Universidade de Vigo

UNIVERSIDADE DA CORUÑA

MASTER UNIVERSITARIO

EN CIBERSEGURIDAD

(Universidade de Vigo-Universidade da Coruña)

1. DESCRIPCIÓN Y OBJETIVOS FORMATIVOS

1.1. Descripción

Denominación del título:	Máster Universitario en Ciberseguridad por la Universidade de Vigo y la Universidade da Coruña
Ámbito de conocimiento:	Interdisciplinar/Ingeniería Informática/Ingeniería de Telecomunicación
Menciones y especialidades:	No hay
Universidad responsable:	Universidade de Vigo
Universidades participantes:	Universidade de Vigo Universidade da Coruña
Centros de impartición:	Escola de Enxeñaría de Telecomunicación (UVIGO) Facultade de Enxeñaría Informática (UDC)
Modalidad de enseñanza:	Presencial
Número total de créditos:	90
Idiomas de impartición:	Gallego/ Español /Inglés

1.2. Justificación del título

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

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

conocimientos para poder desempeñar las funciones que se requieren.

(ISC)² -la mayor asociación sin ánimo de lucro del mundo de profesionales de ciberseguridad- en su informe sobre el mercado laboral 2021, aunque revela una disminución de la escasez de mano de obra mundial por segundo año consecutivo, sigue registrando un déficit de 2,72 millones de profesionales de la ciberseguridad. Hay dos factores significativos que contribuyen a la estimación del déficit de mano de obra de este año. Para ver estas cifras en perspectiva, se debe recalcar que, a nivel mundial, la mano de obra en ciberseguridad necesita crecer un 65% para una defensa eficaz de la sociedad digital. Por tanto, **resulta evidente que la demanda sigue creciendo a una velocidad muy superior a la que las escuelas tecnológicas pueden formar a los profesionales TIC en el ámbito ciberseguridad**. Es, por tanto, una obligación de las instituciones académicas, de las universidades y, especialmente, de las escuelas y facultades TIC, poner en marcha programas formativos que ayuden a cubrir la demanda de profesionales cualificados que exista en el futuro y, al tiempo, generar oportunidades de empleabilidad y de desarrollo de talento que tengan una repercusión muy positiva en su entorno de influencia, especialmente ayudando a reforzar las capacidades del tejido empresarial y el sector público, en este caso, de la Comunidad Autónoma de Galicia, el Reino de España y la Unión Europea.

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

La propuesta MUniCS, impartido entre UVIGO y UDC implica a dos centros: Escuela de Ingeniería de Telecomunicación (en adelante EET) de UVIGO y Facultade de Informática (en adelante FIC) de UDC; y complementa las titulaciones TIC de ambas instituciones: Grado en Ingeniería de Tecnologías de Telecomunicación, en UVIGO; y los grados en Ingeniería Informática, Ciencia de datos e Inteligencia Artificial, en UDC. MUniCS se ha convertido en un referente regional y nacional en su ámbito, **se concibe como un título con una marcada vocación profesional, pensado con la misión de formar especialistas que la empresa gallega, nacional e internacional** pueda incorporar en cualquiera de sus procesos para suplir las carencias a las que actualmente se enfrentan en el campo de la seguridad digital y la protección de la información, y dirigido fundamentalmente a las personas que quieran adquirir formación especializada pero de carácter aplicado en estas disciplinas.

1.3. Objetivos formativos

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

- Formar expertos técnicos que puedan proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación.
- Formar expertos técnicos que puedan evaluar el nivel de riesgo de cualquier infraestructura y/o sistema y contribuir a su reducción frente a vulnerabilidades y amenazas en los activos de información, de comunicación y de sistemas. En concreto favorecer una transformación digital segura, la privacidad de la sociedad y los ciudadanos y la lucha contra la ciberdelincuencia y el cibercrimen.
- Concienciar a los profesionales formados del compromiso ético, deontología profesional y la perspectiva de género en el área de ciberseguridad.

- Proporcionar a los profesionales de los conocimientos teóricos y las habilidades y competencias que permitan aportar garantías de privacidad y seguridad en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos.
- Habilitar egresados para investigar, innovar y contribuir al avance de los principios, las técnicas y los procesos referidos a su ámbito profesional, diseñando nuevos algoritmos, dispositivos, técnicas o modelos útiles para la protección de los activos digitales públicos, privados o comerciales.
- Crear una comunidad de jóvenes que impulsen la industria de la ciberseguridad en Galicia, así como contribuyan a una sociedad digital segura a nivel europeo, español y gallego.

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

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

2. ADMISIÓN

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

Los criterios específicos de admisión al Máster serán, por orden de prevalencia, la titulación de acceso de los solicitantes, el expediente académico y otros méritos relacionados con el ámbito de la ciberseguridad. Tendrán preferencia en la admisión quienes posean un título de grado relacionado directamente con las tecnologías de la información y las comunicaciones seguidos por quienes posean un título de grado en disciplinas científicas básicas (Matemáticas, Física o estudios afines), y estos tendrán preferencia sobre cualquier otro título académico. La experiencia profesional previa en el ámbito de la ciberseguridad informática se tendrá en cuenta por la Comisión Académica del Máster como criterio adicional para decidir las admisiones, así como también, si lo considera necesario, la entrevista personal con las personas solicitantes para calibrar debidamente su aptitud y motivación. No se

establecen complementos formativos de ninguna clase para las personas que no se adecuen significativamente a los criterios de admisión anteriores.

Los criterios de admisión se basarán en los siguientes aspectos:

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

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

Los criterios de acceso se publican en la página Web de MUniCS (munics.es) y en los portales de preinscripción y matrícula de la Universidade de Vigo y la Universidade da Coruña.

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

3. PLANIFICACIÓN DE LAS ENSEÑANZAS

Estructura básica de las enseñanzas

Resumen de la distribución de créditos en la titulación	
Créditos Obligatorios	**63**
Créditos Optativos	**6**
Prácticas externas	**9**
Créditos trabajo fin de máster	**12**
Créditos de complementos formativos	**0**
Número Total de Créditos ECTS	**90**

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

Curso 1: Semestre 1

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

Curso 1: Semestre 2

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

Curso 2: Semestre 1

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

Plan de estudios detallado

Seguridad de la información (SI)

ECTS	5
Descripción de 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.

Análisis de Malware (MWR)

ECTS	5
Descripción de 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.

Privacidad y anonimidad (PAN)

ECTS	5
Descripción de 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.

Seguridad de Aplicaciones (SAPP)

Número de créditos ECTS	5
Breve descripción de los 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.

Redes Seguras (RED)

Número de créditos ECTS	5
Breve descripción de los 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, next-generation firewalls, importancia de NAT/PAT, políticas de seguridad de red - Dispositivos complementarios: sistemas de detección y prevención de intrusiones, servicios proxy - Monitorización segura: implicaciones de diseño, sincronización horaria, syslog, SNMP, netflow, NMS y SIEM.

Tecnologías de Registro Distribuido y Blockchain (BC)

ECTS	5
Descripción de 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.

Seguridad en Comunicaciones (SCOM)

ECTS	5
Descripción de contenidos	- Seguridad en capa física y de enlace. - Seguridad en capa de red. - Seguridad en capa de transporte. - Seguridad en capa de aplicación.

Fortificación Sistemas (FORT)

ECTS	5
Descripción de contenidos	- Fortificación del proceso de arranque - Fortificación cuentas de los usuarios - Fortificación sistemas de ficheros - Fortificación de aplicaciones - Fortificación de la red. - Mantenimiento -

Ciberseguridad Industrial e IoT (CSIoT)

ECTS	5
Idioma	Inglés / Español /Gallego
Descripción de 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.

Hacking ético y Test de intrusión (INT)

ECTS	5
Breve descripción de los 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

Negocio en Ciberseguridad y Emprendimiento (NEG)

ECTS	4
Descripción de 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.

Análisis Forense (AF)

ECTS	3
Descripción de contenidos	- Introducción a la Informática Forense - Proceso de adquisición de evidencias - Técnicas de Análisis Forense - Análisis de casos

Seguridad en centros de datos (CD)

ECTS	3
Descripción de 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.

Seguridad en dispositivos móviles (MOV)

ECTS	3
Descripción de 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)

Smart Contracts y Distributed Applications (CIAD)

ECTS	3
Descripción de 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.

Gestión de la Seguridad de la Información (GSI)

ECTS	5
Descripción de 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

Conceptos y Leyes (CL)

Número de créditos ECTS	4
Descripción de 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.

Prácticas en Empresas (PRA)

ECTS	9
Descripción de los 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 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.

Trabajo Fin de Máster (TFM)

ECTS	12
Descripción de contenidos	El Trabajo Fin de Máster es un trabajo académico, personal y original en el que el estudiante tiene que mostrar los conocimientos adquiridos durante el máster. Por lo tanto, el contenido de cada trabajo debe ser único, aunque deberá mostrar la capacidad del alumno para analizar un problema de una forma sistemática, proponer soluciones, analizar los resultados obtenidos y exponerlos de forma clara.