

ACUERDO NÚMERO 21/2026

POR EL QUE LA COMISIÓN ACADÉMICA DEL CONSEJO SOCIAL, POR DELEGACIÓN DEL PLENO, EMITE INFORME PRECEPTIVO FAVORABLE SOBRE LOS SIGUIENTES PLANES DE ESTUDIO: GRADO EN FISIOTERAPIA; GRADO EN INGENIERÍA FORESTAL: INDUSTRIAS FORESTALES; GRADO EN FINANZAS Y CONTABILIDAD; MÁSTER EN INGENIERÍA DE AUTOMOCIÓN; MÁSTER EN TECNOLOGÍAS DIGITALES E INTELIGENCIA ARTIFICIAL APLICADAS A LAS HUMANIDADES; MÁSTER EN SEGURIDAD DE LAS TELECOMUNICACIONES Y MÁSTER EN DERECHO DEL VINO, DE LA UNIVERSIDAD DE VALLADOLID

El artículo 24.3.b) de la Ley de Universidades de Castilla y León, texto consolidado tras la modificación realizada por la Ley 12/2010, de 28 de octubre, y de 6 de julio de 2017, señala en su última redacción como competencia del Consejo Social la de *"Informar la implantación y supresión de enseñanzas conducentes a la obtención de títulos universitarios de carácter oficial y validez en todo el territorio nacional"*.

El Vicerrector de Política Académica y Calidad Docente de la Universidad de Valladolid remitió al Consejo Social, con fecha 8 de julio de 2026 la solicitud de informe preceptivo relativo a los anteproyectos de los siguientes Planes de Estudio: Grado en Fisioterapia; Grado en Ingeniería Forestal: Industrias Forestales; Grado en Finanzas y Contabilidad; Máster en Ingeniería de Automoción; Máster en Tecnologías Digitales e Inteligencia Artificial aplicadas a las Humanidades; Máster en Seguridad de las Telecomunicaciones y Máster en Derecho del Vino.

La Comisión de Ordenación Académica y Profesorado (COAP), en su reunión del 21 de julio, informó favorablemente de los citados Planes de Estudio.

La Comisión Académica del Consejo Social, por delegación del Pleno, en sesión de fecha 22 de julio de 2026, tras examinar y analizar las propuestas y documentación, adoptó el siguiente **ACUERDO**:

"Informar favorablemente los siguientes Planes de Estudio: Grado en Fisioterapia; Grado en Ingeniería Forestal: Industrias Forestales; Grado en Finanzas y Contabilidad; Máster en Ingeniería de Automoción; Máster en Tecnologías Digitales e Inteligencia Artificial aplicadas a las Humanidades; Máster en Seguridad de las Telecomunicaciones y Máster en Derecho del Vino de la Universidad de Valladolid".

Se hace la salvedad de que el Acta de la sesión en el que se ha tomado el presente Acuerdo se encuentra pendiente de aprobación y, al amparo de la legislación vigente, expido el presente documento.

En Valladolid a la fecha de la firma electrónica.

El presidente de la Comisión Académica – D. Luis Díaz González
El secretario del Consejo Social – D. Enrique Berzal de la Rosa

Contra el presente acto de trámite, de conformidad con las previsiones contenidas en el artículo 112.1 de la LPAC, no cabrá recurso administrativo alguno, sin perjuicio de que su oposición al mismo pueda ser alegada por los interesados para su consideración en la resolución que ponga fin al procedimiento



**Universidad
de Valladolid**

**Vicerrectorado
de Política Académica
y Calidad Docente**

FECHA: 8 de julio de 2026
PARA: Sr. PRESIDENTE DEL CONSEJO SOCIAL
ASUNTO: Solicitud de informe relativo a nuevas propuestas de planes de estudio

Estimado Sr. presidente:

En virtud del artículo 24.3.b) de la Ley de Universidades de Castilla y León es competencia del Consejo Social de cada universidad “*informar la implantación y supresión de enseñanzas conducentes a la obtención de títulos universitarios de carácter oficial y validez en todo el territorio nacional*” razón por la que, le remito los siguientes anteproyectos de nuevo plan de estudio para su informe preceptivo.

Le informo que la Comisión de Ordenación Académica y Profesorado (COAP), de fecha 21 de abril de 2026, informó favorablemente su exposición pública a toda la comunidad universitaria.

Grado en Fisioterapia
Grado en Ingeniería Forestal: Industrias Forestales
Grado en Finanzas y Contabilidad
Máster en Ingeniería de Automoción
Máster en Tecnologías Digitales e Inteligencia Artificial aplicadas a las Humanidades
Máster en Seguridad de las Telecomunicaciones
Máster en Derecho del Vino

Atentamente,

Valladolid, a fecha de firma electrónica
EL VICERRECTOR DE POLÍTICA ACADÉMICA Y
CALIDAD DOCENTE,
Fdo.: José María Marbán Prieto

Normativa	Este documento tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de original (art. 27 Ley 39/2015).	Estado	Fecha y hora	
Firmado por	Jose Maria Marban Prieto - Vicerrector de Política Académica y Calidad Docente	Firmado	08/07/2026 11:04:39	
URL de verificación	https://sede.uva.es/validador-documentos?code=5YBuz5w9tUicn%2BiKAbRmA%3D%3D			



ASUNTO: Acuerdos Comisión de Ordenación Académica y Profesorado (COAP).
FECHA: A fecha de firma electrónica
PARA: secretario general de la UVa
COPIA: decana de la Facultad de Ciencias de la Salud (Campus de Soria)
director de la EIFAB
decana de la Facultad de CCEE y Empresariales
director de la EII
decano de la Facultad de Filosofía y Letras
director de la ETSIT
decano de la Facultad de Derecho (Campus de Valladolid)

La Comisión de Ordenación Académica y Profesorado (COAP), en su reunión de 21 de julio de 2026, informó favorablemente las siguientes propuestas de nuevos planes de estudios y su tramitación al próximo Consejo de Gobierno.

- Grado en Fisioterapia
- Grado en Ingeniería Forestal: Industrias Forestales
- Grado en Finanzas y Contabilidad
- Máster en Ingeniería de Automoción
- Máster en Tecnologías Digitales e Inteligencia Artificial aplicadas a las Humanidades
- Máster en Seguridad de las Telecomunicaciones
- Máster en Derecho del Vino

Valladolid, a fecha de firma electrónica
EL PRESIDENTE DE LA COMISIÓN DE ORDENACIÓN ACADÉMICA Y PROFESORADO
Fdo. José María Marbán Prieto
LA SECRETARIA DE LA COMISIÓN DE ORDENACIÓN ACADÉMICA y PROFESORADO
Fdo. M^a Ángeles Sastre Ruano

Normativa	Este documento tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de original (art. 27 Ley 39/2015).	Estado	Fecha y hora	
Firmado por	Jose Maria Marban Prieto - Vicerrector de Política Académica y Calidad Docente	Firmado	21/07/2026 13:30:03	
	Maria Angeles Sastre Ruano - Dir. Dpto. Lengua Española	Firmado	21/07/2026 13:11:51	
URL de verificación	https://sede.uva.es/validador-documentos?code=hwkTkSCC4H4ouxPQTGCooA%3D%3D			



EJECUCIÓN DE ACUERDOS JUNTA DE ESCUELA DE 15 DE ABRIL DE 2026

La Junta de Escuela de la ETSI de Telecomunicación, en sesión celebrada el 15 de abril de 2026, **informó favorablemente la propuesta de anteproyecto del Máster en Seguridad de las Telecomunicaciones** que se impartirá en la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universidad de Valladolid en los términos previstos en la presente convocatoria de modificación de planes de estudio.

Valladolid, a fecha de firma electrónica

El Secretario

Carlos Alonso Gómez

Universidad de Valladolid - Campus Miguel Delibes - Pº de Belén 15, 47011 Valladolid - ☎ 983 423662 - tel@uva.es - www.tel.uva.es

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-9b52-d7de-0d13-d51f-f8d9-ac68-4743-769e

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvympyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-9b52-d7de-0d13-d51f-f8d9-ac68-4743-769e

INFORME DE FIRMA, no sustituye al documento original | C.S.V. : GEISER-9b52-d7de-0d13-d51f-f8d9-ac68-4743-769e | Puede verificar la integridad de este documento en la siguiente dirección: <https://run.gob.es/hsbzvympyF>
CSV: MJTTP0eqmXHQFYjn08E/g== Puede verificar la integridad de este documento en: <https://sede.uva.es/validador-documentos> Página: 2/2

Normativa	Este documento tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de original (art. 27 Ley 39/2015).	Estado	Fecha y hora	
Firmado por	Carlos Alonso Gomez - Secretario/a de la Escuela Técnica Superior de Ingenieros de Telecomunicación	Firmado	16/04/2026 09:45:14	
URL de verificación	https://sede.uva.es/validador-documentos?code=MJTTP0eqmXHQFYjn08E%2Fg%3D%3D			

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-9b52-d7de-0d13-d51f-f8d9-ac68-4743-769e

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvympyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-9b52-d7de-0d13-d51f-f8d9-ac68-4743-769e

EJECUCIÓN DE ACUERDOS
JUNTA DE ESCUELA DE 15 DE ABRIL DE 2026

La Junta de Escuela de la ETSI de Telecomunicación, en sesión celebrada el 15 de abril de 2026, **informó favorablemente la propuesta de anteproyecto del Máster en Seguridad de las Telecomunicaciones** que se impartirá en la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universidad de Valladolid y el compromiso de no reverificación de este título en 5 años.

Valladolid, a fecha de firma electrónica

El Secretario

Carlos Alonso Gómez

Normativa	Este documento tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de original (art. 27 Ley 39/2015).	Estado	Fecha y hora	
Firmado por	Carlos Alonso Gomez - Secretario/a de la Escuela Técnica Superior de Ingenieros de Telecomunicación	Firmado	20/04/2026 12:10:04	
URL de verificación	https://sede.uva.es/validador-documentos?code=CSluxajVxnw2%2Fi86X08LZQ%3D%3D			



Para la elaboración de este anteproyecto, se ha incluido en cada epígrafe la información más relevante para cumplimentar cada uno de los criterios, pero se puede ampliar consultando el documento *Guía ACSUCYL - Guía de evaluación para la Verificación y Modificación sustancial de los planes de estudio. Aprobado por la Comisión de Evaluación de Titulaciones de la Agencia para la Calidad del Sistema Universitario de Castilla y León en su sesión de 14 de julio de 2025.*

Este documento se encuentra disponible en: *Mi portal UVA - inicio/ pdi / docencia e investigación / evaluación de títulos oficiales y se considera especialmente relevante para la cumplimentación de la Memoria VERIFICA una vez aprobado, por los órganos correspondientes, el anteproyecto*

1.1 DENOMINACIÓN

Grado ☐

Máster ☒

Curso Implantación Previsto:

Denominación

1.2 CRÉDITOS ECTS

Total ECTS

Distribución de créditos:

FB

OB

OP

PE

TFG / TFM

1.3 TIPO DE ENSEÑANZA

Presencial

Semipresencial/híbrida

Virtual (no presencial)

1.4 CAMPO DE ESTUDIO

Rama

Campo de estudio

1.5 EL TÍTULO INCLUYE MENCIONES O ESPECIALIDADES

Sí ☐ No ☒

DENOMINACIÓN	Nº ECTS

¿Es obligatorio cursar una mención/especialidad de las existentes para la obtención del título?

Sí ☐

No ☐



Mención Dual*:

No ☒

1.6 LA TITULACIÓN ES CONJUNTA

Sí ☐ No ☒

EN EL CASO DE TITULACIONES CONJUNTAS, INDIQUE LAS UNIVERSIDADES QUE PARTICIPAN

1.7 PROFESIONES REGULADAS PARA LAS QUE CAPACITA UNA VEZ OBTENIDO EL TÍTULO.

Sí ☐ No ☒

NOMBRE DE LA PROFESIÓN REGULADA Y LA ORDEN DE REFERENCIA

1.8 PLAZAS DE NUEVO INGRESO OFERTADAS EN LOS PRIMEROS AÑOS DE IMPLANTACIÓN

Plazas ofertadas:

Número total de plazas ofertadas en el centro
(título):

20

Número de plazas de nuevo ingreso para primer
curso:

20

Oferta de plazas en modalidad presencial:

20

Oferta de plazas en modalidad semipresencial o
híbrida:

0

Oferta de plazas en modalidad no presencial o
virtual:

0

1.9 CENTRO/S UNIVERSITARIOS EN LOS QUE SE IMPARTE EL TÍTULO EN LA UNIVERSIDAD O UNIVERSIDADES

CÓDIGO RUCT	CENTRO DE IMPARTICIÓN RESPONSABLE
47007069	ETSI Telecomunicación

CÓDIGO RUCT	CENTROS DE IMPARTICIÓN (INDICANDO LA UNIVERSIDAD SI NO ES UVA)



1.10 DEPARTAMENTO/CENTRO/INSTITUTO QUE FORMULA LA PROPUESTA

CENTROS/DEPARTAMENTOS/INSTITUTOS QUE FORMULAN Y AVALAN LA PROPUESTA
ETSI Telecomunicación

1.11 PROFESOR RESPONSABLE DE LA PROPUESTA

APELLIDOS, NOMBRE	Simmross Wattenberg, Federico
CATEGORÍA	Profesor Titular de Universidad
EMAIL	fedsim@tel.uva.es
TELÉFONO	5539

2 DESCRIPCIÓN DEL TÍTULO

2.1 OBJETIVOS FORMATIVOS

El objetivo fundamental del máster es **formar a personas que sean competentes en el ámbito de la seguridad de las Telecomunicaciones**. Este objetivo global se puede concretar en los siguientes puntos:

- Proporcionar a los estudiantes una base sólida sobre los fundamentos generales de la ciberseguridad, incluyendo:
 - Criptografía.
 - Aprendizaje automático.
 - Técnicas de ataque.
 - Respuesta a incidentes.
 - Administración y gestión de redes de comunicaciones.
- Impartir, dentro del ámbito general de la seguridad, una formación especializada dirigida y aplicada a las Telecomunicaciones, claramente diferenciada de los aspectos que generalmente se atribuyen a la seguridad puramente informática. Concretamente se abordarán las siguientes temáticas:
 - Seguridad cuántica.
 - Seguridad en redes inalámbricas.
 - Seguridad en la automoción.
 - Seguridad de la Internet de las cosas (IoT).
 - Protocolos de comunicación seguros.
- Facilitar a los egresados la incorporación laboral tanto en empresas del sector de las Telecomunicaciones en general (que por descontado han de dar una importancia de calado a la seguridad de sus redes) como a aquellas cuyo plan de negocio se encuentra de lleno en la seguridad, incluido el sector de la defensa.
- Desarrollar la capacidad de los estudiantes para adaptarse a situaciones siempre cambiantes y para afrontar adecuadamente retos que cambian día a día.



- Proporcionar a los estudiantes un nivel de competencia suficiente para asumir responsabilidades relacionadas con la seguridad de las Telecomunicaciones en ámbitos profesionales, así como para desarrollar actividades de investigación en dicho campo.
- Ofrecer a los estudiantes la experiencia de expertos en el ámbito de la seguridad mediante conferencias y charlas de ponentes de reconocido prestigio.

2.2 PERFIL DE INGRESO / REQUISITOS DE ACCESO

Este máster es adecuado para egresados de grados de Ingeniería de Telecomunicación y también para alumnos procedentes de grados de Ingeniería Informática. En general, se puede considerar que tienen un perfil adecuado los egresados de estudios universitarios de grado en alguna disciplina afín a las mencionadas, que tengan interés en la seguridad de las Telecomunicaciones.

En todos los casos, se da por sentado que los estudiantes poseen conocimientos de un nivel equiparable al de un grado en Ingeniería de Telecomunicación o de Ingeniería Informática sobre:

- Redes de comunicaciones.
- Sistemas de radiocomunicaciones.
- Programación e ingeniería del *software*.
- Sistemas UNIX.
- Servicios telemáticos.
- Sistemas electrónicos digitales.

Del mismo modo, se da por supuesto un nivel correspondiente al de cualquier grado de Ingeniería en las materias de Física y Matemáticas.

Por último, dado que parte de la formación del máster provendrá de conferencias y charlas de expertos de prestigio internacional, se recomienda un nivel de inglés mínimo equivalente al B2 según el Marco Europeo Común de Referencia de Lenguas.

2.3 PERFIL DE EGRESADOS.

Los egresados del máster tendrán dos perfiles superpuestos: uno de corte generalista en cuanto a ciberseguridad se refiere, y otro más específico, dirigido especialmente a las Telecomunicaciones:

- Perfil 1 (generalista). Personas competentes en la realización de tareas que se asocian generalmente con la ciberseguridad: programación segura, detección de ataques, respuesta a incidentes, trabajo con algoritmos criptográficos, uso de técnicas de aprendizaje automático, administración segura de redes de comunicaciones, etc.
- Perfil 2 (específico). Personas competentes en la implantación y mantenimiento de telecomunicaciones seguras, incluyendo comunicaciones cuánticas, comunicaciones inalámbricas en entornos no fiables, comunicaciones entre pequeños dispositivos electrónicos y entre vehículos en marcha y uso de protocolos avanzados para comunicaciones seguras.

2.4 POTENCIAL MERCADO /ANÁLISIS DE LA COMPETENCIA /EMPLEABILIDAD

Huelga decir, en términos generales, que las Telecomunicaciones están presentes en la vida diaria de millones de personas y que la importancia de su seguridad es palmaria, sobre todo en los últimos años, con una tendencia al alza a juzgar por la frecuente presencia de noticias sobre robos de credenciales, estafas,



ataques a infraestructuras críticas, etc, en medios de comunicación generalistas. Redundando en ello, cabe decir también que la seguridad de las Telecomunicaciones no es de aplicación exclusivamente civil, sino que tiene una importancia igualmente patente en el ámbito de la defensa, de nuevo con una tendencia al alza en los últimos años. Para sustentar estas afirmaciones podemos acudir a datos concretos:

- En primer lugar, el informe de AMETIC “Barómetro de la Economía Digital 2025”¹ señala que el sector tecnológico digital tiene un impacto en el 26% del PIB de España, con un aumento interanual del 7,4%, y un peso del 19,8% en el total de la innovación del sector privado en porcentaje de empresas (de un total de 36.737 empresas). Medido en número de empleados, el sector cuenta con más de 722.000, con un aumento interanual del 7,8%. En términos de volumen de negocio, el sector es responsable de un total de 95.000 millones de euros, con un aumento del 13,1% interanual.
- En segundo lugar, el Observatorio Nacional de Tecnología y Sociedad (Ontsi), en su estudio sobre la empleabilidad del sector de las TIC de 2021² (el más reciente disponible) señala que la Comisión Europea estimó en 168.000 el número de expertos necesarios en ciberseguridad en el año 2020 y que el Gobierno se fijó como meta incrementar en 20.000 el número de expertos en ciberseguridad, inteligencia artificial y datos hasta 2025.
- En tercer lugar, atendiendo al Catálogo de Formación en Ciberseguridad en España de Másteres, Grados y otras especializaciones del INCIBE³, en su edición de 2025, recoge un total de 138 titulaciones universitarias relacionadas con la ciberseguridad, de las cuales 31 son másteres oficiales (17 en las universidades públicas, 10 de ellos presenciales). Sin embargo, y a pesar de la palpable demanda, ninguno de ellos se imparte en la Universidad de Valladolid.
- En cuarto lugar, la gran mayoría de dichos másteres se concentran en la ciberseguridad entendida como seguridad de los sistemas informáticos, relegando así al problema de la seguridad en las Telecomunicaciones a un segundo plano. Para sostener esta afirmación, nos basamos en un estudio realizado por la propia ETSI Telecomunicación en 2025 (véase el estudio completo en la sección de anexos de este documento). Dicho estudio encontró que tan solo un 5,50% de los créditos ofertados en los másteres oficiales presenciales de las universidades públicas españolas están dedicados a la seguridad de las Telecomunicaciones (SEGCOM, en el citado estudio).
- En quinto lugar, el Ministerio para la Transformación Digital y de la Función Pública trabaja actualmente en un real decreto sobre seguridad y resiliencia de las redes de telecomunicaciones⁴, lo cual pone de manifiesto que existe un gran interés institucional por la seguridad de las Telecomunicaciones.
- En sexto y último lugar, el INCIBE informa de que el gestionó un total de 122.223 incidentes de seguridad en 2025 y que, de entre los dispositivos que los ciberdelincuentes consiguieron controlar, un 85% están relacionados con dispositivos IoT⁵ (televisores, decodificadores, reproductores multimedia, etc), consustanciales al ámbito de las Telecomunicaciones.

En conclusión, podemos afirmar que nuestra propuesta de *Máster en seguridad de las Telecomunicaciones* tiene un mercado potencial fuerte, que existe una marcada competencia pero a la vez nuestra propuesta ofrece una especialización destacada, y que las titulaciones afines ya implantadas parecen gozar de una muy alta tasa de empleabilidad si nos atenemos a los análisis referenciados.

¹<https://ametic.es/publicacion/barometro-de-la-economia-digital-2025/>

²https://www.ontsi.es/sites/ontsi/files/2021-12/informeempleotecnologiconov2021_0.pdf

³https://www.incibe.es/sites/default/files/paginas/incibe/formacion/Cat%C3%A1logo%20de%20Formaci%C3%B3n%20Grados%20y%20M%C3%A1sters_2025.pdf

⁴<https://digital.gob.es/comunicacion/notas-prensa/secretaria-estado-telecomunicaciones-e-infraestructuras-digitales/2025/12/2025-12-02>

⁵<https://www.incibe.es/incibe/sala-de-prensa/incibe-detecto-mas-de-122000-incidentes-de-ciberseguridad-en-2025>



3 JUSTIFICACIÓN:

3.1 OPORTUNIDAD Y NECESIDAD

La ETSI Telecomunicación, en su Grado en Ingeniería de Telecomunicación, cuenta con algunas asignaturas en las que se tratan temas relacionados con la seguridad, siendo los ejemplos más notables *Seguridad en Redes de Comunicaciones* y *Administración y Gestión de Redes de Comunicaciones* (obligatorias de mención, 4º curso de la mención en Telemática, 6 ECTS). Del mismo modo, el Máster en Ingeniería de Telecomunicación cuenta con la asignatura *Ciberseguridad* (optativa, primer curso, 3 ECTS). Por otra parte, la Escuela de Ingeniería Informática, en su Grado en Ingeniería Informática, ofrece una mención en Tecnologías de la Información que incluye asignaturas del ámbito de la ciberseguridad, como son *Administración de Sistemas Operativos*, *Garantía y Seguridad de la Información*, *Diseño*, *Administración y Seguridad de Redes e Informática Forense*, todas ellas de carácter obligatorio para la mención y de 6 ECTS. Con la excepción de *Seguridad en Redes de Comunicaciones*, que pone el énfasis en los protocolos de comunicación, todas las asignaturas citadas adoptan un enfoque dirigido a la seguridad de los sistemas informáticos y, en cualquier caso, no existe ninguna titulación de máster relacionada con la ciberseguridad (ni, por tanto, con la seguridad de las Telecomunicaciones) en toda la Universidad de Valladolid.

Ampliando la extensión geográfica a toda Castilla y León, solamente la Universidad de León y la Universidad Internacional Isabel I de Castilla ofrecen másteres oficiales de seguridad. En cuanto a esta última, la única asignatura que se centra en la seguridad de las Telecomunicaciones es *Ciberseguridad Móvil* (obligatoria, 6 ECTS). En cuanto a la Universidad de León, se ofrecen dos másteres relacionados con la ciberseguridad: el primero de ellos, el Máster Universitario en Derecho de la Ciberseguridad y Entorno Digital, está pensado para graduados en Derecho y (consecuentemente) no aborda temas técnicos. El segundo, el Máster Universitario en Investigación en Ciberseguridad, es un máster de ciberseguridad puramente técnico, pero no aborda la temática de las Telecomunicaciones al no ofrecer ninguna asignatura de temática SEGCOM, atendiendo al ya citado estudio realizado por la ETSI Telecomunicación (véase la sección de anexos). No existe, por lo tanto, en toda Castilla y León, ninguna titulación que ofrezca a los egresados un perfil como el que se pretende dar en el máster que aquí se propone. Esta circunstancia abre una ventana de interés en lo que a planificación estratégica se refiere, ya que, como ya se expuso en la sección 2.4 y de acuerdo al mencionado estudio de la ETSI Telecomunicación, solamente un 5,50% de los créditos de todos los másteres oficiales presenciales de las universidades públicas españolas (no ya de Castilla y León) está dedicado a un tema hoy en día crucial como es la seguridad de las Telecomunicaciones.

Volviendo al ámbito de la Universidad de Valladolid, y en concreto a la ETSI Telecomunicación, está previsto el encaje del máster propuesto con el ya existente Máster de Ingeniería de Telecomunicación (MIT), de 90 ECTS. Así, los alumnos del MIT podrán consignar sus 18 créditos optativos cursando asignaturas del Máster en Seguridad de las Telecomunicaciones, de forma que los estudiantes podrán obtener dos titulaciones de máster (150 ECTS en total) en cuatro cuatrimestres, según se detalla en la sección 4.2.

En cuanto a los beneficios económicos y sociales que pueda traer el Máster en Seguridad de las Telecomunicaciones al conjunto de Castilla y León, cabe mencionar que varias empresas, entidades y expertos de reconocido prestigio de ámbito nacional e internacional han manifestado su apoyo explícito a nuestra propuesta, así como egresados de titulaciones afines (véase la sección de anexos). Además, el sector TIC en Castilla y León está bien establecido y numerosas empresas conforman el tejido empresarial local. En particular, las tres grandes operadoras están ubicadas en Valladolid (Telefónica, Vodafone y Orange-MásMóvil) y disponemos de implantación también de otros agentes relevantes del sector (NTT Data, Cellnex Telecom, GMV y Satec_). Por otra parte, el sector de la automoción se encuentra en plena expansión hacia el vehículo conectado (con Renault liderando el sector en esta comunidad autónoma) y otras grandes empresas, como Michelin, se encuentran en pleno proceso de digitalización. Existen unas extraordinarias relaciones entre las empresas mencionadas y la ETSI Telecomunicación, y contamos con ciclos de talleres impartidos por estas empresas, así como convenios para desarrollos específicos en materia docente e investigadora.



Conviene destacar, asimismo, que la seguridad de las Telecomunicaciones tiene inherente y necesariamente un ámbito de aplicación global, de forma que exactamente los mismos procedimientos que puedan aplicarse en Castilla y León son directamente aplicables en cualquier otra parte de la Unión Europea y del resto del mundo. Sumando esto a la visible escasez de titulaciones de seguridad centradas en las Telecomunicaciones, el resultado es una titulación con (*a priori*) un gran potencial para atraer alumnos procedentes del ámbito nacional e internacional.

Por último, cabe añadir que la implantación del máster propuesto puede abrir nuevas líneas de investigación relacionadas con la seguridad, las cuales son, a día de hoy, escasas en la Universidad de Valladolid. En efecto, en la relación de grupos del área de Ingeniería y Tecnología del portal de investigación UVA⁶ no figura ningún grupo cuya investigación se centre en la ciberseguridad, si bien se tiene constancia de dos grupos de investigación de la ETSI Informática (*Tecnologías de Gestión de Información e Inteligencia de Mercado y Marketing*) que en el pasado han tocado diversos temas en relación a dicho campo. No obstante, no tenemos constancia alguna de ningún grupo de investigación perteneciente a la Universidad de Valladolid que haya contribuido al área de la seguridad de las Telecomunicaciones.

3.2 REFERENTES

Tal como se expuso en la sección 2.4, existen de acuerdo al catálogo del INCIBE 31 másteres oficiales sobre seguridad en España, de los cuales 17 se imparten en universidades públicas. 10 de estos son presenciales, como el que aquí se propone.

A la hora de elaborar el proyecto de plan de estudios que se detalla en la sección 4.2, se ha tenido muy en cuenta la estructura, contenidos y reparto de carga de todos ellos (véase el estudio realizado por la ETSI Telecomunicación en la sección de anexos), tratando de diferenciar, por una parte, las materias que necesariamente han de formar parte integral de un máster sobre seguridad, y, por otra parte, las materias que han de proporcionar el carácter diferenciador de nuestra propuesta. Másteres de ciberseguridad como los que ofrecen la Universidad Carlos III de Madrid o la Universidades de Vigo y La Coruña (entre varios otros analizados en el mencionado estudio) han formado la base de nuestra propuesta. El otro pilar del máster que proponemos es la experiencia y los diversos campos de especialidad del profesorado de la ETSI Telecomunicación, algo que valoramos como estratégico de cara a proponer un máster que se ocupe específicamente de la seguridad de las Telecomunicaciones. Así, en la ETSI Telecomunicación podemos contar con una pericia amplia y demostrada en sectores como las comunicaciones cuánticas, las radiocomunicaciones, la criptografía, la automoción y la electrónica, además de en otras áreas más transversales como la el aprendizaje automático, la administración de redes o la programación.

3.3 VIABILIDAD

No existe en la Universidad de Valladolid una titulación análoga al máster que proponemos. Sin embargo, la ETSI Telecomunicación ofrece el Grado en Ingeniería de Telecomunicación, que es la vía de acceso natural para el máster propuesto, además del Máster en Ingeniería de Telecomunicación, que puede imbricarse con la presente propuesta de forma que los alumnos obtengan dos titulaciones de 90+60 ECTS en dos cursos académicos (véase la sección 4.2).

La ETSI Telecomunicación comenzó a impartir titulaciones de la familia de las Telecomunicaciones a partir de 1992. Desde entonces, y partiendo de la titulación original *Ingeniero de Telecomunicación*, la ETSIT ha impartido numerosas titulaciones de grado medio y superior (de acuerdo a la antigua LRU), así como titulaciones de grado y máster (a partir de la implantación del Plan Bolonia). La ETSI Telecomunicación cuenta, pues, con una experiencia de más de 30 años en la impartición de titulaciones relacionadas con la materia.

⁶ <https://investigacion.uva.es/CawDOS/jsf/principal/principal.jsf>



Asimismo, la ETSI Telecomunicación cuenta actualmente con la acreditación institucional del Consejo de Universidades, distintivo que poseen muy pocas escuelas de Ingeniería de Telecomunicación, en vigor desde 2019 y actualmente en proceso de renovación. Este sello de calidad supone la renovación de la acreditación de todos los títulos oficiales de la ETSIT, tal y como recoge el RUCT (Registro de Universidades, Centros y Títulos). La acreditación institucional otorga a los centros que la poseen un reconocimiento de la eficiencia en la gestión de la calidad de la formación universitaria que imparten. En la ETSI Telecomunicación, dicha gestión se materializa en un Sistema de Garantía Interna de Calidad que desde 2019 cuenta con el certificado ELENCHOS, concedido por la Agencia para la Calidad del Sistema Universitario de Castilla y León (ACSUCYL), también en vigor y actualmente en proceso de renovación.

El máster que se propone es complementario para con los títulos que ya ofrece la ETSI Telecomunicación en cuanto a que estos no poseen un enfoque centrado en la *seguridad* de las Telecomunicaciones (de acuerdo, en este sentido, a sus correspondientes órdenes CIN). Sin embargo, y como se ha puesto de manifiesto en secciones anteriores, la seguridad es un área de vital importancia para las Telecomunicaciones en el mundo actual, tal como corroboran diversos organismos públicos y privados citados anteriormente.

Dado que el título que proponemos es nuevo, no es posible estimar el número de matriculados que éste tendrá a partir de la experiencia de cursos anteriores, pero sí que podemos acudir a indicios que apuntan a una demanda sólida de titulaciones relacionadas con la seguridad entre el alumnado (y, en particular, con la seguridad de las Telecomunicaciones). Además de los ya expuestos en la sección 2.4, podemos contar los siguientes:

- La Comisión Europea, en su Brújula Digital 2030⁷, menciona como objetivo lograr que haya 20 millones de especialistas en tecnologías de la información y las comunicaciones empleados, con convergencia entre mujeres y hombres, y cita como referencia que en 2019 existían 7,8 millones.
- Del mismo modo, un segundo objetivo de la Brújula Digital 2030 es conseguir que Europa disponga de su primer ordenador cuántico. En este sentido, el plan de estudios del máster que proponemos contiene dos asignaturas sobre seguridad cuántica.
- El informe «Estado de las Comunicaciones Digitales» de Connect Europe (antes ETNO – *European Telecommunications Network Operators' Association*), de 2026⁸, cita varios operadores de telecomunicación europeos que están invirtiendo activamente en comunicaciones cuánticas y postcuánticas.
- La misma organización, en su informe «Contribución del sector de las telecomunicaciones a la seguridad y resiliencia de Europa»⁹, de 2025, cifra en 300.000 personas el déficit de expertos en seguridad de las Telecomunicaciones.
- OBSERVACIBER (el observatorio de ciberseguridad formado por el INCIBE y el Ontsi), en su informe *Análisis y Diagnóstico del Talento de Ciberseguridad en España* de 2022¹⁰, resalta varios datos de interés:
 - Los profesionales españoles de la ciberseguridad son valorados internacionalmente.
 - La Estrategia Nacional de Ciberseguridad 2019 enfatiza la necesidad de apoyar el impulso de la industria cibernética, con mención expresa a la investigación, la innovación y las instituciones educativas.
 - La oferta de profesionales formados en ciberseguridad asciende a 39.072 personas (en 2022), con una proyección a futuro de 42.283 en 2024, mientras que la demanda es de 63.191 personas (en 2022), con una proyección a futuro de 83.007 personas en 2024.

⁷ <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021DC0118>

⁸ <https://connecteurope.org/sites/default/files/2026-02/connectEU-Rapport-web-2026-onepage-v2.pdf>

⁹ [https://connecteurope.org/sites/default/files/2025-](https://connecteurope.org/sites/default/files/2025-10/Resilience%20and%20security%20study_CopenhagenEconomics%20for%20Connect%20Europe_Oct2025.pdf)

[10/Resilience%20and%20security%20study_CopenhagenEconomics%20for%20Connect%20Europe_Oct2025.pdf](https://connecteurope.org/sites/default/files/2025-10/Resilience%20and%20security%20study_CopenhagenEconomics%20for%20Connect%20Europe_Oct2025.pdf)

¹⁰ https://files.incibe.es/incibe/talento/INCIBE_InformeCompleto_DIAG.pdf



- Uno de los problemas principales detectados es la escasez de profesorado cualificado para impartir formación en ciberseguridad.
- La mayoría de los programas de grado y posgrado adolecen de parte práctica (incluyendo prácticas en empresa).

3.4 MOTIVOS QUE ORIGINAN UN NUEVO TÍTULO

No procede, al no extinguir el título propuesto a ningún otro ya implantado.

4 PLAN DE ESTUDIOS

4.1 RESULTADOS DEL PROCESO DE FORMACIÓN Y APRENDIZAJE

CONOCIMIENTOS

- **C1:** estándares y buenas prácticas en ciberseguridad e importancia de no usar seguridad por oscuridad o soluciones propias.
- **C2:** normativa y regulación de la ciberseguridad en el ámbito de las Telecomunicaciones. Estrategia de Seguridad Nacional.
- **C3:** Tendencias actuales en el panorama global del ámbito de la seguridad de las Telecomunicaciones.
- **C4:** sistemas de cifrado simétrico y asimétricos, funciones hash y firma digital y su uso práctico.
- **C5:** herramientas utilizadas en tareas tanto de ciberseguridad en general como de aplicación específica al ámbito de la seguridad de las Telecomunicaciones.
- **C6:** diseño e implantación de sistemas seguros de Telecomunicación.
- **C7:** técnicas y modelos de aprendizaje automático.
- **C8:** fases de las pruebas de penetración: reconocimiento, explotación, ocultación y persistencia.
- **C9:** identificación y explotación de vulnerabilidades, vectores habituales de ataque.
- **C10:** patrones de diseño seguros y entradas no confiables.
- **C11:** obtención y análisis de indicios de ciberdelitos.
- **C12:** ataques dirigidos al hardware y al software.
- **C13:** seguridad en radiocomunicaciones: fijas, móviles, satélites y sistemas de posición, navegación y tiempo.
- **C14:** arquitectura electrónica del vehículo y del hardware IoT.
- **C15:** mecanismos de seguridad disponibles en los protocolos de la arquitectura de comunicaciones TCP/IP, incluyendo el protocolo IPv6.
- **C16:** compromisos de ingeniería en la selección y configuración de los diferentes mecanismos de seguridad disponibles en las Telecomunicaciones.
- **C17:** configuración y mantenimiento de cortafuegos.
- **C18:** seguridad de los sistemas virtualizados. Contenedores de aplicaciones.
- **C19:** conceptos clave de la mecánica cuántica aplicados a la información cuántica, distribución cuántica de claves y blindaje poscuántico.



HABILIDADES

- **H1:** planificar e implantar redes de Telecomunicaciones seguras.
- **H2:** diseñar, aplicar e integrar sistemas seguros de Telecomunicación tanto en entornos nuevos como ya existentes y multidisciplinares.
- **H3:** identificar correctamente indicios y pruebas de la comisión de un delito digital y distinguirlas de sucesos normales o fortuitos.
- **H4:** elaborar informes que puedan ser utilizados como prueba en un proceso legal o interno y como guía para mejorar la seguridad del entorno de trabajo.
- **H5:** analizar, describir y comprender, desde la perspectiva de la seguridad, el *hardware* y el *software* de los sistemas de Telecomunicación, incluyendo sistemas de radiocomunicaciones, sistemas cuánticos, sistemas telemáticos y sistemas electrónicos.
- **H6:** comprender y prevenir vulnerabilidades del *hardware* y del *software*.
- **H7:** aplicar estrategias de diseño y fabricación que dificulten el acceso físico en los sistemas IoT y mejoren su seguridad.
- **H8:** desarrollar, entrenar y desplegar modelos de aprendizaje automático para detectar intrusiones, anomalías y amenazas en infraestructuras de Telecomunicaciones.
- **H9:** manejar herramientas estándar de seguridad de los ámbitos del *hardware* y *software*, así como herramientas del ámbito de las radiocomunicaciones y la seguridad cuántica.
- **H10:** implantar mecanismos de seguridad sobre arquitecturas de comunicaciones TCP/IP, así como sobre arquitecturas de comunicaciones vehiculares y arquitecturas de interconexión de sistemas electrónicos.
- **H11:** aplicar principios de información cuántica a la seguridad de las Telecomunicaciones.
- **H12:** encontrar y analizar información y documentación técnica y de realizar tareas de aprendizaje autónomo.
- **H13:** proponer soluciones técnicas alineadas con normativa y la Estrategia de Seguridad Nacional.
- **H14:** resolver problemas con iniciativa, creatividad y razonamiento crítico.

COMPETENCIAS

A) Transversales

- **K1:** capacidad para analizar y valorar el impacto social y medioambiental de las soluciones técnicas, así como el desarrollo sostenible del ámbito correspondiente.
- **K2:** capacidad y compromiso ético en la elaboración de soluciones de ingeniería y en las diversas situaciones de gestión de recursos humanos y de gestión económica, así como capacidad para comprender el impacto de las soluciones de Ingeniería en un contexto social global.
- **K3:** capacidad de organización, planificación y gestión del tiempo.
- **K4:** capacidad para comunicar y argumentar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la seguridad de las Telecomunicaciones.
- **K5:** capacidad para trabajar en cualquier contexto, individual o en grupo, de aprendizaje o profesional, local o internacional, desde el respeto a los derechos fundamentales, de igualdad de sexo, raza y religión y los principios de accesibilidad universal, así como la cultura de paz.
- **K6:** capacidad para resolver problemas abiertos con iniciativa, creatividad y razonamiento crítico.
- **K7:** capacidad para diseñar y llevar a cabo experimentos, así como analizar e interpretar datos.

- **K8:** capacidad para integrar la experiencia ajena en el haber propio y aplicar el conocimiento adquirido a la resolución de problemas en entornos nuevos.
- **K9:** capacidad para llevar a cabo un diseño y evaluación de un sistema de Telecomunicación desde un punto de vista de la seguridad.
- **K10:** capacidad para aplicar criterios técnicos para seleccionar soluciones comerciales y abiertas, considerando limitaciones físicas, tecnológicas y estratégicas, así como el estado actual de la industria y los estándares emergentes.

B) Específicas

- **K11:** capacidad para manejar herramientas estándar de ciberseguridad, incluyendo herramientas de análisis de sistemas de ficheros, memoria y redes de datos y de depuración de *hardware* y *software*, así como herramientas del ámbito de las radiocomunicaciones y la seguridad cuántica.
- **K12:** capacidad para evaluar la seguridad de un sistema de Telecomunicación frente a distintos modelos de ataque.
- **K13:** capacidad para implementar sistemas de ciberseguridad basados en aprendizaje automático.
- **K14:** capacidad para diseñar, implantar, operar, administrar y mantener de forma segura redes y servicios de Telecomunicación.
- **K15:** capacidad para resolver los problemas de convergencia e interoperabilidad en el diseño del software y el hardware de redes de Telecomunicación seguras.
- **K16:** capacidad para desarrollar una visión global del problema de la seguridad de las Telecomunicaciones.
- **K17:** capacidad para reconocer los errores de código más comunes que dan lugar a vulnerabilidades habituales durante la implementación y el despliegue del software y el *hardware*.
- **K18:** ser capaz de elaborar informes rigurosos tanto desde un punto de vista técnico como legal.
- **K19:** capacidad para comprender la arquitectura electrónica y de comunicaciones de un sistema seguro de Telecomunicación.
- **K20:** ser capaz de identificar vulnerabilidades en sistemas de Telecomunicación, detectar ataques contra ellos y tomar medidas para mitigarlos y documentarlos.
- **K21:** ser capaz de aplicar la normativa del sector de la ciberseguridad y de la seguridad de las Telecomunicaciones.
- **K22:** ser competente en el dominio de la inteligencia de señal y la seguridad en el espectro radioeléctrico.

4.2 ESTRUCTURA GENERAL Y DISTRIBUCIÓN DEL PLAN DE ESTUDIOS

El Máster en Seguridad de las Telecomunicaciones que aquí se propone consta de un único curso académico (60 ECTS, 2 cuatrimestres). En líneas generales, el plan de estudios se estructura de la siguiente manera:

- Primer cuatrimestre (30 ECTS):
 - 9 asignaturas de 3 ECTS.
 - Un laboratorio de seguridad de 3 ECTS.
- Segundo cuatrimestre (30 ECTS):
 - 5 asignaturas de 3 ECTS.



- 1 asignatura de seminarios impartidos por expertos de reconocido prestigio (3 ECTS).
- Prácticas en empresa (6 ECTS).
- Trabajo de Fin de Máster (6 ECTS).
- Todas las asignaturas, incluidas las prácticas en empresa, tienen carácter obligatorio.

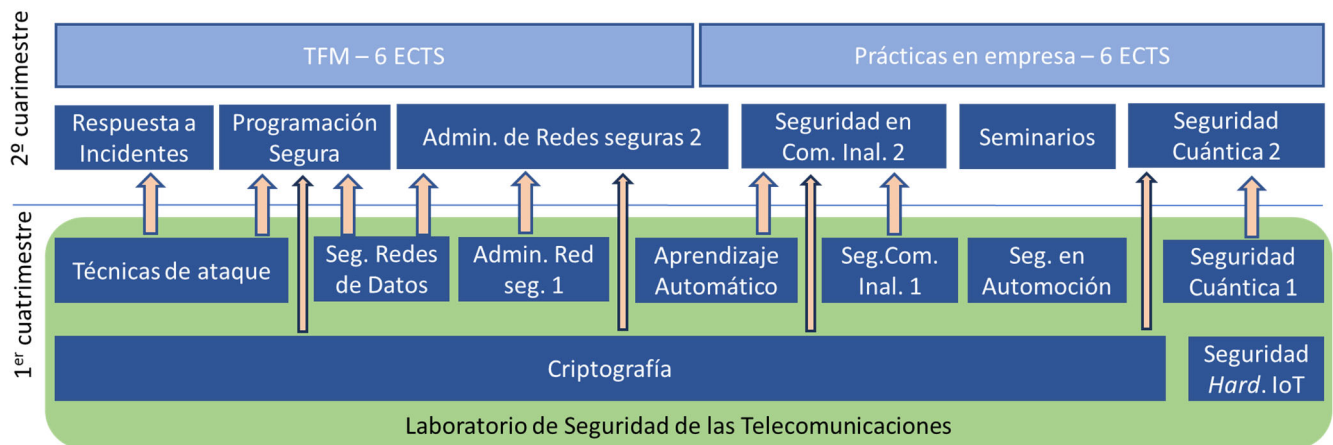
Esta estructura se puede observar de forma gráfica en la Figura 1, junto con las dependencias entre ellas (entendidas éstas únicamente como una recomendación del orden en que deberían cursarse). El tipo, temporización y asignación de asignaturas a sus respectivas materias se especifica en la Tabla 1.

El plan de estudios consta de un primer cuatrimestre formado por nueve asignaturas que se consideran base fundamental de la seguridad en las redes de Telecomunicaciones, y están complementadas con una décima asignatura denominada Laboratorio de seguridad. Esta asignatura pretende aunar los conocimientos y competencias adquiridas en todas las demás en un caso práctico de una red vulnerable, cuya seguridad los estudiantes deberán afianzar de acuerdo al escenario propuesto en cada año.

El segundo cuatrimestre consta de cinco asignaturas que se apoyan en la experiencia adquirida por los estudiantes durante el primer cuatrimestre, además de una sexta asignatura formada íntegramente por charlas de expertos de reconocido prestigio. Esta última estará coordinada por un profesor de la UVa, que será el encargado de evaluar a los alumnos.

A su vez, el máster que se propone deberá coexistir con el Máster en Ingeniería de Telecomunicación (MIT), que ya está implantado y en funcionamiento en la ETSI Telecomunicación desde septiembre de 2023. En este sentido, y con el fin de que el efecto en las cifras de matrícula de ambos másteres sea aditivo en lugar de sustractivo, el Máster en Seguridad de las Telecomunicaciones (MST) ha sido diseñado teniendo en cuenta la posibilidad de que el alumnado tenga la opción de conseguir una doble titulación de 90+60 ECTS en dos cursos académicos (sujeta esta posibilidad a la pertinente modificación del plan de estudios del MIT y a que se apruebe el mencionado doble título). Así, los estudiantes podrán cursar asignaturas obligatorias del MST como optativas del MIT, cubriendo así los 18 ECTS optativos de éste a la vez que 18 ECTS obligatorios de aquél.

Más concretamente, los alumnos interesados en la doble titulación cursarían un primer año (dos cuatrimestres) dedicado en exclusiva al MIT; posteriormente un tercer cuatrimestre dedicado al MST y a comenzar con el TFM del MIT, y por último un cuarto cuatrimestre destinado a finalizar las últimas asignaturas del MST junto con las prácticas en empresa y los correspondientes TFM de cada titulación. Adicionalmente, el alumnado se verá beneficiado por la proximidad temática de las asignaturas *Aprendizaje automático en las TIC* y *Ciberseguridad* del MIT con *Aprendizaje automático* y *Administración de redes seguras 1* del MST, de forma que sea posible cursar sólo una de cada par respectivo, aligerando así la carga lectiva del estudiante. Y, del mismo modo, se prevé que pueda apreciarse equivalencia entre las prácticas en empresa de ambos másteres, de forma que los estudiantes necesiten realizarlas solamente una vez. En relación a esto último, es esperable (e incluso deseable) que la temática de ambos TFM se integre con la orientación de las prácticas en empresa que realice cada alumno. Se puede observar de forma esquemática el plan de estudios que se prevé para la doble titulación en la Figura 2 y la Figura 3.



■ Asignaturas: 3 ECTS

■ Laboratorio de seguridad de las Telecomunicaciones: 3 ECTS

Figura 1: esquema gráfico de distribución de asignaturas por cuatrimestres, junto con sus dependencias, del Máster en Seguridad de las Telecomunicaciones.

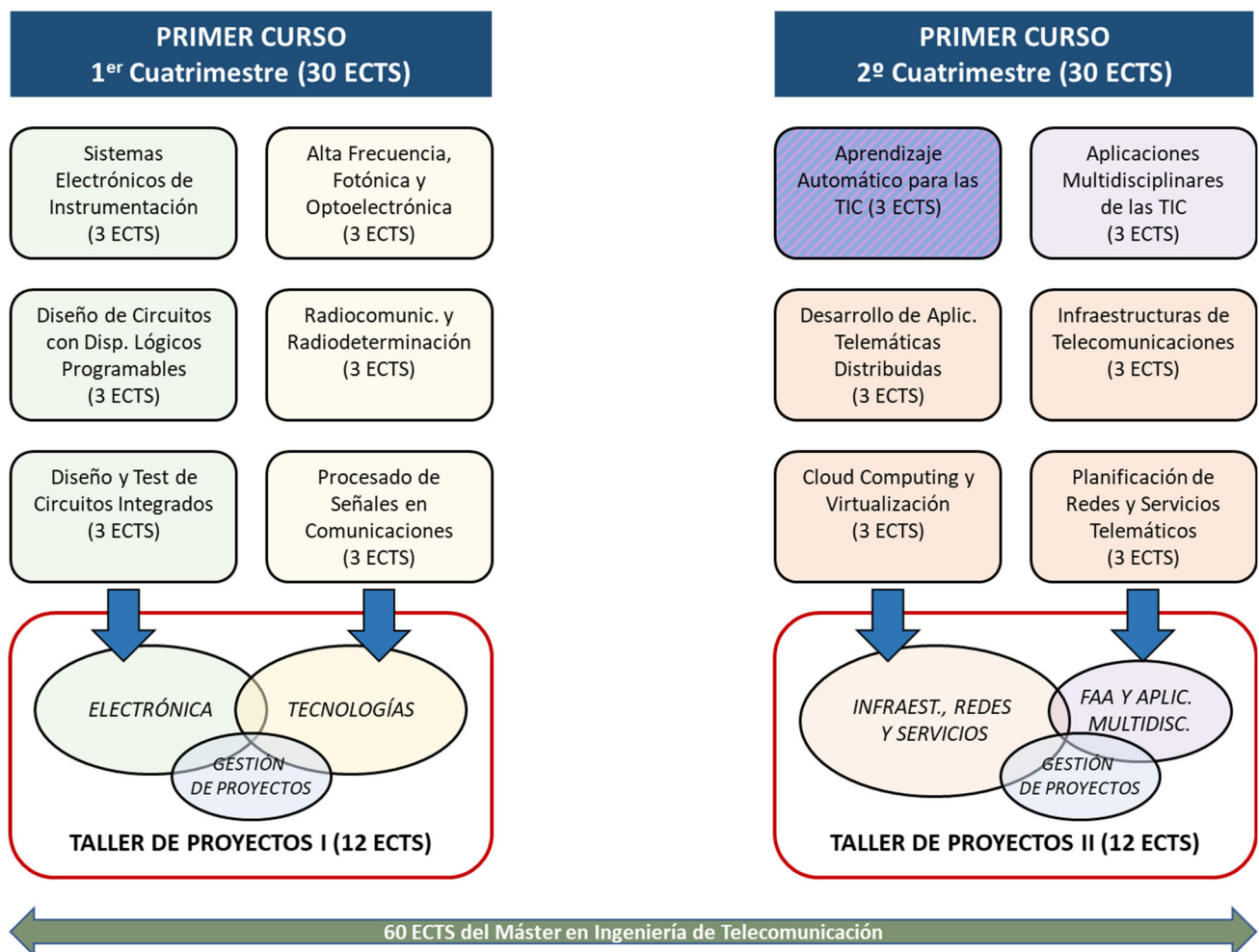


Figura 2: imbricación del Máster en Ingeniería de Telecomunicación con el Máster en Seguridad de las Telecomunicaciones (primer curso).



MATERIA	ASIGNATURA	ECTS	CUATR.	TIPO	MODALIDAD
TÉCNICAS Y MÉTODOS TRANSVERSALES	Criptografía	3	1	OB	Presencial
	Aprendizaje automático	3	1	OB	Presencial
	Laboratorio de seguridad de las Telecomunicaciones	3	1	OB	Presencial
	Seminarios	3	2	OB	Presencial
SEGURIDAD DEL SOFTWARE	Técnicas de ataque	3	1	OB	Presencial
	Programación segura	3	2	OB	Presencial
	Respuesta a incidentes	3	2	OB	Presencial
SEGURIDAD DEL HARDWARE	Seguridad en automoción	3	1	OB	Presencial
	Seguridad en el <i>hardware</i> para el IoT	3	1	OB	Presencial
SEGURIDAD EN REDES INALÁMBRICAS	Seguridad en comunicaciones inalámbricas 1	3	1	OB	Presencial
	Seguridad en comunicaciones inalámbricas 2	3	2	OB	Presencial
SEGURIDAD EN REDES Y SERVICIOS TELEMÁTICOS	Seguridad en redes de datos	3	1	OB	Presencial
	Administración de redes seguras 1	3	1	OB	Presencial
	Administración de redes seguras 2	3	2	OB	Presencial
SEGURIDAD CUÁNTICA	Seguridad cuántica 1	3	1	OB	Presencial
	Seguridad cuántica 2	3	2	OB	Presencial
	Prácticas en empresa	6	2	OB	
	Trabajo de Fin de Máster	6	2	OB	

Tabla 1: distribución de materias y asignaturas del Máster en Seguridad de las Telecomunicaciones.

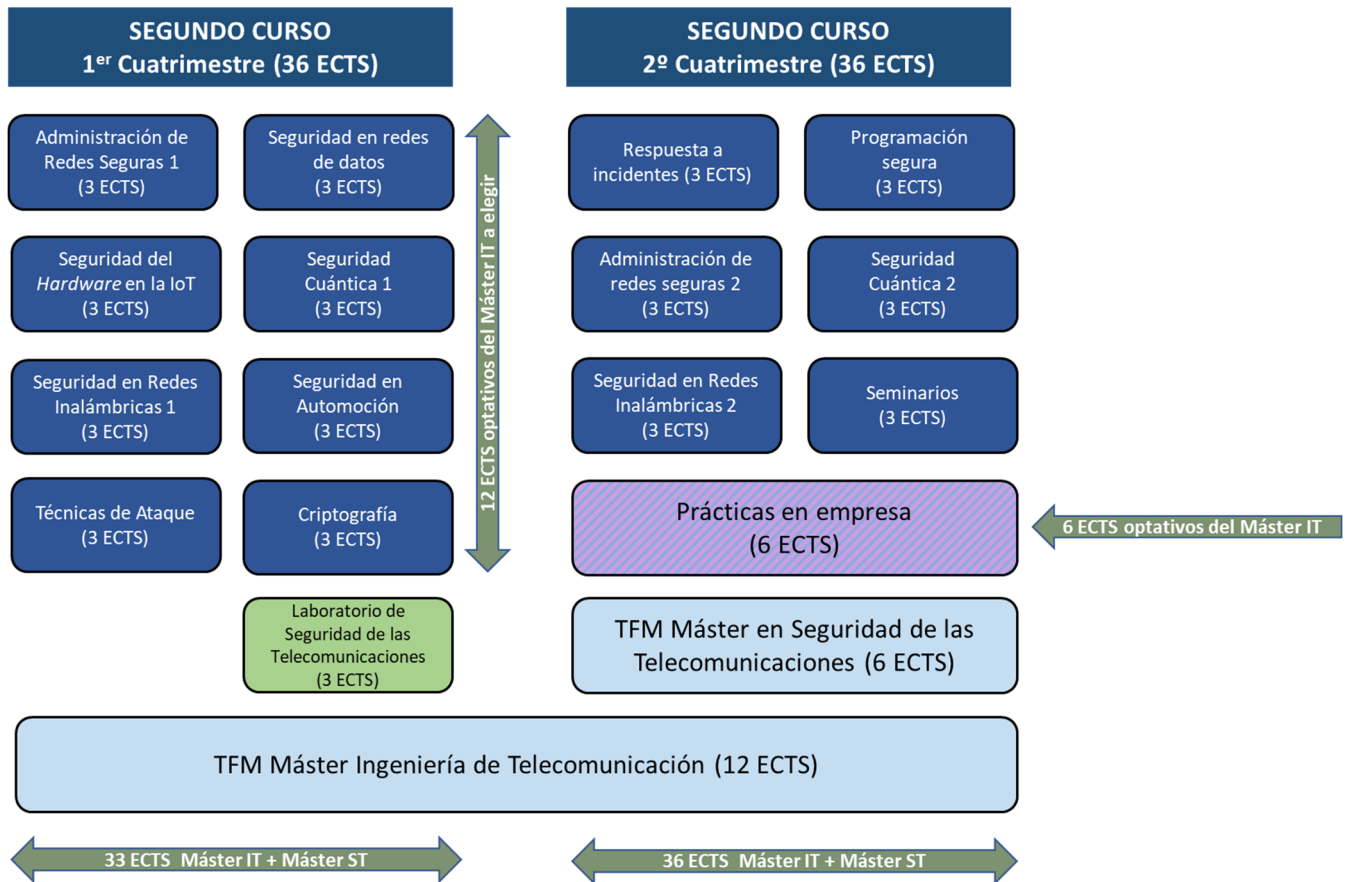


Figura 3: imbricación del Máster en Ingeniería de Telecomunicación con el Máster en Seguridad de las Telecomunicaciones (segundo curso).

4.3 DISTRIBUCIÓN POR TIPO DE MATERIA (OB/OP/TFM/...) Y CORRESPONDENCIA CON LOS RESULTADOS DEL PROCESO DE FORMACIÓN Y APRENDIZAJE

Se presentan en esta sección la matriz de materias – competencias transversales (Tabla 2), la matriz de materias – competencias específicas (Tabla 3), la matriz de materias – conocimientos (Tabla 4) y la matriz de materias – habilidades (Tabla 5).

MATERIA	TIPO	COMPETENCIAS TRANSVERSALES									
		K1	K2	K3	K4	K5	K6	K7	K8	K9	K10
TÉCNICAS Y MÉTODOS TRANSVERSALES	OB	X	X	X	X	X	X	X	X	X	X
SEGURIDAD DEL SOFTWARE	OB	X	X	X	X	X	X	X		X	X
SEGURIDAD DEL HARDWARE	OB	X	X	X	X	X	X	X		X	X
SEGURIDAD EN REDES INALÁMBRICAS	OB	X	X	X	X	X	X	X		X	X
SEGURIDAD EN REDES Y SERVICIOS TELEMÁTICOS	OB	X	X	X	X	X	X	X		X	X
SEGURIDAD CUÁNTICA	OB	X	X	X	X	X	X	X		X	X

Tabla 2: matriz de materias – competencias transversales.



MATERIA	TIPO	COMPETENCIAS ESPECÍFICAS											
		K11	K12	K13	K14	K15	K16	K17	K18	K19	K20	K21	K22
TÉCNICAS Y MÉTODOS TRANSVERSALES	OB	X		X	X	X	X		X		X	X	X
SEGURIDAD DEL SOFTWARE	OB	X	X					X	X	X	X		
SEGURIDAD DEL HARDWARE	OB	X	X					X		X	X		
SEGURIDAD EN REDES INALÁMBRICAS	OB	X	X	X						X	X		X
SEGURIDAD EN REDES Y SERVICIOS TELEMÁTICOS	OB	X	X		X					X	X		
SEGURIDAD CUÁNTICA	OB	X	X							X	X		

Tabla 3: matriz de materias – competencias específicas.

MATERIA	TIPO	CONOCIMIENTOS																		
		C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	C18	C19
TÉCNICAS Y MÉTODOS TRANSVERSALES	OB	X	X	X	X	X		X												
SEGURIDAD DEL SOFTWARE	OB		X			X	X		X	X	X	X	X				X			
SEGURIDAD DEL HARDWARE	OB					X	X		X	X			X		X		X			
SEGURIDAD EN REDES INALÁMBRICAS	OB					X	X		X	X				X			X			X
SEGURIDAD EN REDES Y SERVICIOS TELEMÁTICOS	OB					X	X		X			X				X	X	X	X	
SEGURIDAD CUÁNTICA	OB					X	X		X								X			X

Tabla 4: matriz de materias – conocimientos.

MATERIA	TIPO	HABILIDADES													
		H1	H2	H3	H4	H5	H6	H7	H8	H9	H10	H11	H12	H13	H14
TÉCNICAS Y MÉTODOS TRANSVERSALES	OB	X	X						X	X			X	X	X
SEGURIDAD DEL SOFTWARE	OB	X	X	X	X	X	X			X			X	X	X
SEGURIDAD DEL HARDWARE	OB	X	X			X	X	X		X	X		X	X	X
SEGURIDAD EN REDES INALÁMBRICAS	OB	X	X	X		X	X		X	X			X	X	X
SEGURIDAD EN REDES Y SERVICIOS TELEMÁTICOS	OB	X	X	X		X	X			X	X		X	X	X
SEGURIDAD CUÁNTICA	OB	X	X			X				X		X	X	X	X

Tabla 5: matriz de materias – habilidades.

5 PERSONAL ASOCIADO AL TÍTULO

5.1 RELACIÓN DE PDI / PERFIL DE ADECUACIÓN

A continuación se proporciona una relación individualizada de profesores que manifiestan su interés en impartir docencia en el Máster en Seguridad de las Telecomunicaciones. La Tabla 6 resume los méritos de cada uno de ellos.

Juan Carlos Aguado Manzano ha trabajado intensamente en casos de uso relacionados con el mundo de la automoción, comenzando en la implementación y mantenimiento del Aula Mercedes y las asignaturas que se han impartido en dicha aula, continuando en el desarrollo de una asignatura orientada a proyectos denominada Taller de Proyectos II, donde se fusiona el desarrollo de infraestructura de datos móviles, con aplicaciones IA y caso de uso de vehículo conectado. Además, mantiene una relación estrecha con empresas de sector como Renault, con la que ha participado en proyectos de investigación relacionados con vehículos autónomos. Finalmente, en la mayoría de los proyectos de investigación en competencia pública desarrollado en la última década dentro de su grupo de investigación ha sido el responsable del caso de uso que se ha centrado en vehículos conectados.

Categoría: PTUN. Nº quinquenios: 5. Nº sexenios: 3.

Carlos Alberola López tiene una experiencia de más treinta años de docencia en materias relacionadas con las señales aleatorias, ruido y tratamiento estadístico de señales. Es director de dieciséis tesis doctorales. Fue profesor del máster en Big Data Science, título propio de la Universidad de Valladolid, y es autor de dos libros docentes sobre señales aleatorias y ruido. En materia investigadora es el coordinador de la Unidad de Investigación Consolidada "Laboratorio de Procesado de Imagen", con financiación ininterrumpida desde el año 1997, es director de múltiples proyectos y contratos de investigación y de más de 250 artículos de revistas y congresos. Está en posesión seis quinquenios docentes y seis sexenios investigadores (uno de ellos de transferencia). Es autor de múltiples artículos sobre aprendizaje automático y *deep learning*.

Categoría: CAUN. Nº quinquenios: 6. Nº sexenios: 6 (uno de ellos de transferencia).



Juan Ignacio Asensio Pérez cuenta con más de 30 años de experiencia impartiendo docencia sobre arquitecturas de comunicaciones y gestión de redes de datos. Ha participado en dos proyectos de desarrollo e innovación en el ámbito de la ciberseguridad financiados por el Ministerio de Defensa. Co-coordinador de las Jornadas LexDatum (lexdatum.uva.es) sobre aspectos técnicos y legislativos de la privacidad en las comunicaciones, organizadas por la Universidad de Valladolid.

Categoría: CAUN. **Nº quinquenios:** 6. **Nº sexenios:** 4.

Juan Blas Prieto tiene 25 años de experiencia docente universitaria impartiendo asignaturas de fundamentos de radiación, propagación, antenas, radio definida por software y sistemas de radiocomunicaciones. También ha participado durante 6 años en el título propio de máster en Big Data Science, con una asignatura de Machine Learning. Tiene experiencia investigadora en el campo de la caracterización de entornos radioeléctricos dentro del ámbito de teoría de la señal.

Categoría: PTUN. **Nº quinquenios:** 4. **Nº sexenios:** 2.

Pedro Chamorro Posada cuenta con una trayectoria académica consolidada en el ámbito de la fotónica, la información cuántica y las comunicaciones, desarrollada en la Universidad de Valladolid. Su actividad investigadora ha abordado aspectos directamente relacionados con la seguridad de las comunicaciones, tales como la información y computación cuántica, la fotónica integrada —incluyendo sistemas para aplicaciones cuánticas—, el análisis de vulnerabilidades en sistemas criptográficos basados en láseres de fibra ultra largos y los sistemas de transmisión por fibra óptica. Su experiencia en proyectos competitivos, transferencia de conocimiento y formación de investigadores permite contribuir al programa con un enfoque riguroso, actualizado y alineado con los retos actuales de la ciberseguridad, respaldado por una trayectoria investigadora con 154 publicaciones en revistas indexadas y un índice h de 31 (Google Scholar; 26 en WoS y 26 en Scopus), así como por una participación continuada en proyectos competitivos, entre ellos el proyecto QCAyLE, en el marco del Plan Complementario de I+D+I en Comunicaciones Cuánticas para el impulso de estas tecnologías en Castilla y León.

Categoría: CAUN. **Nº quinquenios:** 6. **Nº sexenios:** 5.

Juan Carlos García Escartín es investigador en computación y comunicaciones cuánticas y seguridad basada en principios físicos. En el plano docente, ha impartido más de cinco años de docencia en asignaturas de seguridad y criptografía a nivel de grado y máster y dirigido varios trabajos de fin de estudios (grado y máster) en temas relacionados. Sus resultados de investigación incluyen publicaciones en revistas indexadas incluyendo temas como distribución cuántica de clave, hackeado cuántico o seguridad del DNI electrónico. Además, tiene dos patentes concedidas sobre sistemas de seguridad (comprobación cuántica de contraseñas e identificación de tarjetas RFID) y ha sido investigador principal en el proyecto nacional "Tecnologías de Seguridad basadas en principios físicos".

Categoría: PTUN. **Nº quinquenios:** 4. **Nº sexenios:** 3.

Jesús M. Hernández Mangas es profesor titular de universidad, licenciado en Físicas e ingeniero en Electrónica y doctor por la Universidad de Valladolid. Con 32 años de experiencia como docente en asignaturas de electrónica digital, desarrollo de sistemas electrónicos, microprocesadores, microcontroladores y procesadores digitales de señal. Tiene experiencia en el método docente de aprendizaje basado en proyectos. Experiencia investigadora en simuladores de procesos tecnológicos empleados en la fabricación de circuitos integrados y en el diseño de circuitos integrados. Experiencia de más de 21 años colaborando con empresas en el desarrollo de productos electrónicos. Inventor de una patente en explotación industrial.

Categoría: PTUN. **Nº quinquenios:** 5 (solicitado el 6º). **Nº sexenios:** 3.

Marcos Martín Fernández es Catedrático de Universidad. En 2004 fue profesor visitante en el Laboratorio de Matemática e Imagen de la Escuela Médica de Harvard (EEUU). Es autor de más de 160 artículos científicos publicados en revistas científicas y congresos. Es revisor de varias revistas científicas del JCR. Su índice H es de 23 y cuenta con más de 1.700 citas recibidas.

Categoría: CAUN. **Nº quinquenios:** 5. **Nº sexenios:** 4.



Ignacio de Miguel Jiménez es Ingeniero de Telecomunicación y Doctor por la Universidad de Valladolid (UVA), donde actualmente trabaja como Catedrático de Universidad. Cuenta con más de 25 años de experiencia docente, impartiendo asignaturas en el ámbito de las comunicaciones ópticas, las redes intra-vehiculares y el aprendizaje automático en estudios de grado y/o de posgrado. Ha participado en 30 proyectos competitivos de I+D de ámbito europeo, nacional o regional, desempeñando el papel de investigador principal (IP) o co-IP en 8 de ellos. Asimismo, ha participado en más de 35 proyectos de innovación docente, liderando 10 como IP. Es autor de más de 50 publicaciones en revistas indexadas en JCR y más de 200 comunicaciones en congresos. Sus principales líneas de investigación se centran en el diseño y control de infraestructuras de comunicaciones, las redes ópticas, la computación en el borde de la red y la aplicación de técnicas de inteligencia artificial en estos entornos.

Categoría: CAUN. **Nº quinquenios:** 5. **Nº sexenios:** 4.

Manuel Rodríguez Cayetano es Ingeniero de Telecomunicación desde 1993 y Doctor Ingeniero de Telecomunicación desde 1999 y cuenta con más de 32 años de experiencia docente. Durante más de 20 años ha ejercido de administrador de redes y ha impartido asignaturas del área de Telemática relacionadas con la administración y gestión de redes (8 cursos) y con la seguridad en redes de comunicaciones (4 cursos). Ha sido participante en el equipo UVA del ejercicio Locked Shields de ciberseguridad de la OTAN durante sus cuatro ediciones hasta el momento. Además, posee un registro de la propiedad intelectual de software en el campo de la programación paralela y en GPU.

Categoría: PTUN. **Nº quinquenios:** 6. **Nº sexenios:** 1.

Ramón de la Rosa Steinz tiene 25 años de experiencia docente universitaria en temas de radiocomunicaciones. Colabora desde el año 2020 en formación del personal de Defensa en temas de satélites, radio definida por software y seguridad en radiocomunicaciones. Es investigador invitado del laboratorio alemán de ingeniería electromagnética ATE (Allgemeine und Theoretische Elektrotechnik) desde el año 2018, además de ser evaluador del Colegio Oficial de Ingenieros de Telecomunicación desde 2014 de trabajos relacionados con radiocomunicaciones y satélites.

Categoría: CDOC (acreditado a PTUN). **Nº quinquenios:** 4 (solicitado el 5º). **Nº sexenios:** 3.

Federico Simmross Wattenberg es ingeniero en Informática y doctor por la Universidad de Valladolid en el programa de Tecnologías de la Información y las Telecomunicaciones. Es Profesor Titular de Universidad desde 2021 y cuenta con más de 20 años de experiencia docente, 13 de ellos en materias directamente relacionadas con la administración, gestión y seguridad de las redes de comunicaciones. Ha sido coordinador del equipo UVA del ejercicio *Locked Shields* de ciberseguridad de la OTAN durante sus cuatro ediciones hasta el momento. Es autor de más de 15 artículos indexados en Q1 y Q2 del JCR y posee dos registros de la propiedad intelectual de software en el campo de la programación paralela y en GPU.

Categoría: PTUN. **Nº quinquenios:** 3 (solicitado el 4º). **Nº sexenios:** 3.

PROFESOR	CATEGORÍA	Nº QUINQUENIOS	Nº SEXENIOS
Juan Carlos Aguado Manzano	PTUN	5	3
Carlos Alberola López	CAUN	6	6
Juan Ignacio Asensio Pérez	CAUN	6	4
Juan Blas Prieto	PTUN	4	2
Pedro Chamorro Posada	CAUN	6	5
Juan Carlos García Escartín	PTUN	4	3
Jesús M. Hernández Mangas	PTUN	5 (sol. 6º)	3



Marcos Martín Fernández	CAUN	5	4
Ignacio de Miguel Jiménez	CAUN	5	4
Manuel Rodríguez Cayetano	PTUN	6	1
Ramón de la Rosa Steinz	CDOC (acred. PTUN)	4 (sol. 5º)	3
Federico Simmross Watenberg	PTUN	3 (sol. 4º)	3

Tabla 6: relación de profesorado para el Máster en Seguridad de las Telecomunicaciones.

5.2 PERFIL DEL PROFESORADO NECESARIO Y NO DISPONIBLE

Las unidades docentes que participan en el máster propuesto tienen un exceso de capacidad docente suficiente como para absorber la nueva docencia en su totalidad. No existen, por lo tanto, necesidades docentes no disponibles. Debe recordarse que el profesorado que actualmente imparte docencia en la ETSI Telecomunicación tiene una contrastada trayectoria en la impartición de todo tipo de asignaturas del ámbito de las Telecomunicaciones. Por otra parte, la ETSIT dispone de profesorado con amplia trayectoria docente e investigadora en campos como el aprendizaje automático, análisis de datos, administración y seguridad en redes de comunicaciones, protocolos de comunicaciones, criptografía, etc, que garantiza las competencias a desarrollar en el máster que se propone.

5.3 PAS DISPONIBLE ASOCIADO AL TÍTULO

PERFIL	VINCULACIÓN	CANTIDAD
OFICIAL DE SERVICIOS E INFORMACIÓN (GRUPO IVA)	Laboral fijo	4
TITULADO SUPERIOR DE REDES Y COMUNICACIONES (GRUPO I)	Laboral fijo	1
TITULADO DE GRADO MEDIO TIC (GRUPO II)	Laboral fijo	2
TÉCNICO ESPECIALISTA DE LABORATORIO EN ELECTRICIDAD Y ELECTRÓNICA (GRUPO III)	Laboral interino	1
TÉCNICO ESPECIALISTA DE OFICIO MANTENIMIENTO GENERAL (GRUPO III)	Laboral interino	1
E. ADMINISTRATIVA UNIV. VALLADOLID/JEFA DE SECCIÓN (NIVEL 22)	Funcionario de carrera	1
E. ADMINISTRATIVA UNIV. VALLADOLID/JEFA DE NEGOCIADO (NIVEL 21)	Funcionario de carrera	2
E. AUXILIAR ADMINISTRATIVA UNIV. VALLADOLID/PUESTO BASE ADMINISTRACIÓN (NIVEL 18)	Funcionario interino	1
E. ADMINISTRATIVA UNIV. VALLADOLID/SECRETARIA DE DIRECCIÓN (NIVEL 21)	Funcionario de carrera	1
E. AUXILIAR ADMINISTRATIVA UNIV. VALLADOLID/SECRETARIA ADMINISTRATIVA (NIVEL 18)	Funcionario interino	2



6 RECURSOS E INSTALACIONES

6.1 PREVISIÓN DE NECESIDADES Y PLAN DE ADQUISICIÓN

La ETSI Telecomunicación cuenta con recursos e instalaciones suficientes para implantar el Máster en Seguridad de las Telecomunicaciones casi en su totalidad, excepción hecha de un servidor apto para poder aplicar técnicas de aprendizaje automático en las asignaturas que de ella dependen.

Por otra parte, se necesitará adquirir material inventariable para hacer prácticas de radio definida por software, además de algún material fungible accesorio.

Para adquirir este equipamiento se cuenta con el programa de apoyo a prácticas docentes de la Universidad de Valladolid, al cual se acudirá en la convocatoria de 2027, con el fin de implantar el máster en el curso 2027/2028.

7 SOSTENIBILIDAD FINANCIERA DE LA PROPUESTA

El profesorado necesario es, esencialmente, personal funcionario o contratado laboral con vinculación permanente, de forma que sus sueldos forman parte del capítulo 1 del presupuesto de la Universidad de Valladolid. Como se ha mencionado anteriormente, no existen necesidades de profesorado adicional para implantar el máster que se propone.

Con respecto a la adquisición de material, es del todo asumible que el equipamiento necesario pueda adquirirse e ir renovándose periódicamente a través del programa de apoyo a prácticas docentes de la Universidad de Valladolid.

8 ANEXOS

Se adjunta la siguiente documentación:

- Cartas de apoyo de las siguientes empresas:
 - Telefónica.
 - Renault España.
 - Michelin España-Portugal.
 - NTTData.
 - Satec.
- Cartas de apoyo de las siguientes entidades:
 - INCIBE (Instituto Nacional de Ciberseguridad).
 - Escuela de Ingeniería Informática de la Universidad de Valladolid.
 - Vigo Quantum Communication Center (Universidad de Vigo).
- Cartas de apoyo de los siguientes expertos en el área:
 - Miguel Herrero Collantes (responsable de seguridad de red del Servicio Europeo de Acción exterior).
 - José Ignacio López Cabido (responsable técnico del Centro de Supercomputación de Galicia).



- José Capmany Franco (responsable de fotónica y comunicaciones cuánticas del Photonics Research Lab, Universitat Politècnica de València).
- Cartas de apoyo de egresados del Grado en Ingeniería de Telecomunicación y del Máster en Ingeniería de Telecomunicación.
- Informe sobre la necesidad y viabilidad académica y social de la implantación del título.
- Tabla para el análisis de la capacidad docente del profesorado.
- Informe del centro favorable a la implantación del título propuesto.
- Acuerdo de Junta de Escuela que hace explícito el compromiso de no reverificación del título en el plazo de 5 cursos tras su implantación.
- Estudio sobre másteres de ciberseguridad en las universidades públicas españolas realizado por la ETSI Telecomunicación – UVa (2025).

[illegible]

IMPLANTACIÓN DE UN MÁSTER SOBRE SEGURIDAD EN LA ETSIT

ENERO 2025

Federico Simmross Wattenberg



Universidad de Valladolid

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

1. TITULACIONES DE SEGURIDAD EN LAS UNIVERSIDADES ESPAÑOLAS

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

- El INCIBE elabora un catálogo de titulaciones de seguridad en España
 - Másteres oficiales
 - Másteres no oficiales
 - Cursos de especialización universitaria
 - Grados
 - Formación profesional



<https://www.incibe.es/incibe/formacion/catalogos-formacion-ciberseguridad> 3

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzympyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica

- Másteres oficiales
 - 31 másteres en 29 universidades
 - 4 en Castilla y León, ninguno en la UVa
- Másteres no oficiales
 - 56 másteres en 45 centros
 - 10 másteres en Valladolid, 9 de ellos UCAM
- Cursos de especialización
 - 9 cursos en 6 centros
 - 3 cursos en Valladolid (UCAM)
- Grados
 - 11 grados en 10 universidades
 - Ninguno en Castilla y León



ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica

Universidades públicas: preferencia por la docencia presencial

Comunidad autónoma	Presencial	Semipresencial	Online
Andalucía	Cádiz, Málaga	Jaén	
Canarias		La Laguna	
Cataluña	UPC, URV		
Castilla y León	ULE (2)		ULE
Comunidad Valenciana		Alicante, UPV	
Galicia	Vigo-Coruña		
Madrid	UC3M, UAH, UPM		UNED
Murcia			UMU
Total	10	4	3

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzympyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica

Universidades privadas: preferencia por la docencia *online*

Comunidad autónoma	Presencial	Semipresencial	Online
Andalucía			INESEM
Cataluña		URL	UOC
Castilla y León		UI1	
Comunidad Valenciana			VIU
Madrid	UE, UNIE	San Pablo	UCJC, INISEG, UE, UAX, UNIE
País Vasco	Mondragón		
La Rioja			UNIR
Total	3	3	9

- INESEM: Instituto Europeo de Estudios Empresariales Business School
- UOC: Universitat Oberta de Catalunya
- URL: Universitat Ramon Llull
- UI1: Universidad Internacional Isabel I de Castilla
- UNIR: Universidad Internacional de La Rioja
- San Pablo: Fundación Universitaria San Pablo CEU
- UCJC: Universidad Camilo José Cela
- INISEG: Instituto Internacional de Estudios en Seguridad Global
- UE: Universidad Europea de Madrid
- UAX: Universidad Alfonso X El Sabio
- VIU: Universidad Internacional de Valencia
- UNIE: Universidad UNIE (UNIE Universidad, S.L.)

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

2. CATEGORIZACIÓN DE ASIGNATURAS RELACIONADAS CON LA SEGURIDAD

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

¿QUÉ SE IMPARTE EN LOS MÁSTERES EXISTENTES?

- La (ciber)seguridad es una disciplina amplísima
 - Diversas orientaciones de los másteres
 - Criptografía, administración de redes, técnicas de ataque y defensa, legislación, ...
 - Multitud de asignaturas de diversas temáticas
 - Nomenclatura de asignaturas muy variada
- Necesidad de un análisis por temáticas de asignaturas
 - Clasificación de las asignaturas en grandes ramas temáticas: «**categorías**»
 - Titulación a titulación, recorriendo la oferta de las universidades españolas
 - Revisión del temario de cada asignatura
 - Posterior análisis basado en dichas categorías



ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica

CATEGORIZACIÓN DE ASIGNATURAS

- **Propuesta:** categorización que comprenda todas las asignaturas de los másteres oficiales de las universidades españolas

Categoría	Abreviatura
Matemáticas / estadística / ciencia de datos / inteligencia artificial	MATEMÁTICAS
Informática forense / auditorías / incidentes	FORENSE
Técnicas de ataque	TÉCNICAS
Seguridad organizativa / planificación / riesgos / legislación / <i>compliance</i>	ORGANIZATIVA
Seguridad de las comunicaciones / capa física / protocolos	SEGCOM
Administración y gestión de redes / monitorización / tráfico de red	ADMIN
Programación segura / seguridad del <i>software</i> / protección de datos	PROSEG
Criptografía / <i>blockchain</i> / criptomonedas	CRIPTOGRAFÍA
Seguridad industrial / <i>hardware</i> / IoT / seguridad física / control de procesos	INDUSTRIAL



3. ANÁLISIS COMPARADO CON LAS UNIVERSIDADES ESPAÑOLAS

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

¿QUÉ SE DEBERÍA IMPARTIR EN LA UVA?

- Un análisis categorizado de las asignaturas permitirá deducir:
 - Las temáticas más importantes
 - El peso relativo del resto de temáticas
- Peso relativo de las temáticas:
 - Relativo a la oferta de ECTS por tipología
 - Obligatorias – nº asignaturas ofertadas = nº asignaturas cursadas
 - Optativas – nº asignaturas ofertadas >> nº asignaturas cursadas
 - Relativo a la oferta total de ECTS del máster
 - Relativo a la duración del máster
 - Sólo aplicable a asignaturas obligatorias (cada alumno decidirá sus temáticas optativas)



ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica

¿QUÉ MODELO DEBE SEGUIRSE EN LA UVA?

- La Universidad de Valladolid es pública y presencial
- Universidad pública española: amplia mayoría de másteres presenciales
- Universidades de reconocido prestigio académico
- **Se analizarán los 10 másteres oficiales presenciales ofrecidos por universidades públicas (ver anexo)**
 - UAH, Cádiz, UC3M, UPC, ULE (2), UPM, Málaga, URV, Vigo-Coruña

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN<https://run.gob.es/hsbzvymPyF>

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica

4. ANÁLISIS POR TEMÁTICAS

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

MÉTODO DE ANÁLISIS

- 10 másteres en total
 - 1 de temática centrada en Derecho (ULE1)
 - 1 de temática incierta (URV)
 - Se eliminan ambos como *outliers* antes del análisis
- **Énfasis:** peso relativo de cada categoría en relación a...
 - Nº ECTS obligatorios – ¿Qué contenidos consideramos imprescindibles?
 - Nº total de ECTS ofertados – ¿Qué contenidos queremos abarcar?
- **Objetivo:** determinar el peso que debería tener cada categoría en un hipotético «máster insesgado sobre seguridad»



ANÁLISIS POR TEMÁTICAS

Proporción de carga por categorías – Sobre asignaturas obligatorias

Categoría	UAH	UCA	UC3M	UPC	ULE2	UPM	UMA	Vigo-UDC	Media	Desv.
MATEMÁTICAS	13%	9%						8%	4,29%	0,06
FORENSE	13%				18%	8%			5,57%	0,08
TÉCNICAS		9%	30%	17%	9%	15%		16%	13,71%	0,09
ORGANIZATIVA	25%	28%	10%		18%	38%		21%	20,00%	0,12
SECOM	13%		20%					8%	5,86%	0,08
ADMIN		21%	30%	50%	20%	31%		16%	24,00%	0,15
PROSEG	25%	19%		17%	9%	8%		8%	12,29%	0,08
CRIPTOGRAFÍA	13%	14%	10%	17%	9%			16%	11,29%	0,06
INDUSTRIAL					9%			8%	2,43%	0,04
Total	100%	100%	100%	100%	92%	100%	100%	100%	100%	



ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica

ANÁLISIS POR TEMÁTICAS

Proporción de carga por categorías – Sobre la oferta global (Ob + Op)

Categoría	UAH	UCA	UC3M	UPC	ULE2	UPM	UMA	Vigo-UDC	Media	Desv.
MATEMÁTICAS	10%	9%		8%	18%			7%	7,43%	0,06
FORENSE	17%		6%		11%	12%	20%	4%	8,75%	0,07
TÉCNICAS	13%	9%	28%	13%	10%	12%	20%	13%	14,75%	0,06
ORGANIZATIVA	20%	28%	17%		11%	41%	20%	17%	19,25%	0,12
SECOM	10%		17%	10%				7%	5,50%	0,07
ADMIN		21%	22%	25%	16%	24%		13%	15,13%	0,10
PROSEG	20%	19%	6%	19%	10%	6%	20%	11%	13,88%	0,06
CRIPTOGRAFÍA	10%	14%	6%	23%	5%			17%	9,38%	0,08
INDUSTRIAL				4%	14%	6%	20%	11%	7,86%	0,07
Total	100%	100%	100%	100%	95%	100%	100%	100%	100%	



DISCUSIÓN

- **1. Existe un «máster típico» en España (universidad presencial, pública)**
 - Máxima importancia: **ORGANIZATIVA, ADMIN**
 - En segundo lugar: **TÉCNICAS, PROSEG, CRIPTOGRAFÍA**
- Profesorado ETSIT en un hipotético máster típico:
 - Categorías críticas:
 - Personal competente pero escaso en **ADMIN, CRIPTOGRAFÍA**
 - Especialidad exigua en **TÉCNICAS, PROSEG**
 - Experiencia nula en **ORGANIZATIVA**
 - Otras categorías:
 - Personal competente y abundante en **MATEMÁTICAS, SEGCOM**
 - Experiencia nula en **FORENSE, INDUSTRIAL**



• 2. Cada máster tiene su propia orientación

- Presumiblemente según la experiencia del profesorado
- Caso extraordinariamente obvio: URV
- Existen áreas importantes para la sociedad que los másteres apenas si tratan:
 - Redes inalámbricas de área amplia/industriales/IoT (5G, Z-wave, LoRA, ...), interferencias, comunicaciones cuánticas, comunicaciones redundantes, etc., además de la electrónica asociada a todo ello
- No obstante, persiste el problema de escasez de profesorado en áreas críticas
 - ORGANIZATIVA en particular



ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzympyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica

CONCLUSIONES

- La ETSIT debe buscar su propia temática de especialidad
 - Un máster típico tendría la mayor competencia posible desde el resto de universidades
 - Cercanía geográfica con León y Madrid
- ETSIT: exceso de capacidad docente en algunas UD, al límite en otras
 - La mayor parte de la plantilla pertenece a Tª Señal y Comunicaciones
 - Es la UD con mayor exceso de capacidad docente
- Ningún máster de las universidades españolas (públicas, presenciales) está centrado en el área de **seguridad de las comunicaciones**



Máster Universitario en Seguridad de las Telecomunicaciones

- Profesorado altamente cualificado en el área de comunicaciones
- Exceso de capacidad docente en el área de Tª Señal y Comunicaciones
- Competencia prácticamente nula desde otros másteres
- Falta de especialidad en áreas críticas: ¿colaboración con otras escuelas?
 - FORENSE, TÉCNICAS, PROSEG: ETSI Informática
 - ORGANIZATIVA: ¿?



ANEXO. REVISIÓN DE LOS MÁSTERES OFICIALES DE LAS UNIVERSIDADES ESPAÑOLAS

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

1. UNIVERSIDAD DE ALCALÁ

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

UNIVERSIDAD DE ALCALÁ

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

- 60 ECTS
- 1 curso académico
- Castellano
- Escuela Politécnica Superior
- Carga de ECTS:
 - 36 ECTS asignaturas obligatorias
 - 6 ECTS optativas (9 ECTS ofertados)
 - 6 ECTS prácticas obligatorias
 - 12 ECTS TFM
- <https://posgrado.uah.es/es/oferta/Ciberseguridad/>



ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzympyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica

UNIVERSIDAD DE ALCALÁ

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

Categorización de asignaturas

Nombre	Cuat	Op/Ob	ECTS	Categoría
Criptografía aplicada	1	Ob	4,5	CRIPTOGRAFÍA
Fundamentos de la seguridad en el software y en los componentes	1	Ob	4,5	PROSEG
Fundamentos de la gestión de la seguridad de la información	1	Ob	4,5	ORGANIZATIVA
Comunicaciones seguras	1	Ob	4,5	SECOM
Sistemas de información para la ciberseguridad	1	Ob	4,5	FORENSE
Diseño y desarrollo de sistemas seguros	2	Ob	4,5	PROSEG
Sistemas de gestión de la seguridad de la información	2	Ob	4,5	ORGANIZATIVA
Análisis de datos para la ciberseguridad	2	Ob	4,5	MATEMÁTICAS
Análisis forense avanzado	2	Op	3	FORENSE
Análisis avanzado de malware	2	Op	3	TÉCNICAS
Ingeniería inversa del software	2	Op	3	TÉCNICAS



UNIVERSIDAD DE ALCALÁ

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

Carga de ECTS por categorías

	Obligatorias				Optativas			Máster	
Categoría	ECTS	% Ob	% Of	% Más	ECTS	% Op	% Of	ECTS	% Of
MATEMÁTICAS	4,5	13%	10%	8%				4,5	10%
FORENSE	4,5	13%	10%	8%	3	33%	7%	7,5	17%
TÉCNICAS					6	67%	13%	6	13%
ORGANIZATIVA	9	25%	20%	15%				9	20%
SECOM	4,5	13%	10%	8%				4,5	10%
ADMIN									
PROSEG	9	25%	20%	15%				9	20%
CRIOGRAFÍA	4,5	13%	10%	8%				4,5	10%
INDUSTRIAL									
Total	36	100%	80%	60%	9	100%	20%	45	100%

% Ob: sobre total obligatorias a cursar (36); % Op: sobre total optativas ofertadas (9); % Of: sobre total asignaturas ofertadas (45); % Más: sobre duración del máster (60)

25



2. UNIVERSIDAD DE CÁDIZ

MÁSTER UNIVERSITARIO EN SEGURIDAD INFORMÁTICA

ÁMBITO- PREFIJO
GEISER
Nº registro
REGAGE26e00037824395

CSV
GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9
DIRECCIÓN DE VALIDACIÓN
<https://run.gob.es/hsbzvymPyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO
16/04/2026 14:29:14 Horario peninsular
Validez del documento
Copia Electrónica Auténtica

- 60 ECTS
- 1 curso académico
- Castellano
- Escuela Superior de Ingeniería
- Carga de ECTS:
 - 43 ECTS asignaturas obligatorias
 - 0 ECTS optativas
 - 10 ECTS prácticas obligatorias
 - 7 ECTS TFM
- <https://esingenieria.uca.es/docencia/masteres/master-en-ciberseguridad-datos-informacion/>



ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



UNIVERSIDAD DE CÁDIZ

MÁSTER UNIVERSITARIO EN SEGURIDAD INFORMÁTICA

Categorización de asignaturas

Nombre	Cuat	Op/Ob	ECTS	Categoría
Auditoría y análisis de riesgos	1	Ob	4	ORGANIZATIVA
Criptografía aplicada y seguridad en software de sistemas	1	Ob	6	CRIPTOGRAFÍA
Desarrollo de aplicaciones seguras	1	Ob	4	PROSEG
Legislación y normativa aplicada a la seguridad informática	1	Ob	4	ORGANIZATIVA
Seguridad en redes	1	Ob	5	ADMIN
Ingeniería inversa y arquitecturas seguras	2	Ob	4	TÉCNICAS
Inteligencia artificial aplicada a la seguridad	2	Ob	4	MATEMÁTICAS
Monitorización y seguridad inalámbrica	2	Ob	4	ADMIN
Seguridad en sistemas distribuidos	2	Ob	4	PROSEG
Seguridad en sistemas e infraestructuras críticas	2	Ob	4	ORGANIZATIVA





Carga de ECTS por categorías

	Obligatorias				Optativas			Máster	
Categoría	ECTS	% Ob	% Of	% Más	ECTS	% Op	% Of	ECTS	% Of
MATEMÁTICAS	4	9%	9%	7%				4	9%
FORENSE									
TÉCNICAS	4	9%	9%	7%				4	9%
ORGANIZATIVA	12	28%	28%	20%				12	28%
SECOM									
ADMIN	9	21%	21%	15%				9	21%
PROSEG	8	19%	19%	14%				8	19%
CRIOGRAFÍA	6	14%	14%	10%				6	14%
INDUSTRIAL									
Total	43	100%	100%	72%				43	100%

% Ob: sobre total obligatorias a cursar (43); % Op: sobre total optativas ofertadas (0); % Of: sobre total asignaturas ofertadas (43); % Más: sobre duración del máster (60)



3. UNIVERSIDAD CARLOS III DE MADRID

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

UNIVERSIDAD CARLOS III DE MADRID

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

- 60 ECTS
- 1 curso académico
- Castellano / Inglés
- Escuela de postgrado de Ingeniería y ciencias básicas
- Carga de ECTS:
 - 30 ECTS asignaturas obligatorias
 - 12 ECTS optativas (24 ECTS ofertados)
 - 6 ECTS conferencias obligatorias
 - 12 ECTS TFM
- <https://www.uc3m.es/master/ciberseguridad>



ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzympyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica

Categorización de asignaturas – Cuatrimestre 1

Nombre	Op/Ob	ECTS	Categoría
Comunicaciones seguras	Ob	6	SECOM
Explotación de sistemas software	Ob	3	TÉCNICAS
Protección de datos	Ob	3	CRIPTOGRAFÍA
Sistemas de ciberdefensa	Ob	6	ADMIN
Técnicas de ciberataque	Ob	6	TÉCNICAS
Ciberdelitos, ciberterrorismo y ciberguerra	Op	3	ORGANIZATIVA
Análisis de riesgos en ciberseguridad	Op	3	ORGANIZATIVA



Categorización de asignaturas – Cuatrimestre 2

Nombre	Op/Ob	ECTS	Categoría
Identificación y autorización	Ob	3	ADMIN
Gestión y administración de la ciberseguridad	Ob	3	ORGANIZATIVA
Ingeniería de sistemas seguros	Op	3	PROSEG
Arquitecturas seguras	Op	3	ADMIN
Seguridad en sistemas y comunicaciones móviles	Op	3	SECOM
Análisis e ingeniería de malware	Op	3	TÉCNICAS
Amenazas persistentes y fugas de información	Op	3	TÉCNICAS
Análisis forense de sistemas informáticos	Op	3	FORENSE



UNIVERSIDAD CARLOS III DE MADRID

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

Carga de ECTS por categorías

	Obligatorias				Optativas			Máster	
Categoría	ECTS	% Ob	% Of	% Más	ECTS	% Op	% Of	ECTS	% Of
MATEMÁTICAS									
FORENSE					3	13%	6%	3	6%
TÉCNICAS	9	30%	17%	15%	6	25%	11%	15	28%
ORGANIZATIVA	3	10%	6%	5%	6	25%	11%	9	17%
SEGCOM	6	20%	11%	10%	3	13%	6%	9	17%
ADMIN	9	30%	17%	15%	3	13%	6%	12	22%
PROSEG					3	13%	6%	3	6%
CRİPTOGRAFÍA	3	10%	6%	5%				3	6%
INDUSTRIAL									
Total	30	100%	56%	50%	24	100%	44%	54	100%

% Ob: sobre total obligatorias a cursar (30); % Op: sobre total optativas ofertadas (24); % Of: sobre total asignaturas ofertadas (54); % Más: sobre duración del máster (60)



4. UNIVERSIDAD POLITÉCNICA DE CATALUÑA

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

UNIVERSIDAD POLITÉCNICA DE CATALUÑA

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

- 60 ECTS
- 1 curso académico
- Inglés
- ETSI Telecomunicación / Facultad de Informática
- Carga de ECTS:
 - 30 ECTS asignaturas obligatorias
 - 18 ECTS optativas (50 ECTS ofertados)
 - 12 ECTS TFM
- <https://www.upc.edu/es/masteres/cybersecurity>



ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica

UNIVERSIDAD POLITÉCNICA DE CATALUÑA

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

Categorización de asignaturas – Cuatrimestre 1

Nombre	Op/Ob	ECTS	Categoría
Álgebra matricial, curso intensivo	Op	3	MATEMÁTICAS
Blockchain	Op	5	CRIPTOGRAFÍA
Gestión de la seguridad	Op	5	ADMIN
Malware	Ob	5	TÉCNICAS
Monitorización y análisis del tráfico de red	Ob	5	ADMIN
Protección de los datos	Ob	5	CRIPTOGRAFÍA
Seguridad de red	Ob	5	ADMIN
Seguridad en aplicaciones	Ob	5	PROSEG



Categorización de asignaturas – Cuatrimestre 2

Nombre	Op/Ob	ECTS	Categoría
Casos de uso en ciberseguridad	Op	5	TÉCNICAS
Comunicaciones seguras en redes de fibra óptica	Op	5	SECOM
Criptografía cuántica	Op	5	CRIPTOGRAFÍA
Curso Breve en las Matemáticas de la Teoría de Códigos y la Criptografía	Op	3	MATEMÁTICAS
Prácticas en Computación Cuántica e Inteligencia Artificial	Op	3	CRIPTOGRAFÍA
Privacidad de datos	Op	5	PROSEG
Redes ópticas seguras	Op	3	SECOM
Seguridad de Red – Autenticación y Autorización	Ob	5	ADMIN
Seguridad Definida por Software (Sds)	Op	5	PROSEG
Seguridad en el Hardware de Sistemas Empotrados. Primitivas, Debilidades y Contramedidas	Op	3	INDUSTRIAL



UNIVERSIDAD POLITÉCNICA DE CATALUÑA

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

Carga de ECTS por categorías

	Obligatorias				Optativas			Máster	
Categoría	ECTS	% Ob	% Of	% Más	ECTS	% Op	% Of	ECTS	% Of
MATEMÁTICAS					6	12%	8%	6	8%
FORENSE									
TÉCNICAS	5	17%	6%	8%	5	10%	6%	10	13%
ORGANIZATIVA									
SEGCOM					8	16%	10%	8	10%
ADMIN	15	50%	19%	25%	5	10%	6%	20	25%
PROSEG	5	17%	6%	8%	10	20%	13%	15	19%
CRIOGRAFÍA	5	17%	6%	8%	13	26%	16%	18	23%
INDUSTRIAL					3	6%	4%	3	4%
Total	30	100%	38%	50%	50	100%	62%	80	100%

% Ob: sobre total obligatorias a cursar (30); % Op: sobre total optativas ofertadas (50); % Of: sobre total asignaturas ofertadas (80); % Más: sobre duración del máster (60)

39



5. UNIVERSIDAD DE LEÓN

MÁSTER UNIVERSITARIO EN DERECHO DE LA CIBERSEGURIDAD Y ENTORNO DIGITAL

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

- 60 ECTS
- 1 curso académico
- Castellano
- Facultad de Derecho
- Carga de ECTS:
 - 42 ECTS asignaturas obligatorias
 - 12 ECTS optativas (12 ECTS ofertados)
 - 6 ECTS prácticas optativas
 - 6 ECTS TFM
- <https://www.unileon.es/estudiantes/oferta-academica/masteres/mu-derecho-ciberseguridad-entorno-digital>



ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



Categorización de asignaturas – Cuatrimestre 1

Nombre	Op/Ob	ECTS	Categoría
Aspectos técnicos de la ciberseguridad: el hacking	Ob	4	FORENSE
Buenas prácticas en la gestión técnica de la información	Ob	4	ORGANIZATIVA
Derechos fundamentales digitales de las personas	Ob	4	ORGANIZATIVA
Ilícitos digitales	Ob	4	ORGANIZATIVA
La ciberseguridad en la empresa	Ob	6	ORGANIZATIVA
Libertad de información, privacidad y protección de datos	Ob	4	ORGANIZATIVA
Propiedad industrial e intelectual y medidas de protección	Ob	4	ORGANIZATIVA





Categorización de asignaturas – Cuatrimestre 2

Nombre	Op/Ob	ECTS	Categoría
Investigación y prueba electrónica	Ob	4	ORGANIZATIVA
La ciberseguridad en las administraciones públicas y otros aspectos regulatorios de la seguridad nacional	Ob	4	ORGANIZATIVA
Responsabilidad legal y social de la empresa	Ob	4	ORGANIZATIVA
Aspectos internacionales de la ciberseguridad	Op	3	ORGANIZATIVA
Inglés aplicado al entorno digital	Op	3	ORGANIZATIVA
La ciberseguridad en el comercio electrónico y el marketing digital	Op	3	ORGANIZATIVA
Supervisión pública para la protección de datos	Op	3	ORGANIZATIVA





Carga de ECTS por categorías

	Obligatorias				Optativas			Máster	
Categoría	ECTS	% Ob	% Of	% Más	ECTS	% Op	% Of	ECTS	% Of
MATEMÁTICAS									
FORENSE	4	10%	7%	7%				4	7%
TÉCNICAS									
ORGANIZATIVA	38	90%	70%	63%	12	100%	22%	50	93%
SECOM									
ADMIN									
PROSEG									
CRİPTOGRAFÍA									
INDUSTRIAL									
Total	42	100%	78%	70%	12	100%	22%	54	100%

% Ob: sobre total obligatorias a cursar (42); % Op: sobre total optativas ofertadas (12); % Of: sobre total asignaturas ofertadas (54); % Más: sobre duración del máster (60)



6. UNIVERSIDAD DE LEÓN

MÁSTER UNIVERSITARIO EN INVESTIGACIÓN EN CIBERSEGURIDAD

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

UNIVERSIDAD DE LEÓN

M. U. EN INVESTIGACIÓN EN CIBERSEGURIDAD

- 60 ECTS
- 1 curso académico
- Castellano / Inglés
- Escuela de Ingenierías Industrial, Informática y Aeroespacial
- Carga de ECTS:
 - 45 ECTS asignaturas obligatorias
 - 9 ECTS optativas (28 ECTS ofertados)
 - 9 ECTS prácticas optativas
 - 6 ECTS TFM
- <https://www.unileon.es/estudiantes/oferta-academica/masteres/mu-investigacion-ciberseguridad-presencial>



ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica

UNIVERSIDAD DE LEÓN

M. U. EN INVESTIGACIÓN EN CIBERSEGURIDAD

Categorización de asignaturas – Cuatrimestre 1

Nombre	Op/Ob	ECTS	Categoría
Análisis de software I	Ob	4	TÉCNICAS
Análisis forense	Ob	4	FORENSE
Criptografía	Ob	4	CRIPTOGRAFÍA
Diseño y programación seguras	Ob	4	PROSEG
Fundamentos de la ciberseguridad, la ciberdefensa y el cibercrimen	Ob	4	ORGANIZATIVA
Seguridad en sistemas ciberfísicos	Ob	4	INDUSTRIAL
Sistemas confiables	Ob	5	ADMIN
Fundamentos de aprendizaje profundo	Op	3	MATEMÁTICAS
Ciberseguridad industrial I	Op	3	INDUSTRIAL
Devsecops en sistemas autónomos	Op	3	PROSEG
Fundamentos de machine learning y aplicaciones a la ciberseguridad	Op	4	MATEMÁTICAS



Categorización de asignaturas – Cuatrimestre 2

Nombre	Op/Ob	ECTS	Categoría
Auditoría de sistemas	Ob	4	FORENSE
Derecho de la ciberseguridad	Ob	4	ORGANIZATIVA
Ecosistemas móviles y distribuidos	Ob	4	ADMIN
Investigación y tendencias en ciberseguridad	Ob	4	(metod. investigación)
Análisis de software II	Op	3	TÉCNICAS
Aprendizaje automático aplicado a la ciberseguridad y el cibercrimen	Op	3	MATEMÁTICAS
Ciberseguridad industrial II	Op	3	INDUSTRIAL
Modelado de redes y aplicaciones en ciberseguridad	Op	3	MATEMÁTICAS
Tecnologías de autenticación	Op	3	ADMIN



UNIVERSIDAD DE LEÓN

M. U. EN INVESTIGACIÓN EN CIBERSEGURIDAD

Carga de ECTS por categorías

	Obligatorias				Optativas			Máster	
Categoría	ECTS	% Ob	% Of	% Más	ECTS	% Op	% Of	ECTS	% Of
MATEMÁTICAS					13	46%	18%	13	18%
FORENSE	8	18%	11%	13%				8	11%
TÉCNICAS	4	9%	5%	7%	3	11%	4%	7	10%
ORGANIZATIVA	8	18%	11%	13%				8	11%
SEGCOM									
ADMIN	9	20%	12%	15%	3	32%	4%	12	16%
PROSEG	4	9%	5%	7%	3	32%	4%	7	10%
CRİPTOGRAFÍA	4	9%	5%	7%				4	5%
INDUSTRIAL	4	9%	5%	7%	6	21%	8%	10	14%
Total	41	91%	56%	68%	28	100%	38%	69	95%

% Ob: sobre total obligatorias a cursar (45); **% Op:** sobre total optativas ofertadas (28); **% Of:** sobre total asignaturas ofertadas (73); **% Más:** sobre duración del máster (60)
Nota: 4 ECTS obligatorios sin clasificar (metodología de la investigación)



7. UNIVERSIDAD POLITÉCNICA DE MADRID

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

UNIVERSIDAD POLITÉCNICA DE MADRID

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

- 60 ECTS
- 1 curso académico
- Castellano
- ETS de Ingenieros Informáticos, de Ingeniería de Sistemas Informáticos y de Ingeniería y Sistemas de Telecomunicación
- Carga de ECTS:
 - 39 ECTS asignaturas obligatorias
 - 9 ECTS optativas (12 ECTS ofertados)
 - 6 ECTS prácticas optativas
 - 12 ECTS TFM
- <https://masterciberseguridad.etsit.upm.es/>



ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica

Categorización de asignaturas – Cuatrimestre 1

Nombre	Op/Ob	ECTS	Categoría
Ciberseguridad: contexto y amenazas	Ob	6	ORGANIZATIVA
Servicios de control de acceso	Ob	4,5	ADMIN
Servicios de seguridad en red	Ob	3	ADMIN
Protección de sistemas y servicios	Ob	4,5	ADMIN
Protección de la información	Ob	3	ORGANIZATIVA
Ingeniería inversa y análisis de Malware	Ob	6	TÉCNICAS
Auditoría técnica de seguridad	Ob	3	FORENSE



Categorización de asignaturas – Cuatrimestre 2

Nombre	Op/Ob	ECTS	Categoría
Seguridad en el desarrollo software	Ob	3	PROSEG
Gestión de riesgos y operaciones en ciberseguridad	Ob	6	ORGANIZATIVA
Evidencias forenses	Op	3	FORENSE
Diseño de estrategias corporativas de ciberseguridad	Op	3	ORGANIZATIVA
Sistemas de gestión de seguridad de la información	Op	3	ORGANIZATIVA
Seguridad física y convergencia	Op	3	INDUSTRIAL





UNIVERSIDAD POLITÉCNICA DE MADRID

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

Carga de ECTS por categorías

	Obligatorias				Optativas			Máster	
Categoría	ECTS	% Ob	% Of	% Más	ECTS	% Op	% Of	ECTS	% Of
MATEMÁTICAS									
FORENSE	3	8%	6%	5%	3	25%	6%	6	12%
TÉCNICAS	6	15%	12%	10%				6	12%
ORGANIZATIVA	15	38%	29%	25%	6	50%	12%	21	41%
SEGCOM									
ADMIN	12	31%	24%	20%				12	24%
PROSEG	3	8%	6%	5%				3	6%
CRİPTOGRAFÍA									
INDUSTRIAL					3	25%	6%	3	6%
Total	39	100%	76%	65%	12	100%	24%	51	100%

% Ob: sobre total obligatorias a cursar (39); % Op: sobre total optativas ofertadas (12); % Of: sobre total asignaturas ofertadas (51); % Más: sobre duración del máster (60)

54

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvympyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica

8. UNIVERSIDAD DE MÁLAGA

MÁSTER UNIVERSITARIO EN INGENIERÍA INFORMÁTICA

ESPECIALIDAD EN CIBERSEGURIDAD

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

- 90 ECTS
- 2 cursos académicos
- Castellano / Inglés
- ETS Ingeniería Informática
- Carga de ECTS:
 - 60 ECTS asignaturas comunes (primer curso)
 - 18 ECTS optativas de especialidad (22,5 ECTS ofertados)
 - 12 ECTS TFM
- <https://www.uma.es/master-en-ingenieria-informatica/>





Categorización de asignaturas (especialidad de ciberseguridad)

Nombre	Op/Ob	ECTS	Categoría
Informática forense	Op	4,5	FORENSE
Análisis de malware	Op	4,5	TÉCNICAS
Ingeniería de seguridad	Op	4,5	ORGANIZATIVA
Programación segura	Op	4,5	PROSEG
Seguridad en sistemas industriales y ciberfísicos	Op	4,5	INDUSTRIAL



Carga de ECTS por categorías

	Obligatorias				Optativas			Máster	
Categoría	ECTS	% Ob	% Of	% Más	ECTS	% Op	% Of	ECTS	% Of
MATEMÁTICAS									
FORENSE					4,5	20%	20%	4,5	20%
TÉCNICAS					4,5	20%	20%	4,5	20%
ORGANIZATIVA					4,5	20%	20%	4,5	20%
SEGCOM									
ADMIN									
PROSEG					4,5	20%	20%	4,5	20%
CRİPTOGRAFÍA									
INDUSTRIAL					4,5	20%	20%	4,5	20%
Total					22,5	100%	100%	22,5	100%

% Ob: sobre total obligatorias a cursar (0); **% Op:** sobre total optativas ofertadas (22,5); **% Of:** sobre total asignaturas ofertadas (22,5); **% Más:** sobre duración del máster (60)



9. UNIVERSITAT ROVIRA I VIRGILI

MÁSTER UNIVERSITARIO EN INGENIERÍA DE LA SEGURIDAD INFORMÁTICA E INTELIGENCIA ARTIFICIAL

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

UNIVERSITAT ROVIRA I VIRGILI

MUII SEGURIDAD INFORMÁTICA E INTELIGENCIA ARTIFICIAL

- 60 ECTS
- 1 curso académico
- Inglés
- ETS de Ingeniería
- Carga de ECTS:
 - 36 ECTS asignaturas obligatorias
 - 15 ECTS optativas (33 ECTS ofertados)
 - 9 ECTS TFM
- <https://www.urv.cat/es/estudios/masteres/oferta/ingenieria-seguridad-informatica/>

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzympyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9



UNIVERSITAT ROVIRA I VIRGILI

MUII SEGURIDAD INFORMÁTICA E INTELIGENCIA ARTIFICIAL

Categorización de asignaturas – Cuatrimestre 1

Nombre	Op/Ob	ECTS	Categoría
Criptografía y seguridad de la información	Ob	4,5	CRIPTOGRAFÍA
Informática forense	Ob	4,5	(procesado imágenes)
Identificación biométrica	Ob	4,5	(recon. patrones)
Sistemas multiagente	Ob	4,5	(sist. distribuidos)
Visión artificial y reconocimiento de patrones	Ob	4,5	(recon. patrones)
Computación neuronal y evolutiva	Ob	4,5	MATEMÁTICAS
Arquitecturas seguras de sistemas distribuidos	Op	3	(sist. distribuidos)
Planificación y razonamiento aproximado	Op	6	(temario no disponible)

ÁMBITO- PREFIJO**GEISER**Nº registro**REGAGE26e00037824395**CSV**GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9**DIRECCIÓN DE VALIDACIÓN**<https://run.gob.es/hsbzvymPyF>**

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO**16/04/2026 14:29:14 Horario peninsular**Validez del documento**Copia Electrónica Auténtica**



UNIVERSITAT ROVIRA I VIRGILI

MUII SEGURIDAD INFORMÁTICA E INTELIGENCIA ARTIFICIAL

Categorización de asignaturas – Cuatrimestre 2

Nombre	Op/Ob	ECTS	Categoría
Protección de la privacidad	Ob	4,5	MATEMÁTICAS
Sistemas de ayuda en la toma de decisiones multicriterio	Ob	4,5	MATEMÁTICAS
Computación ubicua	Op	3	(no se imparte)
Investigación y emprendimiento en seguridad e inteligencia artificial	Op	3	(met. investigación)
Representación e ingeniería del conocimiento	Op	6	(no se imparte)
Sistemas de visualización e interacción	Op	3	(temario no disponible)
Seguridad multimedia	Op	3	MATEMÁTICAS
Redes complejas	Op	6	MATEMÁTICAS





UNIVERSITAT ROVIRA I VIRGILI

MUII SEGURIDAD INFORMÁTICA E INTELIGENCIA ARTIFICIAL

Carga de ECTS por categorías

	Obligatorias				Optativas			Máster	
Categoría	ECTS	% Ob	% Of	% Más	ECTS	% Op	% Of	ECTS	% Of
MATEMÁTICAS	13,5	38%	20%	23%	9	27%	13%	22,5	33%
FORENSE									
TÉCNICAS									
ORGANIZATIVA									
SECOM									
ADMIN									
PROSEG									
CRİPTOGRAFÍA	4,5	13%	7%	8%				4,5	7%
INDUSTRIAL									
Total	18	50%	26%	30%	9	27%	13%	27	39%

% Ob: sobre total obligatorias a cursar (36); % Op: sobre total optativas ofertadas (33); % Of: sobre total asignaturas ofertadas (69); % Más: sobre duración del máster (60)

Nota: 18 ECTS obligatorios, 24 optativos sin clasificar (temática diversa o no disponible)



10. UNIVERSIDAD DE VIGO – UNIVERSIDAD DE LA CORUÑA MÁSTER INTER-UNIVERSITARIO EN CIBERSEGURIDAD

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica

UNIV. DE VIGO – UNIV. DE LA CORUÑA

MÁSTER INTER-UNIVERSITARIO EN CIBERSEGURIDAD

- 90 ECTS
- 2 cursos académicos
- Castellano / Inglés
- Escuela de Ingeniería de Telecomunicación (UVIGO) / Facultad de Informática (UDC)
- Carga de ECTS:
 - 63 ECTS asignaturas obligatorias
 - 6 ECTS optativas (12 ECTS ofertados)
 - 9 ECTS prácticas obligatorias
 - 12 ECTS TFM
- <https://www.munics.es/>



ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica

Categorización de asignaturas – Cuatrimestre 1

Nombre	Op/Ob	ECTS	Categoría
Seguridad de la información	Ob	5	CRIPTOGRAFÍA
Análisis de malware	Ob	5	TÉCNICAS
Privacidad y anonimidad	Ob	5	MATEMÁTICAS
Seguridad de aplicaciones	Ob	5	PROSEG
Redes seguras	Ob	5	ADMIN
Tecnologías de registro distribuido y blockchain	Ob	5	CRIPTOGRAFÍA



ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



UNIV. DE VIGO – UNIV. DE LA CORUÑA

MÁSTER INTER-UNIVERSITARIO EN CIBERSEGURIDAD

Categorización de asignaturas – Cuatrimestre 2

Nombre	Op/Ob	ECTS	Categoría
Seguridad en comunicaciones	Ob	5	SECOM
Fortificación de sistemas	Ob	5	ADMIN
Ciberseguridad industrial e IoT	Ob	5	INDUSTRIAL
Hacking ético y test de intrusión	Ob	5	TÉCNICAS
Negocio en ciberseguridad y emprendimiento	Ob	4	ORGANIZATIVA
Análisis forense	Op	3	FORENSE
Seguridad en centros de datos	Op	3	INDUSTRIAL
Seguridad en dispositivos móviles	Op	3	PROSEG
Smart Contracts y dApps	Op	3	CRIPTOGRAFÍA

ÁMBITO- PREFIJO**GEISER**Nº registro**REGAGE26e00037824395**CSV**GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9**DIRECCIÓN DE VALIDACIÓN**<https://run.gob.es/hsbzvymPyF>**

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO**16/04/2026 14:29:14 Horario peninsular**Validez del documento**Copia Electrónica Auténtica**

Categorización de asignaturas – Cuatrimestre 3

Nombre	Op/Ob	ECTS	Categoría
Gestión de seguridad de la información	Ob	5	ORGANIZATIVA
Conceptos y leyes	Ob	4	ORGANIZATIVA





UNIV. DE VIGO – UNIV. DE LA CORUÑA

MÁSTER INTER-UNIVERSITARIO EN CIBERSEGURIDAD

Carga de ECTS por categorías

	Obligatorias				Optativas			Máster	
Categoría	ECTS	% Ob	% Of	% Más	ECTS	% Op	% Of	ECTS	% Of
MATEMÁTICAS	5	8%	7%	6%				5	7%
FORENSE					3	25%	4%	3	4%
TÉCNICAS	10	16%	13%	11%				10	13%
ORGANIZATIVA	13	21%	17%	14%				13	17%
SEGCOM	5	8%	7%	6%				5	7%
ADMIN	10	16%	13%	11%				10	13%
PROSEG	5	8%	7%	6%	3	25%	4%	8	11%
CRIPTOGRAFÍA	10	16%	13%	11%	3	25%	4%	13	17%
INDUSTRIAL	5	8%	7%	6%	3	25%	4%	8	11%
Total	63	100%	84%	70%	12	100%	16%	75	100%

% Ob: sobre total obligatorias a cursar (63); % Op: sobre total optativas ofertadas (12); % Of: sobre total asignaturas ofertadas (75); % Más: sobre duración del máster (90)

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>



GEISER-52dd-c107-a16f-b2f8-8050-db75-02f3-95e9

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica

SOLICITUD DE EMISIÓN DE INFORME DE NECESIDAD Y VIABILIDAD ACADÉMICA Y SOCIAL DE IMPLANTACIÓN DE ENSEÑANZAS UNIVERSITARIAS OFICIALES. (Art. 26.3 Real Decreto 822/2021, de 28 de septiembre)

1. DATOS DEL SOLICITANTE

APELLIDOS Y NOMBRE: ☐ RECTOR/A: ☐ VICERRECTOR/A: Resolución de delegación: Fecha publicación BOCYL:	NIF:
UNIVERSIDAD:	
E-MAIL A EFECTOS DE NOTIFICACIONES:	

2. DATOS DE LA ENSEÑANZA UNIVERSITARIA OFICIAL

TIPO DE ESTUDIO:	☐ GRADO	☒ MÁSTER UNIVERSITARIO	☐ DOCTORADO
DENOMINACIÓN:			
MODALIDAD:	☒ PRESENCIAL	☐ HÍBRIDA/SEMPRESENCIAL	☐ VIRTUAL/NO PRESENCIAL
CENTRO/S RESPONSABLE/S: ETSI Telecomunicación			



Nº IAPA 2298 Modelo 7909

TITULACIÓN INTERUNIVERSITARIA:	SÍ ☐	NO ☒
UNIVERSIDAD COORDINADORA:		
OTRAS UNIVERSIDADES COLABORADORAS: - - - - - - - -		
PROFESIONES REGULADAS PARA LAS QUE CAPACITA UNA VEZ OBTENIDO EL TÍTULO	☐ SÍ	☐ NO
Nombre de la profesión regulada y normativa reguladora -		
PLAZAS DE NUEVO INGRESO OFERTADAS EN LOS PRIMEROS AÑOS DE IMPLANTACIÓN (Si se imparte en varios centros, desglosado por cada uno de ellos). 20		



3. JUSTIFICACIÓN DE LA NECESIDAD Y VIABILIDAD ACADÉMICA Y SOCIAL DE LA IMPLANTACIÓN DE LAS ENSEÑANZAS:

Objetivos formativos:

El objetivo fundamental del máster es formar a personas que sean competentes en el ámbito de la seguridad de las Telecomunicaciones. Este objetivo global se puede concretar en los siguientes puntos:

- Proporcionar a los estudiantes una base sólida sobre los fundamentos generales de la ciberseguridad, incluyendo:
 - o Criptografía.
 - o Aprendizaje automático.
 - o Técnicas de ataque.
 - o Respuesta a incidentes.
 - o Administración y gestión de redes de comunicaciones.
- Impartir, dentro del ámbito general de la seguridad, una formación especializada dirigida y aplicada a las Telecomunicaciones, claramente diferenciada de los aspectos que generalmente se atribuyen a la seguridad puramente informática. Concretamente se abordarán las siguientes temáticas:
 - o Seguridad cuántica.
 - o Seguridad en redes inalámbricas.
 - o Seguridad en la automoción.
 - o Seguridad de la Internet de las cosas (IoT).
 - o Protocolos de comunicación seguros.
- Facilitar a los egresados la incorporación laboral tanto en empresas del sector de las Telecomunicaciones en general (que por descontado han de dar una importancia de calado a la seguridad de sus redes) como a aquellas cuyo plan de negocio se encuentra de lleno en la seguridad, incluido el sector de la defensa.
- Desarrollar la capacidad de los estudiantes para adaptarse a situaciones siempre cambiantes y para enfrentar adecuadamente retos que cambian día a día.
- Proporcionar a los estudiantes un nivel de competencia suficiente para asumir responsabilidades relacionadas con la seguridad de las Telecomunicaciones en ámbitos profesionales, así como para desarrollar actividades de investigación en dicho campo.
- Ofrecer a los estudiantes la experiencia de expertos en el ámbito de la seguridad mediante conferencias y charlas de ponentes de reconocido prestigio.

Perfil de egresados:

Los egresados del máster tendrán dos perfiles superpuestos: uno de corte generalista en cuanto a ciberseguridad se refiere, y otro más específico, dirigido especialmente a las Telecomunicaciones:

- Perfil 1 (generalista). Personas competentes en la realización de tareas que se asocian generalmente con la ciberseguridad: programación segura, detección de ataques, respuesta a incidentes, trabajo con algoritmos criptográficos, uso de técnicas de aprendizaje automático, administración segura de redes de comunicaciones, etc.
- Perfil 2 (específico). Personas competentes en la implantación y mantenimiento de telecomunicaciones seguras, incluyendo comunicaciones cuánticas, comunicaciones inalámbricas en entornos no fiables, comunicaciones entre pequeños dispositivos electrónicos y entre vehículos en marcha y uso de protocolos avanzados para comunicaciones seguras.

Potencial mercado/análisis de competencia/empleabilidad:

Huelga decir, en términos generales, que las Telecomunicaciones están presentes en la vida diaria de millones de personas y que la importancia de su seguridad es palmaria, sobre todo en los últimos años, con una tendencia al alza a juzgar por la frecuente presencia de noticias sobre robos de credenciales, estafas, ataques a infraestructuras críticas, etc. en medios de comunicación generalistas. Redundando en ello, cabe decir también que la seguridad de las Telecomunicaciones no es de aplicación exclusivamente civil, sino que tiene una importancia igualmente patente en el ámbito de la defensa, de nuevo con una tendencia al alza en los últimos años. Para sustentar estas afirmaciones podemos acudir a datos concretos:

- En primer lugar, el informe de AMETIC “Barómetro de la Economía Digital 2025” (<https://ametic.es/publicacion/barometro-de-la-economia-digital-2025/>) señala que el sector tecnológico digital tiene un impacto en el 26% del PIB de España, con un aumento interanual del 7,4%, y un peso del 19,8% en el total de la innovación del sector privado en porcentaje de empresas (de un total de 36.737 empresas). Medido en número de empleados, el sector cuenta con más de 722.000, con un aumento interanual del 7,8%. En términos de volumen de negocio, el sector es responsable de un total de 95.000 millones de euros, con un aumento del 13,1% interanual.
- En segundo lugar, el Observatorio Nacional de Tecnología y Sociedad (Ontsi), en su estudio sobre la empleabilidad del sector de las TIC de 2021 (el más reciente disponible) (https://www.ontsi.es/sites/ontsi/files/2021-12/informeempleotecnologiconov2021_0.pdf) señala que la Comisión Europea estimó en 168.000 el número de expertos necesarios en ciberseguridad en el año 2020 y que el Gobierno se fijó como meta incrementar en 20.000 el número de expertos en ciberseguridad, inteligencia artificial y datos hasta 2025.
- En tercer lugar, atendiendo al Catálogo de Formación en Ciberseguridad en España de Másteres, Grados y otras especializaciones del INCIBE (https://www.incibe.es/sites/default/files/paginas/incibe/formacion/Cat%C3%A1logo%20de%20Formaci%C3%B3n%20Grados%20y%20M%C3%Asters_2025.pdf), en su edición de 2025, recoge un total de 138 titulaciones universitarias relacionadas con la ciberseguridad, de las cuales 31 son másteres oficiales (17 en las universidades públicas, 10 de ellos presenciales). Sin embargo, y a pesar de la palpable demanda, ninguno de ellos se imparte en la Universidad de Valladolid.
- En cuarto lugar, la gran mayoría de dichos másteres se concentran en la ciberseguridad entendida como seguridad de los sistemas informáticos, relegando así al problema de la seguridad en las Telecomunicaciones a un segundo plano. Para sostener esta afirmación, nos basamos en un estudio realizado por la propia ETSI Telecomunicación en 2025 (véase el estudio completo en la documentación adjunta a este documento). Dicho estudio encontró que tan solo un 5,50% de los créditos ofertados en los másteres oficiales presenciales de las universidades públicas españolas están dedicados a la seguridad de las Telecomunicaciones (SEGGOM, en el citado estudio).
- En quinto lugar, el Ministerio para la Transformación Digital y de la Función Pública trabaja actualmente en un real decreto sobre seguridad y resiliencia de las redes de telecomunicaciones (<https://digital.gob.es/comunicacion/notas/secretaria-estado-telecomunicaciones-e-infraestructuras-digitales/2025/12/2025-12-02>), lo cual pone de manifiesto que existe un gran interés institucional por la seguridad de las Telecomunicaciones.
- En sexto y último lugar, el INCIBE informa de que el gestionó un total de 122.223 incidentes de seguridad en 2025 y que, de entre los dispositivos que los ciberdelincuentes consiguieron controlar, un 85% están relacionados con dispositivos IoT (televisores, decodificadores, reproductores multimedia, etc.), consustanciales al ámbito de las Telecomunicaciones (<https://www.incibe.es/incibe/sala-de-prensa/incibe-detecto-mas-de-122000-incidentes-de-ciberseguridad-en-2025>).

En conclusión, podemos afirmar que nuestra propuesta de Máster en seguridad de las Telecomunicaciones tiene un mercado potencial fuerte, que existe una marcada competencia pero a la vez nuestra propuesta ofrece una especialización destacada, y que las titulaciones afines ya implantadas parecen gozar de una muy alta tasa de empleabilidad si nos atenemos a los análisis referenciados.

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-3117-3cb7-f95c-14d5-f82a-d76b-c883-df94

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymppyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-3117-3cb7-f95c-14d5-f82a-d76b-c883-df94

Nº IAPA 2298 Modelo 7909



Junta de
Castilla y León
Consejería de Educación

MODELO NORMALIZADO Nº 8

Oportunidad y necesidad:

La ETSI Telecomunicación, en su Grado en Ingeniería de Telecomunicación, cuenta con algunas asignaturas en las que se tratan temas relacionados con la seguridad, siendo los ejemplos más notables Seguridad en Redes de Comunicaciones y Administración y Gestión de Redes de Comunicaciones (obligatorias de mención, 4º curso de la mención en Telemática, 6 ECTS). Del mismo modo, el Máster en Ingeniería de Telecomunicación cuenta con la asignatura Ciberseguridad (optativa, primer curso, 3 ECTS). Por otra parte, la Escuela de Ingeniería Informática, en su Grado en Ingeniería Informática, ofrece una mención en Tecnologías de la Información que incluye asignaturas del ámbito de la ciberseguridad, como son Administración de Sistemas Operativos, Garantía y Seguridad de la Información, Diseño, Administración y Seguridad de Redes e Informática Forense, todas ellas de carácter obligatorio para la mención y de 6 ECTS. Con la excepción de Seguridad en Redes de Comunicaciones, que pone el énfasis en los protocolos de comunicación, todas las asignaturas citadas adoptan un enfoque dirigido a la seguridad de los sistemas informáticos y, en cualquier caso, no existe ninguna titulación de máster relacionada con la ciberseguridad (ni, por tanto, con la seguridad de las Telecomunicaciones) en toda la Universidad de Valladolid.

Ampliando la extensión geográfica a toda Castilla y León, solamente la Universidad de León y la Universidad Internacional Isabel I de Castilla ofrecen másteres oficiales de seguridad. En cuanto a esta última, la única asignatura que se centra en la seguridad de las Telecomunicaciones es Ciberseguridad Móvil (obligatoria, 6 ECTS). En cuanto a la Universidad de León, se ofrecen dos másteres relacionados con la ciberseguridad: el primero de ellos, el Máster Universitario en Derecho de la Ciberseguridad y Entorno Digital, está pensado para graduados en Derecho y (consecuentemente) no aborda temas técnicos. El segundo, el Máster Universitario en Investigación en Ciberseguridad, es un máster de ciberseguridad puramente técnico, pero no aborda la temática de las Telecomunicaciones al no ofrecer ninguna asignatura de temática SEGCOM, atendiendo al ya citado estudio realizado por la ETSI Telecomunicación (véase la documentación adjunta). No existe, por lo tanto, en toda Castilla y León, ninguna titulación que ofrezca a los egresados un perfil como el que se pretende dar en el máster que aquí se propone. Esta circunstancia abre una ventana de interés en lo que a planificación estratégica se refiere, ya que, como ya se expuso en la sección 3 y de acuerdo al mencionado estudio de la ETSI Telecomunicación, solamente un 5,50% de los créditos de todos los másteres oficiales presenciales de las universidades públicas españolas (no ya de Castilla y León) está dedicado a un tema hoy en día crucial como es la seguridad de las Telecomunicaciones.

Volviendo al ámbito de la Universidad de Valladolid, y en concreto a la ETSI Telecomunicación, está previsto el encaje del máster propuesto con el ya existente Máster de Ingeniería de Telecomunicación (MIT), de 90 ECTS. Así, los alumnos del MIT podrán consignar sus 18 créditos optativos cursando asignaturas del Máster en Seguridad de las Telecomunicaciones, de forma que los estudiantes podrán obtener dos titulaciones de máster (150 ECTS en total) en cuatro cuatrimestres, según se detalla en la sección 4.2.

En cuanto a los beneficios económicos y sociales que pueda traer el Máster en Seguridad de las Telecomunicaciones al conjunto de Castilla y León, cabe mencionar que varias empresas, entidades y expertos de reconocido prestigio de ámbito nacional e internacional han manifestado su apoyo explícito a nuestra propuesta, así como egresados de titulaciones afines (véase la documentación adjunta). Además, el sector TIC en Castilla y León está bien establecido y numerosas empresas conforman el tejido empresarial local. En particular, las tres grandes operadoras están ubicadas en Valladolid (Telefónica, Vodafone y Orange-MásMóvil) y disponemos de implantación también de otros agentes relevantes del sector (NTT Data, Cellnex Telecom, GMV y Satec...). Por otra parte, el sector de la automoción se encuentra en plena expansión hacia el vehículo conectado (con Renault liderando el sector en esta comunidad autónoma) y otras grandes empresas, como Michelin, se encuentran en pleno proceso de digitalización. Existen unas extraordinarias relaciones entre las empresas mencionadas y la ETSI Telecomunicación, y contamos con ciclos de talleres impartidos por estas empresas, así como convenios para desarrollos específicos en materia docente e investigadora.

Conviene destacar, asimismo, que la seguridad de las Telecomunicaciones tiene inherente y necesariamente un ámbito de aplicación global, de forma que exactamente los mismos procedimientos que puedan aplicarse en Castilla y León son directamente aplicables en cualquier otra parte de la Unión Europea y del resto del mundo.

Sumando esto a la visible escasez de titulaciones de seguridad centradas en las Telecomunicaciones, el resultado es una titulación con (a priori) un gran potencial para atraer alumnos procedentes del ámbito nacional e internacional.

Por último, cabe añadir que la implantación del máster propuesto puede abrir nuevas líneas de investigación relacionadas con la seguridad, las cuales son, a día de hoy, escasas en la Universidad de Valladolid. En efecto, en la relación de grupos del área de Ingeniería y Tecnología del portal de investigación UVA no figura ningún grupo cuya investigación se centre en la ciberseguridad, si bien se tiene constancia de dos grupos de investigación de la ETSI Informática (Tecnologías de Gestión de Información e Inteligencia de Mercado y Marketing) que en el pasado han tocado diversos temas en relación a dicho campo. No obstante, no tenemos constancia alguna de ningún grupo de investigación perteneciente a la Universidad de Valladolid que haya contribuido al área de la seguridad de las Telecomunicaciones.

Viabilidad:

- a) Experiencias anteriores de la Universidad en la impartición de títulos de características similares

No existe en la Universidad de Valladolid una titulación análoga al máster que proponemos. Sin embargo, la ETSI Telecomunicación ofrece el Grado en Ingeniería de Telecomunicación, que es la vía de acceso natural para el máster propuesto, además del Máster en Ingeniería de Telecomunicación, que puede imbricarse con la presente propuesta de forma que los alumnos obtengan dos titulaciones de 90+60 ECTS en dos cursos académicos.

La ETSI Telecomunicación comenzó a impartir titulaciones de la familia de las Telecomunicaciones a partir de 1992. Desde entonces, y partiendo de la titulación original Ingeniero de Telecomunicación, la ETSIT ha impartido numerosas titulaciones de grado medio y superior (de acuerdo a la antigua LRU), así como titulaciones de grado y máster (a partir de la implantación del Plan Bolonia). La ETSI Telecomunicación cuenta, pues, con una experiencia de más de 30 años en la impartición de titulaciones relacionadas con la materia.

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-3117-3cb7-f95c-14d5-f82a-d76b-c883-df94

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymppyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-3117-3cb7-f95c-14d5-f82a-d76b-c883-df94

Nº IAPA 2298 Modelo 7909

b) Capacidad de la universidad para afrontar la nueva titulación:

- ☒ b.1. Si se están ofertando titulaciones relacionadas, grado de complementariedad y experiencia en la rama u ámbito de conocimiento.

La ETSI Telecomunicación cuenta actualmente con la acreditación institucional del Consejo de Universidades, distintivo que poseen muy pocas escuelas de Ingeniería de Telecomunicación, en vigor desde 2019 y actualmente en proceso de renovación. Este sello de calidad supone la renovación de la acreditación de todos los títulos oficiales de la ETSIT, tal y como recoge el RUCT (Registro de Universidades, Centros y Títulos). La acreditación institucional otorga a los centros que la poseen un reconocimiento de la eficiencia en la gestión de la calidad de la formación universitaria que imparten. En la ETSI Telecomunicación, dicha gestión se materializa en un Sistema de Garantía Interna de Calidad que desde 2019 cuenta con el certificado ELENCHOS, concedido por la Agencia para la Calidad del Sistema Universitario de Castilla y León (ACSUCYL), también en vigor y actualmente en proceso de renovación.

El máster que se propone es complementario para con los títulos que ya ofrece la ETSI Telecomunicación en cuanto a que estos no poseen un enfoque centrado en la seguridad de las Telecomunicaciones (de acuerdo, en este sentido, a sus correspondientes órdenes CIN). Sin embargo, y como se ha puesto de manifiesto en secciones anteriores, la seguridad es un área de vital importancia para las Telecomunicaciones en el mundo actual, tal como corroboran diversos organismos públicos y privados citados anteriormente.

- ☐ b.2. En otros casos, prospectiva de alianzas con otras universidades; contratos o compromisos con expertos que asesoren en el proceso y aseguren la implantación.

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-3117-3cb7-f95c-14d5-f82a-d76b-c883-df94

DIRECCIÓN DE VALIDACIÓN

<https://run.gob.es/hsbzvymPyF>

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-3117-3cb7-f95c-14d5-f82a-d76b-c883-df94

Nº IAPA 2298 Modelo 7909

Otra información que avale la necesidad y viabilidad del título:

Dado que el título que proponemos es nuevo, no es posible estimar el número de matriculados que éste tendrá a partir de la experiencia de cursos anteriores, pero sí que podemos acudir a indicios que apuntan a una demanda sólida de titulaciones relacionadas con la seguridad entre el alumnado (y, en particular, con la seguridad de las Telecomunicaciones). Además de los ya expuestos en la sección 2.4, podemos contar los siguientes:

- La Comisión Europea, en su Brújula Digital 2030 , menciona como objetivo lograr que haya 20 millones de especialistas en tecnologías de la información y las comunicaciones empleados, con convergencia entre mujeres y hombres, y cita como referencia que en 2019 existían 7,8 millones.
- Del mismo modo, un segundo objetivo de la Brújula Digital 2030 es conseguir que Europa disponga de su primer ordenador cuántico. En este sentido, el plan de estudios del máster que proponemos contiene dos asignaturas sobre seguridad cuántica.
- El informe «Estado de las Comunicaciones Digitales» de Connect Europe (antes ETNO -- European Telecommunications Network Operators' Association), de 2026 , cita varios operadores de telecomunicación europeos que están invirtiendo activamente en comunicaciones cuánticas y postcuánticas.
- La misma organización, en su informe «Contribución del sector de las telecomunicaciones a la seguridad y resiliencia de Europa» , de 2025, cifra en 300.000 personas el déficit de expertos en seguridad de las Telecomunicaciones.
- OBSERVACIBER (el observatorio de ciberseguridad formado por el INCIBE y el Ontsi), en su informe Análisis y Diagnóstico del Talento de Ciberseguridad en España de 2022 , resalta varios datos de interés:
 - * Los profesionales españoles de la ciberseguridad son valorados internacionalmente.
 - * La Estrategia Nacional de Ciberseguridad 2019 enfatiza la necesidad de apoyar el impulso de la industria cibernética, con mención expresa a la investigación, la innovación y las instituciones educativas.
 - * La oferta de profesionales formados en ciberseguridad asciende a 39.072 personas (en 2022), con una proyección a futuro de 42.283 en 2024, mientras que la demanda es de 63.191 personas (en 2022), con una proyección a futuro de 83.007 personas en 2024.
 - * Uno de los problemas principales problemas detectados es la escasez de profesorado cualificado para impartir formación en ciberseguridad.
 - * La mayoría de los programas de grado y posgrado adolecen de parte práctica (incluyendo prácticas en empresa).

Fdo.:

TITULAR DE LA CONSEJERÍA DE EDUCACIÓNINFORMACIÓN SOBRE DATOS DE CARÁCTER PERSONAL	
Responsable del	Dirección General de Universidades e Investigación
Finalidad del tratamiento	La ordenación de las enseñanzas universitarias en la Comunidad de Castilla y León
Legitimación	Cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos.
Destinatarios	No se cederán datos a terceros, salvo obligación legal
Derechos	Derecho a acceder, rectificar y suprimir los datos, así como otros derechos recogidos en la información adicional.
Información adicional	Puede consultar la información adicional y detallada sobre protección de datos en la Sede Electrónica
CONSEJERÍA/OO.AA/EEPPDPI/DELEGACIÓN TERRITORIAL	CONSEJERÍA DE EDUCACIÓN
CENTRO O UNIDAD ADMINISTRATIVA AL QUE SE DIRIGE:	DIRECCIÓN GENERAL DE UNIVERSIDADES E INVESTIGACIÓN

ÁMBITO- PREFIJO

GEISER

Nº registro

REGAGE26e00037824395

CSV

GEISER-3117-3cb7-f95c-14d5-f82a-d76b-c883-df94

DIRECCIÓN DE VALIDACIÓN

https://run.gob.es/hsbzvymPyF

FECHA Y HORA DEL DOCUMENTO

16/04/2026 14:29:14 Horario peninsular

Validez del documento

Copia Electrónica Auténtica



GEISER-3117-3cb7-f95c-14d5-f82a-d76b-c883-df94

Sr. Rector de la Universidad de Valladolid:

Recientemente hemos conocido el proyecto de implantación del Máster en Seguridad de las Telecomunicaciones que está promoviendo la Escuela Técnica Superior de Ingenieros de Telecomunicación de la universidad que Ud. dirige, y que tendría comienzo, al parecer, en el curso académico 2027-2028.

Como egresados del Grado en Ingeniería de Tecnologías de Telecomunicación, del Grado en Ingeniería de Tecnologías Específicas de Telecomunicación y del Máster Universitario en Ingeniería de Telecomunicación, consideramos que la implantación de este máster es especialmente pertinente, tanto por los contenidos previstos como por el momento en que se pretende lanzar. En relación con los contenidos, estimamos que abordan de manera adecuada y actualizada las principales áreas de seguridad en las telecomunicaciones, incluyendo aspectos clave como la ciberseguridad en distintos tipos de redes, la criptografía aplicada y la respuesta a incidentes. Estos ámbitos no solo resultan altamente relevantes desde el punto de vista técnico, sino que también responden de forma directa a las necesidades emergentes de la industria.

Al respecto del momento en que se promulga, percibimos la seguridad en las comunicaciones como un activo tecnológico de enorme demanda. Consideramos, en consecuencia, que las expectativas de empleabilidad de los egresados de este máster serán elevadas además de que se estará dando una respuesta a una necesidad formativa real.

Por todo ello apoyamos el mencionado proyecto como una vía de gran interés para complementar nuestra formación académica y nos gustaría tener información de su evolución con el mismo fin.

En Valladolid, a 24 de marzo de 2026,

Fdo.

Graduados en Ingeniería de Tecnologías de Telecomunicación

Alejandro González

 SIGNED VIA ILOVEPDF
D78E25DA-4E74-47A8-89F2-497DBA357EEF

Jimena

 SIGNED VIA ILOVEPDF
C13A984C-4A4E-4304-9212-6FAE22030DA4

[Signature]

Alberto M.F.

 SIGNED VIA ILOVEPDF
2082C13B-C088-46F3-B743-E5ED8237CAB3

 SIGNED VIA ILOVEPDF
A5DB37B1-6565-4C92-BA81-7DCEF5B72B52

Gabino

 SIGNED VIA ILOVEPDF
14612135-ED77-46E6-A9DC-E1B1F7DF8060

Victor S

 SIGNED VIA ILOVEPDF
208302EE-6B80-4ABB-AA95-77262CB72D43

Victor R

 SIGNED VIA ILOVEPDF
DBBD327D-D30D-4BB7-80B1-9A9955F634DA

Marco V

 SIGNED VIA ILOVEPDF
746E72FA-7BC4-4505-AB21-F8ED75BA272E

Graduados en Ingeniería de Tecnologías Específicas de Telecomunicación

Alberto González

 SIGNED VIA ILOVEPDF
CF4BF9D8-D282-4306-B298-3F1F11EAE947

Juan Gómez López

 SIGNED VIA ILOVEPDF
0F2FE8BE-0D55-4166-B380-02BE7EDB34F1

[Signature]

 SIGNED VIA ILOVEPDF
2378E3C9-1E32-45AE-A50C-30933D307B34

Iván

 SIGNED VIA ILOVEPDF
B8B886F5-EBD6-46F9-8BF1-70CAEFF4684D

Graduados en Máster Universitario en Ingeniería de Telecomunicación

[Signature]

 SIGNED VIA ILOVEPDF
12C4616A-4E9C-4178-B5DF-D068BD3699D6

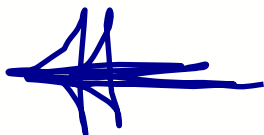
Sr. Rector de la Universidad de Valladolid:

Recientemente he conocido el proyecto de implantación del Máster en Seguridad de las Telecomunicaciones que está promoviendo la Escuela Técnica Superior de Ingenieros de Telecomunicación de la universidad que Ud. dirige, y que tendría comienzo, al parecer, en el curso académico 2027-2028.

Como responsable de fotónica y comunicaciones cuánticas del Photonics Research Lab de la Universitat Politècnica de València, considero que la implantación de este máster es pertinente, tanto por los contenidos previstos como por el momento en que se pretende lanzar. Al respecto de los primeros, los contenidos se encuentran en línea con las principales tendencias en el sector de la seguridad en las comunicaciones. Al respecto del momento en que se promulga, la seguridad en las comunicaciones representa un activo tecnológico de enorme demanda. Considero, en consecuencia, que las expectativas de empleabilidad de los egresados de este máster serán elevadas.

Por todo ello apoyo el mencionado proyecto y me gustaría tener información de su evolución para posibles colaboraciones futuras en cuantas actividades nos sean de interés mutuo.

En Valencia, a 24 de marzo de 2026,



Fdo. José Capmany Franco

Catedrático de Universidad

Universitat Politècnica de València

Sr. Rector de la Universidad de Valladolid:

Recientemente he conocido el proyecto de implantación del Máster en Seguridad de las Telecomunicaciones que está promoviendo la Escuela Técnica Superior de Ingenieros de Telecomunicación de la universidad que Ud. dirige, y que tendría comienzo, al parecer, en el curso académico 2027-2028.

Como Responsable de Seguridad de Red del Servicio Europeo de Acción exterior, considero a título puramente personal que la implantación de este máster es pertinente, tanto por los contenidos previstos como por el momento en que se pretende lanzar. Al respecto de los primeros, los contenidos se encuentran en línea con las principales tendencias en el sector de la seguridad en las comunicaciones. Al respecto del momento en que se promulga, la seguridad en las comunicaciones representa un activo tecnológico de enorme demanda. Considero, en consecuencia, que las expectativas de empleabilidad de los egresados de este máster serán elevadas.

Por todo ello apoyo el mencionado proyecto y me gustaría tener información de su evolución para posibles colaboraciones futuras en cuantas actividades nos sean de interés mutuo.

En Bruselas, a 24 de marzo de 2026,

Fdo. Miguel Herrero Collantes
IT Security Officer
Servicio Europeo de Accion Exterior.

Sr. Rector de la Universidad de Valladolid:

Recientemente he conocido el proyecto de implantación del Máster en Seguridad de las Telecomunicaciones que está promoviendo la Escuela Técnica Superior de Ingenieros de Telecomunicación de la universidad que Ud. dirige, y que tendría comienzo, al parecer, en el curso académico 2027-2028.

Como Director Científico del Vigo Quantum Communication Center y experto en criptografía cuántica, considero que la implantación de este máster es pertinente, tanto por los contenidos previstos como por el momento en que se pretende lanzar. Al respecto de los primeros, los contenidos se encuentran en línea con las principales tendencias en el sector de la seguridad en las comunicaciones. Al respecto del momento en que se promulga, la seguridad en las comunicaciones representa un activo tecnológico de enorme demanda. Considero, en consecuencia, que las expectativas de empleabilidad de los egresados de este máster serán elevadas.

Por todo ello apoyo el mencionado proyecto y me gustaría tener información de su evolución para posibles colaboraciones futuras en cuantas actividades nos sean de interés mutuo.

En Vigo, a 24 de marzo de 2026,

Fdo. Marcos Curty
Catedrático de Universidad
Director Científico del Vigo Quantum Communication Center

Sr. Rector de la Universidad de Valladolid:

Recientemente he conocido el proyecto de implantación del Máster en Seguridad de las Telecomunicaciones que está promoviendo la Escuela Técnica Superior de Ingenieros de Telecomunicación de la universidad que Ud. dirige, y que tendría comienzo, al parecer, en el curso académico 2027-2028.

Como responsable técnico de una Infraestructura Científica de Supercomputación en el ámbito de las Instalaciones Científico-Técnicas Singulares del Estado Español considero que la implantación de este máster es pertinente, tanto por los contenidos previstos como por el momento en que se pretende lanzar. Al respecto de los primeros, los contenidos se encuentran en línea con las principales tendencias en el sector de la seguridad en las comunicaciones. Al respecto del momento en que se promulga, la seguridad en las comunicaciones representa un activo tecnológico de enorme demanda. Considero, en consecuencia, que las expectativas de empleabilidad de los egresados de este máster serán elevadas.

Por todo ello apoyo el mencionado proyecto y me gustaría tener información de su evolución para posibles colaboraciones futuras en cuantas actividades nos sean de interés mutuo.

En Santiago, a 26 de marzo de 2026,



Fdo. Jose Ignacio López Cabido
Director de Infraestructuras Científicas y Apoyo a la Investigación

D. Félix Barrio Juárez
Director General
Instituto Nacional de Ciberseguridad (INCIBE)

Excmo. Sr. Rector Mgfc. D. Antonio Largo Cabrerizo
Universidad de Valladolid

León, 10 de abril de 2026

Excmo. Sr. Rector Magnífico de la Universidad de Valladolid:

Hemos conocido el proyecto de implantación del Máster en Seguridad de las Telecomunicaciones que está promoviendo la Escuela Técnica Superior de Ingenieros de Telecomunicación de la universidad que Ud. dirige, y que tendría comienzo en el curso académico 2027-2028.

Esta entidad considera que la implantación de este máster es pertinente, ya que la seguridad digital representa un activo tecnológico de enorme demanda, motivo por el cual, la ciberseguridad mantiene en los últimos años un déficit creciente de profesionales que puedan atender demanda no satisfecha de talento. Igualmente, valoramos positivamente los contenidos incluidos, que se encuentran en línea con las principales tendencias en el sector de la seguridad en las comunicaciones.

Consideramos, en consecuencia, que las expectativas de empleabilidad de los egresados de este máster serán elevadas, y mostramos nuestro apoyo al mismo.

Fdo. Félix Barrio Juárez
Director General
Instituto Nacional de Ciberseguridad (INCIBE)

Sr. Rector de la Universidad de Valladolid:

Hemos conocido el proyecto de implantación del Máster en Seguridad de las Telecomunicaciones que está promoviendo la Escuela Técnica Superior de Ingenieros de Telecomunicación de la universidad que Ud. dirige, y que tendría comienzo, al parecer, en el curso académico 2027-2028.

Esta entidad considera que la implantación de este máster es pertinente, tanto por los contenidos previstos como por el momento en que se pretende lanzar. Al respecto de los primeros, los contenidos se encuentran en línea con las principales tendencias en el sector de la seguridad en las comunicaciones. Al respecto del momento en que se promulga, la seguridad en las comunicaciones representa un activo tecnológico de enorme demanda. Consideramos, en consecuencia, que las expectativas de empleabilidad de los egresados de este máster serán elevadas.

Por todo ello apoyamos el mencionado proyecto y nos gustaría tener información de su evolución para posibles colaboraciones futuras en cuantas actividades sean de interés para ambas partes.

Valladolid, 9 de abril de 2026



Fdo. Miguel Ángel Hernández Bajo
Director NTT DATA Castilla y León

Sr. Rector de la Universidad de Valladolid:

Hemos conocido el proyecto de implantación del Máster en Seguridad de las Telecomunicaciones que está promoviendo la Escuela Técnica Superior de Ingenieros de Telecomunicación de la universidad que Ud. dirige, y que tendría comienzo previsto en el curso académico 2027-2028.

La abajo firmante, en representación del equipo directivo de la Escuela de Ingeniería Informática de Valladolid, considera que la implantación de este máster es pertinente, tanto por los contenidos previstos como por el momento en que se pretende lanzar. Al respecto de los primeros, los contenidos se encuentran en línea con las principales tendencias en el sector de la seguridad en las telecomunicaciones. Al respecto del momento en que se promulga, la seguridad en las telecomunicaciones representa un activo tecnológico de enorme demanda. Consideramos, en consecuencia, que las expectativas de empleabilidad de los egresados de este máster serán elevadas.

Por todo ello apoyamos el mencionado proyecto y nos gustaría tener información de su evolución para posibles colaboraciones futuras en cuantas actividades sean de interés para ambas partes.

Valladolid, a 10 de abril de 2026

Fdo. Alejandra Martínez Monés
Directora de la Escuela de Ingeniería Informática de Valladolid
Universidad de Valladolid



Sr. Rector de la Universidad de Valladolid:

Hemos conocido el proyecto de implantación del Máster en Seguridad de las Telecomunicaciones que está promoviendo la Escuela Técnica Superior de Ingenieros de Telecomunicación de la universidad que Ud. dirige, y que tendría comienzo, al parecer, en el curso académico 2027-2028.

Esta entidad considera que la implantación de este máster es pertinente, tanto por los contenidos previstos como por el momento en que se pretende lanzar. Al respecto de los primeros, los contenidos se encuentran en línea con las principales tendencias en el sector de la seguridad en las comunicaciones. Al respecto del momento en que se promulga, la seguridad en las comunicaciones representa un activo tecnológico de enorme demanda. Consideramos, en consecuencia, que las expectativas de empleabilidad de los egresados de este máster serán elevadas.

Por todo ello apoyamos el mencionado proyecto y nos gustaría tener información de su evolución para posibles colaboraciones futuras en cuantas actividades sean de interés para ambas partes.

Valladolid, 24 de marzo de 2026

Julián Picapiedra Puga
Responsable Relaciones Externas Castilla y León

Sr. Rector de la Universidad de Valladolid:

Hemos conocido el proyecto de implantación del Máster en Seguridad de las Telecomunicaciones que está promoviendo la Escuela Técnica Superior de Ingenieros de Telecomunicación de la universidad que Ud. dirige, y que tendría comienzo, al parecer, en el curso académico 2027-2028.

Esta entidad considera que la implantación de este máster es pertinente, tanto por los contenidos previstos como por el momento en que se pretende lanzar. Al respecto de los primeros, los contenidos se encuentran en línea con las principales tendencias en el sector de la seguridad en las comunicaciones. Al respecto del momento en que se promulga, la seguridad en las comunicaciones representa un activo tecnológico de enorme demanda. Consideramos, en consecuencia, que las expectativas de empleabilidad de los egresados de este máster serán elevadas.

Por todo ello apoyamos el mencionado proyecto y nos gustaría tener información de su evolución para posibles colaboraciones futuras en cuantas actividades sean de interés para ambas partes.

Valladolid, 24 de marzo de 2026



Fdo. Leticia Picado Alonso
Responsable de SW y Tecnología en el Centro de I+D+i - Renault España

Sr. Rector de la Universidad de Valladolid:

Hemos conocido el proyecto de implantación del Máster en Seguridad de las Telecomunicaciones que está promoviendo la Escuela Técnica Superior de Ingenieros de Telecomunicación de la universidad que Ud. dirige, y que tendría comienzo, al parecer, en el curso académico 2027-2028.

Esta entidad considera que la implantación de este máster es pertinente, tanto por los contenidos previstos como por el momento en que se pretende lanzar. Al respecto de los primeros, los contenidos se encuentran en línea con las principales tendencias en el sector de la seguridad en las comunicaciones. Al respecto del momento en que se promulga, la seguridad en las comunicaciones representa un activo tecnológico de enorme demanda. Consideramos, en consecuencia, que las expectativas de empleabilidad de los egresados de este máster serán elevadas.

Por todo ello apoyamos el mencionado proyecto y nos gustaría tener información de su evolución para posibles colaboraciones futuras en cuantas actividades sean de interés para ambas partes.

Valladolid, 25 de marzo de 2026

Fdo. Javier Alonso Sánchez
Director Autonómico CyL

Normativa	Este documento tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de original (art. 27 Ley 39/2015).	Estado	Fecha y hora	
Firmado por	Enrique Berzal de la Rosa - Secretario del Consejo Social	Firmado	22/07/2026 13:25:22	
	Luis Nicanor Diaz Gonzalez - Presidente Comisión Académica Consejo Social	Firmado	22/07/2026 13:24:44	
URL de verificación	https://sede.uva.es/validador-documentos?code=CvEI6oUF5vzcX8vNpw8EEQ%3D%3D			