IMPRESO SOLICITUD PARA VERIFICACIÓN DE TÍTULOS OFICIALES

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

De conformidad con el Real Decreto 822/2021, de 28 de septiembre, por el que se establece la organización de las enseñanzas universitarias y del procedimiento de aseguramiento de su calidad.

UNIVERSIDAD SOLICITANTE	CENTRO	CÓDIGO CENTRO
Universidad de Salamanca	Facultad de Ciencias	37007912
	Instituto Universitario de Estudios sobre la Ciencia y la Tecnología	37010303

NIVEL	DENOMINACIÓN CORTA
Máster	Ciberseguridad

DENOMINACIÓN ESPECÍFICA
Máster Universitario en Ciberseguridad por la Universidad de Salamanca

NIVEL MECES
3

RAMA DE CONOCIMIENTO	ÁMBITO DE CONOCIMIENTO	CONJUNTO
Ingeniería y Arquitectura	Ingeniería informática y de sistemas	No

SOLICITANTE	
NOMBRE Y APELLIDOS	**CARGO**
Javier Peña González	Director Académico de Postgrado

REPRESENTANTE LEGAL	
NOMBRE Y APELLIDOS	**CARGO**
María Teresa Escribano Bailón	Delegada del Rector para Estudios de Postgrado y Formación Permanente

RESPONSABLE DEL TÍTULO	
NOMBRE Y APELLIDOS	**CARGO**
PABLO CHAMOSO SANTOS	Director del Máster

2. DIRECCIÓN A EFECTOS DE NOTIFICACIÓN

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

DOMICILIO	CÓDIGO POSTAL	MUNICIPIO	TELÉFONO
Hospedería Fonseca, Fonseca, nº 2, 1ª planta	37002	Salamanca	686443690
E-MAIL	**PROVINCIA**		**FAX**
delegadapostgrado@usal.es	Salamanca		

3. PROTECCIÓN DE DATOS PERSONALES

De acuerdo con lo previsto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se informa que los datos solicitados en este impreso son necesarios para la tramitación de la solicitud y podrán ser objeto de tratamiento automatizado. La responsabilidad del fichero automatizado corresponde al Consejo de Universidades. Los solicitantes, como cedentes de los datos podrán ejercer ante el Consejo de Universidades los derechos de información, acceso, rectificación y cancelación a los que se refiere el Título III de la citada Ley Orgánica 3/2018, de 5 de diciembre, sin perjuicio de lo dispuesto en otra normativa que ampare los derechos como cedentes de los datos de carácter personal.

El solicitante declara conocer los términos de la convocatoria y se compromete a cumplir los requisitos de la misma, consintiendo expresamente la notificación por medios telemáticos a los efectos de lo dispuesto en el artículo 43 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

	En: Salamanca, AM 30 de septiembre de 2024
	Firma: Representante legal de la Universidad

1. DESCRIPCIÓN, OBJETIVOS FORMATIVOS Y JUSTIFICACIÓN DEL TÍTULO

1.1-1.3 DENOMINACIÓN, ÁMBITO, MENCIONES/ESPECIALIDADES Y OTROS DATOS BÁSICOS

NIVEL	DENOMINACIÓN ESPECIFICA	CONJUNTO	CONVENIO	CONV. ADJUNTO
Máster	Máster Universitario en Ciberseguridad por la Universidad de Salamanca	No		Ver Apartado 1: Anexo 1.

RAMA
Ingeniería y Arquitectura
ÁMBITO
Ingeniería informática y de sistemas
AGENCIA EVALUADORA
Agencia para la Calidad del Sistema Universitario de Castilla y León
LISTADO DE ESPECIALIDADES
No existen datos
MENCIÓN DUAL
No

1.4-1.9 UNIVERSIDADES, CENTROS, MODALIDADES, CRÉDITOS, IDIOMAS Y PLAZAS

UNIVERSIDAD SOLICITANTE
Universidad de Salamanca
LISTADO DE UNIVERSIDADES

CÓDIGO	UNIVERSIDAD
014	Universidad de Salamanca
LISTADO DE UNIVERSIDADES EXTRANJERAS	
CÓDIGO	**UNIVERSIDAD**
No existen datos	

CRÉDITOS TOTALES	CRÉDITOS DE COMPLEMENTOS FORMATIVOS	CRÉDITOS EN PRÁCTICAS EXTERNAS
60	0	0
CRÉDITOS OPTATIVOS	**CRÉDITOS OBLIGATORIOS**	**CRÉDITOS TRABAJO FIN GRADO/ MÁSTER**
15	30	15

1.4-1.9 Universidad de Salamanca

1.4-1.9.1 CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS			
CÓDIGO	**CENTRO**	**CENTRO RESPONSABLE**	**CENTRO ACREDITADO INSTITUCIONALMENTE**
37007912	Facultad de Ciencias	No	No
37010303	Instituto Universitario de Estudios sobre la Ciencia y la Tecnología	Si	No

1.4-1.9.2 Facultad de Ciencias

1.4-1.9.2.1 Datos asociados al centro

MODALIDADES DE ENSEÑANZA EN LAS QUE SE IMPARTE EL TITULO		
PRESENCIAL	**SEMIPRESENCIAL/HÍBRIDA**	**A DISTANCIA/VIRTUAL**
No	Sí	No
PLAZAS POR MODALIDAD		
	30	
NÚMERO TOTAL DE PLAZAS	**NÚMERO DE PLAZAS DE NUEVO INGRESO PARA PRIMER CURSO**	

30	30	
IDIOMAS EN LOS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

1.4-1.9.2 Instituto Universitario de Estudios sobre la Ciencia y la Tecnología

1.4-1.9.2.1 Datos asociados al centro

MODALIDADES DE ENSEÑANZA EN LAS QUE SE IMPARTE EL TITULO		
PRESENCIAL	**SEMIPRESENCIAL/HÍBRIDA**	**A DISTANCIA/VIRTUAL**
No	Sí	No
PLAZAS POR MODALIDAD		
	30	
NÚMERO TOTAL DE PLAZAS	**NÚMERO DE PLAZAS DE NUEVO INGRESO PARA PRIMER CURSO**	
30	30	
IDIOMAS EN LOS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

1.10 JUSTIFICACIÓN

JUSTIFICACIÓN DEL INTERÉS DEL TÍTULO Y CONTEXTUALIZACIÓN
Ver Apartado 1: Anexo 6.

1.11-1.13 OBJETIVOS FORMATIVOS, ESTRUCTURAS CURRICULARES ESPECÍFICAS Y DE INNOVACIÓN DOCENTE

OBJETIVOS FORMATIVOS

1.3. Objetivos formativos

1.3.1.a) Principales objetivos formativos del título

El objetivo es la formación de profesionales con experiencia en el marco de las TIC que deseen especializar su perfil, de forma que adquieran los conocimientos técnicos para diseñar, desarrollar, evaluar, auditar la seguridad en sistemas informáticos, así como para la evaluación y la propuesta de mejora de las políticas de seguridad en un entorno empresarial a la luz de la legislación vigente. La principal finalidad es desarrollar un perfil de profesionales especialistas en ciberseguridad, sector para el que se ha detectado una necesidad real y que, por tanto, tendrán una rápida incorporación en el mercado laboral nacional e internacional.

Específicamente el programa profundiza en la formación de expertos en seguridad en equipos informáticos, seguridad en redes, peritaje informático, auditoría de seguridad en sistemas informáticos, etcétera, y se propone abordar el tema de la seguridad desde un punto de vista tecnológico e informático~~, en combinación con aspectos jurídicos, éticos, sociales, de economía y de empresa~~.

A continuación, se describen específicamente algunos de los objetivos principales del título:

- Proporcionar una formación avanzada e interdisciplinar sobre las amenazas y debilidades más comunes en los entornos digitales, sobre las técnicas y metodologías para prevenir, detectar y responder a incidentes de seguridad, así como las regulaciones y estándares nacionales e internacional relacionados con la ciberseguridad.

- Desarrollar en los futuros egresados la capacidad para proponer mejoras en las políticas, en estrategias de seguridad informática de las organizaciones y en la aplicación de medidas correctivas y preventivas.
- ~~Formar futuros profesionales capaces de integrar conocimientos tecnológicos, jurídicos, sociales, éticos, económicos y empresariales en el ámbito de la ciberseguridad.~~
- Ofrecer a los estudiantes un entorno de aprendizaje práctico, basado en situaciones reales y apoyado en los últimos avances y desarrollos tecnológicos realizados por empresas del sector de la ciberseguridad y por grupos de investigación implicados en la docencia.
- **Formar profesionales capaces de diseñar, implantar y evaluar protocolos de seguridad para prevenir y proteger ante ataques informáticos en equipos informáticos y en redes.**
- **Formar expertos técnicos en ciberseguridad que respondan a las demandas actuales y futuras que presenta la sociedad de la información sobre la Inteligencia Artificial (IA) el Internet de las cosas (IoT) y el Aprendizaje Automático (Machine Learning).**

Por otro lado, el presente Máster también quiere crear una estructura de reflexión que permita fomentar el interés en los egresados para continuar sus estudios en los programas de doctorado **relacionados con el área** ~~de las diferentes áreas~~ de conocimiento, ~~que contribuyen al plan de estudios, siempre~~ manteniendo como objeto de investigación la ciberseguridad. ~~en sus múltiples facetas.~~

1.3.1.b). Objetivos formativos de las menciones o especialidades

No procede.

~~El interés por la seguridad en Internet y por promover la detección y prevención de riesgos de los sistemas de información que pueden ser blanco de ataques no es del dominio exclusivo de los profesionales de un área concreta. Por ello el programa de máster contempla dos especialidades:~~

1. ~~**Especialidad en Tecnología:**~~

~~Los objetivos formativos que específicos de esta especialidad son:~~
- ~~Formar profesionales capaces de diseñar, implantar y evaluar protocolos de seguridad para prevenir y proteger ante ataques informáticos en equipos informáticos y en redes.~~
- ~~Formar expertos técnicos en ciberseguridad que respondan a las demandas actuales y futuras que presenta la sociedad de la información sobre la Inteligencia Artificial (IA) el Internet de las cosas (IoT) y el Aprendizaje Automático (Machine Learning).~~

1. ~~**Especialidad en Aspectos Jurídico-sociales:**~~

~~Los objetivos formativos que específicos de esta especialidad son:~~
- ~~Formar profesionales capaces de abordar los riesgos y desafíos de la ciberseguridad desde una perspectiva jurídico y social.~~
- ~~Formar expertos en prevenir y blindar la protección de la seguridad de los activos informáticos y en resolver problemas de ciberseguridad desde un enfoque criminológico y legal.~~

~~En ambos itinerarios formativos de especialidad, el estudiante contará con varias asignaturas optativas para fundamentar sus conocimientos específicos en el contexto social y económico en el que la ciberseguridad se ha vuelto una seña de identidad de la sociedad del conocimiento.~~

1.3.2. En su caso, estructuras curriculares específicas y justificación de sus objetivos

No procede

ESTRUCTURAS CURRICULARES ESPECÍFICAS Y ESTRATEGIAS METODOLÓGICAS DE INNOVACIÓN DOCENTE

1.14 PERFILES FUNDAMENTALES DE EGRESO Y PROFESIONES REGULADAS

PERFILES DE EGRESO

Ver apartado 1.10 Justificación (pdf)

HABILITA PARA EL EJERCICIO DE PROFESIONES REGULADAS	No	

NO ES CONDICIÓN DE ACCESO PARA TITULO PROFESIONAL

2. RESULTADOS DEL PROCESO DE FORMACIÓN Y DE APRENDIZAJE

RESULTADOS DEL PROCESO DE FORMACIÓN Y DE APRENDIZAJE

C1 - Relacionar los fundamentos teóricos de la ciberseguridad, incluyendo conceptos básicos de la información, criptografía, redes y sistemas operativos para proteger la integridad y la confidencialidad de la información. TIPO: Conocimientos o contenidos

C10 - Caracterizar normativas y regulaciones en materia de protección de datos, cumplimiento normativo y responsabilidad jurídica en casos de incidentes de seguridad. TIPO: Conocimientos o contenidos

C2 - Identificar las amenazas y vulnerabilidades más comunes en entornos digitales, así como las técnicas y metodologías utilizadas para prevenir, detectar y responder a incidentes de seguridad. TIPO: Conocimientos o contenidos

C3 - Identificar las leyes, regulaciones y estándares nacionales e internacionales relacionados con la ciberseguridad. TIPO: Conocimientos o contenidos

C4 - Valorar el impacto de la ciberseguridad sobre la economía, la empresa y la ciudadanía. TIPO: Conocimientos o contenidos

C5 - Examinar aspectos interdisciplinarios de la ciberseguridad, como la gestión de riesgos, la ética y la privacidad, con el fin de proporcionar una visión integral de la disciplina. TIPO: Conocimientos o contenidos

C6 - Identificar protocolos de seguridad contra amenazas informáticas a partir de conocimientos especializados en ciberseguridad, centrándose en su desarrollo, implementación y evaluación. TIPO: Conocimientos o contenidos
C7 - Describir los aspectos técnicos e informáticos de la seguridad, incluyendo el diseño seguro de sistemas, la seguridad en redes y comunicaciones, la protección de datos y la gestión de incidentes de seguridad. TIPO: Conocimientos o contenidos
C8 - Distinguir las últimas tendencias y tecnologías en el campo de la ciberseguridad, como el Internet de las cosas (IoT), la inteligencia artificial (IA) y el aprendizaje automático (Machine Learning), para estar preparados ante los desafíos futuros. TIPO: Conocimientos o contenidos
C9 - Recopilar información pertinente de la legislación nacional e internacional que afecta a los sistemas de información y la ciberseguridad, así como en los aspectos legales y sociales relacionados. TIPO: Conocimientos o contenidos
H1 - Implementar medidas de seguridad en diferentes entornos y sistemas, incluyendo la configuración de firewalls, la gestión de accesos, la detección de intrusiones y el análisis forense digital. TIPO: Habilidades o destrezas
H10 - Desarrollar habilidades de investigación y análisis en materia de delitos informáticos para comprender los motivos e impacto en el entorno digital. TIPO: Habilidades o destrezas
H11 - Mejorar en habilidades de comunicación y argumentación legal, y desarrollar habilidades éticas y profesionales para enfrentar los desafíos éticos y legales en el ámbito de la ciberseguridad. TIPO: Habilidades o destrezas
H2 - Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad de sistemas y redes, así como para llevar a cabo pruebas de penetración y auditorías de seguridad. TIPO: Habilidades o destrezas
H3 - Analizar y evaluar los riesgos de seguridad en entornos digitales, identificando posibles debilidades y proponiendo soluciones efectivas. TIPO: Habilidades o destrezas
H4 - Trabajar en equipo para colaborar con otros profesionales de la ciberseguridad, así como para educar a usuarios finales y promover buenas prácticas de seguridad. TIPO: Habilidades o destrezas
H5 - Trabajar en equipo en entornos multidisciplinares, para el análisis y resolución de problemas concretos de inseguridad en equipos y sistemas informáticos. TIPO: Habilidades o destrezas
H6 - Desarrollar habilidades técnicas para implementar soluciones de seguridad en sistemas y redes, realizar pruebas de penetración y responder a incidentes de seguridad de manera eficiente. TIPO: Habilidades o destrezas
H7 - Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad de sistemas informáticos y redes. TIPO: Habilidades o destrezas
H8 - Desarrollar habilidades de análisis y resolución de problemas en el ámbito de la seguridad informática, así como habilidades de comunicación y trabajo en equipo. TIPO: Habilidades o destrezas
H9 - Adquirir habilidades para analizar y evaluar los aspectos legales de la ciberseguridad, asesorar en la implementación de políticas y normatives y colaborar con equipos técnicos en la resolución de casos jurídicos relacionados con la ciberseguridad. TIPO: Habilidades o destrezas
K1 - Diseñar, desarrollar, evaluar y asegurar la seguridad de un sistema informático, con independencia de su tamaño y características. TIPO: Competencias
K2 - Desarrollar, implantar y mantener sistemas, servicios y aplicaciones informáticas de seguridad empleando los métodos de la ingeniería del software como instrumento para el aseguramiento de su calidad. TIPO: Competencias
K3 - Analizar, diseñar, construir y mantener aplicaciones de seguridad de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados en cada caso, según el entorno de despliegue (entorno web, escritorio). TIPO: Competencias
K4 - Diseñar, desplegar, administrar de forma segura y fiable servicios en una red de ordenadores. TIPO: Competencias
K5 - Validar la garantía y seguridad de los sistemas informáticos pertinentes, como redes locales, servidores, bases de datos y sistemas de gestión de información. TIPO: Competencias
K6 - Diseñar políticas de monitorización y copia de segura, para la recuperación de sistemas y el aseguramiento en la información en caso de malfuncionamiento. TIPO: Competencias
K7 - Elaborar la política de seguridad de una empresa. TIPO: Competencias
K8 - Auditar las políticas de seguridad de una empresa a todos los niveles (sistemas, red, información, etc.). TIPO: Competencias
K9 - Aplicar las restricciones legales asociados a la seguridad informática sobre el manejo y procesamiento de datos personales. TIPO: Competencias

3. ADMISIÓN, RECONOCIMIENTO Y MOVILIDAD

3.1 REQUISITOS DE ACCESO Y PROCEDIMIENTOS DE ADMISIÓN

3. Admisión, reconocimiento y movilidad

3.1. Requisitos de acceso y procedimientos de admisión de estudiantes

Perfil de ingreso recomendado

Este Máster Universitario está dirigido, ~~sin ser un requisito excluyente~~ y a evaluar en el proceso de admisión, a **perfiles en posesión de al menos una de las siguientes titulaciones:** ~~graduados en Ingeniería Informática o similar si opta por la especialidad en Tecnología; a graduados en titulaciones de Ciencias Sociales o Jurídicas si opta por la especialidad en Aspectos Jurídico-sociales; y a graduados en cualquier ingeniería o carrera de la rama de ciencias o ciencias sociales con conocimientos o experiencia laboral acreditada superior a 5 años en el ámbito de la ciberseguridad.~~

- **Grado en Ingeniería Informática (o titulación equivalente).**
- **Grado en Ingeniería Informática en Sistemas de Información (o titulación equivalente).**
- **Grado en Sistemas de Información (o titulación equivalente).**
- **Grado en Ingeniería del Software (o titulación equivalente).**
- **Grado en Inteligencia Artificial (o titulación equivalente).**
- **Grado en Ingeniería de Tecnología y Servicios de Telecomunicación (o titulación equivalente).**
- **Grado en Ingeniería Telemática (o titulación equivalente).**
- **Grado en Ingeniería de los Computadores (o titulación equivalente).**
- **Másteres habilitantes para la profesión de Ingeniero de Telecomunicación.**
- **Másteres Universitarios relacionados con la Ingeniería Informática.**

Además, se precisa:

- Tener un nivel de español, en aquellos casos en que su lengua materna no sea este idioma, de C1 del Marco Común Europeo de Referencia para Lenguas (MCERL).
- Tener al menos un nivel de inglés equivalente al nivel B2 del MCERL.
- Disponer de conocimientos básicos en informática y programación.
- Disponer de equipo informático con conexión a internet y equipamiento estándar para seguir una videoconferencia.
- Disponer de una cámara independiente (no integrada en el equipo informático), bien cámara web, bien tablet o bien smartphone con cámara

Requisitos de acceso

Los requisitos de acceso son los generales que figuran en el artículo 18 del Real Decreto RD 822/2021, (accesible a través de la dirección **https://www.boe.es/buscar/act.php?id=BOE-A-2021-15781**).

Los estudiantes cuyo título de licenciado o graduado provenga de una Institución que no se encuentre dentro del EEES podrán tener acceso al máster, previa autorización de la Universidad, para lo que deberán acreditar que los estudios realizados alcanzan un nivel de formación equivalente a los correspondientes títulos españoles de Grado y que le facultan para realizar estudios de máster en el país que emitió el título. El estudiante deberá presentar la solicitud de equivalencia en la Sección de Estudios de Grado y Máster. El acceso por esta vía no implica la homologación del título previo con el que se solicitó el ingreso al máster y tampoco supone su reconocimiento a otros efectos, simplemente concede la posibilidad de cursar estas enseñanzas de Máster.

Dentro del proceso y mecanismos de difusión de los estudios de posgrado de la Universidad de Salamanca, con carácter previo, se ofrecerá información sobre el programa formativo y las distintas salidas profesionales a los colectivos interesados. Toda la información está adecuadamente descrita en la siguiente página web pública de la Universidad de Salamanca: **https://www.usal.es/preinscripcion-masteres**.

3.1.b) Procedimiento y criterios de admisión

Las personas interesadas en la admisión en el máster deberán formalizar la correspondiente solicitud, acreditando que están en posesión de alguno de los títulos que permite el ingreso en estos estudios de postgrado (ver **http://www.usal.es/preinscripcion-Másteres**).

La Comisión Académica será la encargada de evaluar las solicitudes y estará formada por el/la director/a del Máster, cuatro profesores que impartan docencia en el mismo, un representante del PAS y dos estudiantes. Los profesores y representante del PAS serán renovados cada cuatro años y los estudiantes cada año; la renovación tendrá lugar en sesión ordinaria de la Comisión Académica.

La admisión de los estudiantes, hasta completar las plazas ofertadas, se realizará atendiendo al orden que se ocupe en un listado (ordenado de mayor a menor puntuación), resultante de la aplicación de los siguientes criterios de valoración objetiva:

- Expediente académico: 50%
- Dominio de inglés (nivel mínimo B2): 20%
- Actividad profesional previa: 15%
- Otros méritos (como, por ejemplo, disponer de certificaciones): 15%

Cuando exista igualdad de puntuación, después de haber valorado todos los elementos mencionados, se procederá a realizar una entrevista personal para decidir la admisión o exclusión de los candidatos empatados.

El estudiante deberá acompañar a su solicitud:

- Curriculum Vitae.
- Expediente académico de la titulación principal que permite el acceso al máster oficial con indicación de la nota media ponderada o, en su defecto, datos sobre la nota media de la titulación, incluyendo la escala de evaluación.
- Acreditación, en su caso, de que se posee otra u otras titulaciones universitarias oficiales que también permitirían el acceso al máster.
- Acreditación, en su caso, de experiencia profesional relacionada con el contenido del máster
- Acreditación de un nivel C1 de dominio del español para los hablantes no nativos.
- En caso de disponer de ella, certificación oficial que acredite los conocimientos de inglés (en caso de no disponer de certificado, se evaluará el nivel de inglés mediante entrevista personal).
- Documentación que acredite los otros méritos consignados en el Curriculum Vitae.

También podrá incorporar, de forma opcional, las cartas de recomendación que considere pertinentes.

Se precisa tener un nivel de español, en aquellos casos en que su lengua materna no sea este idioma, de C1 del Marco Común Europeo de Referencia para Lenguas (MCERL).

3.2 CRITERIOS PARA EL RECONOCIMIENTO Y TRANSFERENCIAS DE CRÉDITOS	
Reconocimiento de Créditos cursados en centros de formación profesional de grado superior	
MÍNIMO	**MÁXIMO**
0	0
Adjuntar Convenio	
Reconocimiento de Créditos Cursados en Títulos Propios	
MÍNIMO	**MÁXIMO**
0	9
Adjuntar Título Propio	
Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional	
MÍNIMO	**MÁXIMO**
0	9
DESCRIPCIÓN	

3.2. Criterios para el reconocimiento y transferencias de créditos

Los criterios generales, la normativa (Reglamento sobre reconocimiento y transferencia de créditos en la Universidad de Salamanca, aprobado en Consejo de Gobierno de 24/03/2023) y los formularios sobre el reconocimiento y transferencia de ECTS en la USAL están en: **https://www.usal.es/reconocimiento-y-transferencia-de-creditos**

De forma general, será de aplicación lo dispuesto en el **REGLAMENTO SOBRE RECONOCIMIENTO Y TRANSFERENCIA DE CRÉDITOS EN LA UNIVERSIDAD DE SALAMANCA (Aprobado por el Consejo de Gobierno de 24 de marzo de 2023)**, en adelante y en este apartado simplemente #Reglamento#.

Reconocimiento de ECTS cursados por Acreditación de Experiencia Laboral y Profesional.

- Nº mínimo de ECTS reconocidos: 0
- Nº máximo de ECTS reconocidos: 9

Específicamente, para el reconocimiento de ECTS cursados por Acreditación de Experiencia Laboral y Profesional se procederá, en su caso, a la valoración de la experiencia profesional acreditada convenientemente por el estudiante matriculado en el Máster, aportada junto a su solicitud de ingreso. Para ello se considerará el tipo de institución o empresa en la que se ha trabajado, la duración de dicho trabajo y el puesto desempeñado; siempre que se trate de un trabajo relacionado con la experiencia aportada en el *Curriculum Vitae*. La experiencia profesional permitirá reconocer una o varias asignaturas. ~~La experiencia profesional permitirá reconocer una o varias asignaturas.~~

Reconocimiento de ECTS cursados en Formación Permanente, Títulos Propios inclusive:

- Nº mínimo ECTS reconocidos: 0
- Nº máximo ECTS reconocidos: 9

Se podrán reconocer créditos obtenidos en títulos propios de universidad, ~~incluido~~ **en especial** el Título Propio de Máster de Formación Permanente en Ciberseguridad de la Universidad de Salamanca, que hayan sido superados por el estudiante matriculado en el presente Máster Universitario siempre que se acredite, en el certificado de la universidad de procedencia, que la formación a reconocer forma parte de la oferta de formación permanente en los términos descritos en el artículo 37 del RD 822/2021; que certifique la superación de los créditos cuyo reconocimiento se solicita, junto al programa de contenidos y actividades cursados, que debe ser coincidente con una o varias materias de las que se compone el presente Máster Universitario.

Además, en el reconocimiento de créditos, se tendrá en cuenta el Artículo 12.4 del Reglamento de la USAL, el cual dispone que, con carácter general, los créditos reconocidos a partir de la formación permanente, combinado con el procedente de la experiencia profesional o laboral, no podrá superar, globalmente, el quince por ciento del total de 60 ECTS del plan de estudios del Máster de Ciberseguridad.

Complementos de formación para Máster

No existen complementos formativos.

—

REGLAMENTO SOBRE RECONOCIMIENTO Y TRANSFERENCIA DE CRÉDITOS EN LA UNIVERSIDAD DE SALAMANCA (Aprobado por el Consejo de Gobierno de 24 de marzo de 2023), **https://campus.usal.es/~gesacad/coordinacion/REGLAMENTO_Reconocimiento_y_Transferencia_de_creditos_CG_20230324.pdf** (consultado en enero de 2024)

3.3 MOVILIDAD DE LOS ESTUDIANTES PROPIOS Y DE ACOGIDA

3.3. Procedimientos para la organización de la movilidad de los estudiantes propios y de acogida

La Universidad de Salamanca ofrece una amplia gama de programas de movilidad para estudiantes de máster, facilitando intercambios nacionales e internacionales y experiencias enriquecedoras en el extranjero. A través del Servicio de Relaciones Internacionales, se promueve la colaboración con instituciones globales y se brindan oportunidades como becas Erasmus y otros programas de intercambio.

En el ámbito nacional, las becas SICUE (Sistema de Intercambio entre Centros Universitarios Españoles), proporcionan a los estudiantes la oportunidad de cursar parte de sus estudios en una universidad diferente dentro del territorio español.

Para más información sobre estos programas y cómo participar, visita la página web de la Universidad de Salamanca sobre Programas de Movilidad (**https://www.usal.es/movilidad**) o consulta el portal específico de becas SICUE (https://becas.usal.es/sicue.htm).

—

4. PLANIFICACIÓN DE LAS ENSEÑANZAS

4.1 ESTRUCTURA BÁSICA DE LAS ENSEÑANZAS		
DESCRIPCIÓN DEL PLAN DE ESTUDIOS		
Ver Apartado 4: Anexo 1.		
4.1 SIN NIVEL 1		
NIVEL 2: Fundamentos teóricos. Ciberseguridad y ciberinteligencia		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	15	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
15		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Gestión y administración de la ciberseguridad		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Ciberinteligencia		

4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Aspectos legales de la ciberseguridad		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
3		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
C1 - Relacionar los fundamentos teóricos de la ciberseguridad, incluyendo conceptos básicos de la información, criptografía, redes y sistemas operativos para proteger la integridad y la confidencialidad de la información. TIPO: Conocimientos o contenidos		
C10 - Caracterizar normativas y regulaciones en materia de protección de datos, cumplimiento normativo y responsabilidad jurídica en casos de incidentes de seguridad. TIPO: Conocimientos o contenidos		
C2 - Identificar las amenazas y vulnerabilidades más comunes en entornos digitales, así como las técnicas y metodologías utilizadas para prevenir, detectar y responder a incidentes de seguridad. TIPO: Conocimientos o contenidos		
C3 - Identificar las leyes, regulaciones y estándares nacionales e internacionales relacionados con la ciberseguridad. TIPO: Conocimientos o contenidos		
C5 - Examinar aspectos interdisciplinarios de la ciberseguridad, como la gestión de riesgos, la ética y la privacidad, con el fin de proporcionar una visión integral de la disciplina. TIPO: Conocimientos o contenidos		
C8 - Distinguir las últimas tendencias y tecnologías en el campo de la ciberseguridad, como el Internet de las cosas (IoT), la inteligencia artificial (IA) y el aprendizaje automático (Machine Learning), para estar preparados ante los desafíos futuros. TIPO: Conocimientos o contenidos		
C9 - Recopilar información pertinente de la legislación nacional e internacional que afecta a los sistemas de información y la ciberseguridad, así como en los aspectos legales y sociales relacionados. TIPO: Conocimientos o contenidos		
H3 - Analizar y evaluar los riesgos de seguridad en entornos digitales, identificando posibles debilidades y proponiendo soluciones efectivas. TIPO: Habilidades o destrezas		
H4 - Trabajar en equipo para colaborar con otros profesionales de la ciberseguridad, así como para educar a usuarios finales y promover buenas prácticas de seguridad. TIPO: Habilidades o destrezas		
C6 - Identificar protocolos de seguridad contra amenazas informáticas a partir de conocimientos especializados en ciberseguridad, centrándose en su desarrollo, implementación y evaluación. TIPO: Conocimientos o contenidos		
C7 - Describir los aspectos técnicos e informáticos de la seguridad, incluyendo el diseño seguro de sistemas, la seguridad en redes y comunicaciones, la protección de datos y la gestión de incidentes de seguridad. TIPO: Conocimientos o contenidos		
H2 - Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad de sistemas y redes, así como para llevar a cabo pruebas de penetración y auditorías de seguridad. TIPO: Habilidades o destrezas		
H11 - Mejorar en habilidades de comunicación y argumentación legal, y desarrollar habilidades éticas y profesionales para enfrentar los desafíos éticos y legales en el ámbito de la ciberseguridad. TIPO: Habilidades o destrezas		

H5 - Trabajar en equipo en entornos multidisciplinares, para el análisis y resolución de problemas concretos de inseguridad en equipos y sistemas informáticos. TIPO: Habilidades o destrezas
H6 - Desarrollar habilidades técnicas para implementar soluciones de seguridad en sistemas y redes, realizar pruebas de penetración y responder a incidentes de seguridad de manera eficiente. TIPO: Habilidades o destrezas
H7 - Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad de sistemas informáticos y redes. TIPO: Habilidades o destrezas
H8 - Desarrollar habilidades de análisis y resolución de problemas en el ámbito de la seguridad informática, así como habilidades de comunicación y trabajo en equipo. TIPO: Habilidades o destrezas
H9 - Adquirir habilidades para analizar y evaluar los aspectos legales de la ciberseguridad, asesorar en la implementación de políticas y normativas y colaborar con equipos técnicos en la resolución de casos jurídicos relacionados con la ciberseguridad. TIPO: Habilidades o destrezas
K1 - Diseñar, desarrollar, evaluar y asegurar la seguridad de un sistema informático, con independencia de su tamaño y características. TIPO: Competencias
K2 - Desarrollar, implantar y mantener sistemas, servicios y aplicaciones informáticas de seguridad empleando los métodos de la ingeniería del software como instrumento para el aseguramiento de su calidad. TIPO: Competencias
K3 - Analizar, diseñar, construir y mantener aplicaciones de seguridad de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados en cada caso, según el entorno de despliegue (entorno web, escritorio). TIPO: Competencias
K5 - Validar la garantía y seguridad de los sistemas informáticos pertinentes, como redes locales, servidores, bases de datos y sistemas de gestión de información. TIPO: Competencias
K6 - Diseñar políticas de monitorización y copia de segura, para la recuperación de sistemas y el aseguramiento en la información en caso de malfuncionamiento. TIPO: Competencias
K7 - Elaborar la política de seguridad de una empresa. TIPO: Competencias
K8 - Auditar las políticas de seguridad de una empresa a todos los niveles (sistemas, red, información, etc.). TIPO: Competencias
K9 - Aplicar las restricciones legales asociados a la seguridad informática sobre el manejo y procesamiento de datos personales. TIPO: Competencias

NIVEL 2: Herramientas y técnicas para la ciberseguridad		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Mixta	
ECTS OPTATIVAS	**ECTS OBLIGATORIAS**	**ECTS BÁSICAS**
3	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
9		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**

NIVEL 3: La ciberseguridad en la sociedad del riesgo: economía y protección del dato		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Optativa	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
3		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**

NIVEL 3: Investigación en seguridad		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
C10 - Caracterizar normativas y regulaciones en materia de protección de datos, cumplimiento normativo y responsabilidad jurídica en casos de incidentes de seguridad. TIPO: Conocimientos o contenidos		
C2 - Identificar las amenazas y vulnerabilidades más comunes en entornos digitales, así como las técnicas y metodologías utilizadas para prevenir, detectar y responder a incidentes de seguridad. TIPO: Conocimientos o contenidos		
C4 - Valorar el impacto de la ciberseguridad sobre la economía, la empresa y la ciudadanía. TIPO: Conocimientos o contenidos		
C3 - Identificar las leyes, regulaciones y estándares nacionales e internacionales relacionados con la ciberseguridad. TIPO: Conocimientos o contenidos		
C5 - Examinar aspectos interdisciplinarios de la ciberseguridad, como la gestión de riesgos, la ética y la privacidad, con el fin de proporcionar una visión integral de la disciplina. TIPO: Conocimientos o contenidos		
C8 - Distinguir las últimas tendencias y tecnologías en el campo de la ciberseguridad, como el Internet de las cosas (IoT), la inteligencia artificial (IA) y el aprendizaje automático (Machine Learning), para estar preparados ante los desafíos futuros. TIPO: Conocimientos o contenidos		
C9 - Recopilar información pertinente de la legislación nacional e internacional que afecta a los sistemas de información y la ciberseguridad, así como en los aspectos legales y sociales relacionados. TIPO: Conocimientos o contenidos		
H1 - Implementar medidas de seguridad en diferentes entornos y sistemas, incluyendo la configuración de firewalls, la gestión de accesos, la detección de intrusiones y el análisis forense digital. TIPO: Habilidades o destrezas		
H3 - Analizar y evaluar los riesgos de seguridad en entornos digitales, identificando posibles debilidades y proponiendo soluciones efectivas. TIPO: Habilidades o destrezas		
C6 - Identificar protocolos de seguridad contra amenazas informáticas a partir de conocimientos especializados en ciberseguridad, centrándose en su desarrollo, implementación y evaluación. TIPO: Conocimientos o contenidos		
C7 - Describir los aspectos técnicos e informáticos de la seguridad, incluyendo el diseño seguro de sistemas, la seguridad en redes y comunicaciones, la protección de datos y la gestión de incidentes de seguridad. TIPO: Conocimientos o contenidos		
H2 - Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad de sistemas y redes, así como para llevar a cabo pruebas de penetración y auditorías de seguridad. TIPO: Habilidades o destrezas		
H6 - Desarrollar habilidades técnicas para implementar soluciones de seguridad en sistemas y redes, realizar pruebas de penetración y responder a incidentes de seguridad de manera eficiente. TIPO: Habilidades o destrezas		
H7 - Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad de sistemas informáticos y redes. TIPO: Habilidades o destrezas		
H8 - Desarrollar habilidades de análisis y resolución de problemas en el ámbito de la seguridad informática, así como habilidades de comunicación y trabajo en equipo. TIPO: Habilidades o destrezas		
H9 - Adquirir habilidades para analizar y evaluar los aspectos legales de la ciberseguridad, asesorar en la implementación de políticas y normativas y colaborar con equipos técnicos en la resolución de casos jurídicos relacionados con la ciberseguridad. TIPO: Habilidades o destrezas		
K5 - Validar la garantía y seguridad de los sistemas informáticos pertinentes, como redes locales, servidores, bases de datos y sistemas de gestión de información. TIPO: Competencias		
K6 - Diseñar políticas de monitorización y copia de segura, para la recuperación de sistemas y el aseguramiento en la información en caso de malfuncionamiento. TIPO: Competencias		

K7 - Elaborar la política de seguridad de una empresa. TIPO: Competencias		
K8 - Auditar las políticas de seguridad de una empresa a todos los niveles (sistemas, red, información, etc.). TIPO: Competencias		
K9 - Aplicar las restricciones legales asociados a la seguridad informática sobre el manejo y procesamiento de datos personales. TIPO: Competencias		
NIVEL 2: Conocimientos técnicos para la ciberseguridad		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Mixta	
ECTS OPTATIVAS	**ECTS OBLIGATORIAS**	**ECTS BÁSICAS**
12	9	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6	15	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Hacking ético		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Análisis forense		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Optativa	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Criptografía, blockchain y criptomonedas		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Optativa	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**

ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Taller de investigación en inteligencia artificial y ciberseguridad		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	3	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
C1 - Relacionar los fundamentos teóricos de la ciberseguridad, incluyendo conceptos básicos de la información, criptografía, redes y sistemas operativos para proteger la integridad y la confidencialidad de la información. TIPO: Conocimientos o contenidos		
C2 - Identificar las amenazas y vulnerabilidades más comunes en entornos digitales, así como las técnicas y metodologías utilizadas para prevenir, detectar y responder a incidentes de seguridad. TIPO: Conocimientos o contenidos		
C8 - Distinguir las últimas tendencias y tecnologías en el campo de la ciberseguridad, como el Internet de las cosas (IoT), la inteligencia artificial (IA) y el aprendizaje automático (Machine Learning), para estar preparados ante los desafíos futuros. TIPO: Conocimientos o contenidos		
H1 - Implementar medidas de seguridad en diferentes entornos y sistemas, incluyendo la configuración de firewalls, la gestión de accesos, la detección de intrusiones y el análisis forense digital. TIPO: Habilidades o destrezas		
C6 - Identificar protocolos de seguridad contra amenazas informáticas a partir de conocimientos especializados en ciberseguridad, centrándose en su desarrollo, implementación y evaluación. TIPO: Conocimientos o contenidos		
C7 - Describir los aspectos técnicos e informáticos de la seguridad, incluyendo el diseño seguro de sistemas, la seguridad en redes y comunicaciones, la protección de datos y la gestión de incidentes de seguridad. TIPO: Conocimientos o contenidos		
H2 - Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad de sistemas y redes, así como para llevar a cabo pruebas de penetración y auditorías de seguridad. TIPO: Habilidades o destrezas		
H6 - Desarrollar habilidades técnicas para implementar soluciones de seguridad en sistemas y redes, realizar pruebas de penetración y responder a incidentes de seguridad de manera eficiente. TIPO: Habilidades o destrezas		
H7 - Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad de sistemas informáticos y redes. TIPO: Habilidades o destrezas		
H8 - Desarrollar habilidades de análisis y resolución de problemas en el ámbito de la seguridad informática, así como habilidades de comunicación y trabajo en equipo. TIPO: Habilidades o destrezas		
K1 - Diseñar, desarrollar, evaluar y asegurar la seguridad de un sistema informático, con independencia de su tamaño y características. TIPO: Competencias		
K2 - Desarrollar, implantar y mantener sistemas, servicios y aplicaciones informáticas de seguridad empleando los métodos de la ingeniería del software como instrumento para el aseguramiento de su calidad. TIPO: Competencias		
K3 - Analizar, diseñar, construir y mantener aplicaciones de seguridad de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados en cada caso, según el entorno de despliegue (entorno web, escritorio). TIPO: Competencias		
K4 - Diseñar, desplegar, administrar de forma segura y fiable servicios en una red de ordenadores. TIPO: Competencias		
K5 - Validar la garantía y seguridad de los sistemas informáticos pertinentes, como redes locales, servidores, bases de datos y sistemas de gestión de información. TIPO: Competencias		
K6 - Diseñar políticas de monitorización y copia de segura, para la recuperación de sistemas y el aseguramiento en la información en caso de malfuncionamiento. TIPO: Competencias		
K7 - Elaborar la política de seguridad de una empresa. TIPO: Competencias		

K8 - Auditar las políticas de seguridad de una empresa a todos los niveles (sistemas, red, información, etc.). TIPO: Competencias		
NIVEL 2: Conocimientos jurídicos y económicos sobre ciberseguridad		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
ECTS NIVEL 2	15	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
3	12	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Compliance y cumplimiento normativo		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Optativa	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Diligencias de investigación tecnológica y prueba electrónica		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Optativa	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Economía y Empresa digital		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Optativa	3	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
3		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**

4.1.1.2 RESULTADOS DE APRENDIZAJE
C10 - Caracterizar normativas y regulaciones en materia de protección de datos, cumplimiento normativo y responsabilidad jurídica en casos de incidentes de seguridad. TIPO: Conocimientos o contenidos
C4 - Valorar el impacto de la ciberseguridad sobre la economía, la empresa y la ciudadanía. TIPO: Conocimientos o contenidos
C3 - Identificar las leyes, regulaciones y estándares nacionales e internacionales relacionados con la ciberseguridad. TIPO: Conocimientos o contenidos
C9 - Recopilar información pertinente de la legislación nacional e internacional que afecta a los sistemas de información y la ciberseguridad, así como en los aspectos legales y sociales relacionados. TIPO: Conocimientos o contenidos
H3 - Analizar y evaluar los riesgos de seguridad en entornos digitales, identificando posibles debilidades y proponiendo soluciones efectivas. TIPO: Habilidades o destrezas
H4 - Trabajar en equipo para colaborar con otros profesionales de la ciberseguridad, así como para educar a usuarios finales y promover buenas prácticas de seguridad. TIPO: Habilidades o destrezas
H10 - Desarrollar habilidades de investigación y análisis en materia de delitos informáticos para comprender los motivos e impacto en el entorno digital. TIPO: Habilidades o destrezas
H11 - Mejorar en habilidades de comunicación y argumentación legal, y desarrollar habilidades éticas y profesionales para enfrentar los desafíos éticos y legales en el ámbito de la ciberseguridad. TIPO: Habilidades o destrezas
H5 - Trabajar en equipo en entornos multidisciplinares, para el análisis y resolución de problemas concretos de inseguridad en equipos y sistemas informáticos. TIPO: Habilidades o destrezas
H9 - Adquirir habilidades para analizar y evaluar los aspectos legales de la ciberseguridad, asesorar en la implementación de políticas y normatives y colaborar con equipos técnicos en la resolución de casos jurídicos relacionados con la ciberseguridad. TIPO: Habilidades o destrezas
K5 - Validar la garantía y seguridad de los sistemas informáticos pertinentes, como redes locales, servidores, bases de datos y sistemas de gestión de información. TIPO: Competencias
K6 - Diseñar políticas de monitorización y copia de segura, para la recuperación de sistemas y el aseguramiento en la información en caso de malfuncionamiento. TIPO: Competencias
K9 - Aplicar las restricciones legales asociados a la seguridad informática sobre el manejo y procesamiento de datos personales. TIPO: Competencias

NIVEL 2: Trabajo de Fin de Máster		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Trabajo Fin de Grado / Máster	
ECTS NIVEL 2	15	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	15	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**

NIVEL 3: Trabajo de Fin de Máster		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Trabajo Fin de Grado / Máster	15	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	15	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**

4.1.1.2 RESULTADOS DE APRENDIZAJE
C1 - Relacionar los fundamentos teóricos de la ciberseguridad, incluyendo conceptos básicos de la información, criptografía, redes y sistemas operativos para proteger la integridad y la confidencialidad de la información. TIPO: Conocimientos o contenidos
C10 - Caracterizar normativas y regulaciones en materia de protección de datos, cumplimiento normativo y responsabilidad jurídica en casos de incidentes de seguridad. TIPO: Conocimientos o contenidos
C2 - Identificar las amenazas y vulnerabilidades más comunes en entornos digitales, así como las técnicas y metodologías utilizadas para prevenir, detectar y responder a incidentes de seguridad. TIPO: Conocimientos o contenidos
C4 - Valorar el impacto de la ciberseguridad sobre la economía, la empresa y la ciudadanía. TIPO: Conocimientos o contenidos
C3 - Identificar las leyes, regulaciones y estándares nacionales e internacionales relacionados con la ciberseguridad. TIPO: Conocimientos o contenidos
C5 - Examinar aspectos interdisciplinarios de la ciberseguridad, como la gestión de riesgos, la ética y la privacidad, con el fin de proporcionar una visión integral de la disciplina. TIPO: Conocimientos o contenidos
C8 - Distinguir las últimas tendencias y tecnologías en el campo de la ciberseguridad, como el Internet de las cosas (IoT), la inteligencia artificial (IA) y el aprendizaje automático (Machine Learning), para estar preparados ante los desafíos futuros. TIPO: Conocimientos o contenidos
C9 - Recopilar información pertinente de la legislación nacional e internacional que afecta a los sistemas de información y la ciberseguridad, así como en los aspectos legales y sociales relacionados. TIPO: Conocimientos o contenidos
H1 - Implementar medidas de seguridad en diferentes entornos y sistemas, incluyendo la configuración de firewalls, la gestión de accesos, la detección de intrusiones y el análisis forense digital. TIPO: Habilidades o destrezas
H3 - Analizar y evaluar los riesgos de seguridad en entornos digitales, identificando posibles debilidades y proponiendo soluciones efectivas. TIPO: Habilidades o destrezas
H4 - Trabajar en equipo para colaborar con otros profesionales de la ciberseguridad, así como para educar a usuarios finales y promover buenas prácticas de seguridad. TIPO: Habilidades o destrezas
C6 - Identificar protocolos de seguridad contra amenazas informáticas a partir de conocimientos especializados en ciberseguridad, centrándose en su desarrollo, implementación y evaluación. TIPO: Conocimientos o contenidos
C7 - Describir los aspectos técnicos e informáticos de la seguridad, incluyendo el diseño seguro de sistemas, la seguridad en redes y comunicaciones, la protección de datos y la gestión de incidentes de seguridad. TIPO: Conocimientos o contenidos
H2 - Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad de sistemas y redes, así como para llevar a cabo pruebas de penetración y auditorías de seguridad. TIPO: Habilidades o destrezas
H10 - Desarrollar habilidades de investigación y análisis en materia de delitos informáticos para comprender los motivos e impacto en el entorno digital. TIPO: Habilidades o destrezas
H11 - Mejorar en habilidades de comunicación y argumentación legal, y desarrollar habilidades éticas y profesionales para enfrentar los desafíos éticos y legales en el ámbito de la ciberseguridad. TIPO: Habilidades o destrezas
H5 - Trabajar en equipo en entornos multidisciplinares, para el análisis y resolución de problemas concretos de inseguridad en equipos y sistemas informáticos. TIPO: Habilidades o destrezas
H6 - Desarrollar habilidades técnicas para implementar soluciones de seguridad en sistemas y redes, realizar pruebas de penetración y responder a incidentes de seguridad de manera eficiente. TIPO: Habilidades o destrezas
H7 - Adquirir destrezas en el uso de herramientas y software especializados para evaluar la seguridad de sistemas informáticos y redes. TIPO: Habilidades o destrezas
H8 - Desarrollar habilidades de análisis y resolución de problemas en el ámbito de la seguridad informática, así como habilidades de comunicación y trabajo en equipo. TIPO: Habilidades o destrezas
H9 - Adquirir habilidades para analizar y evaluar los aspectos legales de la ciberseguridad, asesorar en la implementación de políticas y normatives y colaborar con equipos técnicos en la resolución de casos jurídicos relacionados con la ciberseguridad. TIPO: Habilidades o destrezas
K1 - Diseñar, desarrollar, evaluar y asegurar la seguridad de un sistema informático, con independencia de su tamaño y características. TIPO: Competencias
K2 - Desarrollar, implantar y mantener sistemas, servicios y aplicaciones informáticas de seguridad empleando los métodos de la ingeniería del software como instrumento para el aseguramiento de su calidad. TIPO: Competencias
K3 - Analizar, diseñar, construir y mantener aplicaciones de seguridad de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados en cada caso, según el entorno de despliegue (entorno web, escritorio). TIPO: Competencias

K4 - Diseñar, desplegar, administrar de forma segura y fiable servicios en una red de ordenadores. TIPO: Competencias
K5 - Validar la garantía y seguridad de los sistemas informáticos pertinentes, como redes locales, servidores, bases de datos y sistemas de gestión de información. TIPO: Competencias
K6 - Diseñar políticas de monitorización y copia de segura, para la recuperación de sistemas y el aseguramiento en la información en caso de malfuncionamiento. TIPO: Competencias
K7 - Elaborar la política de seguridad de una empresa. TIPO: Competencias
K8 - Auditar las políticas de seguridad de una empresa a todos los niveles (sistemas, red, información, etc.). TIPO: Competencias
K9 - Aplicar las restricciones legales asociados a la seguridad informática sobre el manejo y procesamiento de datos personales. TIPO: Competencias
NO CONSTAN ELEMENTOS DE NIVEL 2

4.2 ACTIVIDADES Y METODOLOGÍAS DOCENTES

ACTIVIDADES FORMATIVAS

4.2. Actividades y metodologías docentes

Con el objetivo de maximizar el aprendizaje de los estudiantes, promover la interacción y el pensamiento crítico, así como fomentar la autonomía en el estudio. Estas actividades se describen a continuación, detallando su contenido y la modalidad docente aplicable:

- **Sesiones Magistrales**: Sesiones conducidas por especialistas en la materia, donde se presentan los fundamentos teóricos de los temas de cada asignatura del curso. Estas sesiones son de carácter expositivo y buscan proporcionar una visión amplia y detallada de los conceptos clave, fomentando al mismo tiempo el diálogo y la reflexión crítica entre los estudiantes. Pueden llegar a tener aplicabilidad tanto de forma presencial como en formatos no presenciales, utilizando plataformas de videoconferencia para su realización u otros canales.
- **Seminarios**: Sesiones en grupos más reducidos, donde los estudiantes tienen la oportunidad de discutir y profundizar en los temas tratados en los seminarios magistrales. Esta metodología fomenta la participación, el intercambio de ideas y la construcción colaborativa del conocimiento. Se promueve el uso de metodologías activas, como el debate, el análisis de casos o la resolución de problemas, adaptable tanto a modalidades presenciales como a distancia.
- **Sesiones Prácticas**: Diseñadas para aplicar de manera concreta los conocimientos adquiridos. A través de ejercicios, experimentos, simulaciones o el uso de herramientas y software específico, donde los estudiantes pondrán en práctica los conceptos teóricos, desarrollando habilidades técnicas y analíticas. Estas sesiones requieren de un entorno controlado, ya sea en laboratorios o plataformas digitales especializadas.
- **Tutorías**: Sesiones individualizadas o en pequeños grupos donde los estudiantes pueden resolver dudas específicas con el docente, recibir orientación personalizada y profundizar en temas de interés. Estas sesiones son flexibles y se pueden llevar a cabo tanto de forma presencial como virtual.
- **Preparación de trabajos autónomos**: Asignaciones que los estudiantes deben realizar de manera independiente, aplicando los conocimientos adquiridos para desarrollar proyectos, informes, ensayos o investigaciones, con el objetivo de fomentar la capacidad de análisis, síntesis y crítica, así como el desarrollo de habilidades de investigación y escritura académica.
- **Preparación de trabajos en grupo**: Actividades colaborativas donde los estudiantes trabajen conjuntamente aplicado los conocimientos previos, con el objetivo de fomentar habilidades de comunicación, liderazgo, negociación y gestión de conflictos, promoviendo el trabajo en equipo.
- **Trabajo Fin de Máster (TFM):** Este trabajo representa la aplicación integral de los conocimientos, habilidades y competencias adquiridas a lo largo del programa, permitiendo a los estudiantes abordar y resolver de manera autónoma un problema o proyecto de investigación dentro de su campo de estudio. La realización del TFM evidencia la capacidad analítica y creativa del estudiante, además de fomentar el desarrollo de competencias en investigación, gestión de proyectos y comunicación efectiva, siendo el reflejo final del aprendizaje y desarrollo profesional alcanzado durante el máster. Este componente del programa se enmarca dentro las actividades y metodologías docentes, destacando la importancia de la autonomía, el pensamiento crítico y la especialización académica y profesional.

Mecanismos de coordinación docente.

Los mecanismos de coordinación docente quedan garantizados a través de las figuras del Director o Directora del Máster, la Comisión Académica del Máster y la Comisión de Calidad del Título. La Comisión Académica del Máster ejercerá las funciones de ordenación académica de las enseñanzas, en coordinación y bajo la supervisión y aprobación del órgano académicamente responsable del título (Instituto de Estudios de la Ciencia y la Tecnología de la Universidad de Salamanca). Son funciones de esta comisión, entre otras: a) Coordinar las actividades formativas y de evaluación y el desarrollo docente entre las asignaturas, lo que implica establecer un calendario de desarrollo de las asignaturas; b) Mantener una comunicación directa con los estudiantes mediante el correo electrónico de referencia de la comisión y reuniones a final de cada semestre, para poder conocer el desarrollo del plan de estudios y corregir ágilmente las disfunciones que puedan surgir; c) Garantizar la coherencia de los criterios de evaluación y velar por su cumplimiento según la normativa vigente; d) Establecer los criterios y realizar la asignación de un tutor de TFM a cada estudiante. Para coordinar la organización y desarrollo de la actividad docente del Máster se organizarán reuniones del profesorado.

La coordinación de la actividad docente del máster se llevará a cabo mediante reuniones del profesorado, que podrán ser en formato *online*, y que tendrán lugar por una parte al inicio del curso, para planificar las actividades docentes, acordar criterios de evaluación comunes y asegurar el no solapamiento de contenidos, y por otra parte al final del curso, para evaluar el desarrollo del programa formativo y adoptar acuerdos en caso necesario.

Cada comisión que evalúe TFMs se reunirá previamente a la sesión de presentaciones presenciales de los estudiantes, con vistas a establecer una plantilla de la rúbrica de evaluación con las puntuaciones para cada uno de los criterios que se han descrito que forman parte de la evaluación.

La Comisión de Calidad del Título se encargará principalmente de evaluar y dar seguimiento al título, siguiendo las directrices del Sistema de Garantía de Calidad. Será responsable de recopilar datos sobre el programa formativo, proponer planes de mejora, dar seguimiento a dichos planes, gestionar el archivo documental del título y atender las posibles quejas y sugerencias.

Composición de la Comisión Académica de Máster (CAM)

De acuerdo con la normativa interna de la USAL (Bases para la armonización del mapa de titulaciones de la Universidad de Salamanca, Aprobado en Consejo de Gobierno de 22 de febrero de 2011 y modificado parcialmente en Consejo de Gobierno de 31 de octubre de 2019), el Máster contará con una Comisión Académica, que ejercerá las funciones de ordenación académica de las enseñanzas, en coordinación y bajo la supervisión y aprobación del órgano académicamente responsable del título. En particular, serán funciones de la Comisión Académica:

1. **Elaborar la propuesta de la programación docente anual del curso académico.**
2. **Proponer los acuerdos de colaboración con instituciones y empresas.**
3. **Establecer y publicar los criterios de valoración de méritos para la admisión de estudiantes.**
4. **Resolver las solicitudes de admisión de estudiantes según los criterios de admisión y selección definidos.**
5. **Velar por el cumplimiento de los mecanismos de coordinación docente que se hayan establecido en la Memoria de Verificación del título.**
6. **Elaborar el presupuesto económico anual del Máster.**

La Comisión Académica estará presidida por el/la Director/a de Máster, que actuará como coordinador/a de la titulación, que será un docente con vinculación permanente y dedicación a tiempo completo.

El director/a estará asistido en sus labores de coordinación por la propia Comisión Académica, compuesta por:

- **Coordinadores de las materias uno de los cuales actuará como Secretario/a.**
- **Representantes de alumnos, para que la representación de los estudiantes sea de, al menos, el 25%.**
- **Representante del PAS.**

METODOLOGÍAS DOCENTES

4.2. Actividades y metodologías docentes

Con el objetivo de maximizar el aprendizaje de los estudiantes, promover la interacción y el pensamiento crítico, así como fomentar la autonomía en el estudio. Estas actividades se describen a continuación, detallando su contenido y la modalidad docente aplicable:

- **Sesiones Magistrales**: Sesiones conducidas por especialistas en la materia, donde se presentan los fundamentos teóricos de los temas de cada asignatura del curso. Estas sesiones son de carácter expositivo y buscan proporcionar una visión amplia y detallada de los conceptos clave, fomentando al mismo tiempo el diálogo y la reflexión crítica entre los estudiantes. Pueden llegar a tener aplicabilidad tanto de forma presencial como en formatos no presenciales, utilizando plataformas de videoconferencia para su realización u otros canales.
- **Seminarios**: Sesiones en grupos más reducidos, donde los estudiantes tienen la oportunidad de discutir y profundizar en los temas tratados en los seminarios magistrales. Esta metodología fomenta la participación, el intercambio de ideas y la construcción colaborativa del conocimiento. Se promueve el uso de metodologías activas, como el debate, el análisis de casos o la resolución de problemas, adaptable tanto a modalidades presenciales como a distancia.
- **Sesiones Prácticas**: Diseñadas para aplicar de manera concreta los conocimientos adquiridos. A través de ejercicios, experimentos, simulaciones o el uso de herramientas y software específico, donde los estudiantes pondrán en práctica los conceptos teóricos, desarrollando habilidades técnicas y analíticas. Estas sesiones requieren de un entorno controlado, ya sea en laboratorios o plataformas digitales especializadas.
- **Tutorías**: Sesiones individualizadas o en pequeños grupos donde los estudiantes pueden resolver dudas específicas con el docente, recibir orientación personalizada y profundizar en temas de interés. Estas sesiones son flexibles y se pueden llevar a cabo tanto de forma presencial como virtual.
- **Preparación de trabajos autónomos**: Asignaciones que los estudiantes deben realizar de manera independiente, aplicando los conocimientos adquiridos para desarrollar proyectos, informes, ensayos o investigaciones, con el objetivo de fomentar la capacidad de análisis, síntesis y crítica, así como el desarrollo de habilidades de investigación y escritura académica.
- **Preparación de trabajos en grupo**: Actividades colaborativas donde los estudiantes trabajen conjuntamente aplicado los conocimientos previos, con el objetivo de fomentar habilidades de comunicación, liderazgo, negociación y gestión de conflictos, promoviendo el trabajo en equipo.
- **Trabajo Fin de Máster (TFM):** Este trabajo representa la aplicación integral de los conocimientos, habilidades y competencias adquiridas a lo largo del programa, permitiendo a los estudiantes abordar y resolver de manera autónoma un problema o proyecto de investigación dentro de su campo de estudio. La realización del TFM evidencia la capacidad analítica y creativa del estudiante, además de fomentar el desarrollo de competencias en investigación, gestión de proyectos y comunicación efectiva, siendo el reflejo final del aprendizaje y desarrollo profesional alcanzado durante el máster. Este componente del programa se enmarca dentro las actividades y metodologías docentes, destacando la importancia de la autonomía, el pensamiento crítico y la especialización académica y profesional.

Mecanismos de coordinación docente.

Los mecanismos de coordinación docente quedan garantizados a través de las figuras del Director o Directora del Máster, la Comisión Académica del Máster y la Comisión de Calidad del Título. La Comisión Académica del Máster ejercerá las funciones de ordenación académica de las enseñanzas, en coordinación y bajo la supervisión y aprobación del órgano académicamente responsable del título (Instituto de Estudios de la Ciencia y la Tecnología de la Universidad de Salamanca). Son funciones de esta comisión, entre otras: a) Coordinar las actividades formativas y de evaluación y el desarrollo docente entre las asignaturas, lo que implica establecer un calendario de desarrollo de las asignaturas; b) Mantener una comunicación directa con los estudiantes mediante el correo electrónico de referencia de la comisión y reuniones a final de cada semestre, para poder conocer el desarrollo del plan de estudios y corregir ágilmente las disfunciones que puedan surgir; c) Garantizar la coherencia de los criterios de evaluación y velar por su cumplimiento según la normativa vigente; d) Establecer los criterios y realizar la asignación de un tutor de TFM a cada estudiante. Para coordinar la organización y desarrollo de la actividad docente del Máster se organizarán reuniones del profesorado.

La coordinación de la actividad docente del máster se llevará a cabo mediante reuniones del profesorado, que podrán ser en formato *online*, y que tendrán lugar por una parte al inicio del curso, para planificar las actividades docentes, acordar criterios de evaluación comunes y asegurar el no solapamiento de contenidos, y por otra parte al final del curso, para evaluar el desarrollo del programa formativo y adoptar acuerdos en caso necesario.

Cada comisión que evalúe TFMs se reunirá previamente a la sesión de presentaciones presenciales de los estudiantes, con vistas a establecer una plantilla de la rúbrica de evaluación con las puntuaciones para cada uno de los criterios que se han descrito que forman parte de la evaluación.

La Comisión de Calidad del Título se encargará principalmente de evaluar y dar seguimiento al título, siguiendo las directrices del Sistema de Garantía de Calidad. Será responsable de recopilar datos sobre el programa formativo, proponer planes de mejora, dar seguimiento a dichos planes, gestionar el archivo documental del título y atender las posibles quejas y sugerencias.

Composición de la Comisión Académica de Máster (CAM)

De acuerdo con la normativa interna de la USAL (Bases para la armonización del mapa de titulaciones de la Universidad de Salamanca, Aprobado en Consejo de Gobierno de 22 de febrero de 2011 y modificado parcialmente en Consejo de Gobierno de 31 de octubre de 2019), el Máster contará con una Comisión Académica, que ejercerá las funciones de ordenación académica de las enseñanzas, en coordinación y bajo la supervisión y aprobación del órgano académicamente responsable del título. En particular, serán funciones de la Comisión Académica:

1. **Elaborar la propuesta de la programación docente anual del curso académico.**
2. **Proponer los acuerdos de colaboración con instituciones y empresas.**
3. **Establecer y publicar los criterios de valoración de méritos para la admisión de estudiantes.**
4. **Resolver las solicitudes de admisión de estudiantes según los criterios de admisión y selección definidos.**

5. **Velar por el cumplimiento de los mecanismos de coordinación docente que se hayan establecido en la Memoria de Verificación del título.**
6. **Elaborar el presupuesto económico anual del Máster.**

La Comisión Académica estará presidida por el/la Director/a de Máster, que actuará como coordinador/a de la titulación, que será un docente con vinculación permanente y dedicación a tiempo completo.

El director/a estará asistido en sus labores de coordinación por la propia Comisión Académica, compuesta por:

- **Coordinadores de las materias uno de los cuales actuará como Secretario/a.**
- **Representantes de alumnos, para que la representación de los estudiantes sea de, al menos, el 25%.**
- **Representante del PAS.**

4.3 SISTEMAS DE EVALUACIÓN

4.3. Sistemas de evaluación

Los criterios e instrumentos de evaluación, así como la repercusión que tendrán en las calificaciones finales, se fijarán por asignaturas. Los estudiantes tendrán a su disposición en la Guía Académica los sistemas de evaluación de cada una de las asignaturas que componen el plan de estudios antes de comenzar el curso académico, previa revisión por parte de la Comisión Académica del título.

El sistema de evaluación adoptado permitirá medir el rendimiento académico de los egresados. Concebido como un proceso integral que abarca diversas dimensiones del aprendizaje, incluyendo tanto el desarrollo de habilidades y competencias como la adquisición de conocimientos teóricos y prácticos. En este contexto, se han definido cuatro pilares fundamentales para el sistema de evaluación que cada una de las diferentes asignaturas podrán adoptar, los cuales se detallan a continuación:

- **Participación en actividades presenciales**: Evaluación de la interacción directa en el aula, así como el compromiso y la implicación del estudiante en las dinámicas de grupo, discusiones, seminarios y sesiones prácticas. Se tendrán en cuenta la calidad de la contribución individual, preparación para las sesiones, capacidad de análisis y síntesis, y habilidades para el trabajo en equipo.
- **Entrega de informes de los supuestos prácticos**: Permite evaluar la capacidad del estudiantado de aplicar los conocimientos teóricos a situaciones concretas y realistas. A través de esta modalidad evaluativa, se busca desarrollar competencias analíticas, de resolución de problemas y de comunicación efectiva. Los informes deben reflejar un entendimiento profundo de los conceptos trabajados en clase, una capacidad crítica para analizar los datos y situaciones presentadas, y una habilidad para proponer soluciones innovadoras y fundamentadas. La elaboración de estos informes fomenta el aprendizaje autónomo y la investigación, incentivando a los estudiantes a explorar fuentes de información adicionales, utilizar herramientas metodológicas adecuadas y presentar sus resultados de manera clara y estructurada.

- **Prueba final**: Herramienta de evaluación para medir el grado de comprensión y asimilación de los contenidos por parte del estudiantado. Pueden ser escritas u orales, y se diseñan para evaluar tanto conocimientos teóricos como habilidades prácticas. Los exámenes se adaptan a todas las modalidades docentes, pudiendo realizarse de manera presencial o a través de plataformas digitales seguras que garantizan la integridad del proceso evaluativo.
- **Elaboración y defensa del TFM**: Conforme al Reglamento de Trabajos de Fin de Máster de la Universidad de Salamanca (aprobado por el Consejo de Gobierno en sesión ordinaria de 27 de mayo de 2022 y modificado en la sesión ordinaria del Consejo de Gobierno de 24 de marzo de 2023), se realizará mediante la elaboración individual de un proyecto de investigación por parte de cada estudiante, el cual será expuesto y defendido en acto público ante un tribunal nombrado a tal efecto. Este tribunal estará compuesto por tres docentes del Máster, quienes realizarán una evaluación personalizada de cómo cada alumno ha incorporado y manifestado los conocimientos y habilidades adquiridos durante su proceso educativo. El texto escrito como la defensa pública se valorarán de acuerdo con la rúbrica que elaboren conjuntamente el profesorado implicado en la docencia del MU.

La combinación de medios y pruebas, así como su peso en la evaluación global, la ajustará el profesorado en cada asignatura.

Para garantizar la identidad del estudiante en los sistemas de evaluación no presenciales, se contará con herramientas de evaluación online y #proctoring# tipo SMOWL. Esta constituye una herramienta especializada en la supervisión y monitorización de actividades en línea con el propósito de asegurar la integridad del proceso y prevenir posibles actos fraudulentos. Posibilita la incorporación de una supervisión integral de 360° mediante el uso de una segunda cámara (como un smartphone o una tablet), permitiendo verificar que el entorno donde se lleva a cabo la evaluación cumple con todas las garantías necesarias. Asimismo, el requisito del registro previo por parte del alumnado incluyendo una fotografía o documento nacional de identidad para su reconocimiento, permite garantizar la identidad del estudiante en todas las actividades de evaluación síncronas.

4.4 ESTRUCTURAS CURRICULARES ESPECÍFICAS

5. PERSONAL ACADÉMICO Y DE APOYO A LA DOCENCIA

PERSONAL ACADÉMICO
Ver Apartado 5: Anexo 1.
OTROS RECURSOS HUMANOS
Ver Apartado 5: Anexo 2.

6. RECURSOS MATERIALES E INFRAESTRUCTURALES, PRÁCTICAS Y SERVICIOS

Justificación de que los medios materiales disponibles son adecuados: Ver Apartado 6: Anexo 1.

7. CALENDARIO DE IMPLANTACIÓN

7.1 CRONOGRAMA DE IMPLANTACIÓN	
CURSO DE INICIO	2025
Ver Apartado 7: Anexo 1.	
7.2 PROCEDIMIENTO DE ADAPTACIÓN	

7.2 Procedimiento de adaptación

Se trata de un título oficial de nueva creación, por lo que no procede este apartado.

7.3 ENSEÑANZAS QUE SE EXTINGUEN	
CÓDIGO	**ESTUDIO - CENTRO**

8. SISTEMA INTERNO DE GARANTÍA DE LA CALIDAD Y ANEXOS

8.1 SISTEMA INTERNO DE GARANTÍA DE LA CALIDAD	
ENLACE	https://calidad.usal.es/
8.2 INFORMACIÓN PÚBLICA	

8.2. Medios para la información pública

El medio principal de información pública del plan de estudios es la web institucional del Máster Universitario (**https://www.usal.es/masteres**). Ésta contará con la información que la Agencia para la Calidad del Sistema de Castilla y León, ACSUCyl, requiere actualmente para superar con éxito los procesos de renovación de acreditación de los títulos y que puede consultarse en ACSUCyL 2021, II. Manual de evaluación (**https://www.acsucyl.es/web/jcyl/binarios/448/438/ACSUCYL_RenovacionAcreditacion_II.ManualEvaluacion_Ed2021.pdf?blobheader=application%2Fpdf%3Bcharset%3DUTF-8&blobnocache=true**): Descripción del título (centro, modalidad, idioma, plazas de nuevo ingreso ofertadas, salidas profesionales, etc), Objetivos (Objetivos formativos y Resultados del proceso de formación y de aprendizaje), Acceso y admisión de estudiantes (Perfil de ingreso, Acceso, preinscripción y matrícula, Criterios de admisión, Apoyo y orientación, Reconocimiento y Transferencia de créditos), Planificación de las enseñanzas (plan de estudios general, guías docentes), Calendario de implantación, Sistema de garantía de calidad (Informes externos de evaluación del título, Información sobre evaluaciones de la actividad docente del profesorado), Resultados (Académicos, y de encuestas, incluidas las de inserción laboral), Normativa.

Adicionalmente, se contempla la difusión del programa a través redes sociales y otros canales, lo que contribuirá a enriquecer los canales de comunicación y seguimiento académico de la comunidad estudiantil. Se ha reservado ya la dirección **https://ciberseguridad.usal.es** para la difusión de información sobre el Máster.

Las necesidades de información de los estudiantes se atenderán también a través de la web de la Facultad de Ciencias (**https://fciencias.usal.es/**), del IECyT (**https://institutoecyt.usal.es/**) y del correo electrónico, ya que cada estudiante contará con una cuenta personal y que será básica para interactuar a través del Campus Virtual Studium promoviendo la mejora en la experiencia educativa, además de contribuir en el seguimiento del avance formativo de los estudiantes.

8.3 ANEXOS
Ver Apartado 8: Anexo 1.

PERSONAS ASOCIADAS A LA SOLICITUD

RESPONSABLE DEL TÍTULO			
CARGO	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
Director del Máster	PABLO	CHAMOSO	SANTOS
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Calle Espejo sn, Edificio I+D +i, Lab 24.2	37007	Salamanca	Salamanca
EMAIL	**FAX**		
chamoso@usal.es			

REPRESENTANTE LEGAL			
CARGO	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**

Delegada del Rector para Estudios de Postgrado y Formación Permanente	María Teresa	Escribano	Bailón
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Hospedería Fonseca, Fonseca, nº 2, 1ª planta	37002	Salamanca	Salamanca
EMAIL	**FAX**		
delegadapostgrado@usal.es			

El Rector de la Universidad no es el Representante Legal
Ver Personas asociadas a la solicitud: Anexo 1.
SOLICITANTE
El responsable del título no es el solicitante

CARGO	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
Director Académico de Postgrado	Javier	Peña	González
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Patio de Escuelas 1, 2ª planta	37008	Salamanca	Salamanca
EMAIL	**FAX**		
dir.postgrado@usal.es			

INFORME PREVIO DE LA COMUNIDAD AUTÓNOMA

Informe previo de la Comunidad Autónoma: Ver Apartado Informe previo de la Comunidad Autónoma: Anexo 1.

Apartado 1: Anexo 6

Nombre :1. Justificación.pdf

HASH SHA1 :8DEB181507F7B3CA9BBE81F70B12B7444C4D0FA8

Código CSV :833390625073489704195714

Ver Fichero: 1. Justificación.pdf

Apartado 4: Anexo 1

Nombre :4.1. Planificación de las enseñanzas.pdf

HASH SHA1 :D01D03754D3495D306CF1FA42E13D1A1BDBA0645

Código CSV :833743638527139896921018

Ver Fichero: 4.1. Planificación de las enseñanzas.pdf

Apartado 5: Anexo 1

Nombre :5.1 Perfil básico del profesorado.pdf

HASH SHA1 :FF57B4A71C7D1598B157910DB8CC0C9C92B2428E

Código CSV :833430892465369216740104

Ver Fichero: 5.1 Perfil básico del profesorado.pdf

Apartado 5: Anexo 2

Nombre :5.2 Perfil básico de otros recursos de apoyo a la docencia.pdf

HASH SHA1 :F69CD9204A53BBE43AE75AC54F877AF72770D2DB

Código CSV :79881316156568692641409 5

Ver Fichero: 5.2 Perfil básico de otros recursos de apoyo a la docencia.pdf

Apartado 6: Anexo 1

Nombre :6. Recursos para el aprendizaje.pdf

HASH SHA1 :4E2436C840AA19C6815A498905C94948EDAE2B5E

Código CSV :833438063878953618416239

Ver Fichero: 6. Recursos para el aprendizaje.pdf

Apartado 7: Anexo 1

Nombre :7.1. Cronograma de implantación.pdf

HASH SHA1 :AECF5353469ACBEC94105F123B0EDA18AED2783B

Código CSV :79881852680970120549164O

Ver Fichero: 7.1. Cronograma de implantación.pdf

Apartado Personas asociadas a la solicitud: Anexo 1

Nombre : Delegacion competencias Rector RUCT.pdf

HASH SHA1 :9B6AEF8390521A37C4CB0C3E82A93429E0905A6A

Código CSV :797860738077600564292935

Ver Fichero: Delegacion competencias Rector RUCT.pdf

Apartado Informe previo de la Comunidad Autónoma: Anexo 1

Nombre : Inf Viabilidad MU Ciberseguridad - VHHMX4SFXAY5XTOWYDEJTM.pdf

HASH SHA1 :DC7D4376977DC278E5F12A2FA36B55368A429964

Código CSV :801202075398859616359568

Ver Fichero: Inf Viabilidad MU Ciberseguridad - VHHMX4SFXAY5XTOWYDEJTM.pdf