IMPRESO SOLICITUD PARA VERIFICACIÓN DE TÍTULOS OFICIALES

1. DATOS DE LA UNIVERSIDAD, CENTRO Y TÍTULO QUE PRESENTA LA SOLICITUD

De conformidad con el Real Decreto 1393/2007, por el que se establece la ordenación de las Enseñanzas Universitarias Oficiales

UNIVERSIDAD SOLICITANTE	CENTRO	CÓDIGO CENTRO
Universidad de Vigo	Escuela de Ingeniería de Telecomunicación	36016981
NIVEL	**DENOMINACIÓN CORTA**	
Máster	Ciberseguridad	
DENOMINACIÓN ESPECÍFICA		
Máster Universitario en Ciberseguridad por la Universidad de A Coruña y la Universidad de Vigo		
NIVEL MECES		
3|3		
RAMA DE CONOCIMIENTO	**CONJUNTO**	
Ingeniería y Arquitectura	Nacional	
CONVENIO		
Convenio específico entre la Universidad de Vigo y la Universidad de A Coruña		
UNIVERSIDADES PARTICIPANTES	**CENTRO**	**CÓDIGO CENTRO**
Universidad de A Coruña	Facultad de Informática	15025451
HABILITA PARA EL EJERCICIO DE PROFESIONES REGULADAS	**NORMA HABILITACIÓN**	
No		
SOLICITANTE		
NOMBRE Y APELLIDOS	**CARGO**	
Alfonso Lago Ferreiro	Vicerrector de Profesorado, Docencia y Titulaciones	
Tipo Documento	**Número Documento**	
NIF	76808276Y	
REPRESENTANTE LEGAL		
NOMBRE Y APELLIDOS	**CARGO**	
Manuel Joaquín Reigosa Roger	Rector	
Tipo Documento	**Número Documento**	
NIF	36023985M	
RESPONSABLE DEL TÍTULO		
NOMBRE Y APELLIDOS	**CARGO**	
Ana Fernández Vilas	Coordinadora	
Tipo Documento	**Número Documento**	
NIF	35307306Y	

2. DIRECCIÓN A EFECTOS DE NOTIFICACIÓN

A los efectos de la práctica de la NOTIFICACIÓN de todos los procedimientos relativos a la presente solicitud, las comunicaciones se dirigirán a la dirección que figure en el presente apartado.

DOMICILIO	CÓDIGO POSTAL	MUNICIPIO	TELÉFONO
Edificio Exeria - Campus Universitario de Vigo	36310	Vigo	626768751
E-MAIL	**PROVINCIA**		**FAX**
verifica@uvigo.es	Pontevedra		986813590

3. PROTECCIÓN DE DATOS PERSONALES
De acuerdo con lo previsto en la Ley Orgánica 5/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa que los datos solicitados en este impreso son necesarios para la tramitación de la solicitud y podrán ser objeto de tratamiento automatizado. La responsabilidad del fichero automatizado corresponde al Consejo de Universidades. Los solicitantes, como cedentes de los datos podrán ejercer ante el Consejo de Universidades los derechos de información, acceso, rectificación y cancelación a los que se refiere el Título III de la citada Ley 5-1999, sin perjuicio de lo dispuesto en otra normativa que ampare los derechos como cedentes de los datos de carácter personal.
El solicitante declara conocer los términos de la convocatoria y se compromete a cumplir los requisitos de la misma, consintiendo expresamente la notificación por medios telemáticos a los efectos de lo dispuesto en el artículo 59 de la 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en su versión dada por la Ley 4/1999 de 13 de enero.

	En: Pontevedra, AM 28 de noviembre de 2022
	Firma: Representante legal de la Universidad

1. DESCRIPCIÓN DEL TÍTULO

1.1. DATOS BÁSICOS

NIVEL	DENOMINACIÓN ESPECIFICA	CONJUNTO	CONVENIO	CONV. ADJUNTO
Máster	Máster Universitario en Ciberseguridad por la Universidad de A Coruña y la Universidad de Vigo	Nacional		Ver Apartado 1: Anexo 1.

LISTADO DE ESPECIALIDADES
No existen datos

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

NO HABILITA O ESTÁ VINCULADO CON PROFESIÓN REGULADA ALGUNA

AGENCIA EVALUADORA
Axencia para a Calidade do Sistema Universitario de Galicia

UNIVERSIDAD SOLICITANTE
Universidad de Vigo

LISTADO DE UNIVERSIDADES	
CÓDIGO	UNIVERSIDAD
037	Universidad de A Coruña
038	Universidad de Vigo

LISTADO DE UNIVERSIDADES EXTRANJERAS	
CÓDIGO	UNIVERSIDAD
No existen datos	

LISTADO DE INSTITUCIONES PARTICIPANTES
No existen datos

1.2. DISTRIBUCIÓN DE CRÉDITOS EN EL TÍTULO

CRÉDITOS TOTALES	CRÉDITOS DE COMPLEMENTOS FORMATIVOS	CRÉDITOS EN PRÁCTICAS EXTERNAS
90	0	9
CRÉDITOS OPTATIVOS	**CRÉDITOS OBLIGATORIOS**	**CRÉDITOS TRABAJO FIN GRADO/ MÁSTER**
6	63	12

LISTADO DE ESPECIALIDADES	
ESPECIALIDAD	CRÉDITOS OPTATIVOS
No existen datos	

1.3. Universidad de Vigo

1.3.1. CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS	
CÓDIGO	CENTRO
36016981	Escuela de Ingeniería de Telecomunicación

1.3.2. Escuela de Ingeniería de Telecomunicación

1.3.2.1. Datos asociados al centro

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

20	20	
	TIEMPO COMPLETO	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	48.0	60.0
RESTO DE AÑOS	48.0	78.0
	TIEMPO PARCIAL	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	18.0	47.0
RESTO DE AÑOS	18.0	47.0
NORMAS DE PERMANENCIA		
https://www.xunta.gal/dog/Publicados/2017/20170630/AnuncioU500-210617-0001_es.html		
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
Sí	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

1.3. Universidad de A Coruña

1.3.1. CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS	
CÓDIGO	**CENTRO**
15025451	Facultad de Informática

1.3.2. Facultad de Informática

1.3.2.1. Datos asociados al centro

TIPOS DE ENSEÑANZA QUE SE IMPARTEN EN EL CENTRO		
PRESENCIAL	**SEMIPRESENCIAL**	**VIRTUAL**
Sí	No	No
PLAZAS DE NUEVO INGRESO OFERTADAS		
PRIMER AÑO IMPLANTACIÓN	**SEGUNDO AÑO IMPLANTACIÓN**	
20	20	
	TIEMPO COMPLETO	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	60.0	60.0
RESTO DE AÑOS	48.0	78.0
	TIEMPO PARCIAL	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	24.0	48.0
RESTO DE AÑOS	24.0	48.0
NORMAS DE PERMANENCIA		
https://www.udc.es/export/sites/udc/normativa/_galeria_down/academica/dedicacion_estudo_permanencia.pdf		
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**

Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
Sí	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

2. JUSTIFICACIÓN, ADECUACIÓN DE LA PROPUESTA Y PROCEDIMIENTOS

Ver Apartado 2: Anexo 1.

3. COMPETENCIAS

3.1 COMPETENCIAS BÁSICAS Y GENERALES
BÁSICAS
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
GENERALES
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-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-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-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.
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-01 - Conocer los métodos y técnicas básicas de la criptografía clásica, estándares y protocolos de seguridad criptográfica, esteganografía y cifrado post-cuántico.
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 en 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.
3.2 COMPETENCIAS TRANSVERSALES
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.
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-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 anonimia 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.
3.3 COMPETENCIAS ESPECÍFICAS
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 mara minimizar su exposición y comprobar su niel 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 interaccionar 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 auditoria 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.

4. ACCESO Y ADMISIÓN DE ESTUDIANTES

4.1 SISTEMAS DE INFORMACIÓN PREVIO

Ver Apartado 4: Anexo 1.

4.2 REQUISITOS DE ACCESO Y CRITERIOS DE ADMISIÓN

El artículo 18 del Real Decreto 822/2021, de 28 de septiembre, establece las siguientes condiciones para acceder a las enseñanzas oficiales de Máster.

Estar en posesión de un título de Graduada/o de Máster.

Poseer un título equivalente extranjero sin necesidad de ser homologado.

Excepcionalmente, existe la posibilidad de matrícula condicionada cuando el máximo pendiente en el Grado sea de 9 ECTS y el TFG. Siempre se dará prioridad de matrícula a los graduados/as.

Se reconocen complementos formativos, con un máximo del 20% de los ECTS del Máster.

Se reserva, al menos, un 5% de plazas para estudiantes con grado de discapacidad igual o mayor del 33% o con necesidades de apoyo educativo permanentes asociadas a circunstancias personales de discapacidad.

Los requisitos de acceso al Máster son, con carácter general, los establecidos por el RD 822/2021, de 28 de septiembre.

El acceso al título se atendrá a las disposiciones del Ministerio, de la Comunidad Autónoma de Galicia, y a lo que se disponga en el desarrollo normativo de la Universidade da Vigo.

En las páginas de la Universidade de Vigo se recogen de forma detallada los aspectos relevantes de admisión y matrícula:

- **https://www.uvigo.gal/estudar/acceder/acceso-masters**

- **https://www.uvigo.gal/es/estudiar/gestiones-estudiantes/matriculate/matricula-masteres**

El Real Decreto 822/2021, de 28 de septiembre, en su artículo 18.5 y en el Anexo 2.3.1, establece que las universidades o los centros regularán la admisión en las enseñanzas de Máster Universitario, estableciendo requisitos específicos de acceso, criterios y procedimientos particulares de admisión, y, en caso de ser necesarios, complementos formativos.

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 **www.munics.es**

y en los portales de preinscripción y matrícula de la Universidad de Vigo y la Universidad de A Coruña.

- **https://www.munics.es/acceso.html**
- **https://www.uvigo.gal/es/estudiar/acceder/acceso-masteres**
- **https://www.estudos.udc.es/gl/StudyAtUdc/master**

4.3 APOYO A ESTUDIANTES

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 apo-

yo 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

4.4 SISTEMA DE TRANSFERENCIA Y RECONOCIMIENTO DE CRÉDITOS

Reconocimiento de Créditos Cursados en Enseñanzas Superiores Oficiales no Universitarias

MÍNIMO	MÁXIMO
0	0

Reconocimiento de Créditos Cursados en Títulos Propios

MÍNIMO	MÁXIMO
0	0

Adjuntar Título Propio

Ver Apartado 4: Anexo 2.

Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional

MÍNIMO	MÁXIMO
0	9

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**

Tal como se indica en el artículo 10 del RD 822/2021, de 28 de septiembre:

Los procedimientos de reconocimiento y de transferencia de créditos académicos en los títulos universitarios oficiales tiene por objeto facilitar la movilidad del estudiantado entre títulos universitarios oficiales españoles, así como entre estos y los títulos universitarios extranjeros. Las universidades aprobarán normativas específicas para regular estos procedimientos conforme a lo dispuesto en el presente real decreto.

Las universidades deberán reflejar en los planes de estudios de cada título el volumen de créditos susceptibles de ser utilizados en estos procedimientos, y las condiciones y características genéricas de los mismos. Estos créditos reconocidos o transferidos serán recogidos en el expediente del o la estudiante y en el Suplemento Europeo del Título.

El reconocimiento de créditos académicos hace referencia al procedimiento de aceptación por parte de una universidad de créditos obtenidos en otros estudios oficiales, en la misma u otra universidad, para que formen parte del expediente del o de la estudiante a efecto de obtener un título universitario oficial diferente del que proceden. En este procedimiento no podrán ser reconocidos los créditos que corresponden a trabajos de fin de Grado o de Máster, a excepción de aquellos que se desarrollen específicamente en un programa de movilidad.

La acreditación de la experiencia profesional y laboral podrá ser reconocida como créditos académicos utilizados para obtener un título de carácter oficial. Esta opción podrá darse cuando esa experiencia se muestre estrechamente relacionada con los conocimientos, competencias y habilidades propias del título universitario oficial. De igual modo, podrán ser reconocidos los créditos superados y cursados en estudios universitarios propios de las universidades o de otros estudios superiores oficiales.

El volumen de créditos reconocibles a partir de la **experiencia profesional o laboral o aquellos procedentes de estudios universitarios no oficiales** (propios o de formación permanente) no podrá superar, globalmente, el 15 por ciento del total de créditos que configuran el plan de estudios del título que se pretende obtener. Estos créditos reconocidos no contarán con calificación numérica y, por lo tanto, no podrán utilizarse en el momento de baremar el expediente del o la estudiante.

Como excepción a lo establecido en el párrafo precedente, podrá superarse este porcentaje hasta llegar incluso a reconocerse la totalidad de los créditos que provienen de estudios universitarios no oficiales, a condición de que el correspondiente título no oficial deje de impartirse y sea extinguido y reemplazado por el nuevo título universitario oficial en el cual se reconozcan los créditos académicos. En este caso, los sistemas internos de garantía de la calidad velarán por la idoneidad académica de este procedimiento.

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. 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.

La transferencia de créditos académicos hace referencia a la inclusión, en el expediente académico y en el Suplemento Europeo al Título, de la totalidad de los créditos obtenidos en enseñanzas oficiales cursadas previamente, indistintamente de la universidad, que no hayan conducido a la obtención de un título universitario oficial.

4.6 COMPLEMENTOS FORMATIVOS

5. PLANIFICACIÓN DE LAS ENSEÑANZAS

5.1 DESCRIPCIÓN DEL PLAN DE ESTUDIOS
Ver Apartado 5: Anexo 1.
5.2 ACTIVIDADES FORMATIVAS
Lección magistral
Resolución de problemas
Prácticas en aulas informáticas
Actividades introductorias
Practicas TIC
Estudio de casos
Presentaciones
Seminarios
Trabajo autónomo del alumno
Atención personalizada
Prácticas de laboratorio
Trabajos y/o proyectos (individuales o en grupo)
Prácticas Externas
Debate
Taller
Eventos científicos
5.3 METODOLOGÍAS DOCENTES
Lección magistral
Resolución de problemas
Prácticas en aulas informáticas
Actividades introductorias
Practicas TIC
Estudio de casos
Presentaciones
Seminarios
Trabajo autónomo del alumno
Atención personalizada
Prácticas de laboratorio
Trabajos y/o proyectos (individuales o en grupo)
Eventos científicos
Prácticas Externas
Debate
Taller
5.4 SISTEMAS DE EVALUACIÓN
Examen de preguntas de desarrollo
Resolución de problemas y ejercicios
Informes de prácticas
Examen de pruebas objetivas y de desarrollo
Evaluación de trabajos y actividades

Evaluación de presentaciones		
Debate		
Observación sistemática		
Simulación		
Trabajo		
Proyecto		
Prácticas de laboratorio		
Presentación		
Examen de prácticas		
5.5 NIVEL 1: FUNDAMENTOS DE CIBERSEGURIDAD		
5.5.1 Datos Básicos del Nivel 1		
NIVEL 2: Seguridad de la información		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	5	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
5		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
Sí	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
K-01 HD-01 C-01, C-13		
5.5.1.3 CONTENIDOS		
· 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.		

5.5.1.4 OBSERVACIONES		
Modalidad: Presencial Presencialidad: 42 horas		
5.5.1.5 COMPETENCIAS		
5.5.1.5.1 BÁSICAS Y GENERALES		
K-01 - Conocer los métodos y técnicas básicas de la criptografía clásica, estándares y protocolos de seguridad criptográfica, esteganografía y cifrado post-cuántico.		
5.5.1.5.2 TRANSVERSALES		
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-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 anonimia y la privacidad.		
5.5.1.5.3 ESPECÍFICAS		
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.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Lección magistral	0	0
Resolución de problemas	0	0
Prácticas en aulas informáticas	0	0
5.5.1.7 METODOLOGÍAS DOCENTES		
Lección magistral		
Resolución de problemas		
Prácticas en aulas informáticas		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Examen de preguntas de desarrollo	0.0	100.0
Resolución de problemas y ejercicios	0.0	100.0
Informes de prácticas	0.0	100.0
NIVEL 2: Análisis de malware		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	5	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
5		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
Sí	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**

No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
K-02 HD-02 C-03, C-06		
5.5.1.3 CONTENIDOS		
- 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.		
5.5.1.4 OBSERVACIONES		
Modalidad: Presencial Presencialidad: 42 horas		
5.5.1.5 COMPETENCIAS		
5.5.1.5.1 BÁSICAS Y GENERALES		
K-02 - Conocer las técnicas de ocultación y persistencia de malware; así como las tendencias actuales en malware mediante el estudio de casos reales.		
5.5.1.5.2 TRANSVERSALES		
C-03 - Trabajar como analista de malware, para proteger aplicaciones, así como analizar su seguridad en cualquier área de aplicación.		
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.		
5.5.1.5.3 ESPECÍFICAS		
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.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Lección magistral	0	0
Actividades introductorias	0	0
Practicas TIC	0	0
Estudio de casos	0	0
Presentaciones	0	0
Seminarios	0	0
5.5.1.7 METODOLOGÍAS DOCENTES		
Lección magistral		
Actividades introductorias		
Practicas TIC		
Estudio de casos		
Presentaciones		
Seminarios		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**

Resolución de problemas y ejercicios	0.0	100.0
Examen de pruebas objetivas y de desarrollo	0.0	100.0
Evaluación de trabajos y actividades	0.0	100.0
Evaluación de presentaciones	0.0	100.0

NIVEL 2: Privacidad y anonimidad		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	5	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
5		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
Sí	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
K-03 HD-03 C-01, C-14		
5.5.1.3 CONTENIDOS		
- 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.		
5.5.1.4 OBSERVACIONES		
Modalidad: Presencial Presencialidad: 42 horas		
5.5.1.5 COMPETENCIAS		

5.5.1.5.1 BÁSICAS Y GENERALES
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 en computación segura multi-partita.
5.5.1.5.2 TRANSVERSALES
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-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 anonimia y la privacidad.
5.5.1.5.3 ESPECÍFICAS
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.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Lección magistral	0	0
Resolución de problemas	0	0
Prácticas en aulas informáticas	0	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección magistral
Resolución de problemas
Prácticas en aulas informáticas

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Examen de preguntas de desarrollo	0.0	100.0
Resolución de problemas y ejercicios	0.0	100.0
Informes de prácticas	0.0	100.0

NIVEL 2: Seguridad de aplicaciones

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	5

DESPLIEGUE TEMPORAL: Cuatrimestral

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

LENGUAS EN LAS QUE SE IMPARTE

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

No	No
NO CONSTAN ELEMENTOS DE NIVEL 3	
5.5.1.2 RESULTADOS DE APRENDIZAJE	
K-04 HD-04 C-03, C-14	
5.5.1.3 CONTENIDOS	
- 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.	
5.5.1.4 OBSERVACIONES	
Modalidad: Presencial Presencialidad:42	
5.5.1.5 COMPETENCIAS	
5.5.1.5.1 BÁSICAS Y GENERALES	
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.	
5.5.1.5.2 TRANSVERSALES	
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-03 - Trabajar como analista de malware, para proteger aplicaciones, así como analizar su seguridad en cualquier área de aplicación.	
5.5.1.5.3 ESPECÍFICAS	
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.	

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Lección magistral	0	0
Prácticas en aulas informáticas	0	0
Actividades introductorias	0	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección magistral
Prácticas en aulas informáticas
Actividades introductorias

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Examen de pruebas objetivas y de desarrollo	0.0	100.0
Prácticas de laboratorio	0.0	100.0

NIVEL 2: Redes seguras
5.5.1.1 Datos Básicos del Nivel 2

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

5.5.1.2 RESULTADOS DE APRENDIZAJE

K-05

HD-05

C-02, C-05, C-10

5.5.1.3 CONTENIDOS

- 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, nextgeneration 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.

5.5.1.4 OBSERVACIONES

Modalidad: Presencial
Presencialidad: 42 horas

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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.

5.5.1.5.2 TRANSVERSALES

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-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-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.
5.5.1.5.3 ESPECÍFICAS
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.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Lección magistral	0	0
Practicas TIC	0	0
Trabajo autónomo del alumno	0	0
Atención personalizada	0	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección magistral
Practicas TIC
Trabajo autónomo del alumno
Atención personalizada

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Informes de prácticas	0.0	100.0
Examen de pruebas objetivas y de desarrollo	0.0	100.0
Examen de prácticas	0.0	100.0

NIVEL 2: Tecnologías de registro distribuido y blockchain

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	5

DESPLIEGUE TEMPORAL: Cuatrimestral

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

LENGUAS EN LAS QUE SE IMPARTE

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

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

K-06

HD-06

C-02, C-04

5.5.1.3 CONTENIDOS

- 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.

5.5.1.4 OBSERVACIONES

Modalidad: Presencial
Presencialidad: 42 horas.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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.

5.5.1.5.2 TRANSVERSALES

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-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.

5.5.1.5.3 ESPECÍFICAS

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.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Lección magistral	0	0
Estudio de casos	0	0
Prácticas de laboratorio	0	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección magistral

Estudio de casos

Prácticas de laboratorio

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Informes de prácticas	0.0	100.0
Examen de pruebas objetivas y de desarrollo	0.0	100.0
Proyecto	0.0	100.0

5.5 NIVEL 1: TÉCNICAS DE CIBERSEGURIDAD

5.5.1 Datos Básicos del Nivel 1

NIVEL 2: Seguridad en comunicaciones

5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	5	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
5		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
Sí	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
K-07 HD-07 C-02, C-05, C-10		
5.5.1.3 CONTENIDOS		
- Seguridad en capa física y de enlace. - Seguridad en capa de red. - Seguridad en capa de transporte. - Seguridad en capa de aplicación.		
5.5.1.4 OBSERVACIONES		
Modalidad: Presencial Presencialidad: 42 horas		
5.5.1.5 COMPETENCIAS		
5.5.1.5.1 BÁSICAS Y GENERALES		
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.		
5.5.1.5.2 TRANSVERSALES		
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-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-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.		
5.5.1.5.3 ESPECÍFICAS		

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.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Lección magistral	0	0
Practicas TIC	0	0
Trabajo autónomo del alumno	0	0
Atención personalizada	0	0
Trabajos y/o proyectos (individuales o en grupo)	0	0
5.5.1.7 METODOLOGÍAS DOCENTES		
Lección magistral		
Practicas TIC		
Trabajo autónomo del alumno		
Atención personalizada		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Resolución de problemas y ejercicios	0.0	100.0
Examen de pruebas objetivas y de desarrollo	0.0	100.0
Evaluación de trabajos y actividades	0.0	100.0
Examen de prácticas	0.0	100.0
NIVEL 2: Fortificación de sistemas		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	5	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	5	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
Sí	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		

K-08

HD-08

C-06, C-10

5.5.1.3 CONTENIDOS

Fortificación del proceso de arranque

Fortificación cuentas de los usuarios

Fortificación sistemas de ficheros

Fortificación de aplicaciones

Fortificación de la red

Mantenimiento

5.5.1.4 OBSERVACIONES

Modalidad: Presencial
Presencialidad: 42 horas

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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.

5.5.1.5.2 TRANSVERSALES

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-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.

5.5.1.5.3 ESPECÍFICAS

HD-08 - Identificar las vulnerabilidades de un SO en un entorno de uso concreto, modificar la configuración mara minimizar su exposición y comprobar su niel de seguridad.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Lección magistral	0	0
Practicas TIC	0	0
Trabajo autónomo del alumno	0	0
Atención personalizada	0	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección magistral

Practicas TIC

Trabajo autónomo del alumno

Atención personalizada

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Informes de prácticas	0.0	100.0
Examen de pruebas objetivas y de desarrollo	0.0	100.0
Simulación	0.0	100.0

NIVEL 2: Ciberseguridad industrial e IoT

5.5.1.1 Datos Básicos del Nivel 2

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

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

K-09

HD-09

C-02, C-05, C-07

5.5.1.3 CONTENIDOS

- 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.

5.5.1.4 OBSERVACIONES

Modalidad: Presencial
Presencialidad: 42 horas

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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.

5.5.1.5.2 TRANSVERSALES

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-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-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.

5.5.1.5.3 ESPECÍFICAS

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.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Lección magistral	0	0
Estudio de casos	0	0
Prácticas de laboratorio	0	0
5.5.1.7 METODOLOGÍAS DOCENTES		
Lección magistral		
Estudio de casos		
Prácticas de laboratorio		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Informes de prácticas	0.0	100.0
Examen de pruebas objetivas y de desarrollo	0.0	100.0
Trabajo	0.0	100.0
Proyecto	0.0	100.0
NIVEL 2: Hacking ético y test de intrusión		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	5	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	5	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
Sí	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
K-10 HD-10 C-06, C-08, C-09, C-10		
5.5.1.3 CONTENIDOS		

- 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

5.5.1.4 OBSERVACIONES

Modalidad: Presencial
Presencialidad: 42

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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.

5.5.1.5.2 TRANSVERSALES

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-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.

5.5.1.5.3 ESPECÍFICAS

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.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Lección magistral	0	0
Actividades introductorias	0	0
Estudio de casos	0	0
Prácticas de laboratorio	0	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección magistral

Actividades introductorias

Estudio de casos

Prácticas de laboratorio

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Examen de pruebas objetivas y de desarrollo	0.0	100.0
Prácticas de laboratorio	0.0	100.0

NIVEL 2: Análisis forense

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Optativa
ECTS NIVEL 2	3

DESPLIEGUE TEMPORAL: Cuatrimestral

ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
	3	

ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
Sí	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
K-12 HD-12 C-06, C-08, C-09		
5.5.1.3 CONTENIDOS		
1. Introducción a la Informática Forense 2. Proceso de adquisición de evidencias 3. Técnicas de Análisis Forense 4. Análisis de casos		
5.5.1.4 OBSERVACIONES		
Modalidad:Presencial Presencialidad:22,5 horas		
5.5.1.5 COMPETENCIAS		
5.5.1.5.1 BÁSICAS Y GENERALES		
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.		
5.5.1.5.2 TRANSVERSALES		
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-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.		
5.5.1.5.3 ESPECÍFICAS		
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		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Lección magistral	0	0
Resolución de problemas	0	0

Prácticas en aulas informáticas	0	0
5.5.1.7 METODOLOGÍAS DOCENTES		
Lección magistral		
Resolución de problemas		
Prácticas en aulas informáticas		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Resolución de problemas y ejercicios	0.0	100.0
Informes de prácticas	0.0	100.0
Examen de pruebas objetivas y de desarrollo	0.0	100.0
NIVEL 2: Seguridad en centros de datos		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
ECTS NIVEL 2	3	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	3	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
Sí	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
K-13 HD-13 C-02, C-05, C-10		
5.5.1.3 CONTENIDOS		
- 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.

5.5.1.4 OBSERVACIONES

Modalidad: Presencial
Presencialidad: 22,5 horas

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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.

5.5.1.5.2 TRANSVERSALES

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-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-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.

5.5.1.5.3 ESPECÍFICAS

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.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Lección magistral	0	0
Resolución de problemas	0	0
Prácticas en aulas informáticas	0	0
Presentaciones	0	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección magistral

Resolución de problemas

Prácticas en aulas informáticas

Presentaciones

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Resolución de problemas y ejercicios	0.0	100.0
Informes de prácticas	0.0	100.0
Examen de pruebas objetivas y de desarrollo	0.0	100.0

NIVEL 2: Seguridad en dispositivos móviles

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Optativa
ECTS NIVEL 2	3

DESPLIEGUE TEMPORAL: Cuatrimestral

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

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

LISTADO DE ESPECIALIDADES
No existen datos
NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

K-14

HD-14

C-03, C-08 ,C-09

5.5.1.3 CONTENIDOS

-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)

5.5.1.4 OBSERVACIONES

Modalidad: Presencial
Presencialidad: 22,5

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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.

5.5.1.5.2 TRANSVERSALES

C-03 - Trabajar como analista de malware, para proteger aplicaciones, así como analizar su seguridad en cualquier área de aplicación.

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.

5.5.1.5.3 ESPECÍFICAS

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.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD

Lección magistral	0	0
Prácticas de laboratorio	0	0
5.5.1.7 METODOLOGÍAS DOCENTES		
Lección magistral		
Prácticas de laboratorio		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Resolución de problemas y ejercicios	0.0	100.0
Informes de prácticas	0.0	100.0
Examen de pruebas objetivas y de desarrollo	0.0	100.0
NIVEL 2: Smart Contracts y Distributed Applications		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
ECTS NIVEL 2	3	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	3	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
Sí	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
K-15 HD-15 C-03, C-04		
5.5.1.3 CONTENIDOS		
- 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.		
5.5.1.4 OBSERVACIONES		

Modalidad: Presencial
Presencialidad: 22,5 horas

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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).

5.5.1.5.2 TRANSVERSALES

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.

5.5.1.5.3 ESPECÍFICAS

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 interaccionar con contratos inteligentes, así como usar oráculos bajo condiciones de robustez y seguridad.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Lección magistral	0	0
Estudio de casos	0	0
Prácticas de laboratorio	0	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección magistral

Estudio de casos

Prácticas de laboratorio

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Informes de prácticas	0.0	100.0
Examen de pruebas objetivas y de desarrollo	0.0	100.0
Proyecto	0.0	100.0

5.5 NIVEL 1: CAPACITACIÓN ACADÉMICO-PROFESIONAL

5.5.1 Datos Básicos del Nivel 1

NIVEL 2: Negocio en ciberseguridad y emprendimiento

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	4

DESPLIEGUE TEMPORAL: Cuatrimestral

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

LENGUAS EN LAS QUE SE IMPARTE

CASTELLANO	CATALÁN	EUSKERA
Sí	No	No

GALLEGO	VALENCIANO	INGLÉS
Sí	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

K-11

HD-11

C-16, C-17,C-18

5.5.1.3 CONTENIDOS

- 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.

5.5.1.4 OBSERVACIONES

Modalidad: Presencial
Presencialidad: 30 horas

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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.

5.5.1.5.2 TRANSVERSALES

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.

5.5.1.5.3 ESPECÍFICAS

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.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Lección magistral	0	0
Resolución de problemas	0	0
Trabajos y/o proyectos (individuales o en grupo)	0	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección magistral

Resolución de problemas

Trabajos y/o proyectos (individuales o en grupo)

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA

Examen de pruebas objetivas y de desarrollo	0.0	100.0
Evaluación de trabajos y actividades	0.0	100.0

NIVEL 2: Gestión de la seguridad de la información		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	5	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
		5
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
Sí	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
K-16 HD-16 C-11, C-14		
5.5.1.3 CONTENIDOS		
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		
5.5.1.4 OBSERVACIONES		
Modalidad: Presencial Presencialidad: 42 horas		
5.5.1.5 COMPETENCIAS		
5.5.1.5.1 BÁSICAS Y GENERALES		
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.		
5.5.1.5.2 TRANSVERSALES		
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-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.
5.5.1.5.3 ESPECÍFICAS
HD-16 - Gestionar la seguridad de la información, utilizar herramientas de análisis de riesgos y la auditoria de seguridad, identificar y clasificar posibles incidentes de forma proactiva y definir los cauces para su gestión y resolución.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Lección magistral	0	0
Resolución de problemas	0	0
Prácticas en aulas informáticas	0	0
Presentaciones	0	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección magistral
Resolución de problemas
Prácticas en aulas informáticas
Presentaciones

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Informes de prácticas	0.0	100.0
Examen de pruebas objetivas y de desarrollo	0.0	100.0

NIVEL 2: Conceptos y leyes

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	4

DESPLIEGUE TEMPORAL: Cuatrimestral

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

LENGUAS EN LAS QUE SE IMPARTE

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

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

K-17

HD-17

C-12, C-13, C-19

5.5.1.3 CONTENIDOS

- 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.
- 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.

5.5.1.4 OBSERVACIONES

Modalidad: Presencial
Presencialidad: 30 horas

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

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.

5.5.1.5.2 TRANSVERSALES

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.

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-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.

5.5.1.5.3 ESPECÍFICAS

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.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Lección magistral	0	0
Resolución de problemas	0	0
Estudio de casos	0	0
Seminarios	0	0
Eventos científicos	0	0

5.5.1.7 METODOLOGÍAS DOCENTES

Lección magistral

Resolución de problemas

Estudio de casos

Seminarios

Eventos científicos

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Resolución de problemas y ejercicios	0.0	100.0
Examen de pruebas objetivas y de desarrollo	0.0	100.0

NIVEL 2: Prácticas en empresas

5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Prácticas Externas	
ECTS NIVEL 2	9	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
		9
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
Sí	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
HD-18, HD-19 C-16, C-17, C-18		
5.5.1.3 CONTENIDOS		
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 los 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.		
5.5.1.4 OBSERVACIONES		
Modalidad: Presencial, semipresencial o virtual Presencialidad: 225 horas		
5.5.1.5 COMPETENCIAS		
5.5.1.5.1 BÁSICAS Y GENERALES		
No existen datos		
5.5.1.5.2 TRANSVERSALES		
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.		
5.5.1.5.3 ESPECÍFICAS		
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.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Presentaciones	0	0
Prácticas Externas	0	0
Debate	0	0
5.5.1.7 METODOLOGÍAS DOCENTES		
Presentaciones		
Prácticas Externas		
Debate		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Informes de prácticas	0.0	100.0
Debate	0.0	100.0
Observación sistemática	0.0	100.0
NIVEL 2: Trabajo fin de máster		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Trabajo Fin de Grado / Máster	
ECTS NIVEL 2	12	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
		12
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
Sí	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
HD-19 C-13, C-14, C-15, C-16		
5.5.1.3 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.

5.5.1.4 OBSERVACIONES

Modalidad: Semipresencial

Presencialidad: 1

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

No existen datos

5.5.1.5.2 TRANSVERSALES

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.

5.5.1.5.3 ESPECÍFICAS

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.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Estudio de casos	0	0
Taller	0	0

5.5.1.7 METODOLOGÍAS DOCENTES

Estudio de casos

Taller

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Trabajo	0.0	100.0
Presentación	0.0	100.0

6. PERSONAL ACADÉMICO

6.1 PROFESORADO Y OTROS RECURSOS HUMANOS				
Universidad	**Categoría**	**Total %**	**Doctores %**	**Horas %**
Universidad de A Coruña	Profesor Contratado Doctor	17	100	15
Universidad de Vigo	Catedrático de Universidad	5	100	20
Universidad de Vigo	Profesor Titular de Universidad	30	100	15
Universidad de Vigo	Profesor Contratado Doctor	15	100	15
Universidad de A Coruña	Catedrático de Universidad	5	100	5
Universidad de A Coruña	Profesor Titular de Universidad	18	100	10
Universidad de A Coruña	Profesor Titular de Escuela Universitaria	5	45	10
Universidad de A Coruña	Ayudante Doctor	5	100	10

PERSONAL ACADÉMICO

Ver Apartado 6: Anexo 1.

6.2 OTROS RECURSOS HUMANOS

Ver Apartado 6: Anexo 2.

7. RECURSOS MATERIALES Y SERVICIOS

Justificación de que los medios materiales disponibles son adecuados: Ver Apartado 7: Anexo 1.

8. RESULTADOS PREVISTOS

8.1 ESTIMACIÓN DE VALORES CUANTITATIVOS		
TASA DE GRADUACIÓN %	**TASA DE ABANDONO %**	**TASA DE EFICIENCIA %**
70	20	80
CODIGO	**TASA**	**VALOR %**
No existen datos		

Justificación de los Indicadores Propuestos:

Ver Apartado 8: Anexo 1.

8.2 PROCEDIMIENTO GENERAL PARA VALORAR EL PROCESO Y LOS RESULTADOS

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 09/10/2017). 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 documenta-

ción relevante relacionada con la docencia; h) La relación de docentes con un breve perfil de este: nombre, categoría, dedicación, distinciones y breve currículo; 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 (**https://estudos.udc.es/gl/study/start/4530V01**)

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.

9. SISTEMA DE GARANTÍA DE CALIDAD

ENLACE	https://teleco.uvigo.es/a-escola/calidade/manual-e-procedementos/

10. CALENDARIO DE IMPLANTACIÓN

10.1 CRONOGRAMA DE IMPLANTACIÓN	
CURSO DE INICIO	2023
Ver Apartado 10: Anexo 1.	
10.2 PROCEDIMIENTO DE ADAPTACIÓN	

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	4
Gestión de la seguridad de la información	6	Gestión de 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 *malware*	5	Análisis de *malware*	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	Ciberseguridad IoT e Industrial	5
Prácticas en empresa	15	Prácticas en empresa	9

10.3 ENSEÑANZAS QUE SE EXTINGUEN

CÓDIGO	**ESTUDIO - CENTRO**

11. PERSONAS ASOCIADAS A LA SOLICITUD

11.1 RESPONSABLE DEL TÍTULO

NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
35307306Y	Ana	Fernández	Vilas
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Escuela de Ingeniería de Telecomunicación	36310	Pontevedra	Vigo
EMAIL	**MÓVIL**	**FAX**	**CARGO**
avilas@det.uvigo.es	661047558	986812116	Coordinadora

11.2 REPRESENTANTE LEGAL

NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
36023985M	Manuel Joaquín	Reigosa	Roger
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Edificio Exeria - Campus Universitario de Vigo	36310	Pontevedra	Vigo
EMAIL	**MÓVIL**	**FAX**	**CARGO**
verifica@uvigo.es	626768751	986813590	Rector

11.3 SOLICITANTE

El responsable del título no es el solicitante

NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
76808276Y	Alfonso	Lago	Ferreiro
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Edificio Ernestina Otero - Campus Universitario de Vigo	36310	Pontevedra	Vigo
EMAIL	**MÓVIL**	**FAX**	**CARGO**

vicoap@uvigo.es	661047558	986813818	Vicerrector de Profesorado, Docencia y Titulaciones

Apartado 1: Anexo 1

Nombre : Convenio_Ciberseguridade-1.pdf

HASH SHA1 : 791D7EFE50EC3ACD7D1D3900C85745801460CEC8

Código CSV : 274375855483385434724854

Ver Fichero: Convenio_Ciberseguridade-1.pdf

Apartado 2: Anexo 1

Nombre : Justificación.pdf

HASH SHA1 : A16AEE9785A9DBB589C9B8973F8E98EFFD719243

Código CSV : 625292509366639672883759

Ver Fichero: Justificación.pdf

Apartado 4: Anexo 1

Nombre : 3.1.pdf

HASH SHA1 : 84C223C30EFEF1EE670E26E850A87F233A886391

Código CSV : 625301219801015228054724

Ver Fichero: 3.1.pdf

Apartado 5: Anexo 1

Nombre : Planificación_enseñanzas.pdf

HASH SHA1 : 75FBFA230A7D4D6325AC9A6D3EBE231067F7415A

Código CSV : 626017169616672734397188

Ver Fichero: Planificación_enseñanzas.pdf

Apartado 6: Anexo 1

Nombre : 5.pdf

HASH SHA1 : 08AA4A28F0E89E7951F73110EFE9AAF139D39436

Código CSV : 547267863026125412713383

Ver Fichero: 5.pdf

Apartado 6: Anexo 2

Nombre : 6.2.pdf

HASH SHA1 : 16E9D5D17157D1AAF69AE790488BBE88895AF81C

Código CSV : 625498436318217730300978

Ver Fichero: 6.2.pdf

Apartado 7: Anexo 1

Nombre : 6.pdf

HASH SHA1 : B24CD5C7AAF1833068777A13C0BB018DF9AD3471

Código CSV : 626024838317144806181373

Ver Fichero: 6.pdf

Apartado 8: Anexo 1

Nombre : 8.1.pdf

HASH SHA1 : 67E46ECDAE43BA4142FFF6CA0795A820FBB374E2

Código CSV : 560124975298789278651449

Ver Fichero: 8.1.pdf

Apartado 10: Anexo 1

Nombre : Calendario_imp.pdf

HASH SHA1 : 8035CA370B55DEFB64788A79FB0359A11096241A

Código CSV : 547288499976917649418287

Ver Fichero: Calendario_imp.pdf