la ciberseguridad a lo largo de Europa (programa Erasmus, acciones MCSA, posibles másteres y doctorados ITN, etc.), dentro del marco de acciones de colaboración universidad-empresa del programa H2020 de la UE.
- Establecimiento de nuevos convenios de colaboración académica e intercambio de estudiantes con universidades europeas (Telecom Paris SUD), orientados específicamente al envío y acogida de estudiantes de máster.
- Extensión del Plan de Internacionalización de la docencia, al que ya se ha acogido la Escuela de ingeniería de Telecomunicación para el caso del Máster en Ingeniería de Telecomunicación, al Máster en Ciberseguridad, con el fin de contar a medio plazo con una oferta formativa en inglés suficiente que permita

atraer a estudiantes extranjeros.

- Acciones individuales de promoción de la movilidad (presentaciones, ponencias, conferencias, estudios comparativas) por parte de la Cátedra Deloitte de Ciberseguridad de la Universidad de Vigo.

En la propuesta de titulación resulta relativamente fácil preservar su unidad e integridad dentro de un contrato de estudios de intercambio. Además, el tercer cuatrimestre (primero y único del segundo curso) concentra todos los contenidos con menor presencialidad (prácticas en empresas, trabajo de fin de máster). Estas características facilitarán la movilidad de los estudiantes. Si se cumplen las previsiones de establecimiento de convenios de colaboración con empresas del territorio nacional e internacional, y teniendo en cuenta que, tal como se ha diseñado el plan de estudios, el trabajo de fin de máster tiene una fuerte vocación aplicada a la resolución de problemas técnicos en empresas del sector, cabe esperar que se incremente la movilidad internacional y nacional de estudiantes. La Comisión Académica de Máster se ocupará de la gestión de los contratos de estudios/prácticas de los estudiantes que participen en programas de movilidad, velando por que la formación que reciban los alumnos sea adecuada.

CONVENIOS CON UNIVERSIDADES EXTRANJERAS:

En el caso de UVigo, la larga tradición de intercambio de estudiantes del centro se ve reflejada en el número de destinos (45 universidades de otros países europeos) que han acogido alumnos de la Escuela del Programa Erasmus durante los últimos cursos. El listado completo se encuentra en el apartado 7.2, en el que se detallan los convenios con Universidades, empresas e instituciones que permiten completar la formación de nuestros alumnos

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

La planificación, desarrollo y gestión de los convenios relativos al intercambio de profesores y estudiantes tanto de la Universidad de Vigo como extranjeros con otros centros de educación superior se realiza atendiendo, entre otros, a los siguientes criterios, programas de becas y ámbitos de actuación:

- La movilidad a nivel local y nacional se lleva a cabo mediante la negociación y firma de convenios de colaboración directa con instituciones, realizando las gestiones a través del servicio/vicerrectorado correspondiente y fomentando la cooperación con aquellos centros vinculados a la formación.
- La movilidad y los intercambios internacionales se gestionan a través de la Oficina de Relaciones Internacionales de la Universidad de Vigo y la Oficina de Relaciones Internacionales de la Universidade da Coruña. La planificación responde a dos ámbitos de actuación: movilidad entrante y saliente cara a Europa (Erasmus principalmente), y movilidad entrante y saliente hacia el resto de países (ISEP, estudiantes de convenio, programa de bolsas propias).

En relación a la movilidad de estudiantes con Europa se contempla la participación y la obtención de becas a través de los programas y acciones promovidas por la Comisión Europea y la Agencia Ejecutiva de Educación, Audiovisual y Cultura, especialmente el programa Erasmus+ (dentro del Programa de Aprendizaje y Formación Permanente: *Lifelong Learning Programme*), para lo cual se firman acuerdos bilaterales Sócrates-Erasmus+ plurianuales. Para la movilidad de profesores con Europa (tanto para los profesores de las universidades participantes, como para los visitantes de

universidades extranjeras) se prevén diversas actuaciones en el marco del programa Erasmus+ para el que se dispondrá de financiación: visitas OM y PV a universidades asociadas para preparar la movilidad de estudiantes y promover la firma de los acuerdos de cooperación y movilidad TS para impartir docencia. Esta movilidad TS es esencial para desarrollar la dimensión europea dentro de la propia universidad y entre las universidades europeas. El periodo para impartir docencia en el extranjero le permite a los docentes conocer otros sistemas universitarios diferentes y otro idioma, aportando una perspectiva europea a los cursos que siguen los estudiantes de la universidad anfitriona y de la universidad de origen, abriendo además nuevas posibilidades de cooperación y de realización de proyectos conjuntos entre instituciones de varios países.

Dentro del nuevo programa LLP se incluye la movilidad del PAS y se contemplan nuevas acciones dentro de la movilidad docente. La Universidad de Vigo participa también desde hace años en el programa europeo Jean Monnet que facilita el desarrollo en el mundo universitario de actividades académicas relacionadas con la integración europea, el estudio de la construcción de la Europa comunitaria, su desarrollo institucional, político, económico y social. Anualmente se promociona también la movilidad y recepción de docentes Jean Monnet expertos en políticas comunitarias, a través de los diferentes módulos aprobados y del Centro de Excelencia Europeo Jean Monnet de la Universidad de Vigo.

Para la movilidad con otros países no europeos, a través de la ORI, se promueve y tramita la firma de convenios marco y específico con universidades de otros países, como instrumento para facilitar la movilidad tanto de estudiantes como de docentes. En el caso de Estados Unidos, la ORI participa activamente en el programa ISEP de intercambio de estudiantes. Si nos referimos a las relaciones y movilidad con Iberoamérica, norte de África, etc. se fomenta la participación en las convocatorias anuales del Ministerio de Asuntos Exteriores y en concreto las acciones: Programa de Cooperación Interuniversitaria y becas MAEC-AECI. Los estudiantes podrán beneficiarse dentro de este tipo de movilidad con países no europeos del programa de becas de intercambio propias de la Universidad de Vigo (excepto los estudiantes ISEP), así como de la convocatoria de ayudas complementarias de la Xunta de Galicia para estudiantes que participan en movilidad no europea y en la convocatoria anual de becas internacionales de la Universidad de Vigo.

Por su parte, los estudiantes extranjeros podrán participar, entre otros, en los siguientes programas: programa de becas destinados a gallegos/as de origen gallego y a sus descendientes para la realización de estudios universitarios de la Consellería de Educación y Ordenación Universitaria de la Xunta de Galicia; becas MAEC-AECI que constituyen la oferta de formación a nivel postgrado del Ministerio de Asuntos Exteriores para estudiantes extranjeros y becas Alban de la Unión Europea y América Latina para la formación especializada superior para profesionales y futuros cuadros directivos latinoamericanos en centros de la Unión Europea.

En relación a las unidades de apoyo y sistemas de información para envío y acogida de estudiantes y profesores de intercambio, la Universidad de Vigo, a través de la Oficina de Relaciones Internacionales presta apoyo tanto a estudiantes, como a docentes propios y extranjeros, antes de su llegada y durante la estancia.

Con respecto a los estudiantes extranjeros, gestiona la aceptación de estos estudiantes, les remite las cartas de aceptación para que, si procede, puedan tramitar

sus visados, elabora anualmente una [Guía del estudiante extranjero](#)⁸ (trilingüe) y envía al domicilio de los interesados paquetes informativos sobre la Universidad de Vigo, con información sobre los diferentes campus y ciudades, recepción, visados, viaje, búsqueda de alojamiento, matrícula y posibilidades de estudios, etc.

La ORI es el punto de referencia de llegada de los estudiantes extranjeros de intercambio a la Universidad de Vigo. Este servicio se ocupa de asesorarlos y proporcionarles alojamiento y de organizar actividades y visitas culturales específicas para ellos. Con respecto a los docentes extranjeros, la ORI les facilita igualmente información sobre la Universidad de Vigo, realiza las reservas de alojamiento en hoteles o residencias concertadas y presta su apoyo en todas aquellas cuestiones que el docente necesite en colaboración con los responsables de relaciones internacionales en cada centro. Cuenta además con un programa propio de voluntariado y acogida de estudiantes de intercambio coordinado por la ORI y formado por aquellos estudiantes de la Universidad de Vigo que se ofrecen como voluntarios para ayudar a los estudiantes extranjeros que llegan por primera vez a la Universidad de Vigo. Para fomentar la integración de los estudiantes extranjeros de intercambio y que puedan mejorar su conocimiento del idioma, la ORI ha puesto en marcha una acción denominada “tándem de conversa” (más información en la [página web de la ORI](#),⁹ dentro de información para estudiantes extranjeros).

En resumen, la Oficina de Relaciones internacionales (ORI) centraliza, coordina y gestiona las actividades de cooperación internacional en el seno de la Universidad de Vigo; informa y asesora a la comunidad universitaria sobre los diferentes programas internacionales en el ámbito de la educación superior, especialmente los programas propios y los financiados por la Unión Europea o el Ministerio de Asuntos Exteriores, a través de la AECl; fomenta y gestiona la movilidad internacional de estudiantes y profesores, en especial en el marco de los programas Erasmus, ISEP, Jean Monnet, becas MAEC, PCI y programas propios; elabora y negocia acuerdos de cooperación internacional con otras instituciones de educación superior; propicia la movilización de la comunidad académica para su participación en la cooperación internacional, especialmente mediante la suscripción a redes institucionales internacionales y la presentación de proyectos de cooperación internacionales; asegura la presencia de la Universidad de Vigo en foros y encuentros de educación internacionales y participa activamente en las principales redes internacionales de universidades como el Grupo Compostela de Universidades, donde coordina el programa Stella de intercambio del personal de administración y servicios, o la EAIE (*European Association for International Education*). Para finalizar, comentar que en [página web de la ORI](#) se encuentra información disponible sobre todas las iniciativas y tareas descritas.

Con respecto a los estudiantes extranjeros, además de informarles de cuestiones académicas (planes de estudio, horarios,...) mucho antes de su llegada, facilitándoles así la elaboración de su precontrato de estudios, la Escuela se preocupa de hacerles más sencillas las tareas de matriculación en nuestro Centro, les da de alta en las diferentes plataformas de docencia virtual que utilizamos, facilita su inscripción en los grupos de prácticas de laboratorio, y, en definitiva, cualquier acción que les haga no sentirse solos entre nosotros y sí arropados en todo momento.

Descripción de los módulos/materias/asignaturas (Incluir ficha por asignatura o

⁸ http://www.uvigo.es/uvigo_es/administracion/ori/estranxeiros/guia/index.html

⁹ http://www.uvigo.es/uvigo_es/administracion/ori/

materia según esté definido el título)

En las páginas siguientes se describe en detalle el plan de estudios en su configuración módulo/asignatura, en fichas individualizadas. Previamente, en los párrafos siguientes, se detallan las actividades formativas y los procedimientos de evaluación, de modo que las fichas de cada asignatura enuncian actividades y evaluación en función de esta descripción, que ya no se repite individualmente.

ACTIVIDADES FORMATIVAS

En cada una de las asignaturas se estructuran las actividades formativas en dos apartados: clases de aula, que se corresponden a grupos de hasta 30 alumnos; y clases prácticas, en grupos de 15 alumnos. A continuación se muestran las posibles actividades formativas, y en cada ficha de asignatura se indica cuáles de ellas se emplean en la docencia de la propia asignatura:

- Sesión magistral: exposición de los contenidos de la asignatura; incluye exposición de conceptos; introducción de prácticas y ejercicios; y resolución de problemas y/o ejercicios en aula ordinaria.
- Seminarios y eventos: docencia en formato seminario, en el que el alumno participa muy activamente en la evolución de las clases profundizando en un tema específico, ampliándolo y relacionándolo con contenidos orientados a la práctica profesional; incluyendo la participación en eventos científicos y/o divulgativos, organizados o no en los propios centros; la organización de debates que permitan confrontar ideas y propuestas, guiados por docentes, tanto presenciales como online; y el estudio de casos/análisis de situaciones (análisis de un problema o caso real, con la finalidad de conocerlo, interpretarlo, resolverlo, generar hipótesis, diagnosticarlo y adentrarse en procedimientos alternativos de solución, para ver la aplicación de los conceptos teóricos en la realidad). Estas actividades pueden tener relacionada una carga de trabajo autónomo del alumno.
- Trabajos y/o proyectos: realización de trabajos, individuales o en grupo, para la resolución de un caso o un proyecto concreto, así como la presentación de los resultados por escrito y/o mediante una presentación que puede seguir diferentes formatos: oral, póster, multimedia. Se incluyen las metodologías integradas: aprendizaje basado en problemas (ABP), resolución de problemas de diseño propuestos por el profesor, enseñanza basada en proyectos de aprendizaje (PBL), *design thinking* (DT).
- Prácticas TIC: aplicación, a nivel práctico, de los conocimientos y habilidades adquiridos en las clases teóricas, incluyendo prácticas de laboratorio realizadas sobre ordenadores (simulaciones, análisis, procesados, etc.), ejercicios de programación, trabajos realizados online, etc.
- Estancia en empresas: Actividades realizadas en empresas o instituciones ajenas al centro de estudios, realizando actividades de ingeniería o de gestión de procesos, que contribuyen a completar la formación y/o a introducir al alumno en la práctica profesional. La actividad estará tutorizada por un profesor de la titulación y un profesional de la empresa.
- Trabajo autónomo del alumno: realización de las tareas previas preparatorias para la realización de las actividades docentes presenciales (lecturas y otros materiales, prácticas de laboratorio, estancias en empresas, etc.), y las tareas posteriores a la realización de las mismas: el análisis y estudio de los resultados prácticos, comparación con el análisis teórico y obtención de conclusiones; resolución de problemas y/o ejercicios de forma autónoma, actividades on-line,

estudio de los contenidos explicados en las sesiones presenciales, elaboración de informes sobre las actividades formativas desarrolladas, preparación del examen, preparación de discusiones de casos de estudio, etc.

- Atención personalizada: Actividad de encuentro entre profesor y alumno en la que se debaten y resuelven cuestiones o dudas relacionadas con los contenidos de la materia y con las competencias asociadas. Puede ser presencial u en línea.

EVALUACIÓN

La evaluación de las competencias adquiridas se llevará a cabo en cada asignatura. Esta evaluación podrá realizarse tanto de forma continua, con pruebas que se llevan a cabo a lo largo del curso, como en el formato más tradicional de evaluación concentrada en un examen.

Las pruebas correspondientes a la evaluación continua tendrán una ponderación de, al menos, un 30% de la calificación final. Los contenidos y la organización docente de cada asignatura determinan la ponderación máxima de la evaluación continua, que en muchos casos puede llegar al 100% de la calificación final. La guía docente de cada asignatura, elaborada anualmente, aprobada por las Juntas de Centro, y publicada en la web del Máster previamente al periodo de matriculación, detallará la ponderación exacta de las pruebas de evaluación continua en la calificación final. El resto de la calificación final podrá ser alcanzada mediante el examen final.

Tanto en su formato de evaluación continua, a lo largo del curso, como en la configuración de evaluación concentrada en un examen, podrá constar de distintos tipos de pruebas. En las fichas de cada asignatura, mostradas en las siguientes páginas, se indica el procedimiento de evaluación y el tipo de pruebas de las que puede constar, entre las que se enuncian a continuación:

- Pruebas de desarrollo: pruebas que incluyen preguntas abiertas sobre un tema. El alumnado debe desarrollar, relacionar, organizar y presentar los conocimientos que posee sobre la asignatura. La respuesta debe ser extensa. Pueden aplicarse a las pruebas de evaluación continua o al examen final.
- Pruebas objetivas (tipo test y/o preguntas cortas): pruebas que incluyen preguntas directas sobre un aspecto concreto. El alumnado debe responder de forma directa en virtud de los conocimientos que tenga sobre la asignatura. La respuesta es breve. Pueden aplicarse a las pruebas de evaluación continua o al examen final.
- Pruebas prácticas: pruebas que incluyen actividades de laboratorio y/o TIC, problemas o casos a resolver. Los alumnos deben dar respuesta a la actividad suscitada, plasmando de forma práctica los conocimientos teóricos y prácticos de la asignatura, utilizando de ser necesario el equipamiento o instrumentación de las prácticas de laboratorio de la asignatura. Pueden aplicarse a las pruebas de evaluación continua o al examen final.
- Pruebas orales: pruebas que incluyen preguntas abiertas y/o cerradas sobre un tema o aspecto concreto. Los alumnos deben responder de forma directa y oral a la pregunta. Pueden aplicarse a las pruebas de evaluación continua o al examen final.
- Trabajos y actividades: la evaluación de los trabajos, proyectos y actividades se llevará a cabo a partir de las memorias entregadas por los alumnos y de la valoración de las presentaciones que realicen. Las calificaciones se basarán en

rúbricas previamente definidas.

- Participación en actividades. Se refiere a actividades, presenciales o no, en las que se valora que el alumno participe, la actitud ante la tarea, su habilidad para llevarla a cabo, etc.
- Evaluación de prácticas en empresa: se realizará según la rúbrica aprobada previamente por la Comisión Académica de Máster. La evaluación se basará en la memoria de actividades y en el informe del tutor en la empresa.
 - o Memoria de actividades: El alumno entregará en la Escuela, al finalizar sus prácticas en la empresa, una memoria explicativa de las actividades realizadas durante las prácticas, especificando su duración, las unidades o departamentos de la empresa en que se realizaron, la formación recibida (cursos, programas informáticos, etc.), el nivel de integración dentro de la empresa y las relaciones con el personal.
 - o Informe del tutor en la empresa: El tutor de la empresa entregará un informe valorando aspectos relacionados con las prácticas realizadas por el alumno: puntualidad, asistencia, responsabilidad, capacidad de trabajo en equipo e integración en la empresa, calidad del trabajo realizado, etc.
- Evaluación del trabajo de fin de máster: se realizará según la rúbrica aprobada previamente por la Comisión Académica de Máster. La evaluación se basará en la decisión del tribunal nombrado al efecto, que tendrá en cuenta la opinión del tutor.

En cuanto al sistema de calificaciones: se expresará mediante calificación final numérica de 0 a 10 según la legislación vigente (Real Decreto 1125/2003 de 5 de septiembre; BOE 18 de septiembre).

Dado que, en cumplimiento de la normativa de la Universidad de Vigo, un alumno que no opte por evaluación continua debe poder optar a la calificación máxima mediante el examen final, en todas las fichas se especifica que el examen final podrá representar entre el 0% (para aquellas asignaturas en las que la evaluación continua pueda suponer el 100% de la nota final) y el 100% de la nota final.

Los idiomas oficiales en la comunidad autónoma de Galicia son el castellano y el gallego, por lo que serían las lenguas propias de la titulación. Además, debido al peso que el inglés tiene en el ámbito de la ciberseguridad a nivel internacional, se pretende que dicho idioma tenga un peso importante en las actividades formativas del Máster. Por ello, se garantiza que:

- Al menos en el 75% del material docente (presentaciones, ejercicios y problemas, manuales de prácticas, trabajos, etc.) y en el 30% de las actividades formativas de todas las asignaturas de la titulación se utilice el idioma inglés, garantizando que al menos dos de las materias obligatorias estén incluidas en dicho porcentaje.
- Y que los estudiantes que posean una certificación de nivel B2 puedan realizar el trabajo de fin de máster en inglés bajo la tutorización de un/a profesor/a acreditado, si así lo desean. Dicha certificación de idioma se les exigirá para la obtención del título y para la expedición del correspondiente certificado de estudios con constancia de haber realizado y defendido el TFM en inglés, e igualmente constará en el Suplemento Europeo al título de los/las titulados/as.

A medida que el número de profesores de las universidades participantes con docencia

en la titulación y con la correspondiente certificación de idiomas vaya aumentando, el porcentaje de asignaturas y actividades docentes en inglés podrá aumentar también.

Módulo Gestión y legislación en ciberseguridad	Asignatura Gestión de seguridad de la información
Curso	Primero
ECTS	6
Carácter	Obligatoria
Semestre	Primero
Lenguas en las que se imparte	Castellano / Gallego / Inglés
Competencias básicas y generales	(CB2) 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 (CB3) Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar 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 (CG1) Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación (CG2) Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones
Competencias específicas	(CE5) Diseñar, implantar y mantener un sistema de gestión de la seguridad de la información utilizando metodologías de referencia (CE7) Tener capacidad para realizar la auditoría de seguridad de sistemas e instalaciones, el análisis de riesgos derivados de debilidades de ciberseguridad y desarrollar el proceso de certificación de sistemas seguros (CE13) Capacidad para seleccionar y utilizar herramientas de auditoría de seguridad
Competencias transversales	(CT4) Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad (CT5) Tener capacidad para comunicarse oralmente y por escrito en inglés
Resultados de aprendizaje	• Conocer los conceptos fundamentales relacionados con la Gestión de la Seguridad de la Información: vulnerabilidad, amenaza, riesgo, contramedida, política de seguridad, plan de seguridad, auditoría • Conocer las diferentes metodologías de Gestión de Seguridad de la Información, comúnmente aceptadas • Conocer las herramientas propias para llevar a cabo tareas relacionadas con el análisis de riesgos y la auditoría de seguridad, así como saber cuáles son las más adecuadas a cada entorno
Contenidos	1. Fundamentos 2. Análisis de impacto en el negocio

	3. Análisis y gestión de riesgos 4. Plan de seguridad 5. Auditoría de seguridad. 6. Herramientas	
Observaciones		
Metodologías docentes (incluir listado)	Sesión magistral Prácticas TIC Trabajos y/o proyectos (individuales o en grupo) Trabajo autónomo del alumno Atención personalizada	
Actividades formativas		
Denominación de la actividad formativa	Horas	Presencialidad (%)
Sesión magistral y Resolución de problemas/ejercicios	63	33,3
Prácticas de laboratorio	87	24,1
Sistemas de evaluación		
Denominación del sistema de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de examen final)	15	100
Pruebas prácticas (con posibilidad de un examen final)	0	85
Evaluación de trabajos y actividades	0	85

Módulo Gestión y legislación en ciberseguridad	Asignatura Conceptos y leyes en ciberseguridad
Curso	Primero
ECTS	3
Carácter	Obligatoria
Semestre	Segundo
Lenguas en las que se imparte	Castellano / Gallego / Inglés
Competencias básicas y generales	(CB3) Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar 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
Competencias específicas	(CE3) Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información (CE18) Interpretar de forma adecuada las fuentes de información en el ámbito del derecho penal informático (leyes, jurisprudencia y doctrina) de ámbito nacional e internacional
Competencias transversales	(CT1) Capacidad para comprender el significado y aplicación de la perspectiva de género en los distintos ámbitos de conocimiento y en la práctica profesional con el objetivo de alcanzar una sociedad más justa e igualitaria. (CT5) Tener capacidad para comunicarse oralmente y por escrito en inglés.
Resultados de aprendizaje	• Dominio de los conceptos jurídicos relacionados con la cibercriminalidad • Dominio de los criterios de aplicación de los diferentes tipos penales relacionados con la criminalidad • Adquisición de la capacidad crítica sobre legislación, doctrina y jurisprudencia relativa a la criminalidad informática. • Capacidad de afrontar la resolución de casos prácticos con rigor científico
Contenidos	PARTE GENERAL: <i>Computer crime</i> y <i>cybercrime</i>: evolución del Derecho penal informático. Internet y libertad de expresión Problemáticas especiales de los delitos informáticos en el contexto de la parte general del Derecho penal La criminalidad informática desde el punto de vista criminológico PARTE ESPECIAL: Delitos contra la intimidad y la privacidad Delitos contra la libertad: <i>Stalking</i> y <i>Cyberstalking</i> Delitos contra la propiedad: estafa y fraudes informáticos; daños de datos y sistemas informáticos, Delitos contra la fe pública; falsificación electrónica. Delitos contra la propiedad intelectual La cibercriminalidad relacionada con menores: pornografía infantil, <i>child grooming</i>. Ciberterrorismo

Observaciones		
Metodologías docentes (incluir listado)	Sesión magistral Prácticas TIC Trabajos y/o proyectos (individuales o en grupo) Trabajo autónomo del alumno Atención personalizada	
Actividades formativas		
Denominación de la actividad formativa	Horas	Presencialidad (%)
Sesión magistral y resolución de problemas/ejercicios	48	33,3
Prácticas de laboratorio y proyectos individuales o en grupo	27	18,5
Sistemas de evaluación		
Denominación del sistema de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de un examen final)	30	100
Evaluación de trabajos y actividades	0	70

Módulo Fundamentos de ciberseguridad	Asignatura Seguridad de la información
Curso	Primero
ECTS	6
Carácter	Obligatoria
Semestre	Primero
Lenguas en las que se imparte	Castellano/gallego/ inglés (50%)
Competencias básicas y generales	(CB2) 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 (CB4) 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 (CB5) 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
Competencias específicas	(CE1) Conocer, comprender y aplicar los métodos de criptografía y criptoanálisis, los fundamentos de identidad digital y los protocolos de comunicaciones seguras (CE4) Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, sus sistemas operativos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información (CE10) Conocer los fundamentos matemáticos de las técnicas criptográficas, y comprender su evolución y tendencias futuras
Competencias transversales	(CT4) Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad (CT5) Tener capacidad para comunicarse oralmente y por escrito en inglés
Resultados de aprendizaje	Al finalizar esta materia los estudiantes debieran ser capaces de: • Comprender los mecanismos básicos que se esconden tras los algoritmos de cifrado simétrico en bloque, y contrastarlos con los utilizados en los cifradores de flujo. • Explicar qué son las funciones hash, qué papel juegan en el ámbito de la seguridad de la información, y, en particular, cómo se utilizan para confirmar la inviolabilidad (integridad) de los datos. • Explicar los fundamentos que hay detrás de los algoritmos de cifrado asimétrico, sus ventajas/desventajas con respecto al cifrado simétrico, y las aplicaciones de sus diferentes implementaciones (RSA, Diffie-Hellman, DSS, ECC). • Describir en qué consisten los sistemas PKI (infraestructura de clave pública), y cualquier concepto relacionado con los certificados digitales y su estructura/uso/gestión. • Describir en qué consisten los mecanismos/sistemas de

	firma y sobre digital. • Comprender la importancia de los generadores de números aleatorios en el ámbito de la criptografía. • Manejar herramientas criptográficas para el cifrado, autenticación y firma digital de la información, y para la creación de certificados y autoridades de certificación. • Evaluar cuál es la solución más adecuada (tipo, algoritmo, longitud de clave, etc.) para implantar en el sistema que tengan que administrar.	
Contenidos	Confidencialidad, integridad y autenticación. Clasificación de los algoritmos de cifrado. Confidencialidad de la información mediante cifrado simétrico. Autenticación de mensajes y funciones Hash. Cifrado de clave pública. Firmas digitales. Gestión de claves. Generación de números aleatorios.	
Observaciones		
Metodologías docentes (incluir listado)	Sesión magistral Prácticas TIC Trabajos y/o proyectos (individuales o en grupo) Trabajo autónomo del alumno Atención personalizada	
Actividades formativas		
Denominación de la actividad formativa	Horas	Presencialidad (%)
Sesión magistral y Resolución de problemas/ejercicios	63	33,3
Prácticas de laboratorio y Proyectos individuales o en grupo	87	24,1
Sistemas de evaluación		
Denominación del sistema de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Pruebas de desarrollo objetivos y resolución de problemas y/o ejercicios (con posibilidad de un examen final)	15	100
Pruebas prácticas (con posibilidad de un examen final)	0	85
Evaluación de trabajos y actividades	0	85

Módulo Fundamentos de ciberseguridad	Asignatura Seguridad en comunicaciones
Curso	Primero
ECTS	6
Carácter	Obligatoria
Semestre	Primero
Lenguas en las que se imparte	Castellano/gallego/inglés
Competencias básicas y generales	(CB2) 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 (CB4) 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 (CB5) 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) Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación (CG3) Capacidad para el razonamiento crítico y la evaluación crítica de cualquier sistema de protección de la información, cualquier sistema de seguridad de la información, de la seguridad de las redes y/o los sistemas de comunicaciones (CG8) Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos
Competencias específicas	(CE1) Conocer, comprender y aplicar los métodos de criptografía y criptoanálisis, los fundamentos de identidad digital y los protocolos de comunicaciones seguras (CE2) Conocer en profundidad las técnicas de ciberataque y ciberdefensa (CE4) Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, sus sistemas operativos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información (CE8) Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad
Competencias transversales	(CT4) Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad. (CT5) Tener capacidad para comunicarse oralmente y por escrito en inglés.
Resultados de aprendizaje	Al finalizar esta materia los estudiantes: • Conocerán en detalle los protocolos de red que aportan seguridad a la transmisión de la información, y las implicaciones derivadas del lugar que ocupan dentro de la arquitectura en que se organiza el software de comunicaciones.

	• Comprenderán que otros protocolos, siendo auxiliares (no relativos al mundo de la seguridad), presentan vulnerabilidades explotables; y podrán describir los ataques más comunes que tratan de aprovecharlas (mitm, suplantación de DHCP/DNS, DoS, SSL-Stripping, ...), y sus posibles contramedidas. • Sabrán identificar qué solución/protocolo es el adecuado para asegurar un entorno determinado: seguridad en LAN (802.1X), acceso inalámbrico (EAPoW, WPA/WPA2), seguridad extremo a extremo (IPSEC en modo transporte, TLS/SSL), conexiones punto a punto (PPP, IPSEC en modo túnel), etc. • Conocerán las soluciones que se esconden tras ciertos servicios de red y/o aplicaciones universalmente utilizadas (DNSSEC, S/MIME, HTTPS, SSH...). • Serán capaces de configurar las diferentes herramientas (paquetes software) que los distintos sistemas operativos/plataformas nos aportan para activar la seguridad en las comunicaciones.	
Contenidos	Seguridad en capa física y de enlace. Seguridad en capa de red. Seguridad en capa de transporte. Seguridad en capa de aplicación.	
Observaciones		
Metodologías docentes (incluir listado)	Sesión magistral Prácticas TIC Trabajos y/o proyectos (individuales o en grupo) Trabajo autónomo del alumno Atención personalizada	
Actividades formativas		
Denominación de la actividad formativa	Horas	Presencialidad (%)
Sesión magistral y Resolución de problemas/ejercicios	63	33,3
Prácticas de laboratorio y Proyectos individuales o en grupo	87	24,1
Sistemas de evaluación		
Denominación del sistema de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de un examen final)	15	100
Pruebas prácticas (con posibilidad de un examen final)	0	85
Evaluación de trabajos y actividades	0	85

Módulo Fundamentos de ciberseguridad	Asignatura Seguridad de aplicaciones
Curso	Primero
ECTS	6
Carácter	Obligatoria
Semestre	Primero
Lenguas en las que se imparte	Castellano / Gallego / Inglés
Competencias básicas y generales	(CB2) Que los estudiantes sepan aplicar los conocimientos adquiridos y tengan capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio (CG2) Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones
Competencias específicas	(CE2) Conocer en profundidad las técnicas de ciberataque y ciberdefensa (CE7) Tener capacidad para realizar la auditoría de seguridad de sistemas e instalaciones, el análisis de riesgos derivados de debilidades de ciberseguridad y desarrollar el proceso de certificación de sistemas seguros (CE13) Tener capacidad de análisis, detección y eliminación de vulnerabilidades, y del malware susceptible de utilizarlas, en sistemas y redes
Competencias transversales	(CT4) Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad. (CT5) Tener capacidad para comunicarse oralmente y por escrito en inglés.
Resultados de aprendizaje	• Comprender los problemas potenciales de seguridad que presentan las aplicaciones compiladas • Detectar los problemas de seguridad de aplicaciones compiladas. • Comprender los mecanismos de protección diseñados para limitar o anular el impacto de los problemas de seguridad del software compilado • Ser capaz de corregir el software compilado para solucionar problemas detectados • Entender las vulnerabilidades comunes de las aplicaciones web • Encontrar problemas seguridad en aplicaciones web. • Ser capaz de corregir los problemas de seguridad detectados en aplicaciones web.
Contenidos	CWE y OWASP Seguridad del software compilado Vulnerabilidades específicas al código nativo

	Seguridad en aplicaciones web y servicios web (APIs) Autenticación y autorización, y frameworks de aplicación para la protección de recursos Integración de la seguridad en metodologías de desarrollo software Herramientas de protección y testing	
Observaciones		
Metodologías docentes (incluir listado)	Sesión magistral Prácticas TIC Trabajos y/o proyectos (individuales o en grupo) Trabajo autónomo del alumno Atención personalizada	
Actividades formativas		
Denominación de la actividad formativa	Horas	Presencialidad (%)
Sesión magistral y resolución de problemas/ejercicios	63	33,3
Prácticas de laboratorio y proyectos individuales o en grupo	87	24,1
Sistemas de evaluación		
Denominación del sistema de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de un examen final)	15	100
Pruebas prácticas (con posibilidad de un examen final)	0	85
Evaluación de trabajos y actividades	0	85

Módulo Fundamentos de ciberseguridad	Asignatura Redes seguras
Curso	Primero
ECTS	6
Carácter	Obligatoria
Semestre	Primero
Lenguas en las que se imparte	Castellano/gallego/inglés
Competencias básicas y generales	(CB2) 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 (CB4) 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 (CB5) 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) Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación (CG3) Capacidad para el razonamiento crítico y la evaluación crítica de cualquier sistema de protección de la información, cualquier sistema de seguridad de la información, de la seguridad de las redes y/o los sistemas de comunicaciones (CG8) Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos
Competencias específicas	(CE2) Conocer en profundidad las técnicas de ciberataque y ciberdefensa (CE4) Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, sus sistemas operativos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información (CE8) Capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad (CE12) Reunir e interpretar datos relevantes dentro del área de la seguridad informática y de las comunicaciones
Competencias transversales	(CT4) Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad. (CT5) Tener capacidad para comunicarse oralmente y por escrito en inglés.
Resultados de aprendizaje	Al finalizar esta materia los estudiantes: • Comprenderán el papel de un cortafuegos en la estrategia de seguridad de un ordenador o de la red a la que protege.

	• Serán capaces de describir qué son las políticas de acceso, y de diseñar/especificar el conjunto de las mismas que requiere un escenario o caso particular. • Conocerán los diferentes modelos de filtrado de paquetes (con/sin estado) y los cortafuegos de nivel de aplicación, y sabrán configurarlos en diversas plataformas. • Podrán diseñar y describir, para un escenario/topología concreto, configuraciones alternativas para emplazar el cortafuegos dentro de la red corporativa (sistema fortificado, DMZ, cortafuegos distribuido). • Serán capaces de describir los principios básicos que sustentan la detección de intrusiones, los sensores habituales que utilizan para la recopilación de información, y las técnicas de análisis (detección de anomalías versus detección heurística) que deciden cuándo disparar una alarma. Y conocerán posibles soluciones técnicas (HIDS/NIDS, IPS, SIEM, honeypot), que sabrán instalar y configurar para algunas plataformas e implementaciones particulares. • Estarán familiarizados con los conceptos de túnel y virtualización de redes, y serán capaces de elegir e implementar la tecnología de red privada virtual más apropiada para diferentes escenarios. • Podrán explicar los principios sobre los que se construyen las redes anónimas.	
Contenidos	Seguridad perimetral. Cortafuegos. Sistemas de detección de intrusos. VPNs. Redes anónimas.	
Observaciones		
Metodologías docentes (incluir listado)	Sesión magistral Prácticas TIC Trabajos y/o proyectos (individuales o en grupo) Trabajo autónomo del alumno Atención personalizada	
Actividades formativas		
Denominación de la actividad formativa	Horas	Presencialidad (%)
Sesión magistral y Resolución de problemas/ejercicios	63	33,3
Prácticas de laboratorio y Proyectos individuales o en grupo	87	24,1
Sistemas de evaluación		
Denominación del sistema de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de un examen final)	15	100
Pruebas prácticas (con posibilidad de un examen final)	0	85
Evaluación de trabajos y actividades	0	85

Módulo Técnicas de ciberseguridad	Asignatura Fortificación de sistemas operativos
Curso	Primero
ECTS	5
Carácter	Obligatoria
Semestre	Segundo
Lenguas en las que se imparte	Castellano / gallego / inglés
Competencias básicas y generales	(CB2) 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 (CB5) 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) Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación (CG2) Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones (CG5) Tener capacidad de aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos
Competencias específicas	(CE4) Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información (CE8) Capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad
Competencias transversales	(CT4) Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad. (CT5) Tener capacidad para comunicarse oralmente y por escrito en inglés.
Resultados de aprendizaje	• Instalación y administración segura de sistemas (servidores, escritorio) tanto en entornos Microsoft como en entornos Linux • Fortificación escalable de sistemas basada en mecanismos de gestión de identidad centralizada • Reducción de las superficies de ataque en los sistemas operativos más habituales
Contenidos	Seguridad en Sistemas Linux - Fortificación - Despliegue de Servicios Seguridad en Entornos Microsoft - Equipos de Escritorio - Servidores - Directorio Activo

	Entornos virtuales Otros sistemas	
Observaciones		
Metodologías docentes (incluir listado)	Sesión magistral Prácticas TIC Trabajos y/o proyectos (individuales o en grupo) Trabajo autónomo del alumno Atención personalizada	
Actividades formativas		
Denominación de la actividad formativa	Horas	Presencialidad (%)
Sesión magistral y Resolución de problemas/ejercicios	27	33
Prácticas de laboratorio y Proyectos individuales o en grupo	98	26,5
Sistemas de evaluación		
Denominación del sistema de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de un examen final)	15	100
Pruebas prácticas (con posibilidad de un examen final)	0	85
Evaluación de trabajos y actividades	0	85

Módulo Técnicas de ciberseguridad	Asignatura Tests de intrusión
Curso	Primero
ECTS	5
Carácter	Obligatorio
Semestre	Segundo
Lenguas en las que se imparte	Castellano / gallego / inglés
Competencias básicas y generales	(CB2) 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 (CB3) Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar 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 (CB4) 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 (CB5) 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) Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación (CG2) Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones (CG4) Compromiso ético. Capacidad para diseñar e implantar soluciones técnicas y de gestión con criterios éticos de responsabilidad y deontología profesional en el ámbito de la seguridad de la información, las redes y/o los sistemas de comunicaciones
Competencias específicas	(CE2) Conocer en profundidad las técnicas de ciberataque y ciberdefensa (CE4) Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información (CE7) Tener capacidad para realizar la auditoría de seguridad de sistemas e instalaciones, el análisis de riesgos derivados de debilidades de ciberseguridad y desarrollar el proceso de certificación de sistemas seguros
Competencias transversales	(CT4) Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad

	(CT5) Tener capacidad para comunicarse oralmente y por escrito en inglés.	
Resultados de aprendizaje	- El alumno conocerá las herramientas habituales comúnmente utilizadas para el desarrollo de test de intrusión, y a usarlas con responsabilidad - El alumno será capaz de planificar un test de intrusión en una organización, partiendo una información inicial limitada - El alumno será capaz de llevar a cabo test de intrusión con el objetivo de detectar vulnerabilidades y documentarlas adecuadamente, sin provocar daño en las redes o sistemas - El alumno interiorizará la ética relacionada con los test de intrusión y se comportará en base a dicha ética	
Contenidos	Fundamentos. Presentación de herramientas y “frameworks” Estrategias de reconocimiento Estrategias ofensivas Métodos de evasión Principios éticos de los test de intrusión	
Observaciones		
Metodologías docentes (incluir listado)	Sesión magistral Prácticas TIC Trabajos y/o proyectos (individuales o en grupo) Trabajo autónomo del alumno Atención personalizada	
Actividades formativas		
Denominación de la actividad formativa	Horas	Presencialidad (%)
Sesión magistral y Resolución de problemas/ejercicios	27	33,3
Prácticas de laboratorio y Proyectos individuales o en grupo	98	26,5
Sistemas de evaluación		
Denominación del sistema de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de examen final)	15	100
Pruebas prácticas (con posibilidad de un examen final)	0	85
Evaluación de trabajos y actividades	0	85

Módulo Técnicas de ciberseguridad	Asignatura Análisis de <i>malware</i>
Curso	Primero
ECTS	5
Carácter	Obligatoria
Semestre	Segundo
Lenguas en las que se imparte	Castellano / Gallego / Inglés
Competencias básicas y generales	(CB1) Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación (CG1) Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación
Competencias específicas	(CE8) Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad (CE11) Reunir e interpretar datos relevantes dentro del área de la seguridad informática y de las comunicaciones (CE13) Tener capacidad de análisis, detección y eliminación de vulnerabilidades, y del malware susceptible de utilizarlas, en sistemas y redes
Competencias transversales	(CT4) Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad (CT5) Tener capacidad para comunicarse oralmente y por escrito en inglés
Resultados de aprendizaje	• Analizar, detectar y eliminar malware en sistemas y redes. • Conocer, detectar y luchar contra las técnicas de ocultación y persistencia de malware en sistemas y redes. • Estudiar sistemas y redes para detectar y eliminar las vulnerabilidades susceptibles de ser utilizadas por el malware. • Conocer las tendencias actuales en malware y las experiencias aprendidas de casos reales.
Contenidos	• Introducción al análisis e ingeniería de <i>malware</i> • Tipos de <i>malware</i>. Estructura, componentes, vectores de infección • Ingeniería de <i>malware</i>. Técnicas de propagación, infección, persistencia, ocultación • Ingeniería inversa de <i>malware</i> • Herramientas de análisis de <i>malware</i>
Observaciones	
Metodologías docentes (incluir listado)	Sesión magistral Prácticas TIC Trabajos y/o proyectos (individuales o en grupo) Trabajo autónomo del alumno

	Atención personalizada	
Actividades formativas		
Denominación de la actividad formativa	Horas	Presencialidad (%)
Sesión magistral y resolución de problemas/ejercicios	51	33,3
Prácticas de laboratorio y proyectos individuales o en grupo	74	24,3
Sistemas de evaluación		
Denominación del sistema de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de un examen final)	15	100
Pruebas prácticas (con posibilidad de un examen final)	0	85
Evaluación de trabajos y actividades	0	85

Módulo Técnicas de ciberseguridad	Asignatura Seguridad como negocio
Curso	Primero
ECTS	3
Carácter	Obligatoria
Semestre	Segundo
Lenguas en las que se imparte	Castellano / gallego / inglés
Competencias básicas y generales	(CB1) Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación. (CB4) 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. (CG3) Capacidad para el razonamiento crítico y la evaluación crítica de cualquier sistema de protección de la información, cualquier sistema de seguridad de la información, de la seguridad de las redes y/o los sistemas de comunicaciones (CG6) Destreza para investigar. Capacidad para innovar y contribuir al avance de los principios, las técnicas y los procesos referidos a su ámbito profesional, diseñando nuevos algoritmos, dispositivos, técnicas o modelos útiles para la protección de los activos digitales públicos, privados o comerciales
Competencias específicas	(CE9) Tener capacidad para elaborar planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados. (CE11) Reunir e interpretar datos relevantes dentro del área de la seguridad informática y de las comunicaciones. (CE15) Tener capacidad de identificar el valor, tanto económico como de otra índole, de la información de la institución, sus procesos críticos y el impacto que produciría la interrupción de éstos; y, también, las necesidades internas y externas que permitirán estar preparados ante ataques de seguridad. (CE16) Capacidad de vislumbrar y enfocar el esfuerzo de negocio en temáticas relacionadas con la ciberseguridad y con una monetización viable. (CE19) Saber identificar los perfiles de personal necesarios para una institución en función de sus características y su sector (CE20) Conocimiento de las empresas orientadas específicamente al sector de seguridad de nuestro entorno
Competencias transversales	(CT4) Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad (CT5) Tener capacidad para comunicarse oralmente y por escrito en inglés
Resultados de aprendizaje	• Conocer los conceptos fundamentales sobre el negocio de la seguridad digital siendo capaces de monetizar la información. • Entender que es posible orientar una empresa en el ámbito de la seguridad e incluso a sectores más específicos dentro de este ámbito. • Definir los perfiles necesarios, propios de la empresa o

	externos, asociados a la ciberseguridad. ● Conocer empresas del sector, su creación, desarrollo y orientación. ● Conocer los cauces correctos de comunicación en la institución, especialmente con la gerencia.	
Contenidos	1. La seguridad como elemento transversal de la institución. 2. Monetización de los datos y de la seguridad de los mismos. 3. Perfiles de ciberseguridad en las entidades. 4. Oportunidades de negocio y orientación en los sectores productivos 5. Casos de éxito.	
Observaciones		
Metodologías docentes (incluir listado)	Sesión magistral Resolución de problemas/ejercicios Trabajos Tutelados individuales o en grupo	
Actividades formativas		
Denominación de la actividad formativa	Horas	Presencialidad (%)
Sesión magistral y resolución de problemas/ejercicios	30	33,3
Problemas/ejercicios en sesiones presenciales y seguimiento de trabajos tutelados	45	24,4
Sistemas de evaluación		
Denominación del sistema de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Prueba objetiva y resolución de problemas y/o ejercicios (con posibilidad de examen final)	30	70
Evaluación de trabajos y actividades	30	70

Módulo Formación complementaria	Asignatura Seguridad en dispositivos móviles
Curso	Primero
ECTS	3
Carácter	Optativa
Semestre	Segundo
Lenguas en las que se imparte	Castellano / gallego / inglés
Competencias básicas y generales	(CB2) Que los estudiantes sepan aplicar los conocimientos adquiridos y tengan capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio (CB3) Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar 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 (CB4) 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 (CG1) Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación (CG2) Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones (CG5) Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos
Competencias específicas	(CE4) Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, sus sistemas operativos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información (CE6) Desarrollar y aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad (CE9) Tener capacidad para elaborar planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados (CE15) Tener capacidad de identificar el valor, tanto económico como de otra índole, de la información de la institución, sus procesos críticos y el impacto que produciría la interrupción de éstos; y, también, las necesidades internas y externas que permitirán estar preparados ante ataques de seguridad
Competencias transversales	(CT4) Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad. (CT5) Tener capacidad para comunicarse oralmente y por escrito en inglés.
Resultados de aprendizaje	Conocer los conceptos fundamentales asociados con la

	seguridad en los sistemas operativos móviles y el desarrollo de apps seguras. ● Identificar una app con comportamiento malicioso y vulnerabilidades en sistemas operativos y apps ● Ser capaz de realizar una análisis forense de un dispositivo móvil ● Conocer los sistemas gestión de dispositivos móviles	
Contenidos	-Estudio de arquitecturas de sistemas operativos móviles -Desarrollo de apps seguras -Apps maliciosas -Vulnerabilidades de SO y apps -Análisis forense de sistemas operativos móviles -Sistemas Mobile Device Management (MDM)	
Observaciones		
Metodologías docentes (incluir listado)	Sesión magistral Prácticas TIC Trabajos y/o proyectos (individuales o en grupo) Trabajo autónomo del alumno Atención personalizada	
Actividades formativas		
Denominación de la actividad formativa	Horas	Presencialidad (%)
Sesión magistral y Resolución de problemas/ejercicios	30	33,3
Prácticas de laboratorio y Proyectos individuales o en grupo	45	24,4
Sistemas de evaluación		
Denominación del sistema de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de examen final)	15	100
Pruebas prácticas (con posibilidad de examen final)	0	85
Evaluación de trabajos y actividades	0	85

Módulo Formación complementaria	Asignatura Análisis forense de equipos
Curso	Primero
ECTS	3
Carácter	Optativo
Semestre	Segundo
Lenguas en las que se imparte	Castellano / gallego / inglés
Competencias básicas y generales	(CB1) Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación (CB2) 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 (CB3) Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar 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 (CG2) Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones
Competencias específicas	(CE6) Desarrollar y aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad
Competencias transversales	(CT4) Asumir como profesional y ciudadano la importancia del aprendizaje a lo largo de la vida. (CT5) Tener capacidad para comunicarse oralmente y por escrito en inglés.
Resultados de aprendizaje	• Conocimiento de las metodologías adecuadas para la realización de trabajos forenses con validez legal • Capacidad para la realización de análisis forense de los diferentes elementos que forman un sistema de información, en múltiples plataformas y sistemas operativos • Capacidad para generar informes como resultado del análisis forense claro, concisos e inteligibles tanto por expertos como por personas ajenas al ámbito de la seguridad informática
Contenidos	1. Fundamentos 2. Metodología de Análisis Forense 3. Herramientas de Análisis Forense: Entornos Linux Y Windows 4. Casos
Observaciones	
Metodologías docentes (incluir listado)	Sesión magistral Resolución de problemas/ejercicios Prácticas de laboratorio

	Proyectos individuales o en grupo	
Actividades formativas		
Denominación de la actividad formativa	Horas	Presencialidad (%)
Sesión magistral y Resolución de problemas/ejercicios	15	33,3
Prácticas de laboratorio y Proyectos individuales o en grupo	60	26,6
Sistemas de evaluación		
Denominación del sistema de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Preguntas tipo test y/o resolución de problemas/ejercicios	10	80
Prácticas de laboratorio	10	80
Proyectos individuales o en grupo	10	80

Módulo Formación complementaria	Asignatura Seguridad ubicua
Curso	Primero
ECTS	3
Carácter	Optativa
Semestre	Segundo
Lenguas en las que se imparte	Castellano / gallego / inglés
Competencias básicas y generales	(CB2) 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 (CB3) Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar 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 (CB4) 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 (CG1) Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación (CG2) Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones (CG5) Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos
Competencias específicas	(CE4) Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, sus sistemas operativos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información (CE9) Tener capacidad para elaborar planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados
Competencias transversales	(CT4) Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad. (CT5) Tener capacidad para comunicarse oralmente y por escrito en inglés.
Resultados de aprendizaje	• Conocer la seguridad en las diferentes capas relacionadas con los sistemas ubicuos y las tecnologías que utilizan • Entender los problemas de seguridad asociados al mundo ubicuo • Conocer casos reales de ataques a sistemas ubicuos
Contenidos	Seguridad: -física

	-en middleware -en comunicaciones -en percepción del entorno Escenarios reales: -redes PAN -redes de sensores -IoT -drones -coche conectado -etc.	
Observaciones		
Metodologías docentes (incluir listado)	Sesión magistral Prácticas TIC Trabajos y/o proyectos (individuales o en grupo) Trabajo autónomo del alumno Atención personalizada	
Actividades formativas		
Denominación de la actividad formativa	Horas	Presencialidad (%)
Sesión magistral y Resolución de problemas/ejercicios	30	33,3
Prácticas de laboratorio y Proyectos individuales o en grupo	45	24,4
Sistemas de evaluación		
Denominación del sistema de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de examen final)	15	100
Pruebas prácticas (con posibilidad de examen final)	0	85
Evaluación de trabajos y actividades	0	85

Módulo Formación complementaria	Asignatura Ciberseguridad en entornos industriales
Curso	Primero
ECTS	3
Carácter	Optativa
Semestre	Segundo
Lenguas en las que se imparte	Castellano / Gallego / Inglés
Competencias básicas y generales	(CB1) Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación (CG2) Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones (CG5) Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos
Competencias específicas	(CE4) Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, sus sistemas operativos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información (CE7) Tener capacidad para realizar la auditoría de seguridad de sistemas e instalaciones, el análisis de riesgos derivados de debilidades de ciberseguridad y desarrollar el proceso de certificación de sistemas seguros (CE12) Conocer el papel de la ciberseguridad en el diseño de las nuevas industrias, así como las particularidades, restricciones y limitaciones que se han de acometer para obtener una infraestructura industrial segura (CE15) Tener capacidad de identificar el valor, tanto económico como de otra índole, de la información de la institución, sus procesos críticos y el impacto que produciría la interrupción de éstos; y, también, las necesidades internas y externas que permitirán estar preparados ante ataques de seguridad
Competencias transversales	(CT4) Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad. (CT5) Tener capacidad para comunicarse oralmente y por escrito en inglés.
Resultados de aprendizaje	• Comprender la ejecución de políticas de seguridad y sus implicaciones en entornos industriales • Comprender las diferentes técnicas de protección y ataque en sistemas industriales y saber cómo se pueden implementar. • Entender las problemáticas de seguridad y los ataques a redes de control en industria y conocer los mecanismos

	que permiten minimizarlos. • Ser capaz de comprender las implicaciones a nivel de seguridad de la nueva industria 4.0	
Contenidos	Introducción a la Seguridad en Sistemas industriales Análisis activo y pasivo en sistemas SCADA, DSS, PLC´s Protección y ataques de sistemas industriales y redes de control (LCN, Modbus, Fieldbus, RS422, ...) Seguridad de la industria 4.0	
Observaciones		
Metodologías docentes (incluir listado)	Sesión magistral Prácticas TIC Trabajos y/o proyectos (individuales o en grupo) Trabajo autónomo del alumno Atención personalizada	
Actividades formativas		
Denominación de la actividad formativa	Horas	Presencialidad (%)
Sesión magistral y resolución de problemas/ejercicios	30	33,3
Prácticas de laboratorio y proyectos individuales o en grupo	45	24,4
Sistemas de evaluación		
Denominación del sistema de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de un examen final)	15	100
Pruebas prácticas (con posibilidad de un examen final)	0	85
Evaluación de trabajos y actividades	0	85

Módulo Formación complementaria	Asignatura Gestión de incidentes
Curso	Primero
ECTS	3
Carácter	Optativo
Semestre	Segundo
Lenguas en las que se imparte	Castellano / Gallego / Inglés
Competencias básicas y generales	(CB2) 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. (CB3) Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar 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. (CB5) 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) Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación. (CG5) Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos.
Competencias específicas	(CE3) Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información. (CE9) Tener capacidad para elaborar planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados. (CE14) Tener capacidad para desarrollar un plan de continuidad de negocio siguiendo normas y estándares de referencia. (CE15) Tener capacidad de identificar el valor, tanto económico como de otra índole, de la información de la institución, sus procesos críticos y el impacto que produciría la interrupción de éstos; y, también, las necesidades internas y externas que permitirán estar preparados ante ataques de seguridad. (CE17) Tener capacidad de planificar en el tiempo los períodos de detección de incidentes o desastres, y su recuperación
Competencias transversales	(CT4) Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad. (CT5) Tener capacidad para comunicarse oralmente y por escrito en inglés.
Resultados de aprendizaje	• Manejar la proactividad para prevenir y atenuar posibles incidentes de seguridad. • Obtener el conocimiento necesario sobre herramientas que pueden facilitar la gestión de los incidentes y las

	recuperaciones. ● Justificar económicamente los planes propuestos para recuperación y resiliencia. ● Identificar y clasificar los posibles incidentes y definir los cauces para su gestión y resolución.
Contenidos	1. Fundamentos: resiliencia y el valor de la información. 2. Detección de incidentes y gestión de respuesta. 3. Estándares: planes de continuidad y de recuperación. 4. Recuperación de desastres 5. Legislación
Observaciones	
Metodologías docentes (incluir listado)	Sesión magistral Resolución de problemas/ejercicios Prácticas TIC Trabajos y/o proyectos individuales o en grupo
Actividades formativas	
Denominación de la actividad formativa	Horas Presencialidad (%)
Sesión magistral y Resolución de problemas/ejercicios	30 33,3
Prácticas de laboratorio y Proyectos individuales o en grupo	45 24,4
Sistemas de evaluación	
Denominación del sistema de evaluación	Ponderación mínima (%) Ponderación máxima (%)
Prueba objetiva y/o resolución de problemas y/o ejercicios (con posibilidad de un examen final)	30 60
Prácticas TIC	20 50
Evaluación de trabajos y actividades	20 50

Módulo Prácticas en empresa y trabajo de fin de máster	Asignatura Prácticas en empresa
Curso	Segundo
ECTS	15
Carácter	Obligatoria
Semestre	Primero
Lenguas en las que se imparte	Castellano / Gallego / Inglés
Competencias básicas y generales	(CB1) Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación (CB2) Que los estudiantes sepan aplicar los conocimientos adquiridos y tengan capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio (CB3) Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar 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 (CB4) 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 (CB5) 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) Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación (CG2) Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones (CG3) Capacidad para el razonamiento crítico y la evaluación crítica de cualquier sistema de protección de la información, cualquier sistema de seguridad de la información, de la seguridad de las redes y/o los sistemas de comunicaciones (CG4) Compromiso ético. Capacidad para diseñar e implantar soluciones técnicas y de gestión con criterios éticos de responsabilidad y deontología profesional en el ámbito de la seguridad de la información, las redes y/o los sistemas de comunicaciones (CG5) Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos (CG6) Destreza para investigar. Tener capacidad para innovar y contribuir al avance de los principios, las técnicas y los procesos

	referidos a su ámbito profesional, diseñando nuevos algoritmos, dispositivos, técnicas o modelos útiles para la protección de los activos digitales públicos, privados o comerciales	
Competencias específicas	Todas las del título	
Competencias transversales	(CT1) Tener capacidad para comprender el significado y aplicación de la perspectiva de género en los distintos ámbitos de conocimiento y en la práctica profesional con el objetivo de alcanzar una sociedad más justa e igualitaria. (CT3) Incorporar en el ejercicio profesional criterios de sostenibilidad y compromiso ambiental. Incorporar a los proyectos el uso equitativo, responsable y eficiente de los recursos. (CT4) Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad. (CT5) Tener capacidad para comunicarse oralmente y por escrito en inglés.	
Resultados de aprendizaje	- Experiencia en el desempeño de la ciberseguridad, y de sus funciones más habituales en un entorno real de trabajo.	
Contenidos	Estancia de 375 horas de duración en una empresa desarrollando funciones relacionadas con la ciberseguridad; tutorización por profesorado del Máster y personal de la empresa.	
Observaciones	El alumnado puede integrar todas o parte de las competencias adquiridas durante su formación de las demás materias que conforman el título de Máster en Ciberseguridad, de forma que cada estudiante trabajará un conjunto diferente de competencias (ya adquiridas en otras materias), dependiendo de la naturaleza de la práctica que esté realizando en cada empresa determinada.	
Metodologías docentes (incluir listado)	- Estancia en empresas.	
Actividades formativas		
Denominación de la actividad formativa	Horas	Presencialidad (%)
- Estancia en empresas.	375	100
Sistemas de evaluación		
Denominación del sistema de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
- Informe del profesorado tutor de la empresa	30	70
- Memoria de actividades	30	70

Módulo Prácticas en empresa y trabajo de fin de máster	Asignatura Trabajo de fin de máster
Curso	Segundo
ECTS	15
Carácter	Obligatoria
Semestre	Primero
Lenguas en las que se imparte	Castellano / Gallego / Inglés*
Competencias básicas y generales	(CB1) Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación (CB2) Que los estudiantes sepan aplicar los conocimientos adquiridos y tengan capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio (CB3) Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar 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 (CB4) 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 (CB5) 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) Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación (CG2) Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones (CG3) Capacidad para el razonamiento crítico y la evaluación crítica de cualquier sistema de protección de la información, cualquier sistema de seguridad de la información, de la seguridad de las redes y/o los sistemas de comunicaciones (CG4) Compromiso ético. Capacidad para diseñar e implantar soluciones técnicas y de gestión con criterios éticos de responsabilidad y deontología profesional en el ámbito de la seguridad de la información, las redes y/o los sistemas de comunicaciones (CG5) Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos (CG6) Destreza para investigar. Tener capacidad para innovar y contribuir al avance de los principios, las técnicas y los procesos referidos a su ámbito profesional, diseñando nuevos algoritmos,

	dispositivos, técnicas o modelos útiles para la protección de los activos digitales públicos, privados o comerciales	
Competencias específicas	Todas las del título	
Competencias transversales	(CT1) Tener capacidad para comprender el significado y aplicación de la perspectiva de género en los distintos ámbitos de conocimiento y en la práctica profesional con el objetivo de alcanzar una sociedad más justa e igualitaria. (CT3) Incorporar en el ejercicio profesional criterios de sostenibilidad y compromiso ambiental. Incorporar a los proyectos el uso equitativo, responsable y eficiente de los recursos. (CT4) Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad. (CT5) Tener capacidad para comunicarse oralmente y por escrito en inglés	
Resultados de aprendizaje	- Búsqueda, ordenación y estructuración de información sobre Ciberseguridad. - Elaboración de memoria de proyectos en la que se recojan los aspectos fundamentales del trabajo desarrollado. - Diseño de prototipos, programas de simulación, etc., según especificaciones	
Contenidos	Trabajo académico a presentar en público que será evaluado por un Tribunal - Puede ser continuación de las prácticas en empresa	
Observaciones	El alumnado puede integrar todas o parte de las competencias adquiridas durante su formación de las demás materias que conforman el título de Máster en Ciberseguridad, de forma que cada estudiante trabajará un conjunto diferente de competencias (ya adquiridas en otras materias), dependiendo de la naturaleza del TFM que esté realizando. De forma opcional, el alumnado podrá realizar su TFM en el marco de una empresa, en cuyo caso existirá la actividad formativa de Estancia en empresas, cuya presencialidad se detraerá de las horas del trabajo autónomo del alumnado.	
Metodologías docentes (incluir listado)	- Trabajos y/o proyectos. - Atención personalizada.	
Actividades formativas		
Denominación de la actividad formativa	Horas	Presencialidad (%)
- Trabajos y/o proyectos.	350	0
- Atención personalizada.	25	100
Sistemas de evaluación		
Denominación del sistema de evaluación	Ponderación mínima (%)	Ponderación máxima (%)
- Rúbrica aprobada por la Comisión Académica del Máster. La evaluación se basará en la decisión del Tribunal nombrado a tal efecto, y tendrá en cuenta la opinión del profesorado tutor.	100	100

6. PERSONAL ACADÉMICO

Deberá presentarse la Clasificación del profesorado indicando la categoría docente por procedencia, porcentajes de cada categoría de la Universidad respecto al total, y porcentaje de doctores y de horas por categoría de acuerdo con el siguiente esquema:

Universidad	Categoría	Total %	Doctores %	Horas %
UVigo	CU	5	100	20
UdC	CU	5	100	5
UVigo	TU	30	100	15
UdC	TU	18	100	10
UVigo	PCD	15	100	15
UdC	PCD	17	100	15
UdC	TEU	5	45	10
UdC	PAD	5	100	10

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

Plantilla de profesorado disponible								
Universidad	Categoría académica	Nº	Vinculación con la universidad	Dedicación al título		Doctor	Quinquenios	Sexenios
				Total	Parcial			
UVigo – EET ¹	CU	3	Completa		X	3	12	9
	TU	10	Completa		x	19	67	46
	PCD	19	Completa		x	10	14	13
UDC - FIC	CU	21	Completa		x	21	95	62
	TU	64	Completa		x	64	234	142
	TEU	11	Completa		x	5	53	0
	PCD	42	Completa		x	42	85	60
	PAD	11	Completa		x	11	0	0

¹Se indica únicamente el PDI del departamento de Ingeniería Telemática, que asumirá la mayor parte de la docencia en el Máster

En cuanto a las áreas de conocimiento responsables de la docencia de las materias del plan de estudios en la Universidad de La Coruña, la tabla siguiente recoge la adscripción del personal docente.

Conceptos y Leyes en Ciberseguridad	Derecho Penal
Gestión da Seguridad da Información	Ciencia de la Computación e Inteligencia Artificial
Fundamentos de Ciberseguridad	Ciencia de la Computación e Inteligencia Artificial
Seguridad en Comunicación	Ingeniería Telemática
Seguridad en Aplicaciones	Ingeniería Telemática
Redes Seguras	Ingeniería Telemática
Fortificación de Sistemas Operativos	Ciencia de la Computación e Inteligencia Artificial
Test de Intrusión	Ciencia de la Computación e Inteligencia Artificial
Análisis de Malware	Ciencia de la Computación e Inteligencia Artificial
Seguridad como Negocio	Ingeniería Telemática
Seguridad en Dispositivos Móviles	Tecnología Electrónica
Análisis Forense de Equipos	Ciencia de la Computación e Inteligencia Artificial
Seguridad Ubicua	Ciencia de la Computación e Inteligencia Artificial
Ciberseguridad en Entornos Industriales	Tecnología Electrónica
Gestión de Incidentes	Ciencia de la Computación e Inteligencia Artificial
Prácticas en Empresa	Ingeniería Telemática
Trabajo Fin de Máster	Ingeniería Telemática

6.2. OTROS RECURSOS HUMANOS

Como personal de apoyo no docente se dispondrá del personal de administración y técnicos de los centros participantes.

Escuela de Ingeniería de Telecomunicación de la UVigo

La administración de algunos servicios está centralizada por ámbitos en la Universidade de Vigo, perteneciendo la EET al ámbito tecnológico. Según la Relación de Puestos de Trabajo activada en julio de 2017, los recursos humanos no docentes relacionados con el centro son lo que se detallan en la tabla siguiente.

ÁMBITO TECNOLÓGICO					
ESCUELA DE INGENIERÍA DE TELECOMUNICACIÓN					
ESCUELA DE MINAS Y ENERGÍA					
ESCUELA DE INGENIERÍA INDUSTRIAL					
CÓDIGO PUESTO	DENOMINACIÓN	NIVEL	SUBGRUPO	TIPO DE VINCULACIÓN	DEDICACIÓN
33000 PF1020 1	ADMINISTRADOR/A	28	A1/A2	FUNCIONARIO/A	TIEMPO COMPLETO
33000 PF1160 1	PUESTO BASE	16	C1/C2	FUNCIONARIO/A	TIEMPO COMPLETO
33000 PF1160 2	PUESTO BASE	16	C1/C2		
33000 PF1160 3	PUESTO BASE	16	C1/C2		
33000 PF1160 4	PUESTO BASE	16	C1/C2		
33000 PF1160 5	PUESTO BASE	16	C1/C2		
E. DE INGENIERÍA DE TELECOMUNICACIÓN – ESCUELA DE MINAS Y ENERGÍA					
	ÁREA ACADÉMICA				
33410 PF1064 1	JEFE/A DE ÁREA DE ESTUDIOS DE GRADO	22	A2/C1	FUNCIONARIO/A	TIEMPO COMPLETO
33420 PF1064 1	JEFE/A DE ÁREA DE ESTUDIOS DE MÁSTER Y DOCTORADO	22	A2/C1	FUNCIONARIO/A	TIEMPO COMPLETO
33410 PF1110 1	JEFE/A DE NEGOCIADO DE ESTUDIOS DE GRADO	20	C1/C2	FUNCIONARIO/A	TIEMPO COMPLETO
33420 PF1110 1	JEFE/A DE NEGOCIADO DE ESTUDIOS DE MÁSTER Y DOCTORADO	20	C1/C2	FUNCIONARIO/A	TIEMPO COMPLETO
ÁREA DE APOYO A LA INVESTIGACIÓN, A LA TRANSFERENCIA EA LA GESTIÓN DE CENTROS E DEPARTAMENTOS					
33430 PF1064 1	JEFE/A DE ÁREA	22	A2/C1	FUNCIONARIO/A	TIEMPO COMPLETO
33431 PF1141 1	JEFE/A DEL NEGOCIADO DE APOYO A LA INVESTIGACIÓN Y A LA TRANSFERENCIA	18	C1/C2	FUNCIONARIO/A	TIEMPO COMPLETO
33431 PF1141 2	JEFE/A DEL NEGOCIADO DE APOYO A LA INVESTIGACIÓN Y A LA TRANSFERENCIA	18	C1/C2		
33432 PF1141 1	JEFE/A DEL NEGOCIADO DE APOYO A LA GESTIÓN DE CENTROS E DEPARTAMENTOS	18	C1/C2	FUNCIONARIO/A	TIEMPO COMPLETO
33432 PF1141 2	JEFE/A DEL NEGOCIADO DE APOYO A LA GESTIÓN DE CENTROS E DEPARTAMENTOS	18	C1/C2		
33433 PF1151 1	JEFE/A DEL NEGOCIADO DE ASUNTOS GENERALES – E.E. Telecomunicaciones	18	C1/C2	FUNCIONARIO/A	TIEMPO COMPLETO
33434 PF1151 1	JEFE/A DEL NEGOCIADO DE ASUNTOS GENERALES – Escuela de Minas y Energía	18	C1/C2		
ÁREA ECONÓMICA					
33440 PF1064 1	JEFE/A DE ÁREA	22	A2/C1	FUNCIONARIO/A	TIEMPO COMPLETO
33440 PF1110 1	JEFE/A DE NEGOCIADO	20	C1/C2	FUNCIONARIO/A	TIEMPO COMPLETO
33440 PF1110 2	JEFE/A DE NEGOCIADO	20	C1/C2		
BIBLIOTECA UNIVERSITARIA					
39000 PF1010 1	DIRECCIÓN BIBLIOTECA UNIVERSITARIA	28	A1	FUNCIONARIO/A	TIEMPO COMPLETO
39000 PF1030 1	SUBDIRECCIÓN BIBLIOTECA UNIVERSITARIA	26	A1/A2	FUNCIONARIO/A	TIEMPO COMPLETO
39400 PF1041 1	JEFE/A DE SECCIÓN DE ACCESO A DOCUMENTO	25	A1/A2	FUNCIONARIO/A	TIEMPO COMPLETO
39500 PF1041 1	JEFE/A DE SECCIÓN DE ADQUISICIONES	25	A1/A2	FUNCIONARIO/A	TIEMPO COMPLETO
39600 PF1041 1	JEFE/A DE SECCIÓN DE ARCHIVO	25	A1/A2	FUNCIONARIO/A	TIEMPO COMPLETO
40100 PF1041 1	JEFE/A DE SECCIÓN DE AUTOMATIZACIÓN Y PROCESO TÉCNICO	25	A1/A2	FUNCIONARIO/A	TIEMPO COMPLETO

40200 PF1041 1	JEFE/A DE SECCIÓN DE CIRCULACIÓN	25	A1/A2	FUNCIONARIO/A	TIEMPO COMPLETO
40300 PF1041 1	JEFE/A DE SECCIÓN DE PUBLICACIONES PERIÓDICAS	25	A1/A2	FUNCIONARIO/A	TIEMPO COMPLETO
40400 PF1041 1	JEFE/A DE SECCIÓN DE SOPORTE AL APRENDIZAJE Y A LA INVESTIGACIÓN	25	A1/A2	FUNCIONARIO/A	TIEMPO COMPLETO
39010 PF1054 1	DIRECCIÓN BIBLIOTECA TORRECEDEIRA	23	A1/A2	FUNCIONARIO/A	TIEMPO COMPLETO
40101 PF1054 1	JEFE/A DE ÁREA DE PROCESO TÉCNICO	23	A1/A2	FUNCIONARIO/A	TIEMPO COMPLETO
39001 PF1054 1	JEFE/A DE ÁREA DE REPOSITORIO INSTITUCIONAL	23	A1/A2	FUNCIONARIO/A	TIEMPO COMPLETO
40401 PF1054 1	JEFE/A DE ÁREA DE SERVICIOS BIBLIOMÉTRICOS	23	A1/A2	FUNCIONARIO/A	TIEMPO COMPLETO
39000 PF1090 1	AYUDANTE DE ARCHIVOS, BIBLIOTECAS Y MUSEOS	21	A2	FUNCIONARIO/A	TIEMPO COMPLETO
39000 PF1090 2	AYUDANTE DE ARCHIVOS, BIBLIOTECAS Y MUSEOS	21	A2		
39000 PF1090 3	AYUDANTE DE ARCHIVOS, BIBLIOTECAS Y MUSEOS	21	A2		
39000 PF1090 4	AYUDANTE DE ARCHIVOS, BIBLIOTECAS Y MUSEOS	21	A2		
39000 PF1090 5	AYUDANTE DE ARCHIVOS, BIBLIOTECAS Y MUSEOS	21	A2		
39000 PF1090 6	AYUDANTE DE ARCHIVOS, BIBLIOTECAS Y MUSEOS	21	A2		
39000 PF1090 7	AYUDANTE DE ARCHIVOS, BIBLIOTECAS Y MUSEOS	21	A2		
39000 PF1090 8	AYUDANTE DE ARCHIVOS, BIBLIOTECAS Y MUSEOS	21	A2		
39000 PF1090 9	AYUDANTE DE ARCHIVOS, BIBLIOTECAS Y MUSEOS	21	A2		
39000 PF1090 10	AYUDANTE DE ARCHIVOS, BIBLIOTECAS Y MUSEOS	21	A2	FUNCIONARIO/A	TIEMPO COMPLETO
39000 PF1090 11	AYUDANTE DE ARCHIVOS, BIBLIOTECAS Y MUSEOS	21	A2		
39000 PF1090 12	AYUDANTE DE ARCHIVOS, BIBLIOTECAS Y MUSEOS	21	A2		
39002 PF1064 1	JEFE/A DE ÁREA DE ADMINISTRACIÓN	22	A2/C1	FUNCIONARIO/A	TIEMPO COMPLETO
39002 PF1110 1	JEFE/A DE NEGOCIADO	20	C1/C2	FUNCIONARIO/A	TIEMPO COMPLETO
39002 PF1160 1	PUESTO BASE	16	C1/C2	FUNCIONARIO/A	TIEMPO COMPLETO

Facultade de Informática da UDC.

Personal de administración y servicios generales de la Facultad de Informática de la UDC:

- Un responsable de asuntos económicos del centro.
- Dos puestos base de asuntos económicos del centro.
- Una secretaria de decanato.
- Un responsable de administración del centro.
- Un negociado del centro.
- Tres puestos bases para administración del centro.
- Un puesto de dirección de biblioteca.
- Un puesto de bibliotecario.
- Dos puestos de ayudante de biblioteca.
- Diversos auxiliares de servicios.
- Un conserje.
- Cuatro ayudantes de conserjería destinados al edificio de la Facultade de Informática.
- Un ayudante de conserjería destinado al edificio del Área Científica.
- Un analista informático.
- Tres técnicos informáticos.

7. RECURSOS, MATERIALES Y SERVICIOS

Disponibilidad y adecuación de recursos materiales y servicios

7.1. Justificación

Para la impartición de las clases del Máster se utilizarán las aulas y laboratorios disponibles en la Facultad de Informática de la UdC. y en la Escuela de Ingeniería de UVigo. En todos los centros se imparten actualmente titulaciones de Grado y Máster, lo que lleva a diferentes grados de ocupación de sus aulas y laboratorios.

Para la impartición del máster propuesto, idealmente se debería contar, en cada centro, con un aula dedicada, dotada con sistemas de videoconferencia. Además, se precisa en cada centro de un laboratorio de ordenadores con una red de área local y servidores completamente aislados del resto de las instalaciones de telecomunicaciones de los centros y de las propias universidades, de modo que las actividades que realice el alumnado, potencialmente nocivas o agresivas, no tengan impacto más allá de en los propios equipos informáticos implicados. Estos laboratorios proporcionarían también una sede estable y segura para las asignaturas relacionadas con la seguridad en redes y equipos que se imparten en los grados y másteres actuales. Tanto en la Universidad de Vigo como en la Universidad de A Coruña, este laboratorio ocupará espacios ya existentes pero será de nueva dotación, ambos con las mismas características técnicas.

7.1.1. Facultad de Informática

Actualmente, la Facultad de Informática cuenta con recursos materiales y servicios adecuados y suficientes para el desarrollo de las actividades formativas planificadas en el Grado de Ingeniería de Informática, así como en los Másteres oficiales adscritos al centro.

Cuenta además con mecanismos para garantizar la revisión, el mantenimiento y la actualización de los materiales, que son responsabilidad de los equipos rectorales y de los equipos de dirección de cada centro. Para ello la UDC cuenta con los siguientes servicios:

- ☐ Servicio de Arquitectura, Urbanismo y Equipamientos
(https://www.udc.es/centros_departamentos_servizos/servizos_xerais/servizo_arquitectura_urbanismo_equipamentos.html?language=es)
- ☐ Servicio de Informática y Comunicaciones
(<https://www.udc.es/sic/>)
- ☐ Servicio de Recursos Audiovisuales
(<https://www.udc.es/umav/situacion.html?language=es>)
- ☐ Servicio de prevención de riesgos laborales
(<https://www.udc.es/prl/index.html?language=es>)

7.1.2. Escuela de Ingeniería de Telecomunicación

Actualmente, la Escuela de Ingeniería de Telecomunicación cuenta con recursos materiales y servicios adecuados y suficientes para el desarrollo de las actividades formativas planificadas en el Grado de Ingeniería de Tecnologías de

Telecomunicación y en los Másteres de Ingeniería de Telecomunicación y de Matemática Industrial.

Además, existen una serie de rutinas orientadas a garantizar el mantenimiento de los espacios para que desempeñen de forma sostenida en el tiempo la función para la que están previstos. Con ese fin se actúa en colaboración directa con la Unidad Técnica de la Universidad de Vigo.

Los mecanismos para realizar o garantizar la revisión y el mantenimiento de los materiales y servicios disponibles incorporan tanto acciones preventivas como paliativas. Las acciones preventivas se basan en los informes de seguimiento y en los planes de mejoras que, anualmente, se realizan para la Escuela en su conjunto y para el título de Máster en su especificidad. El trabajo previo para la elaboración de los informes de seguimiento permite detectar a priori posibles problemas de mantenimiento o de adecuación a las funciones requeridas para la impartición de la titulación. La solución a estos problemas se incorporaría en el correspondiente plan de mejoras.

Las acciones paliativas comienzan por el procedimiento de emisión de quejas y sugerencias, que puede ponerse en marcha mediante [el formulario web de notificación de daños](#),¹⁰ implantado en base al Sistema de Garantía Interno de Calidad, que permite que los problemas de mantenimiento detectados por los usuarios (básicamente, profesorado y alumnado) lleguen a la Dirección de la Escuela y a la Administración de Centro, para que se tomen las medidas subsanatorias oportunas. Este formulario de notificación de daños está pensado de forma específica para la detección temprana de incidencias relativas a recursos, materiales y servicios.

Dependiendo de la magnitud de las acciones necesarias para el mantenimiento de los recursos y servicios, la Junta de Centro decidirá su realización a cargo del propio presupuesto de mantenimiento de la Escuela o la negociación con la Unidad Técnica de la Universidad para la planificación de las obras correspondientes.

Adicionalmente, las instalaciones cumplen con los requisitos de accesibilidad que marca la normativa vigente. Regularmente se evalúa la accesibilidad de los mismos para personas discapacitadas y todos los años se revisan y se subsanan las posibles incidencias al respecto en colaboración con el Vicerrectorado correspondiente y la mencionada Unidad Técnica.

El programa de formación propuesto define dos tipos de grupos de alumnos para las actividades formativas: clases de aula y clases prácticas (con grupos de hasta 20 alumnos) y trabajo en grupo (en equipos de hasta 5 alumnos). Todas las clases de aula se impartirán en las aulas disponibles en la Escuela, concentrando la docencia en una única aula, adaptada para videoconferencia.

El número de aulas es suficiente para la impartición de la docencia de Máster, suponiendo un grupo de aula en primer curso. Las aulas de la Escuela se comparten con la titulación de Grado en Ingeniería de Tecnologías de Telecomunicación y Máster en Ingeniería de Telecomunicación. La impartición de ambos precisa un máximo de 12 aulas, en el caso de que todos los grupos se impartieran a la vez. Este número, que puede reducirse en función de decisiones de organización académica, como establecer grupos con horario de mañana y tarde, es en todo caso inferior a las 15 aulas disponibles, por lo que se puede afirmar que la disponibilidad de aulas es suficiente.

Los seminarios para trabajo en grupo pequeño se orientan a las sesiones presenciales de los grupos de trabajo de cinco alumnos que se configuran en algunas asignaturas. Su número y disponibilidad (tienen uso docente asignado en las titulaciones de Grado

¹⁰ http://www.teleco.uvigo.es/images/stories/documentos/formularios/notificacion_de_danos.pdf

en Ingeniería de Tecnologías de Telecomunicación y Máster en Ingeniería de Telecomunicación), garantizan la dedicación a la docencia del Máster en Ciberseguridad el tiempo necesario. Su número y capacidad son suficientes con la adecuada organización docente de fechas y horarios.

En las tablas siguientes se muestran las aulas y laboratorios instalados en el propio edificio de la Escuela de Ingeniería de Telecomunicación. El uso de aulas y laboratorios estará dedicado al 100% al Grado en Ingeniería de Tecnologías de Telecomunicación, al Máster en Ingeniería de Telecomunicación, al Máster en Matemática Industrial y al Máster en Ciberseguridad que se define en esta memoria.

Las clases prácticas se orientan principalmente a actividades que se desarrollan en los laboratorios, tanto de ordenadores como de equipamiento hardware. Se dispone de 17 laboratorios en la propia Escuela, gestionados por Departamentos con docencia en este Centro y en los que se imparten parte de las clases prácticas de las asignaturas de Electrónica.

Los 17 laboratorios instalados en el propio Centro se dedican íntegramente a la docencia en el Grado y en el Máster. La distribución de asignaturas por laboratorio se realiza en función de las necesidades de cada una de ellas, tanto en lo referente a equipamiento hardware (instrumentación, dispositivos, sistemas, etc.) como en lo que incide sobre el software empleado por las distintas actividades formativas. La cantidad de espacios y su dotación garantiza la impartición de toda la docencia propuesta en las mejores condiciones. El tamaño de los espacios es más que suficiente, en todos ellos, para los grupos de 20 alumnos propuestos.

Los laboratorios tipo PC siguen un plan plurianual para la renovación de sus equipos informáticos, de modo que se evita su obsolescencia. Por su parte, los laboratorios con equipamiento de test y medida disponen de un presupuesto anual, gestionado desde la dirección de la Escuela y ligado al número de alumnos matriculados, para la adquisición de material fungible necesario para las prácticas. Además, la Universidad de Vigo proporciona fondos anuales para la adquisición de equipamiento de prácticas, cuya distribución realiza la Comisión de Infraestructuras de la Escuela tras el análisis de las solicitudes justificadas realizadas por los coordinadores de las asignaturas.

Como apoyo a la actividad docente presencial, la Universidad de Vigo pone a disposición del profesorado la [plataforma informática FAITIC¹¹](http://faitic.uvigo.es/) con recursos en línea destinados a la teleformación. El profesorado dispone de espacio web para crear sus propias páginas relacionadas con la docencia.

¹¹ <http://faitic.uvigo.es/>

Espacios en la Escuela de Ingeniería de Telecomunicación

TIPOLOGÍA DE ESPACIOS Y DOTACIÓN DE INFRAESTRUCTURAS DE DOCENCIA-APRENDIZAJE		
AULA – TIPO GRANDE		
DESCRIPCIÓN GENÉRICA	USO HABITUAL	CAPACIDAD
Aulas de gran capacidad, en las que el alumnado dispone de lugar para sentarse y para escribir. En todas ellas se dispone de un ordenador con conexión a internet y proyección mediante proyector de vídeo. Una de estas aulas tiene pizarra electrónica interactiva y otra está dotada con equipo de grabación.	Clases magistrales. Exámenes y otras pruebas escritas u orales. Cursos y conferencias.	100 alumnos/as
DENOMINACIÓN DEL ESPACIO Y DOTACIÓN	ASIGNATURAS ESPECIALMENTE VINCULADAS	
Aulas T218, T217, T216, T213, T212, T211		

TIPOLOGÍA DE ESPACIOS Y DOTACIÓN DE INFRAESTRUCTURAS DE DOCENCIA-APRENDIZAJE		
AULA – TIPO PEQUEÑO		
DESCRIPCIÓN GENÉRICA	USO HABITUAL	CAPACIDAD
Aulas de mediana capacidad, en las que el alumnado dispone de lugar para sentarse y para escribir. En todas ellas se dispone de un ordenador con conexión a internet y proyección mediante cañón de vídeo.	Clases magistrales. Exámenes y otras pruebas escritas u orales. Cursos y conferencias.	Entre 50 y 80 alumnos/as
DENOMINACIÓN DEL ESPACIO Y DOTACIÓN	ASIGNATURAS ESPECIALMENTE VINCULADAS	
Aulas T110, T109, T108, T107, T104, T103, T102, T101		

TIPOLOGÍA DE ESPACIOS Y DOTACIÓN DE INFRAESTRUCTURAS DE DOCENCIA-APRENDIZAJE		
LABORATORIOS INFORMÁTICOS		
DESCRIPCIÓN GENÉRICA	USO HABITUAL	CAPACIDAD

Laboratorios informáticos equipados con ordenadores tipo PC con software específico y hardware adicional Conexión a internet. Pizarra, proyector de vídeo	La docencia en estos laboratorios se centra en la parte práctica de las asignaturas de las titulaciones actualmente impartidas en la EIT.	Hasta 32 puestos
DENOMINACIÓN DEL ESPACIO Y DOTACIÓN	ASIGNATURAS ESPECIALMENTE VINCULADAS	
Laboratorio AS01 Ordenadores tipo PC con software específico y hardware adicional (osciloscopios, fuentes de alimentación, generadores de señal, ...). Conexión a internet. Pizarra y cañón de vídeo. Capacidad: hasta 32 alumnos Laboratorios AS02, AS03, AS04, AS05, AS07, AS07, B002, BS02 Ordenadores tipo PC con el software específico correspondiente a distintas asignaturas Conexión a internet. Pizarra y cañón de vídeo. Capacidad : de 24 a 42 alumnos Laboratorios T105, T215 Ordenadores tipo PC con el software específico correspondiente básicamente a asignaturas de procesado de imagen/sonido y diseño microelectrónico Conexión a internet. Pizarra y cañón de vídeo. Capacidad : hasta 24 alumnos		
TIPOLOGÍA DE ESPACIOS Y DOTACIÓN DE INFRAESTRUCTURAS DE DOCENCIA-APRENDIZAJE		
LABORATORIOS INSTRUMENTALES		
DESCRIPCIÓN GENÉRICA	USO HABITUAL	CAPACIDAD
Aulas de laboratorio con instrumentación específica de telecomunicación y electrónica. En todas ellas se dispone de un ordenador con conexión a internet y proyector de vídeo.	Clases prácticas y seminarios. Pruebas prácticas u orales. Cursos y conferencias.	Entre 24 y 32 puestos
DENOMINACIÓN DEL ESPACIO Y DOTACIÓN	ASIGNATURAS ESPECIALMENTE VINCULADAS	
Laboratorio BS01 Bancos de trabajo con instrumentación electrónica y optoelectrónica. Incluye una pequeña sala oscura y otra semioscura. Este laboratorio tiene aplicación en asignaturas de circuitos ópticos y de radiofrecuencia. La adscripción de asignaturas se determinará en		

función de la organización académica del centro. Hasta 24 alumnos Laboratorio BS03 Ordenadores tipo PC con el software y hardware adecuados para trabajar con microprocesadores, FPGAs y circuitos electrónicos en general. Conexión a internet. Pizarra y cañón de vídeo. Este laboratorio tiene aplicación en asignaturas de Electrónica. La adscripción de asignaturas se determinará en función de la organización académica del centro. Hasta 24 alumnos Laboratorio BS04 Antenas y equipos de medida; bancos de microondas; ordenador tipo PC para diseño de placas de circuitos impresos; osciloscopios; fuentes; generadores de señal; analizadores de espectros; medidores de campo. Conexión a internet. Pizarra y cañón de vídeo. Este laboratorio es adecuado para asignaturas del ámbito de Radio. La adscripción de asignaturas se determinará en función de la organización académica del centro. La mayor parte de la instrumentación de estos laboratorios está disponible por octuplicado, lo que permite el trabajo en grupos de laboratorio reducidos. Capacidad hasta 24 alumnos Laboratorio LD01 Ordenadores tipo PC con el software específico para diseño y simulación de circuitos electrónicos. Instrumentación y equipos de medida para trabajar con circuitos electrónicos, tanto analógicos como digitales. Conexión a internet. Pizarra y cañón de vídeo. Este laboratorio tiene aplicación en asignaturas de Electrónica básica. La adscripción de asignaturas se determinará en función de la organización académica del centro. Capacidad hasta 24 alumnos.	
--	--

TIPOLOGÍA DE ESPACIOS Y DOTACIÓN DE INFRAESTRUCTURAS DE DOCENCIA-APRENDIZAJE		
LABORATORIOS INFORMÁTICOS		
DESCRIPCIÓN GENÉRICA	USO HABITUAL	CAPACIDAD

Ordenadores PC y MAC dotados de software de cálculo matemático numérico y simbólico, y de software específico de procesamiento de señal. Conexión a Internet y proyector de vídeo.	Clases prácticas y de laboratorio. Pruebas prácticas y exámenes orales. Cursos y conferencias	20 puestos
DENOMINACIÓN DEL ESPACIO Y DOTACIÓN	ASIGNATURAS ESPECIALMENTE VINCULADAS	
Laboratorios LD08, LD09, T106	Criptografía	

Adicionalmente, se cuenta con el uso compartido de algunos laboratorios dependientes del Departamento de Tecnología Electrónica, sitios físicamente en las E.T.S.I. de Industriales y Escuela de Ingeniería de Minas y de la Energía y de la Energía de la Universidad de Vigo. Todos ellos cuentan con las dotaciones instrumentales necesarias para impartir la docencia prevista. En estos laboratorios el uso estaría compartido con la docencia de Física y Electrónica en las otras titulaciones de Ingeniería de la Universidad de Vigo.

La presencia de un aula con capacidad para 240 alumnos puede parecer excesiva en el planteamiento del EEES, pero su mantenimiento resulta de interés principalmente para la realización de exámenes, o pruebas de seguimiento.

Además de la docencia en el propio Centro, la propuesta de Plan de Estudios contempla la posibilidad de que los alumnos realicen prácticas externas optativas, así como la movilidad de los estudiantes. En este sentido, la Comisión Académica del Máster velará para que las empresas e instituciones con las que se firmen los correspondientes convenios de colaboración dispongan de los medios materiales y humanos necesarios para la consecución de los objetivos fijados, y supervisará las actividades que los alumnos realicen para garantizar que cumplen su función de complementar la formación.

TIPOLOGÍA DE ESPACIOS Y DOTACIÓN DE INFRAESTRUCTURAS DE DOCENCIA-APRENDIZAJE		
OTRAS INSTALACIONES		
DESCRIPCIÓN GENÉRICA	USO HABITUAL	CAPACIDAD
Biblioteca Cuenta con depósito de libros, software, fondos fonográficos y videográficos; servicio de préstamo, sala de lectura, ordenadores conectados a internet.	Consulta de fondos, lectura y estudio, acceso a internet.	288 puestos de lectura
Salas de videoconferencia Espacios de capacidad media con equipamiento específico para realizar videoconferencia. Disponen de sillas y mesas para los alumnos	Docencia en los cursos de máster asociados al Centro. Conferencias.	2 salas con capacidades de entre 25 y 45 alumnos

Sala multimedia Aula dotada de sistema audiovisual, con posibilidad de videoconferencia y ordenadores con capacidades multimedia.	Dotada por el Centro Multimedia de Galicia, se usa habitualmente para los cursos y actividades propias del mismo.	34 puestos
Sala Informática Aula con 14 puestos dotados con ordenadores tipo PC. Abierta en el horario establecido por la dirección del centro.	Disponible para el uso de los alumnos para las actividades que consideren oportunas.	14 puestos
Salón de grados Espacio dotado de capacidad de proyección con cañón de vídeo. Dispone de sillones con mesa auxiliar para escribir.	Presentación y defensa de tesis doctorales y trabajos de fin de grado. Conferencias y mesas redondas.	108 plazas
Salón de actos Espacio grande dotado con sistemas de sonido y proyección de vídeo. Dispone de sillones con pala auxiliar para escribir.	Conferencias y mesas redondas. Conciertos y proyecciones cinematográficas. Actos protocolarios.	300 plazas
Salas de reuniones Salas de pequeñas dimensiones con mesas y sillas movibles.	Reuniones de comisiones de trabajo u otras actividades numerosas.	2 salas con capacidad de entre 15 y 20 personas
Sala de Juntas Sala amplia con mobiliario diseñado para reuniones de grupos numerosos. Dispone de pantalla para proyección.	Reuniones de la Junta de Escuela y de la Comisión Permanente del Centro.	Alrededor de 75 plazas
Sala de audición y cámara semianecoica acústica Instrumentos de medida y análisis de señales acústicas, simulación de acústica de salas, transmisión de sonido en edificios, acústica ambiental y edición de audio	Investigación. Demostraciones a grupos reducidos, trabajos de fin de grado	

Laboratorio de medidas radioeléctricas Espacio singular con dotación específica para realizar medida y análisis de señales radioeléctricas (hasta 40GHz) y de compatibilidad electromagnética	Investigación. Demostraciones a grupos reducidos, trabajos de fin de grado	
Laboratorio NORTEL Dotación donada por NORTEL para usos demostrativo y docente, con equipamiento para redes inalámbricas y móviles.	Demostraciones a grupos reducidos, trabajos de fin de grado	

La Biblioteca cuenta con partidas presupuestarias anuales para la adquisición de nuevos libros o de volúmenes adicionales de aquellos que experimentan una mayor demanda. Los profesores de cada asignatura, en la guía docente elaborada y aprobada anualmente, determinan la bibliografía de cada asignatura, lo que ayuda en la planificación de la adquisición y renovación de material bibliográfico.

Espacios en la Facultad de Informática

Las aulas de docencia se encuentran en los pisos 2 y 3 de la Facultad de Informática y en el piso 3 del Edificio del Área Científica.

En la Facultad de Informática existen actualmente 4 aulas grandes (120 puestos) y 13 pequeñas (60, 40 y 36 puestos). Todas cuentan con proyector y equipo informático para el profesor. Para realizar pruebas de evaluación existe un aula de exámenes con capacidad para 250 alumnos.

En cuanto a los laboratorios de prácticas se encuentran en los pisos 0, 1 y 2 de la Facultade de Informática (FIC).

Existen 4 laboratorios de prácticas equipados con equipos informáticos con sistemas operativos Windows y Linux. A mayores, el centro cuenta con 5 laboratorios wifi, un laboratorio de Electrónica y Robótica (0.6) y un laboratorio para alumnos de proyectos fin de máster y grado en el Edificio del Área Científica (AC). Todos los laboratorios tienen un equipo del profesor y un cañón de proyección. Además cuentan con cableado VGA/HDMI para conectar el portátil del profesor.

En cuanto a los espacios docentes del edificio del Área Científica, situado frente a la Facultad, cuenta con 3 aulas docentes cada una de ellas con 36 puestos para estudiantes y 3 aulas más pequeñas, preparadas para recibir a 12 estudiantes cada una de ellas.

El Máster en Ciberseguridad se impartirá en una de las aulas más amplias de este edificio, que será dotada con el equipo necesario para seguir las clases por videoconferencia y para impartirlas desde dicho espacio.

7.2. Convenios

La docencia de la titulación puede verse completada mediante los programas de movilidad nacional e internacional, o con prácticas en empresas que se incorporen como asignaturas optativas. Para llevar a cabo estas actividades, la Escuela dispone de convenios con Universidades y Empresas, que se indican a continuación.

En cuanto a Universidades Europeas, con las que ya se han realizado intercambios de alumnos o profesores, se encuentran las siguientes:

- Bogazici Universitesi, Turquía
- Czech Technical University in Prague, República Checa
- Dublin Institute of Technology, Irlanda
- Ecole Nat. Sup. de Mecanique, Besancon, Francia
- ESIEE (París) , Francia
- Eindhoven University of Technology, Holanda
- ENSEIRB (Burdeos) , Francia
- Fachhochschule Oldenburg/Ostfriesland/Wilhelmshaven, Alemania
- Fachhochschule Darmstadt, Alemania
- Hochschule für Technik und Wirtschaft des Saarlandes, Alemania
- IMEC, Leuven, Bélgica
- Institut National des Télécommunications, Francia
- Institut National Polytechnique de Toulouse, Francia
- Instituto Politécnico de Leiria, Portugal
- Katholieke Universiteit Leuven, Bélgica
- Otto-Von-Guericke-Universitaet Magdeburg, Alemania
- Technical University of Denmark, Dinamarca
- Technische Universiteit Delft, Holanda
- Technikum Wien, Austria
- TEI Kavala, Grecia
- Tomas Bata University in Zlin, República Checa
- Universidade de Aveiro, Portugal
- Universidade do Minho, Portugal
- Universidade Técnica de Lisboa- IST, Portugal
- Università degli Studi del Sannio, Italia
- Università degli Studi di Bologna, Italia
- Università degli Studi di Ferrara, Italia
- Università degli Studi di Napoli Federico II, Italia
- Università degli Studi di Siena, Italia
- Università di Camerino, Italia
- Università di Trento, Italia
- Università di Roma 3, Italia
- Università Roma 2, Italia
- Université de Nantes-Ecole Polytechnique, Francia
- Université de Reims Champagne-Ardenne, Francia
- Université de Rennes I, Francia

- Université Henri Poincaré-Nancy I, Francia
- Université Jean Monnet de Saint Etienne, Francia
- Université Joseph Fourier-Grenoble 1, Francia
- Université Paris 13. Paris Nord, Francia
- Université Pierre et Marie Curie, Francia
- University of Bielsko-Biala, Polonia
- University of Oulu, Finlandia
- University of Southern Denmark , Dinamarca
- XIOS Hogeschool Limburg, Bélgica

Por otra parte, existen convenios con casi todas las Universidades españolas con titulaciones en el ámbito de la Telecomunicación, para intercambios nacionales de estudiantes.

En cuanto a la Facultad de Informática, algunas de las Universidades Europeas con las que ya se han realizado intercambios de alumnos o profesores son:

- Transnationale Universiteit Limburg, Bélgica y Países Bajos
- Université Catholique de Louvain, Bélgica
- Université de Liège, Bélgica
- Tehničko veleučilište u Zagrebu, Croacia
- Panepistimio Kyprou, Chipre
- Západočeská Univerzita v Plzni, República Checa
- Université Claude Bernard Lyon 1, Francia
- Université de Bretagne Occidentale, Francia
- Université de Rennes I, Francia
- Université de Technologie de Belfort-Montbéliard, Francia
- Université Paris 13 - Paris Nord, Francia
- Université Paul Sabatier - Toulouse III, Francia
- Hochschule für angewandte Wissenschaften FH Ingolstadt, Alemania
- Universität Konstanz, Alemania
- Universität Stuttgart, Alemania
- Pécsi Tudományegyetem, Hungría
- Politecnico di Bari, Italia
- Politecnico di Milano, Italia
- Università degli Studi di Bologna 'Alma Mater Studiorum', Italia
- Università degli Studi di Genova, Italia
- Università degli Studi di Messina, Italia
- Università degli Studi di Milano, Italia
- Università degli Studi di Modena e Reggio Emilia, Italia
- Università degli Studi di Palermo, Italia
- Università degli Studi di Roma 'La Sapienza', Italia
- Università della Calabria, Italia
- Vidzemes Augstskola, Letonia
- Norges Teknisk-Naturvitenskapelige Universitet, Noruega
- Universitetet i Bergen, Noruega
- Universitetet i Stavanger, Noruega
- Pastwowa Wyższa Szkoła Zawodowa im. ks. Bronisawa Markiewicza w Jarosławiu, Polonia
- Uniwersytet Im. Adama Mickiewicza, Polonia
- Uniwersytet Kazimierza Wielkiego w Bydgoszczy, Polonia
- Instituto Politécnico de Bragança, Portugal
- Instituto Politécnico do Cávado E Do Ave, Portugal
- Instituto Politécnico do Porto, Portugal
- Instituto Superior Miguel Torga, Portugal

- Universidade da Beira Interior, Portugal
- Universidade da Madeira, Portugal
- Universidade de Aveiro, Portugal
- Universidade de Coimbra, Portugal
- Universidade de Lisboa, Portugal
- Universidade Lusófona de Humanidades e Tecnologias (ULHT), Portugal
- Universidade Nova de Lisboa, Portugal
- Universidade Portucalense Infante D. Henrique, Portugal
- Universitatea 'Politehnica' din Bucuresti (UPB), Rumanía
- Universitatea de Vest din Timisoara, Rumanía
- Universitatea din Bucuresti, Rumanía
- Universitatea Romano Americana, Rumanía
- Universitatea Tehnică Gheorghe Asachi din Iași, Rumanía
- Paneurópska vysoká škola, Eslovaquia
- Univerza v Mariboru, Eslovenia
- Chalmers tekniska högskola, Suecia
- Linnéuniversitetet, Suecia
- University of South Wales, Reino Unido

En lo que respecta a empresas del sector de las Telecomunicaciones, la Escuela y/o la Universidad de Vigo, mantiene convenios con las siguientes, para realizar prácticas profesionales en las mismas:

- 2MARES
- ARCADELECOM
- BALIDEA
- BITOCEANS
- CARRICK BRACELETS
- CHUVI (Complejo Hospitalario Universitario de Vigo)
- CITIOUS
- COCODIN
- COREMAIN
- COUNCILBLOCK
- CROSNETS
- CTAG
- ENCE
- ESMERANTE
- EVERIS
- FEXMXA
- GESERTEL
- GRADIANT
- IGALIAS
- IMATIA
- IMAXDI
- INDESNOR
- INPROSEC
- INSA
- ITELSIS
- MACRAUT INGENIEROS
- MOONOOF
- PARKAPP, S.L.
- PLEXUS
- POSSIBLE
- QBITIA
- R
- REFLEXION ARTS
- SATEC
- SERVICEL
- SOCIAL WIRELABS

- SONIEN
- SPICA
- STREAMING GALICIA
- TECNOCOM
- TEGNIX
- TELEVES
- TELTEK
- TERRAVANZA
- TRESCE
- TURYELECTRO GALICIA, S.L.
- ULTREIA
- WIRELESS GALICIA

En cuanto a la Facultad de Informática, mantiene convenios para realizar prácticas profesionales con las siguientes empresas:

- Ágora Binaria S.L.
- Aldaba Servicios Profesionales, S.L.
- Allenta Consulting, S.L.
- Alsernet 2000, S.L.
- Altia Consultores, S.A.
- Appentra Solutions S.L.
- Asociación de Autónomos para la Innovación, Desarrollo, Investigación y Formación
- Avansing, S.L.L.
- Bahía Software
- BALIDEA Consulting & Programming, S.L.
- Bricoking, S.A.
- Caamaño Sistemas Metálicos, S.L.
- Cámara Oficial de Comercio, Industria, Servicios y Navegación de A Coruña
- Cenfop Die, S.L.U.
- Classora Technologies, S.L.
- Comasis Consultores de Management y Sistemas, S.L.
- Concello da Coruña
- CORUNET, S.L.
- Denodo Technologies, S.L.
- Domotecnología y Seguridad, S.L.
- Enxenio, S.L.
- Everis Spain, S.L.U.
- Evialis Galicia, S.A.
- Factoría de Software e Multimedia, S.L.
- Fundación Instituto Tecnológico de Galicia
- GT Motive
- Health in Code, S.L.
- Igalia, S.L.
- IGASOTF, S.L.
- Imatia Innovation
- INDITEX
- Indra Software Labs, S.L.U.
- Ingeniería de Software Avanzado
- Instrumentación y Componentes, S.A.
- Lance Talent, S.L.
- LINKNOVATE SCIENCE, S.L.
- MNM PROGRAMACIÓN S.L.
- MOBGEN TECHNOLOGY, S.L.
- Netex Knowledge Factory, S.L.
- Nextgal Soluciones Informáticas, S.L.
- Nomasystems, S.L.
- PricewaterhouseCoopers Auditores, S.L.

- R Cable y Telecomunicaciones Galicia, S.A.
- Redes de Comunicación Galegas RETEGAL, S.A.
- SBS SEIDOR, S.L..
- Selective Outsourcing of Information Technologies
- Serviguide Consultoría, S.L.
- Servizo Galego de Saúde (Consellería de Sanidade)
- Software e Multimedia, S.L.
- Streamnow, S.L.
- Tarlogic Security, S.L.
- Técnicas de Soft, S.A.
- Tecnocon Telecomunicaciones y Energía
- Telecon Galicia, S.A.
- Torus Software Solutions, S.L.
- Transformaciones Globales, S.L.
- Trileuco Solutions
- Zemsania S.L.

M^a DOLORES GONZÁLEZ ÁLVAREZ, VICERRECTORA DE ESTUDIANTES DE LA
UNIVERSIDAD DE VIGO,

HACE CONSTAR:

Que según consta en la documentación archivada en esta universidad, se han firmado los convenios de colaboración con las entidades que se relacionan a continuación para la realización de prácticas externas por parte del alumnado de la Universidad de Vigo:

- 2MARES
- ARCATELECOM
- BALIDEA
- CARRICK BRACELETS
- CHUVI (Complejo hospitalario Universitario de Vigo)
- COCODIN
- COREMAIN
- COUNCILBLOXX
- CTAG
- ENCE
- ESMERANTE
- EVERIS
- FEMXA
- GESERTEL
- GRADIANT
- IGALIAS
- IMATIA
- IMAXDI
- INDESNOR
- INPROSEC
- INSA
- ITELSIS
- MACRAUT IMGEMIEROS
- MOONOOOF
- OPTARE
- PARKAPP, S.L.
- PLEXUS
- POSSIBLE
- QBITIA
- R

- SATEC
- SERVICEL
- SOCIAL WIRELABS
- SONEN
- SPICA
- STREAMING GALICIA
- TECNOCOM
- TEGNIX
- TELEVES
- TELTEK
- TERRAVANZA
- TRESCE
- TURYELECTRO GALICIA, S.L.
- ULTREIA
- WIRELESS GALICIA

Así mismo, que según consta en la documentación archivada en esta universidad, se han firmado los convenios de movilidad con las universidades que se relacionan a continuación:

- Bogazici Universitesi, Turquía
- Czech Technical University in Prague, República Checa
- Ecole Nat. Sup. de Mecanique, Besancon, Francia
- ESIEE (París) , Francia
- Eindhoven University of Technology, Holanda
- ENSEIRB (Burdeos) , Francia
- Fachhochschule Oldenburg/Ostfriesland/Wilhelmshaven, Alemania
- Fachhochschule Darmstadt, Alemania
- Hochschule für Technik und Wirtschaft des Saarlandes, Alemania
- Institut National Polytechnique de Toulouse, Francia
- Instituto Politécnico de Leiria, Portugal
- Katholieke Universiteit Leuven, Bélgica
- Otto-Von-Guericke-Universitaet Magdeburg, Alemania
- Technische Universiteit Delft, Holanda
- Technikum Wien, Austria

- TEI Kavala, Grecia
- Tomas Bata University in Zlin, República Checa
- Universidade de Aveiro, Portugal
- Universidade do Minho, Portugal
- Università degli Studi del Sannio, Italia
- Università degli Studi di Bologna, Italia
- Università degli Studi di Ferrara, Italia
- Università degli Studi di Napoli Federico II, Italia
- Università degli Studi di Siena, Italia
- Università degli Studi di Roma Tre, Italia
- Università di Camerino, Italia
- Università di Trento, Italia
- Università Roma 2, Italia
- Université de Nantes-Ecole Polytechnique, Francia
- Université de Reims Champagne-Ardenne, Francia
- Université de Rennes I, Francia
- Université Jean Monnet de Saint Etienne, Francia
- Université Joseph Fourier-Grenoble 1, Francia
- Université Paris 13. Paris Nord, Francia
- Université Pierre et Marie Curie, Francia
- University of Bielsko-Biala, Polonia
- University of Oulu, Finlandia
- University of Southern Denmark, Dinamarca

Y para que así conste a los efectos oportunos, se expide el presente documento en Vigo a 11 de octubre de 2017



8. RESULTADOS PREVISTOS

8.1. Valores cuantitativos estimados para los siguientes indicadores y su justificación.

8.1.1. Justificación de los indicadores

Para el cálculo de la tasas de resultados propuestas se han considerado los datos de las actuales titulaciones de máster del área de Ingeniería de la Universidad de Vigo en el periodo que comprende los cursos académicos 2010/2011 a 2015/2016 (tomadas del servicio SIIU, Sistema Integrado de Información Universitaria) así como los controles y seguimientos realizados en los procesos de admisión de alumnos de nuevo ingreso y el seguimiento en materia de calidad en relación con el Sistema de Garantía Interna de Calidad (SGIC) de la Escuela de Ingeniería de Telecomunicación. En promedio, la tasa de abandono de la muestra se sitúa en el 14,31%, si bien los datos individuales son dispares y oscilan entre el 5% (la menor de las medidas) y el 25% (la mayor). Aunque dichas tasas actuales en estos estudios se consideran satisfactorias, el diseño del plan de estudios del Máster en Ciberseguridad, y el modelo de docencia, con clases a un grupo reducido y el uso de mecanismos consolidados de evaluación continua, así como las adaptaciones realizadas en la normativa de permanencia y matrícula de la Universidad van a permitir mejorarlos y conseguir los objetivos planteados.

La estructura del plan de estudios del Máster en Ciberseguridad parte de la experiencia previa en el Máster de Ingeniería de Telecomunicación de la Universidad de Vigo y el Máster Universitario en Ingeniería Informática de la Universidad de A Coruña para intentar ajustar los contenidos al tiempo de trabajo real de los estudiantes, concentrando en el último cuatrimestre el trabajo fin de máster y las prácticas profesionales, sin otra carga lectiva. En cuanto a las normas de permanencia y matrícula, estas prevén la modalidad matrícula a tiempo parcial, con el fin de cubrir las necesidades de los diferentes tipos de estudiantes, y se ha flexibilizado el número mínimo de créditos que garantizan la permanencia de los estudiantes. Por estos motivos, esperamos cumplir con una tasa de abandono inferior al 20% y una tasa de graduación superior al 70%.

Se ha preferido no incluir las tasas de rendimiento y éxito en las previsiones, pues los datos de la muestra referida contienen másteres con números de matrícula muy heterogéneos.

Tasas propuestas para el Título	
Denominación	Valor (%)
Tasa de graduación	> 70%
Tasa de abandono	< 20%
Tasa de eficiencia	> 80%
Tasa de rendimiento	
Tasa de éxito	

8.2. Progreso y los resultados de aprendizaje de los estudiantes

El Sistema de Garantía de Calidad de todos los Centros de la Universidad de Vigo, teniendo en cuenta "Los criterios y directrices para el aseguramiento de la calidad en Espacio Europeo de Educación

Superior (ESG).” (ENQA, 2015), incorpora varios procedimientos documentados destinados a seguir, controlar y mejorar los resultados de aprendizaje de los estudiantes:

Procedimientos del SGIC de los Centros de la Universidad de Vigo	Criterios ENQA
DO0201 P1 Planificación y desarrollo de la enseñanza	1.3. Enseñanza, aprendizaje y evaluación centrados en el estudiantes
DE03 P1 Revisión del sistema por la dirección	Criterio 1.7 Gestión de la Información
DE02 P1 Seguimiento y Medición	

8.2.1 DO0201 P1 Planificación y desarrollo de la enseñanza

La finalidad de este procedimiento del sistema de calidad del centro que alcanza a todos los grados y másteres del mismo, es garantizar que la planificación y desarrollo de la enseñanza es coherente con la memoria de la titulación se adecúa al perfil del alumnado destinatario e incluye elementos adecuados de información pública que permite la mejora continua.

8.2.2 DO03 P1 Revisión del sistema por la dirección

Este procedimiento centraliza el análisis global anual de todos los resultados del centro y particularmente de sus titulaciones. El resultado de este procedimiento es la aprobación de un informe anual completo y público que recoge y analiza todos los resultados de las titulaciones y determina las acciones de mejora necesarias para alcanzar mejores resultados, tal y como se recoge a continuación:

8.2.3 DE02 P1 Seguimiento y medición

Este procedimiento supone la puesta en marcha de herramientas de seguimiento y medición que permiten a los centros/títulos la toma de decisiones.

Centraliza un panel de indicadores de satisfacción, de rendimiento académico, de matrícula...etc.

El Sistema de Garantía de Calidad de todos los Centros de la Universidad de Vigo, teniendo en cuenta “Los criterios y directrices para el aseguramiento de la calidad en Espacio Europeo de Educación Superior (ESG).” (ENQA, 2015), incorpora varios procedimientos documentados destinados a seguir, controlar y mejorar los resultados de aprendizaje de los estudiantes:

Procedimientos del SGIC de los Centros de la Universidad de Vigo	Criterios ENQA
DO0201 P1 Planificación y desarrollo de la enseñanza	1.3. Enseñanza, aprendizaje y evaluación centrados en el estudiantes
DE03 P1 Revisión del sistema por la dirección	Criterio 1.7 Gestión de la Información
DE02 P1 Seguimiento y Medición	

9. GARANTÍA DE CALIDAD

La Escuela de Ingeniería de Telecomunicación participó en la primera convocatoria del Programa FIDES-AUDIT, en fase de implantación. Durante la elaboración de esta memoria el centro fue sometido a una auditoría externa para la certificación de la implantación del Sistema de Garantía Interno de Calidad. A finales de julio de 2013 se recibió el informe FAVORABLE, emitido por el equipo auditor, a dicha certificación. En el informe correspondiente, el equipo auditor justifica el informe favorable con los siguientes argumentos:

El equipo auditor, una vez examinado el Sistema de Garantía Interna de Calidad (SGIC) de la Escuela de Ingeniería de Telecomunicación de la Universidad de Vigo y tras el desarrollo de la visita de auditoría, ha evidenciado que, en esta Escuela, se ha logrado una muy razonable implantación y despliegue de la mayor parte de los procedimientos de su SGIC tal y como se definieron en el momento de la evaluación del diseño y tal y como han evolucionado hasta la actualidad. Asimismo se ha constatado que el funcionamiento global del Sistema de Garantía Interna de Calidad de esta Escuela está claramente orientado a la mejora continua de la formación que ofrece a sus estudiantes.

Por otra parte la auditoría ha puesto de manifiesto una activa implicación en la Comisión de Garantía de Calidad de la Escuela de todos los grupos de interés implicados y concernidos, siendo de destacar el grado de implicación y el compromiso de los estudiantes.

Finalmente, se debe destacar que esta valoración positiva es consecuencia directa del apoyo a la Comisión de Garantía de Calidad de la Escuela por parte del Área de Calidad de la Universidad de Vigo y, especialmente, de la implicación del equipo directivo de la Escuela donde se quiere destacar la intensa dedicación, la implicación y el trabajo desarrollado por la Directora de la Escuela y la Coordinadora de Calidad para lograr la correcta y adecuada implantación del Sistema de Garantía Interna de Calidad de la Escuela.

El Sistema de Garantía Interna de Calidad del Centro, adaptado a partir del Documento-Marco elaborado por el área de Calidad de la Universidad de Vigo, se aprobó el 24 de abril del 2008 en Junta de Escuela. El 30 de enero de 2009 la Comisión de Garantía de Calidad recibió por parte de las comisiones evaluadoras de ACSUG el informe final de la evaluación del diseño del SGIC, emitiendo una valoración global POSITIVA.

El detalle de cada uno de los puntos establecidos en el Apartado 9 (Sistemas de Garantía de Calidad) del Real Decreto 1393/2007, del 29 de Octubre, y Real Decreto 861/2010 (que modifica al anterior) se encuentra en la página web de la Escuela, aportando el diagrama de flujo de los procedimientos implicados y la ficha resumen de los mismos. La información completa sobre el Manual del Sistema de Garantía Interna de Garantía de Calidad de la Escuela de Ingeniería de Telecomunicación de la Universidad de Vigo, así como el conjunto de procedimientos asociados, se encuentran disponibles [a través de este enlace](http://teleco.uvigo.es/index.php/es/escuela/calidad).¹²

Toda esta información es accesible para todos los colectivos implicados (estudiantes, personal académico y de administración y servicios, empleadores y sociedad en general) a través de la web de la Escuela (teleco.uvigo.es), siguiendo el menú Escuela -> Calidad.

¹² <http://teleco.uvigo.es/index.php/es/escuela/calidad>

Responsables del Sistema de Garantía Interna de Calidad del Plan de Estudios.

Los órganos designados para la gestión del Sistema de Garantía Interna de Calidad de la Escuela de Ingeniería de Telecomunicación son:

- **Comisión de Calidad**
Es el órgano que participa en las tareas de planificación y seguimiento del SGIC, actuando además como uno de los vehículos de comunicación de la política, objetivos, planes, programas, responsabilidades y logros de este sistema.
La información relativa a la Comisión de Calidad de la Escuela (constitución, listado de miembros, actas) se encuentra disponible en el enlace siguiente:
<http://teleco.uvigo.es/index.php/es/escuela/calidad/cgc>
- **Coordinador de Calidad**
Efectuará las tareas de coordinación derivadas de la implantación del SGIC en la Escuela de Ingeniería de Telecomunicación.
- **Equipo Directivo:**
El Equipo Directivo, como principal responsable, se compromete al establecimiento, desarrollo, revisión y mejora del Sistema de Garantía Interno de Calidad. En este sentido asume las responsabilidades que en los diferentes documentos del SGIC se indican, promoverá la creación de equipos de mejora para atender a los resultados de las revisiones y evaluaciones realizadas, liderando en todo momento las actuaciones correspondientes al SGIC.
- **Junta de Titulación/Junta de Escuela**
Es el órgano que se encarga de aprobar la documentación del SGIC y a su vez velar por el desarrollo y mejora del mismo.

10. CALENDARIO DE IMPLANTACIÓN

10.1. Cronograma de implantación de la titulación

El primer curso del nuevo título tiene prevista su implantación el curso 2018/19. Siguiendo las recomendaciones del documento del *Consello Galego de Universidades*: “Líneas generales la implantación de los Estudios de Grado y Posgrado en el Sistema Universitario de Galicia”, y teniendo en cuenta que los recursos humanos y materiales existentes en la Escuela de Ingeniería de Telecomunicación así lo permiten, se propone preferentemente la implantación anual curso a curso.

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

El acceso al máster está enfocado a titulados y tituladas en cualquier Máster o Grado de la rama de Telecomunicación, de Informática, o de otras ramas científicas o tecnológicas en las condiciones que defina la Comisión Académica del Máster.

No existe en el Sistema Universitario de Galicia una titulación equivalente a la propuesta, por lo que no procede la definición de un plan de adaptación al nuevo Máster para estudiantes de estudios ya existentes.

La adaptación de alguna asignatura de nivel máster de otras titulaciones que hayan cursado previamente los alumnos será decidida por la Comisión Académica de Máster, que irá completando, en su caso, un catálogo de adaptaciones para mantener un criterio coherente en las mismas.

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

La implantación del título de Máster en Ciberseguridad no está acompañada de la extinción de ningún otro título previo.