

Universidade de Vigo

MASTER UNIVERSITARIO

EN CIBERSEGURIDADE

(Universidade de Vigo-Universidade da Coruña)

Versión 2 16/05/2023 tras IP de ACSUG



Memoria para la verificación de titulaciones oficiales de Grado y Máster Universitario de acuerdo con el Real Decreto 822/2021, de 28 de septiembre, por el que se establece la organización de las enseñanzas universitarias y del procedimiento de aseguramiento de su calidad.

CONTENIDO

Contenido.....	2
1. Descripción, objetivos formativos y justificación del título.....	4
1.1. Descripción	4
1.2. Justificación del título.....	5
Relación con las características socioeconómicas de la zona de influencia del Título.....	5
Experiencias previas de la Universidad en títulos similares y procedimientos de consulta.	7
Justificación de la existencia de referentes nacionales e internacionales.	8
1.3. Objetivos formativos	9
Objetivos formativos de las menciones o especialidades	9
Estructuras curriculares específicas y justificación de sus objetivos.....	9
Estrategias metodológicas de innovación docente específicas y justificación de sus objetivos	9
Perfiles fundamentales de egreso a los que se orientan las enseñanzas	10
Actividad profesional regulada habilitada por el título	10
2. Resultados del proceso de formación y de aprendizaje	11
2.1. Conocimientos o contenidos	11
2.2. Habilidades o destrezas.....	12
2.3. Competencias	13
3. Admisión, reconocimiento y movilidad	14
3.1. Requisitos de acceso y procedimientos de admisión de estudiantes	14
3.2. Criterios para el reconocimiento y transferencias de créditos	15
3.3. Procedimientos de movilidad	16
4. Planificación de las enseñanzas	18
4.1. Estructura básica de las enseñanzas	18
Plan de estudios detallado	19
Asignatura 1: Seguridad de la información (SI)	20
Asignatura 2: Análisis de malware (MWR)	20
Asignatura 3: Privacidad y anonimidad (PAN)	21
Asignatura 4: Seguridad de aplicaciones (SAPP)	21
Asignatura 5: Redes Seguras (RED)	22
Asignatura 6: Tecnologías de Registro Distribuido y Blockchain (BC).....	23
Asignatura 7: Seguridad en comunicaciones (SCOM)	23

Asignatura 8: Fortificación de sistemas (FORT).....	24
Asignatura 9: Ciberseguridad Industrial e IoT (CSIoT).....	24
Asignatura 10: Hacking ético y Test de intrusión (INT)	25
Asignatura 11: Negocio en ciberseguridad y emprendimiento (NEG)	25
Asignatura 12: Análisis forense (AF)	26
Asignatura 13: Seguridad en Centros de datos (CD).....	26
Asignatura 14: Seguridad en dispositivos móviles (MOV)	27
Asignatura 15: Smart Contracts y dApps (CIAD)	27
Asignatura 16: Gestión de seguridad de la información GSI	28
Asignatura 17: Conceptos y Leyes (CL)	28
Asignatura 18: Prácticas en empresa (PRA)	29
Asignatura 19: Trabajo de fin de máster (TFM).....	29
5. Personal académico y de apoyo a la docencia.....	30
5.1. Perfil básico del profesorado.....	30
5.2. Perfil básico de otros recursos de apoyo a la docencia necesarios.....	33
6. Recursos para el aprendizaje: materiales e infraestructurales, prácticas y servicios.....	34
6.1. Recursos materiales y servicios	34
6.2 Procedimiento para la gestión de las prácticas externas	34
6.3. Previsión de dotación de recursos materiales y servicios	35
7. Calendario de implantación.....	36
7.1. Cronograma de implantación del título	36
7.2 Procedimiento de adaptación.....	36
7.3 Enseñanzas que se extinguen	36
8. Sistema Interno de Garantía de la Calidad	37
8.1. Sistema Interno de Garantía de la Calidad.....	37
8.2. Medios para la información pública.....	37

1. DESCRIPCIÓN, OBJETIVOS FORMATIVOS Y JUSTIFICACIÓN DEL TÍTULO

1.1. Descripción

TABLA 1. Descripción del título

1.1. Denominación del título:	Máster Universitario en Ciberseguridad por la Universidade de Vigo y la Universidade da Coruña
1.2. Ámbito de conocimiento:	Interdisciplinar/Ingeniería Informática/Ingeniería de Telecomunicación
1.3. Menciones y especialidades:	No hay
1.4.a) Universidad responsable:	Universidade de Vigo
1.4.b) Universidades participantes:	Universidade de Vigo Universidade da Coruña
1.4.c) Convenio:	
1.5.a) Centro de impartición responsable:	Escola de Enxeñaría de Telecomunicación (UVIGO)
1.5.b) Centros de impartición:	Escola de Enxeñaría de Telecomunicación (UVIGO) Facultade de Enxeñaría Informática (UDC)
1.6. Modalidad de enseñanza:	Presencial
1.7. Número total de créditos:	90
1.8. Idiomas de impartición:	Gallego/ Español /Inglés
1.9.a) Número total de plazas:	40
1.9.b) Oferta de plazas en modalidad presencial:	40
1.9.c) Oferta de plazas en modalidad semipresencial o híbrida:	0
1.9.d) Oferta de plazas en modalidad no presencial o virtual:	0

TABLA 2. Centros

Centro:	Escola de Enxeñaría de Telecomunicación	Código RUCT:	36016981
Universidad:	Universidade de Vigo	Código RUCT:	038
Oferta de plazas del Centro:	Presencial: 20		
Menciones / Especialidades:	No hay		
Idiomas de impartición	Gallego/ Español / Inglés		
Centro:	Facultade de Informática	Código RUCT:	15025451
Universidad:	Universidade da Coruña	Código RUCT:	037
Oferta de plazas del Centro:	Presencial: 20		
Menciones / Especialidades:	No hay		

1.2. Justificación del título

Esta memoria corresponde con la modificación del título Máster Universitario en Ciberseguridad (en adelante MUnICS) impartido por la Universidade de Vigo (en adelante UVIGO) y la Universidade da Coruña (en adelante UDC) desde el curso 2018-2019, establecido el carácter oficial del título por Acuerdo del Consejo de Ministros de 5/10/2018 (publicado en el «Boletín Oficial del Estado» de 21/12/2018, por resolución del Secretario General de Universidades de 26/11/2018); y tras Resolución de 16 de mayo de 2019, de la Universidad de Vigo, se publica el plan de estudios de Máster en Ciberseguridad (Máster conjunto de las universidades de Vigo y A Coruña) en la resolución 8548 en el «Boletín Oficial del Estado» de 08/06/2019.

La modificación de la memoria viene motivada por un doble factor, la reducción del tamaño del módulo de prácticas, obteniendo un título que de acuerdo al RD 592/2014, de 11 de julio, por el que se regulan las prácticas académicas externas de los estudiantes universitarios («BOE» núm. 184, de 30 de julio de 2014); permitiendo el reconocimiento profesional de las mismas siempre que se cumplan los criterios académicos para ello y (2) la incorporación de nuevos contenidos relacionados con la ciberseguridad, en concreto, aquellos que se encuentran bajo la definición de “Máster en blockchain y DLT” en el documento resultado del proyecto «Galicia 2030. Perfiles Profesionales de Futuro y Nuevas Titulaciones y Especialidades» de Consellería de Cultura, Educación e Universidade, en el que se promueven perfiles profesionales de futuro en el Sistema Universitario de Galicia. El cotejo de la oferta formativa SUG en dicho documento concluye que, aunque no existen en Galicia titulaciones con un grado de afinidad importante a dicho perfil, la existencia del Máster Interuniversitario en Ciberseguridad impartido por la UDC y la UVIGO podría aportar ciertos contenidos de interés para este rol de experto. Bajo esta motivación se incorporan en la modificación en este documento los conceptos fundamentales bajo el perfil de experto en Blockchain, teniendo en cuenta que hay un cierto solape entre las materias con MUnICS. Estando en vigor el nuevo Real Decreto 822/2021, de 28 de septiembre, “por el que se establece la organización de las enseñanzas universitarias y del procedimiento de aseguramiento de su calidad” la modificación del título de Máster incluye su adecuación a lo estipulado en dicho RD.

Relación con las características socioeconómicas de la zona de influencia del Título.

El presente tecnológico actual está marcado por la capacidad disruptiva de la transformación digital en todos los sectores de producción de bienes y servicios, así como en las administraciones públicas. La nueva Sociedad digital se caracteriza por la omnipresencia de los canales y procesos digitales como evolución/transformación de los canales y procesos tradicionales. En las Estrategia de Ciberseguridad de la UE se reconoce la importancia de reforzar la resistencia a las ciber-amenazas y garantizar que los ciudadanos y las empresas se beneficien de tecnologías digitales en un momento en el que la transformación digital de la sociedad, intensificada por la crisis del COVID-19, ha ampliado el panorama de las amenazas y está planteando nuevos retos, que requieren respuestas adaptadas e innovadoras. El número de ciberataques sigue aumentando, con ataques cada vez más sofisticados procedentes de una amplia gama de fuentes, tanto dentro como fuera de la UE. Esta perspectiva europea se traslada al ámbito nacional y, como no podía ser de otra manera, al ámbito de Galicia,

donde se crea el nodo gallego de ciberseguridad, CIBER.gal, entidad conformada por las administraciones públicas gallegas e instituciones privadas que, de manera colaborativa, buscan hacer frente a la creciente amenaza que suponen los ciberataques y aprovechar las oportunidades que presenta la nueva era digital.

La confianza en la **nueva sociedad digital** es una de las cuestiones que más preocupa a los agentes implicados, ya que la transformación digital ha cambiado los riesgos a los que se ven expuestas empresas, gobiernos y ciudadanos en un mundo hiperconectado donde los innumerables beneficios de la sociedad digital vienen acompañados de nuevas amenazas y nuevas formas de delincuencia. 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. La demanda ya percibida en la puesta en marcha de MUniCS no ha sino crecido y ampliado su espectro hasta alcanzar todos los sectores de la sociedad y la economía. A modo de ejemplo, el Instituto Nacional de Ciberseguridad (INCIBE), en el informe elaborado este mismo año 2022 por parte del observatorio ObservaCibe (“Análisis y Diagnóstico del Talento en Ciberseguridad en España”), en el que se refleja el estado actual del talento en el sector de la ciberseguridad en el país, donde en torno al 40,1% de las organizaciones consultadas reconoce que reciclan el talento proveniente de otros departamentos hacia el área de ciberseguridad y pese a esta tendencia, únicamente 2 de cada 10 posiciones internas reciben formación o poseen conocimientos para poder desempeñar las funciones que se requieren.

(ISC)² -la mayor asociación sin ánimo de lucro del mundo de profesionales de ciberseguridad- en su informe sobre el mercado laboral 2021, aunque revela una disminución de la escasez de mano de obra mundial por segundo año consecutivo, sigue registrando un déficit de 2,72 millones de profesionales de la ciberseguridad. Hay dos factores significativos que contribuyen a la estimación del déficit de mano de obra de este año. Para ver estas cifras en perspectiva, se debe recalcar que, a nivel mundial, la mano de obra en ciberseguridad necesita crecer un 65% para una defensa eficaz de la sociedad digital. Por tanto, **resulta evidente que la demanda sigue creciendo a una velocidad muy superior a la que las escuelas tecnológicas pueden formar a los profesionales TIC en el ámbito ciberseguridad**. 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.

MUniCS responde a la necesidad de la sociedad, de la empresa y de la industria; la demanda por parte de los estudiantes de los centros que imparten títulos en el área TIC; y al profesorado capacitado y motivado que ha puesto en marcha esta titulación. La transformación digital se une ahora a un cambio equivalente en el paradigma industrial, la conocida Industria 4.0, que precisa de una fuerte inversión en seguridad de la información y de los procesos. Todas estas necesidades y demandas tienen respuesta en la colaboración de los centros en este título, con experiencia larga y demostrada en la formación de especialistas en redes, comunicaciones, software y sistemas de información.

La propuesta MUniCS, impartido entre UVIGO y UDC implica a dos centros: Escuela de Ingeniería de Telecomunicación (en adelante EET) de UVIGO y Facultade de Informática (en adelante FIC)

de UDC; y complementa las titulaciones TIC de ambas instituciones: Grado en Ingeniería de Tecnologías de Telecomunicación, en UVIGO; y los grados en Ingeniería Informática, Ciencia de datos e Inteligencia Artificial, en UDC. MUniCS se ha convertido en un referente regional y nacional en su ámbito y, a través de la **Cátedra R en ciberseguridad** (convenio firmado en diciembre 2018, renovado en febrero 2022) ha impulsado numerosas acciones de concienciación y visibilización de la ciberseguridad en Galicia, organizando eventos de gran relevancia a nivel autonómico como el Cybersec@gal 2019 y 2020; así como la participación en el foro ciber.gal 2021.

Al servicio de este ambiente institucional, social y económico-empresarial, **MUniCS 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 modificado 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. Adicionalmente, y según la motivación expuesta viene a cubrir un hueco de formación en el ámbito del Blockchain en el SUG.

Experiencias previas de la Universidad en títulos similares y procedimientos de consulta.

UCIGO y UDC vienen impartiendo el título MUniCS desde el curso 2018/2019. El procedimiento seguido para la modificación de este título de máster se ajusta a las normas y recomendaciones establecidas por las Universidades de A Coruña, y Vigo. Concretamente, se están siguiendo los plazos y procedimientos descritos en el documento [“Calendario e procedemento para a aprobación de verificación e modificación de titulacións de grao, máster e doutoramento para o curso 2023/2024”](#)

En particular, y dado que la iniciativa parte de MUniCS como una modificación del propio título bajo los antecedentes presentados en este documento, la gestión y coordinación de la redacción de la modificación del plan de Estudios ha sido realizada desde la Comisión Interuniversitaria del Máster en Ciberseguridad en colaboración con las Comisiones Académicas de Máster locales en la EET de UVIGO y en FIC de UDC. La CAMI está formada por los coordinadores locales de MUniCS más 2 representantes adicionales del cuerpo docente de ambas sedes (uno por sede) y la subdirección de calidad de la EET, centro coordinador de la titulación.

La modificación del Plan de Estudios ha estado precedida de las actuaciones recogidas en el Informe de seguimiento de la titulación de forma anual, en lo que se refiere a los ajustes necesarios en el mismo. Además, la CAMI ha realizado consultas a todos los centros y Universidades que expresaron intereses en su participación en el MU de Blockchain y tecnologías DLT. EET de UVIGO y FIC de UDC expresaron su interés en dicho Máster como una modificación de MU en Ciberseguridad que actualmente imparten ambos centros. La CAMI como Comisión Redactora mantiene reuniones

periódicas de coordinación internas, así como con la Dirección de Posgrado de la Universidad de Vigo como área que monitoriza el proceso.

En cuanto a los procedimientos de consulta externos, se han tenido en cuenta los planes de estudios de otros programas de máster afines, así como el informe «Galicia 2030. Perfiles Profesionales de Futuro y Nuevas Titulaciones y Especialidades» de Consellería de Cultura, Educación e Universidade, en el que se promueven perfiles profesionales de futuro en el Sistema Universitario de Galicia. Este análisis ha servido para inspirar la modificación de MUniCS para integrar en lo posible los contenidos del MU Blockchain y DLT teniendo en cuenta que una parte relevante de los contenidos identificados en el informe ya formaban parte del currículo de MUniCS. En lo que respecta de forma exclusiva a los estudios de máster en tecnologías Blockchain y DLT se han contrastado los contenidos con el único referente de características similares e España. El Máster Universitario en Tecnologías Blockchain de Universidad Politécnica de Cataluña. A nivel internacional proliferan los Máster en el ámbito del Blockchain relacionados con las criptomonedas o las finanzas; a diferencia de estos, en MUniCS se cubren fundamentalmente los aspectos técnicos de las tecnologías Blockchain y DLT en lo que a sistemas de información y comunicación se refiere.

Justificación de la existencia de referentes nacionales e internacionales.

Se recoge en este apartado una lista actualizada de los referentes nacionales e internacionales relacionados con la Ciberseguridad. En lo que tienen que ver con los referentes nacionales se recogen algunos de los Másteres Universitarios de carácter técnico, que se pueden encontrar en el catálogo del INCIBE:

- Máster Internacional Universitario en Protección de Datos, Transparencia y Acceso a la Información (CEU San Pablo)
- Máster Semipresencial Universitario en Ciberseguridad (UAX)
- Máster Universitario de Ciberseguridad (UCJC)
- Máster Universitario en Ciberseguridad (UC3M)
- Máster Universitario en Ciberseguridad (UAH)
- Máster Universitario en Ciberseguridad (Universidad Politécnica de Cataluña)
- Máster Universitario en Ciberseguridad (Universidad Politécnica de Madrid)
- Máster Universitario en Ciberseguridad (Universidad Politécnica de Valencia)
- Máster Universitario en Ciberseguridad (Universidad Pontificia de Comillas)
- Máster Universitario en Ingeniería de la Seguridad Informática e Inteligencia Artificial (Rovira y Virgil)
- Máster en Ciberseguridad y Privacidad (Universidad Rey Juan Carlos)
- Máster Universitario en Ciberseguridad (Universidad Internacional de Valencia)
- Máster Universitario en Ciberseguridad (Universidad Isabel I de Castilla)
- Máster Universitario en Ciberseguridad (Universidad de Alicante)
- Máster Universitario en Seguridad Informática (Universidad de Cádiz)
- Máster Universitario en Seguridad Informática (Universidad de Jaén)
- Máster Universitario en Seguridad Informática (Universidad Internacional de La Rioja)
- Máster Universitario en Ciberseguridad e Inteligencia de Datos (Universidad de La Laguna)
- Máster Universitario en Ciberseguridad (Universidad de Sevilla)

- Máster Universitario en Seguridad de Tecnologías de la Información y de las Comunicaciones (Universidad Europea de Madrid)

Los referentes a nivel europeo se pueden consultar en la base de datos de ENISA (<https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead#/>), no se recogen en este apartado, pero se resalta que existen 53 programas de máster universitario en ciberseguridad en modalidad presencial, de los que sólo 6 son españoles, entre los que se incluye MUniCS.

1.3. Objetivos formativos

Los principales objetivos formativos del título se corresponden con los enunciados en la memoria de verificación de MUniCS y que se enumeran a continuación:

- Formar expertos técnicos que puedan 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.
- Formar expertos técnicos que puedan evaluar el nivel de riesgo de cualquier infraestructura y/o sistema y contribuir a su reducción frente a vulnerabilidades y amenazas en los activos de información, de comunicación y de sistemas. En concreto favorecer una transformación digital segura, la privacidad de la sociedad y los ciudadanos y la lucha contra la ciberdelincuencia y el cibercrimen.
- Concienciar a los profesionales formados del compromiso ético, deontología profesional y la perspectiva de género en el área de ciberseguridad.
- Proporcionar a los profesionales de los conocimientos teóricos y las habilidades y competencias que permitan aportar garantías de privacidad y seguridad en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos.
- Habilitar egresados para investigar, 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.
- Crear una comunidad de jóvenes que impulsen la industria de la ciberseguridad en Galicia, así como contribuyan a una sociedad digital segura a nivel europeo, español y gallego.

Objetivos formativos de las menciones o especialidades

No hay menciones

Estructuras curriculares específicas y justificación de sus objetivos

No aplica

Estrategias metodológicas de innovación docente específicas y justificación de sus objetivos

Los principales indicadores objetivos de la calidad de MUniCS serán el grado de satisfacción de los estudiantes (en qué medida la formación cumple con sus expectativas), el tiempo necesario para la

graduación y la inserción laboral efectiva, evaluada tanto por el tiempo medio en encontrar trabajo como por la adecuación de este a las preferencias de los estudiantes. Como, por ser un título interuniversitario, se ha demostrado difícil coordinar los mecanismos generales de medición que emplean las universidades para el seguimiento de estas dimensiones y ya que el número plazas en oferta es moderado (40), con esta modificación se pondrá en marcha un programa de mentorización y seguimiento individualizado de los estudiantes que servirá a la vez como observatorio y como apoyo a su desarrollo académico y profesional.

A partir del primer curso de implantación del nuevo plan de estudios, el curso 2023/2024, cada estudiante de nuevo ingreso tendrá asignado un tutor académico de entre el cuadro de profesores de la titulación, quien supervisará su trayectoria académica y orientará al estudiante si es necesario en los procesos de elección de optativas, prácticas en empresa y TFM. Los resultados del programa de mentorización se incorporarán al informe anual de seguimiento de la titulación y se elevarán a la Comisión de Calidad de los centros.

Perfiles fundamentales de egreso a los que se orientan las enseñanzas

Para la presentación de los perfiles de egreso de MUniCS utilizaremos las publicaciones del Grupo de Trabajo 5 de ECSO sobre "educación, formación, concienciación y rangos de ciberseguridad", que tiene como objetivo contribuir al desarrollo de competencias y capacidades en materia de ciberseguridad para la agenda digital europea, a través de un aumento de la educación, la formación profesional y el desarrollo de habilidades, así como de acciones de concienciación e inclusión de género. Así la formación en MUniCS se adapta a los siguientes perfiles de egreso en el documento *"WG5 PAPER European Cybersecurity Education and Professional Training: Minimum Reference Curriculum"*:

- Administrador/soporte / analista de redes; Administrador e ingeniero de sistemas; Desarrollador de Software/Experto de Penetración;
- Gestor de ciberseguridad / Gestor de seguridad de la información / Arquitecto de seguridad / Ingeniero de seguridad de aplicaciones / Analista de Seguridad de Aplicaciones
- Analista / Evaluador / Gestor de riesgo; Analista de Inteligencia de Amenazas; Respuesta a Incidentes; Analista de Cumplimiento
- Hacker ético, *tester* de penetración / analista de vulnerabilidades técnicas/ profesional de ciberseguridad ofensiva
- Investigador/Analista de forensia digital, cibernética e informática
- Experto en blockchain / Ciberseguridad IoT / Ciberseguridad industrial
- Científico y experto en seguridad de datos / Experto en transformación digital
- Analista / Administrador / Consultor / Auditor de Ciberseguridad
- Director de Información / Director de Seguridad de la Información / Director de Ciberseguridad (CIO – CISO y similares)

Actividad profesional regulada habilitada por el título

No hay

2. RESULTADOS DEL PROCESO DE FORMACIÓN Y DE APRENDIZAJE

2.1. Conocimientos o contenidos

TABLA 3. Conocimientos

K-01	Conocer los métodos y técnicas básicas de la criptografía clásica, estándares y protocolos de seguridad criptográfica, esteganografía y cifrado post-cuántico.
K-02	Conocer las técnicas de ocultación y persistencia de malware; así como las tendencias actuales en malware mediante el estudio de casos reales.
K-03	Identificar los métodos de ataque a la privacidad y de los conceptos de preservación de la privacidad y anonimato: privacidad diferencial, cifrado homomórfico y computación segura multi-partita
K-04	Distinguir las principales vulnerabilidades que sufren las aplicaciones, así como los principales mecanismos de autenticación, autorización y control de acceso, con énfasis especial en aplicaciones web y servicios web.
K-05	Conocer de las vulnerabilidades en los dispositivos y tecnologías de acceso de red, las herramientas para explorarlas y las medidas de protección para obtener redes de comunicaciones seguras, así como comprender el concepto de política de seguridad aplicado a redes, la seguridad perimetral y los cortafuegos.
K-06	Comprender los conceptos básicos y el funcionamiento general de las tecnologías basadas en registro distribuido; así como su evaluación en términos de confidencialidad, integridad y disponibilidad; y sus principales aplicaciones y casos de uso.
K-07	Conocer en detalle los protocolos de red que aportan seguridad a la transmisión de la información, y comprender qué otros protocolos, siendo auxiliares (no relativos al mundo de la seguridad), presentan vulnerabilidades explotables y las posibles contramedidas contra los ataques.
K-08	Distinguir los distintos tipos de vulnerabilidades de los SO, su funcionamiento y configuración, así como la forma que limitan la exposición del SO.
K-09	Identificar la arquitectura de los sistemas IoT, su complejidad y sus vulnerabilidades, así como comprender la seguridad en el ámbito los sistemas empotrados y los sistemas de comunicación IoT.
K-10	Diferenciar los vectores y técnicas de ciberataque más comunes, así como comprender y aplicar los métodos y técnicas de detección de vulnerabilidades en equipos informáticos, redes de comunicaciones, bases de datos, programas y/o servicios de información.
K-11	Comprender los conceptos fundamentales sobre el negocio de la seguridad digital y, en este contexto, el funcionamiento de las empresas, las formas de monetización y la comunicación de productos a públicos especializados y no especializados.
K-12	Conocer las técnicas y herramientas para la preservación y análisis de evidencias, así como las metodologías adecuadas para la realización de trabajos forenses con validez legal.
K-13	Interpretar los conceptos fundamentales, tipología y evolución de la arquitectura de los centros de procesos de datos (CPD) desde una visión centrada en la seguridad de la infraestructura física, así como las técnicas básicas de seguridad en CPD como son virtualización, fortificación de elementos físicos y lógicos y securización de datos.
K-14	Distinguir los conceptos fundamentales asociados con la seguridad en los sistemas operativos para móviles y el desarrollo de apps seguras, así como los sistemas gestión de dispositivos móviles.
K-15	Conocer los conceptos básicos sobre contratos inteligentes y aplicaciones descentralizadas, así como las tecnologías para su diseño y desarrollo técnicos y las consideraciones de seguridad (testing y análisis de código).
K-16	Describir los conceptos fundamentales y la normativa técnica relacionada con la Gestión de la Seguridad de la Información, las metodologías de Análisis de Riesgos, así como las herramientas para llevar a cabo tareas de análisis de riesgos, auditoría de seguridad, gestión de incidentes, gestión de continuidad de negocio y recuperaciones.
K-17	Analizar 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.

2.2. Habilidades o destrezas

TABLA 4. Habilidades/Destrezas

HD-01	Determinar el grado de seguridad de una solución criptográfica, elegir la más adecuada a un sistema de información o de comunicaciones, así como aplicar y adaptar sus elementos.
HD-02	Detectar y eliminar las vulnerabilidades susceptibles a malware, así como malware, en sistemas y redes de comunicaciones, así como evadir técnicas de ocultación y persistencia de malware.
HD-03	Elegir la solución de privacidad y anonimato más adecuada para un sistema de información o de comunicaciones, así como saber aplicar y adaptar los elementos de privacidad y de comunicación anónima a un producto, servicio o sistema de información y comunicaciones en función de las necesidades y teniendo en cuenta el compromiso entre utilidad de la información y privacidad de los datos.
HD-04	Prevenir, identificar y corregir las principales vulnerabilidades que sufren las aplicaciones, así como incorporar mecanismos de autenticación, autorización y control de acceso a las aplicaciones.
HD-05	Diseñar e implementar redes seguras, seleccionando y configurando los dispositivos adecuados para cada sección de la red y utilizando proactivamente la monitorización de red como de modo que se implemente correctamente la política de seguridad de la organización.
HD-06	Aplicar tecnologías de registro distribuido a casos de uso específico, así como diseñar, desarrollar y desplegar una solución basada en dichas tecnologías, optimizando sus parámetros esenciales y aplicando mecanismos de protección para evitar y mitigar ataques.
HD-07	Decidir la solución/protocolo adecuado para asegurar la seguridad de comunicaciones extremo a extremo, así como configurar las diferentes herramientas que los distintos sistemas operativos/plataformas nos aportan para activar la seguridad en las comunicaciones.
HD-08	Identificar las vulnerabilidades de un SO en un entorno de uso concreto, modificar la configuración para minimizar su exposición y comprobar su nivel de seguridad.
HD-09	Analizar las implicaciones del nivel de seguridad de tecnologías relacionadas con la digitalización de los sectores de producción, así como valorar y modelar amenazas y ejecutar ataques con el objetivo de diseñar sistemas IoT seguros.
HD-10	Identificar y aprovechar, de manera analítica y práctica, vulnerabilidades de los sistemas de información, así como identificar posibles vectores de ataque e innovar en técnicas y procesos referidos al hacking ético.
HD-11	Valorar una empresa en el ámbito de la seguridad e incluso a sectores más específicos dentro de este ámbito, así como definir los perfiles necesarios, propios de la empresa o externos, asociados a la ciberseguridad.
HD-12	Identificar, preservar y analizar evidencias, realizar análisis forense de un sistema de información, y generar informes que sean claros, concisos e inteligibles tanto por expertos como por personas ajenas al ámbito de la seguridad informática
HD-13	Aplicar herramientas de virtualización de infraestructuras en Centros de Procesado de Datos, así como utilizar herramientas para la monitorización de sus infraestructuras y servicios.
HD-14	Identificar vulnerabilidades en sistemas operativos y aplicaciones propios de los dispositivos móviles, así como realizar un análisis forense y definir la política de seguridad que afecta a las comunicaciones y sistemas móviles de una organización.
HD-15	Aplicar los contratos inteligentes al desarrollo de sistemas descentralizados, evaluar si un desarrollo es adecuado a la problemática y utilizar las herramientas de desarrollo apropiadas para programar, desplegar e interactuar con contratos inteligentes, así como usar oráculos bajo condiciones de robustez y seguridad.
HD-16	Gestionar la seguridad de la información, utilizar herramientas de análisis de riesgos y la auditoría de seguridad, identificar y clasificar posibles incidentes de forma proactiva y definir los cauces para su gestión y resolución.
HD-17	Analizar y comunicar la normativa legal relacionada con la ciberseguridad, sus cuestiones ético-legales y los delitos la criminalidad informática en el contexto nacional, europeo e internacional.
HD-18	Saber 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.
HD-19	Saber 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.

2.3. Competencias

TABLA 5. Competencias

C-01	Resolver problemas relacionados con el uso de información cifrada y tener autonomía e iniciativa para desarrollar soluciones innovadoras en los campos de la criptografía, el criptoanálisis, la anonimidad y la privacidad.
C-02	Demostrar autonomía e iniciativa para resolver problemas complejos que involucren múltiples tecnologías en el ámbito de las redes o los sistemas de comunicaciones, y desarrollar soluciones innovadoras en el campo de las comunicaciones y la computación distribuida privadas.
C-03	Trabajar como analista de malware, para proteger aplicaciones, así como analizar su seguridad en cualquier área de aplicación
C-04	Aplicar la tecnología de cadenas de bloques a la protección descentralizada verificable de la información, ya sea referida ésta a activos digitales de información o referida a activos digitales que representan bienes de uso.
C-05	Analizar la seguridad de los protocolos de comunicación en la capa física; de enlace; de red y de transporte, así como evaluar en una red corporativa las medidas de seguridad que es necesario implantar para la protección de sus activos internos y sus comunicaciones.
C-06	Identificar vulnerabilidades en un sistema real, así como variar sus parámetros y configurarlo para su protección frente a ellas; limitando así la exposición a amenazas conocidas.
C-07	Aplicar políticas de seguridad e implementar las diferentes técnicas de protección en base a la comprensión de los ataques en sistemas industriales para minimizar las problemáticas de seguridad y los ataques a redes de control industrial.
C-08	Realizar test de intrusión en entornos prácticos complejos para la identificación de vulnerabilidades, así como para realizar ataques en entornos controlados con juicio crítico y ético.
C-09	Aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad mediante técnicas científicas y analíticas para identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.
C-10	Diseñar y gestionar la seguridad de infraestructuras para realizar la auditoría de seguridad de la infraestructura y garantizar continuidad de negocio bajo normas y estándares de referencia.
C-11	Diseñar, implantar y mantener un sistema de gestión de la seguridad de la información utilizando metodologías de referencia, analizar los riesgos, planificar periodos de detección de incidentes o desastres, y su recuperación, desarrollar un plan de continuidad de negocio, certificar sistemas seguros y realizar la auditoría de seguridad de sistemas e instalaciones.
C-12	Interpretar de forma adecuada las fuentes de información en el ámbito del derecho penal informático (leyes, jurisprudencia y doctrina) de ámbito nacional e internacional.
C-13	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.
C-14	Proyectar, modelar, calcular y diseñar soluciones técnicas y de gestión de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación, con criterios éticos de responsabilidad y deontología profesional.
C-15	Comunicar conocimientos y conclusiones, así como las razones últimas que las sustentan, a públicos especializados y no especializados de un modo claro y sin ambigüedades.
C-16	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
C-17	Incorporar en el ejercicio profesional criterios de sostenibilidad y compromiso ambiental mediante el uso equitativo, responsable y eficiente de los recursos.
C-18	Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad y tener capacidad para elaborar de planes y proyectos de trabajo claros, concisos y razonados en el ámbito de la ciberseguridad.
C-19	Aplicar 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.

3. ADMISIÓN, RECONOCIMIENTO Y MOVILIDAD

3.1. Requisitos de acceso y procedimientos de admisión de estudiantes

Se podrá acceder al Máster, con carácter general, según los requisitos establecidos por el RD 822/2021, de 28 de septiembre. De forma específica para el Máster de ciberseguridad, los estudiantes que quieran ser admitidos en el título deberán estar en posesión de un Grado en Ingeniería Informática, Ingeniería de Tecnologías de Telecomunicación, Ingeniería en Tecnologías Industriales, Matemáticas, Física y grados afines.

Los criterios específicos de admisión al Máster serán, por orden de prevalencia, la titulación de acceso de los solicitantes, el expediente académico y otros méritos relacionados con el ámbito de la ciberseguridad. Tendrán preferencia en la admisión quienes posean un título de grado relacionado directamente con las tecnologías de la información y las comunicaciones 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 ciberseguridad informática se tendrá en cuenta 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.

Los criterios de admisión se basarán en los siguientes aspectos:

- Adecuación de la titulación de acceso a los contenidos del máster con una ponderación de entre un 50 y un 70 %. La Comisión Académica de Máster será soberana para decidir la adecuación de la titulación cuando esta no esté listada en las incluidas en esta memoria.
- Expediente académico, con una ponderación de entre un 20% y un 40%.
- Otros méritos relacionados con el ámbito de la ciberseguridad (experiencia laboral, formación extracurricular, participación en actividades relacionadas, etc.), con una ponderación de entre un 5% y un 20%.

Los criterios concretos para cada curso académico serán establecidos y publicados con anterioridad al comienzo de los períodos de preinscripción y matrícula. Si en el curso académico en el que se solicita admisión, el título ofrece materias obligatorias para los estudiantes que se impartan en inglés, es requisito necesario de acceso una certificación de, como mínimo, nivel B1, siendo un requisito excluyente que no pondera.

Los criterios de acceso se publican en la página Web de MUnICS ([munics.es](https://www.munics.es)) y en los portales de preinscripción y matrícula de la Universidade de Vigo y la Universidade da Coruña.

- <https://www.munics.es/acceso.html>
- <https://www.uvigo.gal/es/estudiar/acceder/acceso-masteres>
- <https://estudios.udc.es/gl/StudyAtUdc/master>

3.2. Criterios para el reconocimiento y transferencias de créditos

Las dos universidades, UDC y UVIGO, cuentan con una “Normativa de transferencia y reconocimiento de créditos para titulaciones adaptadas al Espacio Europeo de Educación Superior”, de cuya aplicación son responsables los Vicerrectorados con competencias en oferta docente y la Secretaría General con los Servicios de ellos dependientes. Estas normativas están accesibles públicamente a través de la web de las distintas universidades, en los enlaces:

- https://www.udc.gal/export/sites/udc/normativa/_galeria_down/academica/Norm_tceees_adaptada_e.pdf
- <https://secretaria.uvigo.gal/uv/web/normativa/public/show/255>

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.

En cuanto **Criterios de reconocimiento** de créditos, serán aquellos que fije el Gobierno de cada universidad. Las universidades, mediante la normativa de aplicación y las resoluciones rectorales que la desarrollen, establecerán el sistema para el reconocimiento de estos créditos. La Comisión Académica de la titulación establecerá las equivalencias entre estudios superados en otras universidades y los que puedan ser reconocidos en el plan de estudios. Así mismo, podrá establecer tablas de equivalencia especificando los créditos que se reconocen.

La experiencia laboral y profesional acreditada podrá ser también reconocida en forma de créditos, siempre que confieran, al menos, el 75% de las competencias de las materias por las que se quiere obtener reconocimiento de créditos. La Comisión Académica valorará y aprobará, si es el caso, las solicitudes de reconocimiento de créditos, previo informe del profesorado que imparte las materias y a la vista de la documentación que presenten los solicitantes que, como mínimo, ha de ser: copia de la vida o contrato laborales y certificado de la empresa donde consten las funciones y tareas que realiza o ha realizado en el puesto de trabajo.

El número de créditos que pueden ser objeto de reconocimiento a partir de experiencia profesional o laboral no podrá ser superior al 15% de los créditos totales del título. En concreto, en la titulación de Máster en Ciberseguridad se reconocerán créditos de asignaturas optativas o créditos de la asignatura Prácticas en empresas por experiencia laboral o profesional previa, hasta un máximo de 9 ECTS y en módulos de 3 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 3 ECTS por cada seis meses de experiencia profesional, con un máximo acumulable de 9 ECTS.

Por último, el reconocimiento de créditos cursados en estudios superiores oficiales No Universitarios o en créditos cursados en títulos propios no será superior a 9 ECTS.

En cuanto a la **transferencia de créditos**, todos los créditos obtenidos en enseñanzas oficiales cursadas en alguna de las universidades participantes o en otra universidad del EEES serán objeto de incorporación al expediente del estudiante, tras la petición de este a la dirección del centro. La solicitud se resolverá de acuerdo con lo establecido en la normativa vigente de cada universidad.

3.3. Procedimientos de movilidad

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. En MUnICS 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.

De forma más específica, en EET se mantiene una larga tradición de intercambio de estudiantes apoyados en los programas Erasmus/ISEP/SICUE, que gestiona en colaboración con la Oficina de Relaciones Internacionales (ORI) de la UVIGO. La gestión y supervisión de estudiantes que se envían 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 individualizada, se analiza y diseña el contrato de estudios que cada estudiante realizará 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 los estudiantes 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 con la propia ORI.

En FIC, el centro cuenta con un responsable en dirigir y administrar la política de internacionalización del centro; FIC participa en programas de movilidad Erasmus+, Convenios bilaterales, SICUE y otros, para los que la Universidad de A Coruña proporciona financiación a través de su participación en los siguientes programas de ayudas tanto para estudiantes propios como de acogida: Erasmus+ con países comunitarios; Erasmus + KA107 (Países asociados); Programas en el marco de convenios bilaterales o de doble titulación internacional con instituciones fuera de los programas anteriores; Programa NILS de Ciencia y Sostenibilidad; Becas Banco Santander. En la UDC, el vicerrectorado competente en asuntos de Relaciones Internacionales, le corresponde la dirección de la política de movilidad internacional de la Universidad, así como la supervisión y la coordinación de todas las demás instancias de la UDC involucradas en la gestión y la organización de los diferentes programas de movilidad. La Unidad técnica y administrativa que desarrolla esta política es la Oficina de Relaciones

Internacionales (ORI), responsable de la coordinación de la gestión de la movilidad del alumnado en el marco de los programas, acuerdos y convenios suscritos por la UDC.

A continuación, se incluyen los enlaces al del procedimiento para la movilidad y acogida de estudiantes establecidos en UVIGO y UDC:

- UVIGO
 - <https://www.uvigo.gal/estudar/mobilidade>
 - <https://teleco.uvigo.es/es/vida-na-eet/mobilidade/>
- UDC
 - https://www.udc.es/es/ori/inf_estudiantes_UDC/mobilidade_internacional/?language=en
 - <https://www.fic.udc.es/es/international>

4. PLANIFICACIÓN DE LAS ENSEÑANZAS

4.1. Estructura básica de las enseñanzas

TABLA 6. Resumen de la distribución de créditos en la titulación

Créditos Obligatorios	63
Créditos Optativos	6
Prácticas externas	9
Créditos trabajo fin de máster	12
Créditos de complementos formativos	0
Número Total de Créditos ECTS	90

A continuación, se resume el plan de estudios que se organiza en 3 semestres y 3 módulos: FUNDAMENTOS DE CIBERSEGURIDAD, TÉCNICAS DE CIBERSEGURIDAD y CAPACITACIÓN ACADÉMICO-PROFESIONAL.

TABLA 7. Curso 1: Semestre 1

Asignatura			Módulo	ECTS	Tipo	Mod,
Seguridad de la información	1	SI	FUNDAMENTOS	5	Obligatoria	Presencial
Análisis de <i>malware</i>	2	MWR	FUNDAMENTOS	5	Obligatoria	Presencial
Privacidad y anonimidad	3	PAN	FUNDAMENTOS	5	Obligatoria	Presencial
Seguridad de aplicaciones	4	SAPP	FUNDAMENTOS	5	Obligatoria	Presencial
Redes seguras	5	RED	FUNDAMENTOS	5	Obligatoria	Presencial
Tecnologías de Registro Distribuido y Blockchain	6	BC	FUNDAMENTOS	5	Obligatoria	Presencial

TABLA 8. Curso 1: Semestre 2

Asignatura			Módulo	ECTS	Tipo	Modalidad
Seguridad en comunicaciones	7	SCOM	TÉCNICAS	5	Obligatoria	Presencial
Fortificación de sistemas	8	FORT	TÉCNICAS	5	Obligatoria	Presencial
Ciberseguridad Industrial e IoT	9	CSIoY	TÉCNICAS	5	Obligatoria	Presencial
Hacking ético y Test de intrusión	10	INT	TÉCNICAS	5	Obligatoria	Presencial
Negocio en ciberseguridad y emprendimiento	11	NEG	CAPACITACIÓN	4	Obligatoria	Presencial
Análisis forense	12	AF	TÉCNICAS	3	Optativa	Presencial
Seguridad en Centros de datos	13	CD	TÉCNICAS	3	Optativa	Presencial
Seguridad en dispositivos móviles	14	MOV	TÉCNICAS	3	Optativa	Presencial
Smart Contracts y dApps	15	CIAD	TÉCNICAS	3	Optativa	Presencial

TABLA 9. Curso 2: Semestre 1

Asignatura			Módulo	ECTS	Tipo	Modalidad
Gestión de seguridad de la información	16	GSI	CAPACITACIÓN	5	Obligatoria	Presencial
Conceptos y Leyes	17	CL	CAPACITACIÓN	4	Obligatoria	Presencial
Prácticas en empresa	18	PRAC	CAPACITACIÓN	9	Obligatoria	Presencial
Trabajo de fin de máster	19	TFM	CAPACITACIÓN	12	Obligatoria	Presencial

Plan de estudios detallado

A continuación, se muestra una matriz de relación entre las asignaturas y los conocimientos, habilidades/destrezas y competencias del título.

TABLA 10. Matriz de resultados

	Asignatura	Conoc.	Dest/Hab	Comp.
1	Seguridad de la información (SI)	K-01	HD-01	C-01 C-13
2	Análisis de malware (MWR)	K-02	HD-02	C-03 C-06
3	Privacidad y anonimidad (PAN)	K-03	HD-03	C-01 C-14
4	Seguridad de aplicaciones (SAPP)	K-04	HD-04	C-03 C-14
5	Redes Seguras (RED)	K-05	HD-05	C-02 C-05 C-10
6	Tecnologías de Registro Distribuido y Blockchain (BC)	K-06	HD-06	C-02 C-04
7	Seguridad en comunicaciones (SCOM)	K-07	HD-07	C-02 C-05 C-10
8	Fortificación de sistemas (FORT)	K-08	HD-08	C-06 C-10
9	Ciberseguridad Industrial e IoT (CSIOT)	K-09	HD-09	C-02 C-05 C-07
10	Hacking ético y Test de intrusión (INT)	K-10	HD-10	C-06 C-08 C-09 C-10
11	Negocio en ciberseguridad y emprendimiento (NEG)	K-11	HD-11	C-16 C-17 C-18
12	Análisis forense (AF)	K-12	HD-12	C-06 C-08 C-09
13	Seguridad en Centros de datos (CD)	K-13	HD-13	C-02 C-05 C-10
14	Seguridad en dispositivos móviles (MOV)	K-14	HD-14	C-03 C-08 C-09
15	Smart Contracts y dApps (CIAD)	K-15	HD-15	C-03 C-04
16	Gestión de seguridad de la información (GSI)	K-16	HD-16	C-11 C-14
17	Conceptos y Leyes (CL)	K-17	HD-17	C-12 C-13 C-19
18	Prácticas en empresa (PRA)		HD-18, HD-19	C-16 C-17 C-18
19	Trabajo de fin de máster (TFM)		HD-19	C-13 C-14 C-15 C-16

A continuación, se incluyen una tabla por cada asignatura del plan de estudios con la siguiente información:

- Número total de créditos ECTS: cada crédito ECTS equivale a 25 horas de trabajo del alumnado.
- Tipología: Obligatoria, optativa, prácticas académicas externas, y TFM.
- Organización temporal: Indica el semestre y curso académico en que se imparte la asignatura
- Modalidad: que serán presencial para las asignaturas y optativas, así como para el TFM. La modalidad de prácticas en empresa podrá ser presencial, semipresencial o virtual dependiendo de las condiciones de la entidad en la que se realizarán las prácticas.
- Resultados del aprendizaje. Los principales resultados del aprendizaje esperados; expresado en términos de conocimientos o contenidos, habilidades y competencias bajo la nomenclatura: K – Conocimientos; HD - habilidades y destrezas; y C – Competencias

Metodoloxías y sistemas de avaliación. Las indicadas a continuación se corresponden a la descripción que se puede encontrar en el siguiente documento. O

https://www.uvigo.gal/sites/uvigo.gal/files/contents/paragraph-file/2020-11/GUIA_DE_METODOLOXIAS_E_SISTEMAS_DE_AVALIACION_v02_20200724.pdf

La ponderación asociada a los distintos sistemas de avaliación se recogerá explícitamente en las guías docentes, aprobadas y publicadas en cada universidade, atendiendo a sus respectivas normativas. Se ha optado por mantener una horquilla amplia (0%-100%) para permitir la coordinación entre las dos universidades la ponderación final, dando cumplimiento a las normativas aprobadas. En todo caso se asegurará que las dos universidades apliquen criterios coordinados y homogéneos.

Asignatura 1: Seguridad de la información (SI)

Seguridad de la información

ECTS	5
Tipología	Obligatorio
Organización temporal	Semestre 1
Modalidad	Presencial
Presencialidad	35 horas
Resultados de aprendizaje	K-01 HD-01 C-01 C-13
Idioma	Inglés / Español / Gallego
Descripción de contenidos	<ul style="list-style-type: none"> - Fundamentos: teoría de la información, canal wiretap, seguridad perfecta y seguridad computacional - Criptografía clásica: cifrado de flujo, cifrado en bloque, generadores pseudo-aleatorios, funciones aleatorias, integridad (hashing), funciones unidireccionales, hashing universal, cifrado de clave pública, firmas digitales, protocolos de autenticación. Cadenas de bloques. Estándares y casos de estudio. - Criptografía poscuántica: bases de computación cuántica, retículos, anillos y LWE, cifrado y computación homomórfica. Estándares. PUF. - Esteganografía: marcas de agua, detección, seguridad multimedia.
Actividades y metodoloxías	Lección magistral; Resolución de problemas; Prácticas en aulas informáticas
Sistema de avaliación	Examen de preguntas de desarrollo; Resolución de problemas y ejercicios; Informes de prácticas

Asignatura 2: Análisis de malware (MWR)

Análisis de Malware

ECTS	5
Tipología	Obligatoria
Organización temporal	Semestre 1
Modalidad	Presencial
Presencialidad	42 horas

Resultados de aprendizaje	K-02 HD-02 C-03 C-06
Idioma	Inglés / Español /Gallego
Descripción de contenidos	<ul style="list-style-type: none"> - Introducción al análisis de malware. - Tipos de malware: estructura, componentes y vectores de infección. - Malware: técnicas de propagación, infección, persistencia, ocultación y anti-análisis. - Ingeniería inversa de malware. - Herramientas de análisis, detección y eliminación de malware.
Actividades y metodologías	Actividades introductorias; Lección magistral; Practicas TIC; Estudio de casos; Presentaciones; Seminarios
Sistema de evaluación	Examen de pruebas objetivas y de desarrollo; Resolución de problemas y/o ejercicios; Evaluación de trabajos y actividades; Evaluación de presentaciones

Asignatura 3: Privacidad y anonimidad (PAN)

Privacidad y anonimidad

ECTS	5
Tipología	Obligatorio
Organización temporal	Semestre 1
Modalidad	Presencial
Presencialidad	42 horas
Resultados de aprendizaje	K-03 HD-03 C-01 C-14
Idioma	Inglés / Español /Gallego
Descripción de contenidos	<ul style="list-style-type: none"> - Ataques de inferencia. Ataques de análisis de tráfico. Rastreo online. - Privacidad diferencial. Mecanismos para la privacidad diferencial. Teoremas de composición. - Primitivas con mantenimiento de la privacidad: recuperación de información, intersección de conjuntos. - Técnicas PET con cifrado homomórfico y computación multiparte segura. Filtros de Bloom. - Técnicas de anonimidad. K-anonimidad, l-diversidad y t-proximidad. - Privacidad de la localización. Comunicaciones anónimas. Encaminamiento cebolla. Mixes. - Autenticación anónima. Privacidad y aprendizaje máquina. - Ingeniería de la privacidad. Privacidad desde el diseño. Aspectos éticos y legales de la privacidad.
Actividades y metodologías	Lección magistral; Resolución de problemas; Prácticas en aulas informáticas
Sistema de evaluación	Examen de preguntas de desarrollo; Resolución de problemas y ejercicios; Informes de prácticas

Asignatura 4: Seguridad de aplicaciones (SAPP)

Seguridad de Aplicaciones

Número de créditos ECTS	5
Tipología	Obligatoria
Organización temporal	Semestre 1
Modalidad	Presencial
Presencialidad	42 horas

Resultados de aprendizaje	K-04 HD-04 C-03 C-14
Idioma	Inglés / Español /Gallego
Breve descripción de los contenidos	<ul style="list-style-type: none"> - Marcos de referencia de vulnerabilidades en aplicaciones (e.g. CWE, CVE, OWASP). - Vulnerabilidades y mecanismos de prevención. Vulnerabilidades en el tratamiento de los datos de entrada (e.g. inyección de SQL, inyección de JavaScript, inyección en ficheros de log, inyección en XML). - Vulnerabilidades en la autenticación. Vulnerabilidades en la gestión de la sesión en aplicaciones web. - Exposición de información sensible. Vulnerabilidades en el control de acceso. Configuración de seguridad incorrecta. Monitorización y log insuficiente. Vulnerabilidades en las librerías de terceros. - Seguridad en el ciclo de desarrollo software. - Mecanismos de autenticación, autorización y control de acceso: Tokens de acceso (e.g. JSON Web Token). Protocolos de autenticación y autorización (e.g. OAuth, SAML). Control de acceso basado en roles. Control de acceso basado en atributos.
Actividades y metodologías	Actividad introductoria, lección magistral, prácticas en aulas informáticas.
Sistema de evaluación	Examen de preguntas objetivas, práctica de laboratorio.

Asignatura 5: Redes Seguras (RED)

Redes Seguras	
Número de créditos ECTS	5
Tipología	Obligatorio
Organización temporal	Semestre 1
Modalidad	Presencial
Presencialidad	42 horas
Resultados de aprendizaje	K-05 HD-05 C-02 C-05 C-10
Idioma	Inglés / Español /Gallego
Breve descripción de los contenidos	<ul style="list-style-type: none"> - Diseño de redes seguras: modelos de seguridad, seguridad perimetral, dispositivos de red para seguridad - Fortificación de los dispositivos de red: arquitectura lógica de los dispositivos de red, protección del plano de gestión, protección del plano de control - Seguridad LAN en entornos Ethernet: VLANs, vulnerabilidades mitigables, ataques típicos, técnicas de protección - Firewalls: tecnologías firewall, filtrado estático de paquetes, filtrado dinámico de paquetes, filtrado en capa de aplicación, next-generation firewalls, importancia de NAT/PAT, políticas de seguridad de red - Dispositivos complementarios: sistemas de detección y prevención de intrusiones, servicios proxy - Monitorización segura: implicaciones de diseño, sincronización horaria, syslog, SNMP, netflow, NMS y SIEM.
Actividades y metodologías	Sesión magistral; Prácticas TIC; Trabajo autónomo del alumno; Atención personalizada
Sistema de evaluación	Examen de preguntas de preguntas objetivo y/o desarrollo; Informes de prácticas; Examen de prácticas

Asignatura 6: Tecnologías de Registro Distribuido y Blockchain (BC)

Tecnologías de Registro Distribuido y Blockchain

ECTS	5
Tipología	Obligatoria
Organización temporal	Semestre 1
Modalidad	Presencial
Presencialidad	42 horas
Resultados de aprendizaje	K-06 HD-06 C-02 C-04
Idioma	Inglés / Español /Gallego
Descripción de contenidos	<ul style="list-style-type: none"> - Fundamentos de las tecnologías DLT y Blockchain. - Historia de las tecnologías DLT y Blockchain. - Tipos de Blockchain y tecnologías DLT. - Metodologías para determinar el uso de una Blockchain/DLT. - Aplicaciones prácticas de las tecnologías Blockchain/DLT. - Diseño y optimización de arquitecturas basadas en Blockchain/DLT. - Ciberseguridad de las tecnologías DLT y Blockchain.
Actividades y metodologías	Lección magistral, prácticas de laboratorio, estudio de casos
Sistema de evaluación	Examen de preguntas objetivas, informe de prácticas, proyecto

Asignatura 7: Seguridad en comunicaciones (SCOM)

Seguridad en Comunicaciones

ECTS	5
Tipología	Obligatoria
Organización temporal	Semestre 2
Modalidad	Presencial
Presencialidad	42 horas
Resultados de aprendizaje	K-07 HD-07 C-02 C-05 C-10
Idioma	Inglés / Español /Gallego
Descripción de contenidos	<ul style="list-style-type: none"> - Seguridad en capa física y de enlace. - Seguridad en capa de red. - Seguridad en capa de transporte. - Seguridad en capa de aplicación.
Actividades y metodologías	Sesión magistral; Prácticas TIC; Trabajos y/o proyectos (individuales o en grupo); Trabajo autónomo del alumno; Atención personalizada

Sistema de evaluación	Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios; Pruebas prácticas; Evaluación de trabajos y actividades
-----------------------	--

Asignatura 8: Fortificación de sistemas (FORT)

Fortificación Sistemas

ECTS	5
Tipología	Obligatoria
Organización temporal	Semestre 2
Modalidad	Presencial
Presencialidad	42 horas
Resultados de aprendizaje	K-08 HD-08 C-06 C-10
Idioma	Inglés / Español /Gallego
Descripción de contenidos	<ul style="list-style-type: none"> - Fortificación del proceso de arranque - Fortificación cuentas de los usuarios - Fortificación sistemas de ficheros - Fortificación de aplicaciones - Fortificación de la red. - Mantenimiento
Actividades y metodologías	Lección Magístral; Prácticas TIC; Atención Personalizada; Trabajo autónomo del alumno
Sistema de evaluación	Examen de preguntas objetivas; Informe de Practicas; Simulación

Asignatura 9: Ciberseguridad Industrial e IoT (CSIoT)

Ciberseguridad Industrial e IoT

ECTS	5
Tipología	Obligatoria
Organización temporal	Semestre 2
Modalidad	Presencial
Presencialidad	42 horas
Resultados de aprendizaje	K-09 HD-09 C-02 C-05 C-07
Idioma	Inglés / Español /Gallego
Descripción de contenidos	<ul style="list-style-type: none"> - Introducción a los sistemas ciberfísicos e IoT: hardware, firmware, comunicaciones y cloud - Introducción a la ciberseguridad industrial. - Ciberseguridad de sistemas de control y comunicaciones industriales. - Ciberseguridad de tecnologías de la Industria 4.0/5.0. - Ciberseguridad de dispositivos IoT/IIoT: hardware, firmware y middleware. - Ciberseguridad en entornos IIoT: sistemas de posicionamiento y sensórica. - Ciberseguridad en comunicaciones inalámbricas para dispositivos IoT/IIoT.
Actividades y metodologías	Lección magístral, prácticas de laboratorio, estudio de casos

Sistema de evaluación | Examen de preguntas objetivas, Informe de prácticas, Trabajo, Proyecto

Asignatura 10: Hacking ético y Test de intrusión (INT)

Hacking ético y Test de intrusión

ECTS	5
Tipología	Obligatoria
Organización temporal	Semestre 2
Modalidad	Presencial
Presencialidad	42 horas
Resultados de aprendizaje	K-10 HD-10 C-06 C-08 C-09 C-10
Idioma	Inglés / Español /Gallego
Breve descripción de los contenidos	<ul style="list-style-type: none"> - Fundamentos del hacking ético - Presentación de herramientas y “frameworks” de pentesting - Estrategias de reconocimiento - Estrategias ofensivas - Métodos de evasión - Principios éticos de los test de intrusión
Actividades y metodologías	Actividades introductorias; Lecciones magistrales; Casos de estudios; Prácticas de laboratorio
Sistema de evaluación	Examen de preguntas objetivas; Práctica de laboratorio.

Asignatura 11: Negocio en ciberseguridad y emprendimiento (NEG)

Negocio en Ciberseguridad y Emprendimiento

ECTS	4
Tipología	Obligatoria
Organización temporal	Curso 1, Semestre 2
Modalidad	Presencial
Presencialidad	30 horas
Resultados de aprendizaje	K-11 HD-11 C-16 C-17 C-18
Idioma	Inglés / Español /Gallego
Descripción de contenidos	<ul style="list-style-type: none"> - La seguridad como elemento transversal de la institución. - Monetización de los datos y de la seguridad de los mismos. - Perfiles de ciberseguridad en las entidades. - Oportunidades de negocio y orientación en los sectores productivos - Cultura del emprendimiento - Casos de éxito.
Actividades y metodologías	Sesión magistral; Resolución de problemas; Trabajos tutelados individuales o en grupo

Sistema de evaluación	Examen de preguntas objetivas; Examen de preguntas de desarrollo; Evaluación de trabajos
-----------------------	--

Asignatura 12: Análisis forense (AF)

Análisis Forense

ECTS	3
Tipología	Optativo
Organización temporal	Semestre 2
Modalidad	Presencial
Presencialidad	22,5 horas
Resultados de aprendizaje	K-12 HD-12 C-06 C-08 C-09
Idioma	Inglés / Español /Gallego
Descripción de contenidos	<ul style="list-style-type: none"> - Introducción a la Informática Forense - Proceso de adquisición de evidencias - Técnicas de Análisis Forense - Análisis de casos
Actividades y metodologías	Lección magistral; Resolución de problemas; Prácticas en aulas informáticas
Sistema de evaluación	Prueba objetiva; Resolución de problemas y ejercicios; Informes de prácticas

Asignatura 13: Seguridad en Centros de datos (CD)

Seguridad en centros de datos

ECTS	3
Tipología	Optativa
Organización temporal	Semestre 2, Curso 1
Modalidad	Presencial
Presencialidad	22,5 horas
Resultados de aprendizaje	K-13 HD-13 C-02 C-05 C-10
Idioma	Inglés / Español /Gallego
Descripción de contenidos	<ul style="list-style-type: none"> - Arquitectura de los centros de datos: topologías físicas y lógicas, supercomputadores, hipervisores de virtualización y computación en la nube. - Seguridad de las instalaciones físicas: energía, acceso, desastres y recuperación. - Gestión de incidentes en centros de procesos de datos. Seguridad física y lógica. - Fortificación de infraestructura física e hipervisores. - Virtualización de servicios: fortificación de máquinas virtuales y microservicios, redundancia y migración, escalado de servicios, seguridad como servicio (SECaaS), redes virtuales. - Monitorización ante vulnerabilidades y ataques. - Seguridad de los datos: replicación y codificación, almacenamiento y encriptación hardware. Estrategias y herramientas para copias de seguridad. - Gestión de la seguridad: Gestión AAA, modelo integral de seguridad (ITIL, 27000,27002), auditorías y conformidad legal.

Actividades y metodologías	Lección magistral; Resolución de problemas; Presentación; Prácticas en aulas informáticas
Sistema de evaluación	Examen de preguntas de desarrollo; Resolución de problemas y ejercicios; Informes de prácticas

Asignatura 14: Seguridad en dispositivos móviles (MOV)

Seguridad en dispositivos móviles

ECTS	3
Tipología	optativo
Organización temporal	2º Cuatrimestre
Modalidad	Presencial
Presencialidad	22,5 horas
Resultados de aprendizaje	K-14 HD-14 C-03 C-08 C-09
Idioma	Inglés / Español /Gallego
Descripción de contenidos	<ul style="list-style-type: none"> - Estudio de arquitecturas y modelos de seguridad de sistemas operativos móviles - Vulnerabilidades de SO y apps - Desarrollo de apps seguras - Apps maliciosas - Análisis forense de sistemas operativos móviles - Sistemas de gestión de movilidad empresarial (Enterprise Mobile Management, EMM)
Actividades y metodologías	Lección magistral, prácticas de laboratorio
Sistema de evaluación	Examen de preguntas objetivas, Resolución de problemas y/o ejercicios, Informe de prácticas

Asignatura 15: Smart Contracts y dApps (CIAD)

Smart Contracts y Distributed Applications

ECTS	3
Tipología	Optativa
Organización temporal	Semestre 2
Modalidad	Presencial
Presencialidad	22,5 horas
Resultados de aprendizaje	K-15 HD-15 C-03 C-04
Idioma	Inglés / Español /Gallego
Descripción de contenidos	<ul style="list-style-type: none"> - Conceptos básicos. - Diseño y desarrollo de Smart Contracts. - Sistemas de archivos peer-to-peer - Oráculos. Buenas prácticas. - Tokens no fungibles - BaaS como modelo de externalización

	- Aspectos relacionados con la ciberseguridad.
Actividades y metodologías	Lección magistral, prácticas de laboratorio, estudio de casos
Sistema de evaluación	Examen de preguntas objetivas, informe de prácticas, proyecto

Asignatura 16: Gestión de seguridad de la información GSI

Gestión de la Seguridad de la Información

ECTS	5
Tipología	Obligatoria
Organización temporal	Semestre 1, Curso 2
Modalidad	Presencial
Presencialidad	42 horas
Resultados de aprendizaje	K-16 HD-16 C-11 C-14
Idioma	Inglés / Español /Gallego
Descripción de contenidos	<ul style="list-style-type: none"> - Fundamentos: conceptos básicos, marco legal, normalización y entidades relevantes - Análisis de riesgos, gestión y certificación: metodologías y herramientas de análisis de riesgos - Sistemas de Gestión de Seguridad de la Información: familia ISO 27000, Esquema Nacional de Seguridad - Continuidad de negocio: roles, secuencia típica de un ataque, resiliencia, planes de contingencia - Detección de incidentes y gestión de respuesta - Recuperación de desastres
Actividades y metodologías	Lección magistral; Resolución de problemas; Presentación; Prácticas en aulas informáticas
Sistema de evaluación	Examen de preguntas objetivas; Examen de preguntas de desarrollo; Informe de prácticas

Asignatura 17: Conceptos y Leyes (CL)

Conceptos y Leyes

Número de créditos ECTS	4
Tipología	Obligatoria
Organización temporal	Curso 2, Semestre 1
Modalidad	Presencial
Presencialidad	30 horas
Resultados de aprendizaje	K-17 HD-17 C-12 C-13 C-19
Idioma	Inglés / Español /Gallego
Descripción de contenidos	<ul style="list-style-type: none"> - La ciberseguridad en el Esquema de Seguridad Nacional. - Cuestiones ético-legales relacionadas con ciberseguridad. - Computer crime y cybercrime: evolución del Derecho penal informático. - 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.

	<ul style="list-style-type: none"> - El contexto normativo. Especial atención al Convenio de Budapest y normativa de la Unión Europea. La Ley Orgánica de protección de datos personales. - Los delitos informáticos en el Código Penal. Los delitos contra la intimidad y la privacidad. Delitos contra la libertad: cyberstalking. 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 e industrial. La cibercriminalidad relacionada con menores: pornografía infantil, child grooming. Ciberterrorismo.
Actividades y metodologías	Lección magistral, eventos científicos, resolución de problemas, estudio de casos, seminarios
Sistema de evaluación	Examen de preguntas objetivas, Resolución de problemas y/o ejercicios

Asignatura 18: Prácticas en empresa (PRA)

Prácticas en Empresas

ECTS	9
Tipología	Obligatorio
Organización temporal	Curso 2, Semestre 1
Modalidad	Presencial, semipresencial o virtual
Presencialidad	225 horas
Resultados de aprendizaje	HD-18, HD-19 C-16 C-17 C-18
Idioma	Inglés / Español /Gallego
Descripción de los contenidos	<ul style="list-style-type: none"> - Contenido general: A definir por el tutor en la empresa y el tutor académico. - Integración en la empresa y en su entorno de trabajo: Durante su estancia el alumno se integrará en la organización de la empresa y se deberá coordinar con el resto de integrantes del equipo de trabajo al que sea asignado. - Desarrollo de su actividad profesional El alumno realizará las tareas encomendadas, de acuerdo con sus conocimientos y competencias.
Actividades y metodologías	Prácticas Externas/ Debate /Presentación
Sistema de evaluación	Informe de prácticas externas; Debate; Observación sistemática

Asignatura 19: Trabajo de fin de máster (TFM)

Gestión de la Seguridad de la Información

ECTS	12
Tipología	TFM
Organización temporal	Semestre 1, Curso 2
Modalidad	Semipresencial
Presencialidad	1
Resultados de aprendizaje	HD-19 C-13 C-14 C-15 C-16
Idioma	Inglés / Español /Gallego
Descripción de contenidos	El Trabajo Fin de Máster es un trabajo académico, personal y original en el que el estudiante tiene que mostrar los conocimientos adquiridos durante el máster. Por lo tanto, el contenido de cada trabajo debe ser único, aunque deberá mostrar la capacidad del alumno

	para analizar un problema de una forma sistemática, proponer soluciones, analizar los resultados obtenidos y exponerlos de forma clara.
Actividades y metodologías	Estudio de Caso; Taller
Sistema de evaluación	Trabajo; Presentación

5. PERSONAL ACADÉMICO Y DE APOYO A LA DOCENCIA

5.1. Perfil básico del profesorado

Descripción de la plantilla de profesorado del título

A continuación, se incluyen las tablas resumen de la plantilla de profesorado implicado en el título por la UVIGO y la UDC.

TABLA 10. Resumen del profesorado asignado al título UVIGO

Categoría	Número	ECTS	Doctores/as	Acreditados/as	Sexenio	Quinquenio
Catedrático de Universidad	2	9	2	2	8	8
Titular de Universidad	7	42	7	7	36	43
Contratado Doctor	2	7,5	2	2	4	6
Titular de Escuela	0	0	0	0	0	0
Ayudante Doctor	0	0	0	0	0	0
Total	11	58,5	11	11	48	57

TABLA 11. Resumen del profesorado asignado al título UDC

Categoría	Número	ECTS	Doctores/as	Acreditados/as	Sexenio	Quinquenio
Catedrático de Universidad	2	4	2	2	8	8
Titular de Universidad	7	31	7	7	19	23
Contratado Doctor	3	12,5	3	3	3	1
Titular de Escuela	1	5	0	0	0	7

Ayudante	1	4	1	1	0	0
Doctor						
Total	15	57,5	13	13	30	39

Estructura de profesorado

A continuación, se detalla la estructura del profesorado por área de conocimiento.

TABLA 12. Detalle del profesorado asignado al título por ámbitos de conocimiento.

Área o ámbito de conocimiento: Ingeniería Telemática

Número de profesores/as	13
Número de doctores/as	13
Categorías	Catedrático de Universidad, Titular de Universidad, Contratado doctor y Ayudante doctor
Profesorado acreditado	13
Materias / asignaturas	Seguridad de la información , Seguridad de Aplicaciones, Redes Seguras, Seguridad en Comunicaciones, Negocio en ciberseguridad y emprendimiento, Análisis de <i>malware</i> , Redes seguras, Tecnologías de Registro Distribuido y Blockchain, Fortificación de sistemas, Ciberseguridad Industrial e IoT, Hacking ético y Test de intrusión, Negocio en ciberseguridad y emprendimiento, Análisis forense, Seguridad en Centros de datos, Seguridad en dispositivos móviles, Smart Contracts y dApps, Gestión de seguridad de la información
ECTS impartidos (previstos)	16,5
ECTS disponibles (potenciales)	21

Área o ámbito de conocimiento: Ciencia de la Computación e Inteligencia Artificial

Número de profesores/as	7
Número de doctores/as	6
Categorías	Catedrático de universidad, titular, contratado doctor y titular de escuela
Profesorado acreditado	6
Materias / asignaturas	Seguridad de la Información, Análisis de Malware, Privacidad y Anonimidad, Fortificación de Sistemas, Ciberseguridad Industrial e IoT, Test de Intrusión, Análisis Forense, Seguridad en el CPD, Gestión de la Seguridad de la Información
ECTS impartidos (previstos)	28
ECTS disponibles (potenciales)	35

Área o ámbito de conocimiento: Tecnología Electrónica

Número de profesores/as	1
Número de doctores/as	1
Categorías	Titular de universidad
Profesorado acreditado	1
Materias / asignaturas	Ciberseguridad Industrial e IoT, Tecnologías de Registro Distribuido y Blockchain, Seguridad en Móviles, Smart Contracts y dApps
ECTS impartidos (previstos)	11

ECTS disponibles (potenciales)	15
--------------------------------	----

Área o ámbito de conocimiento: Derecho Penal

Número de profesores/as	2
Número de doctores/as	2
Categorías	Catedrática de universidad; Contratado Doctor
Profesorado acreditado	2
Materias / asignaturas	Conceptos y Leyes
ECTS impartidos (previstos)	6
ECTS disponibles (potenciales)	6

Área o ámbito de conocimiento: Teoría de la Señal y Comunicaciones

Número de profesores/as	1
Número de doctores/as	1
Categorías	Catedrático de Universidad
Profesorado acreditado	1
Materias / asignaturas	Privacidad y Anonimato
ECTS impartidos (previstos)	5
ECTS disponibles (potenciales)	5

Área o ámbito de conocimiento: Ingeniería de Sistemas y Automática

Número de profesores/as	1
Número de doctores/as	1
Categorías	Contratado Doctor
Profesorado acreditado	1
Materias / asignaturas	Ciberseguridad Industrial e IoT
ECTS impartidos (previstos)	2,5
ECTS disponibles (potenciales)	2,5

Méritos docentes del profesorado no acreditado

El profesor titular de escuela aportado tiene una gran experiencia en administración avanzada de sistemas operativos y su fortificación. Además, tiene gran experiencia docente (7 quinquenios). Por lo tanto, consideramos que aporta un gran valor añadido al máster. Ha coordinado e impartido la materia Fortificación de Sistemas Operativos desde el comienzo de impartición del máster con un alto grado de satisfacción por parte del alumnado.

Méritos de investigación del profesorado no doctor

El profesor titular de escuela aportado tiene una gran experiencia en administración avanzada de sistemas operativos y su fortificación. Además, tiene gran experiencia docente (7 quinquenios). Por lo tanto, consideramos que aporta un gran valor añadido al máster. Ha coordinado e impartido la materia Fortificación de Sistemas Operativos desde el comienzo de impartición del máster con un alto grado de satisfacción por parte del alumnado.

Perfil del profesorado necesario y no disponible y plan de contratación

No hay

5.2. Perfil básico de otros recursos de apoyo a la docencia necesarios

No se prevén otras necesidades de recursos humanos de apoyo a la docencia.

6. RECURSOS PARA EL APRENDIZAJE: MATERIALES E INFRAESTRUCTURALES, PRÁCTICAS Y SERVICIOS

6.1. Recursos materiales y servicios

Para la impartición de las clases de MUnICS se utilizan las aulas de videoconferencia y laboratorios disponibles en la EET de UVIGO y FIC de UDC. Las salas de videoconferencia MUnICS en UVIGO y UDC están conectadas para la impartición de docencia conjunta en las dos sedes. Los Lab MUnICS cuentan con ordenadores, 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. Tanto en la Universidad de Vigo como en la Universidad de A Coruña, este laboratorio se creó con la puesta en marcha del Máster en el curso 2018/2019.

Además, y de cara a homogeneizar el acceso a los recursos de teledocencia que acompañan a la docencia presencial, MUnICS utiliza la plataforma de la Universidad de Vigo (www.moovi.es plataforma basada en Moodle), en la que a principio de curso se inscriben los alumnos de las dos sedes (de forma automática los de la sede de UVIGO y de forma semiautomática los de la sede de UDC). En la plataforma Moovi, existe un curso por asignatura del Máster además de 2 cursos relacionados con la gestión del Máster: “Espacio Coordinación MUnICS” y “Profesorado MUnICS”). Al margen del espacio físico y los recursos técnicos propios de MUnICS, los dos centros disponen de servicios adicionales que son de relevancia para el desarrollo efectivo y eficiente del Máster. En concreto:

- FIC: Servicio de Informática y Comunicaciones; Servicio de Recursos Audiovisuales y Servicio de prevención de riesgos laborales
- EET: Servicios Informáticos; Servicio de prevención de riesgos laborales.

Toda esta información puede encontrarse en las páginas Web de los centros.

Por último, los mecanismos de revisión y mantenimiento de materiales y servicios de las universidades recae en la dirección de los centros (Escuela de Ingeniería de Telecomunicación y Facultad de Informática).

6.2 Procedimiento para la gestión de las prácticas externas

MUnICS incluye las prácticas académicas externas como una materia obligatoria desde su inicio (cuestión no alternada con la modificación en este documento). Actualmente se rige por la normativa de prácticas académicas externas disponible de forma pública en el siguiente enlace:

- https://teleco.uvigo.es/documentos/normativa/munics-2/munics_practicasempresas_normativa_20190218/

La normativa regula la oferta, la selección, la asignación, la formalización, la tutorización y la evaluación de dichas prácticas. Tanto la EET como FIC tienen un amplio catálogo de empresas con convenio firmado, las relaciones de la EET, FIC y los centros singulares de investigación CITIC y AtlanTTic con el tejido empresarial gallego garantizan una oferta de prácticas que supera el número de estudiantes matriculados en la materia. Este hecho se ha probado cierto desde el lanzamiento de MUniCS.

6.3. Previsión de dotación de recursos materiales y servicios

MUniCS lleva impartándose desde el curso 2018/2019 y, a día de hoy, se cuenta con la totalidad de recursos materiales y servicios necesarios para su impartición.

7. CALENDARIO DE IMPLANTACIÓN

7.1. Cronograma de implantación del título

El primer curso en el que se imparta el título con la modificación aquí presentada será el curso 2023/24 con una implantación anual curso a curso.

7.2 Procedimiento de adaptación

Los alumnos que hayan cursado materias de MUnICS según la memoria previa a esta verificación se adaptarán como sigue:

Memoria Original		Memoria modificada	
Materias	ECTS	Materias	ECTS
Conceptos y leyes en ciberseguridad	3	Conceptos y leyes en ciberseguridad	4
Gestión de la seguridad de la información	6	Gestión de la seguridad de la información	5
Seguridad de la información	6	Seguridad de la información	5
Seguridad en comunicaciones	6	Seguridad en comunicaciones	5
Seguridad de aplicaciones	6	Seguridad de aplicaciones	5
Redes seguras	6	Redes seguras	5
Fortificación de sistemas operativos	5	Fortificación de sistemas	5
Tests de intrusión	5	Hacking ético y Test de intrusión	5
Análisis de <i>malware</i>	5	Análisis de <i>malware</i>	5
Seguridad como negocio	3	Negocio en ciberseguridad y emprendimiento	4
Seguridad en dispositivos móviles	3	Seguridad en dispositivos móviles	3
Análisis forense de equipos	3	Análisis forense	3
Seguridad ubicua	3	Seguridad IOT e Industrial	5
Gestión de incidentes	3	Podrá reconocerse como materia optativa con 3 ECTS	
Ciberseguridad en entornos industriales	3	Seguridad IOT e Industrial	5
Prácticas en empresa	15	Prácticas en empresa	9

7.3 Enseñanzas que se extinguen

La modificación del título Máster Universitario en Ciberseguridad no extingue ningún otro título previo.

8. SISTEMA INTERNO DE GARANTÍA DE LA CALIDAD

8.1. Sistema Interno de Garantía de la Calidad

En el año 2013, la EET participa en la primera convocatoria para a “Certificación da Implantación dos SGIC” de centros del Sistema Universitario de Galicia, conforme a las directrices del programa FIDES-AUDIT, consiguiendo dicha Certificación el 18 de noviembre de 2013. A continuación, se incluyen los enlaces a las páginas Web que contiene el SIGC de la EET de la Universidade de Vigo y de FIC de la Universidade da Coruña:

- EET: <https://teleco.uvigo.es/a-escola/calidade/manual-e-procedementos/>
- FIC: <https://www.fic.udc.es/es/calidad>

El órgano competente en los procesos de admisión, reconocimiento y transferencia de créditos, así como la gestión académica del título, incluyendo la movilidad, las prácticas y el TFM es la Comisión Académica de Máster Interuniversitaria (CAMI). Asimismo, cada sede nombrará un coordinador local del título. La CAMI estará presidida por un/a coordinador/a que coincidirá con el/la coordinador/a local del centro coordinador de la titulación; y se compondrá además de los siguientes miembros:

- Vicepresidente, que coincidirá con el coordinador local en la Universidad que no coordina la titulación.
- Secretario/a, que coincidirá con el secretario del centro que coordina el título.
- Coordinadores de Módulo (6), con el siguiente reparto: Fundamentos (2, uno por sede); Técnicas (2, uno por sede); Capacitación (2, uno por sede)
- Coordinador/a de calidad, que coincidirá con la persona competente en calidad en el centro coordinador del título.
- Coordinador/a de prácticas del título
- Coordinador/a de movilidad del título
- Representantes de estudiantes (uno por sede)
- Representantes de secretaría académica (uno por sede)

La CAMI 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. Por otro lado, el coordinador local del título será el encargado de la gestión del título en el ámbito del propio centro, trasladando las decisiones a la Junta de Escuela y delegando en ella las cuestiones que son exclusivas del centro.

8.2. Medios para la información pública

Las Universidades de Vigo y Coruña cuentan con un portal de transparencia de acuerdo con la Ley nacional 19/2013 de 9 de diciembre de transparencia, acceso a la información pública y buen gobierno (BOE de 10 de diciembre) y autonómica según ley 1/2016 del 18 de enero de transparencia y buen gobierno (DOG do 15 de febrero). Sendos portales de transparencia se encuentran disponibles vía Web en los siguientes enlaces:

- <https://secretaria.uvigo.gal/uv/web/transparencia>
- <https://www.udc.es/es/transparencia/>

La Universidad de Vigo figura en el puesto 2º **del ránking de transparencia de universidades** españolas, según [informe](#) elaborado en el año 2017 por la Fundación Compromiso y transparencia. Su reglamento de transparencia y acceso a la información pública se puede consultar en el siguiente enlace ([aprobado en la sesión de Consello de Goberno 09/10/017](#)). Esta normativa establece los mecanismos y procedimientos internos relacionados con las obligaciones de publicidad activa, el derecho de acceso a la información pública y el buen gobierno. En lo que se refiere a la publicidad activa, UVIGO hace pública la información prevista en la legislación estatal y autonómica en materia de transparencia, y además, la siguiente: a) La oferta académica que incluye las titulaciones oficiales y propias, los cursos complementarios y formativos y los cursos de idiomas; b) Los indicadores incluidos en los procedimientos de verificación, seguimiento y acreditación de títulos oficiales, así como toda la información con carácter de información pública en dichos procedimientos; c) Los resultados relacionados con el rendimiento académico de los estudiantes; d) Los resultados de la evaluación de la docencia y de los títulos; e) Resultados relacionados con los programas de internacionalización; f) Los indicadores relacionados con la inserción laboral de los estudiantes de posgrado; g) Guías docentes y otra documentación relevante relacionada con la docencia; h) La relación de docentes con un breve perfil de este: nombre, categoría, dedicación, distinciones y breve currículum; i) Información sobre los principales canales de representación y comunicación con los estudiantes.

Las dos universidades cuentan con los correspondientes vicerrectorados responsables de la oferta de titulaciones oficiales (grados, másteres y programas de doctorado) y que se encargan de su promoción y publicidad a nivel institucional, con la colaboración de otros vicerrectorados y servicios. En el aspecto relativo a la difusión a nivel estatal e internacional, las dos universidades gallegas participan anualmente en ferias y exposiciones acerca de la oferta docente de Universidades y Centros de Enseñanza Superior, tanto a nivel local como nacional (Aula) e internacional (NAFSA, ACTFL en Estados Unidos, y especialmente Euro posgrado en Latinoamérica), para promocionar su oferta de estudios. Por otro lado, los estudiantes del último año de los grados reciben de sus universidades información sobre la oferta de títulos de máster.

De forma más específica, los futuros estudiantes pueden obtener información detallada del Máster y/o del proceso de preinscripción y matrícula por los siguientes medios:

- Página web de los centros EET (www.teleco.uvigo.es), FIC (www.fic.udc.es)
- Página web de las Universidades UVIGO (www.uvigo.gal/es/estudiar/que-estudiar) y UDC (estudios.udc.es)

Además, los coordinadores locales de MUnICS en cada una de las dos Universidades organizan una sesión informativa en sus centros en el mes de mayo, destinada especialmente a los estudiantes de último curso de grado que puedan estar interesados en continuar sus estudios en este máster, abriendo la posibilidad de asistencia a otras personas potencialmente interesadas. Por otro lado, el máster dispone de una página web con información detallada y actualizada del máster siguiendo los criterios y las recomendaciones de la ANECA (programa, profesorado, metodología docente, procesos administrativos, etc.). Esta página Web es única para las dos Universidades (www.munics.es). También dispone de perfiles en las redes Twitter y LinkedIn. Por último, MUnICS está dado de alta en el catálogo de INCIBE (España) y ENISA (Europa) como formación de posgrado en ciberseguridad, y participa en European Cyber Security Organisation (ECSO) -- organización paneuropea que federa el sector público y privado de la ciberseguridad europea.