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 Internacional de La Rioja	Escuela Superior de Ingeniería y Tecnología	26004007
NIVEL	**DENOMINACIÓN CORTA**	
Máster	Ciberseguridad	
DENOMINACIÓN ESPECÍFICA		
Máster Universitario en Ciberseguridad por la Universidad Internacional de La Rioja		
NIVEL MECES		
3		
RAMA DE CONOCIMIENTO	**ÁMBITO DE CONOCIMIENTO**	**CONJUNTO**
Ingeniería y Arquitectura	Ingeniería informática y de sistemas	No
SOLICITANTE		
NOMBRE Y APELLIDOS	**CARGO**	
Virginia Montiel Martín	Responsable de programas ANECA	
REPRESENTANTE LEGAL		
NOMBRE Y APELLIDOS	**CARGO**	
Juan Pablo Guzmán Palomino	Secretario General de la Universidad	
RESPONSABLE DEL TÍTULO		
NOMBRE Y APELLIDOS	**CARGO**	
Manuel Sánchez Rubio	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
Avenida de la Paz, 137	26006	Logroño	676614276
E-MAIL	**PROVINCIA**		**FAX**
virginia.montiel@unir.net	La Rioja		902877037

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.

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: La Rioja, AM 20 de febrero de 2025
	Firma: Representante legal de la Universidad

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

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 Internacional de La Rioja	No		Ver Apartado 1: Anexo 1.

RAMA
Ingeniería y Arquitectura
ÁMBITO
Ingeniería informática y de sistemas
AGENCIA EVALUADORA
Agencia Nacional de Evaluación de la Calidad y Acreditación
LISTADO DE ESPECIALIDADES
No existen datos
MENCIÓN DUAL
No

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

UNIVERSIDAD SOLICITANTE	
Universidad Internacional de La Rioja	
LISTADO DE UNIVERSIDADES	
CÓDIGO	**UNIVERSIDAD**
077	Universidad Internacional de La Rioja
LISTADO DE UNIVERSIDADES EXTRANJERAS	
CÓDIGO	**UNIVERSIDAD**
No existen datos	

CRÉDITOS TOTALES	CRÉDITOS DE COMPLEMENTOS FORMATIVOS	CRÉDITOS EN PRÁCTICAS EXTERNAS
60		6
CRÉDITOS OPTATIVOS	**CRÉDITOS OBLIGATORIOS**	**CRÉDITOS TRABAJO FIN GRADO/ MÁSTER**
0	42	12

1.4-1.9 Universidad Internacional de La Rioja

1.4-1.9.1 CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS			
CÓDIGO	**CENTRO**	**CENTRO RESPONSABLE**	**CENTRO ACREDITADO INSTITUCIONALMENTE**
26004007	Escuela Superior de Ingeniería y Tecnología	Si	Si

1.4-1.9.2 Escuela Superior de Ingeniería y 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	No	Sí
PLAZAS POR MODALIDAD		
		1350
NÚMERO TOTAL DE PLAZAS	**NÚMERO DE PLAZAS DE NUEVO INGRESO PARA PRIMER CURSO**	
1350	1350	

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

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

El objetivo general del máster es preparar al estudiante para el ejercicio de las funciones de experto en ciberseguridad.

Todo el proceso formativo está dirigido a que los alumnos del Máster alcancen los objetivos que se recogen en este apartado y estará presidido de manera real y efectiva por los siguientes principios informadores:

1. El respeto y la subordinación de toda actuación a los derechos fundamentales de la persona por su carácter de absolutos axiológicos.
2. La subordinación al principio de igualdad, con especial atención a la no discriminación por razón de sexo, de conformidad con lo previsto en el artículo 14 de la Constitución.
3. El fomento del principio de igualdad de oportunidades en lo que comporta de exigencia de implementación de acciones de discriminación positiva respecto a las personas con diversidad de capacidades.
4. El fomento de la estima de la paz, el pluralismo, el respeto a la diferencia y de los demás valores convivenciales propios de una sociedad democrática avanzada.

Los objetivos generales de nuestra propuesta, de conformidad con el Marco Español Cualificaciones para la Educación Superior (MECES) son:

Conocer y comprender la legislación dirigida a la protección de bienes informáticos, sistemas de información, así como en el despliegue de su actividad, en especial la regulación penal de los comportamientos delictivos asociados.	OB1
Analizar riesgos legales de los sistemas de información relacionados con la seguridad en todo tipo de sistemas.	OB2
Conocer y saber aplicar procesos de gestión y mejora de la seguridad en las organizaciones.	OB3
Conocer y saber aplicar los principales estándares y buenas prácticas de auditoría de la seguridad.	OB4
Comprender y saber valorar los diferentes algoritmos y técnicas criptográficas, y los mecanismos de protección asociados a ellas.	OB5
Conocer las plataformas hardware especializadas para la seguridad informática.	OB6
Entender el concepto de vulnerabilidad y su tipología y saber analizar vulnerabilidades en sistemas concretos.	OB7
Conocer las principales técnicas de protección frente a ataques y amenazas en los sistemas operativos, las redes, el software de aplicación, los sistemas Web y las bases de datos.	OB8
Conocer y saber aplicar correctamente las principales técnicas de análisis forense	OB9

ESTRUCTURAS CURRICULARES ESPECÍFICAS Y ESTRATEGIAS METODOLÓGICAS DE INNOVACIÓN DOCENTE

1.14 PERFILES FUNDAMENTALES DE EGRESO Y PROFESIONES REGULADAS

PERFILES DE EGRESO

https://static.unir.net/calidad/Perfil_Fundamental_Egreso_MU_Ciberseguridad.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

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo. TIPO: Habilidades o destrezas

CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación. TIPO: Conocimientos o contenidos

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio. TIPO: Habilidades o destrezas
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. TIPO: Competencias
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades. TIPO: Habilidades o destrezas
CE1 - Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles TIPO: Competencias
CE10 - Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos. TIPO: Competencias
CE11 - Conocer todos los activos del negocio de la empresa y las variables necesarias para poder implementar un SGSI. TIPO: Conocimientos o contenidos
CE12 - Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa. TIPO: Habilidades o destrezas
CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada implantación en su infraestructura. TIPO: Habilidades o destrezas
CE14 - Diseñar las correctas políticas para analizar y reproducir los hechos ante un incidente de seguridad informática. TIPO: Competencias
CE15 - Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad. TIPO: Competencias
CE16 - Conocer y comprender la legislación europea en materia de seguridad, para poder emitir juicios sobre su aplicabilidad y relevancia en cada ámbito. TIPO: Conocimientos o contenidos
CE17 - Discernir los distintos mecanismos criptográficos para seleccionar el óptimo en cada ámbito de aplicación. TIPO: Habilidades o destrezas
CE18 - Optimizar las políticas de seguridad de la infraestructura de la red de la entidad. TIPO: Competencias
CE19 - Proteger la integridad de las bases de datos para asegurar la confidencialidad de la información sensible contenida. TIPO: Competencias
CE2 - Adquirir una visión general e integrada del asesoramiento en seguridad que permita la colaboración con otros departamentos de la entidad. TIPO: Habilidades o destrezas
CE20 - Asesorar sobre las distintas medidas de seguridad aplicables a los sistemas informáticos para disminuir el impacto de sus posibles fallos. TIPO: Competencias
CE21 - Analizar la infraestructura de red para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas, tanto en entorno local como en la nube. TIPO: Competencias
CE22 - Diseñar las políticas de recuperación de datos más adecuadas para disminuir el impacto ante incidentes. TIPO: Competencias
CE23 - Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones. TIPO: Habilidades o destrezas
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención. TIPO: Competencias
CE25 - Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, infraestructuras críticas y principales conceptos de auditoría de sistemas. TIPO: Conocimientos o contenidos
CE26 - Implantar procesos de análisis forense de cualquier sistema informático. TIPO: Competencias
CE27 - Diseñar, implantar e institucionalizar un proceso de análisis y gestión de riesgos de los sistemas de información en cualquier organización. TIPO: Competencias
CE3 - Identificar, analizar y definir los riesgos de los servicios de las empresas para poder gestionarlos con criterio y de manera efectiva, en función de sus perfiles de seguridad. TIPO: Competencias
CE4 - Asesorar sobre el cumplimiento de la legislación reguladora de la protección de datos en materia de seguridad, en especial sobre la adopción de las medidas de índole técnica y organizativas necesarias considerando la problemática de los datos almacenados en la nube. TIPO: Competencias
CE5 - Discernir sobre los distintos entornos de seguridad existentes, tanto en local como en la nube, para poder seleccionar el óptimo siguiendo un razonamiento profesional y completo. TIPO: Competencias
CE6 - Analizar el funcionamiento de herramientas de seguridad y su uso conjugado. TIPO: Competencias

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

CE7 - Identificar y proceder contra aquellas conductas tipificadas como delito informático en el marco jurídico actual. TIPO: Competencias
CE8 - Tomar decisiones proactivas y reactivas frente los posibles fallos de seguridad, investigando las causas que las originan. TIPO: Competencias
CE9 - Comprender el funcionamiento, características y nivel de riesgo de los servicios de las empresas y establecer mecanismos de protección. TIPO: Conocimientos o contenidos
CG1 - Aplicar los conocimientos adquiridos y ser capaces de resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con el área de la seguridad informática. TIPO: Habilidades o destrezas
CG2 - Integrar conocimientos para formular juicios a partir de determinada información. A la vez, incluir reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios en materia de asesoramiento en seguridad informática. TIPO: Competencias
CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación continua en su futuro desempeño profesional como experto en seguridad informática TIPO: Habilidades o destrezas
CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarrollarlos mediante los métodos y procesos adecuados. TIPO: Competencias
CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de las entidades de TI. TIPO: Competencias
CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática. TIPO: Habilidades o destrezas
CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes. TIPO: Habilidades o destrezas
CG8 - Tener la capacidad analítica y de resolución para atender a los problemas reales de acuerdo con los valores éticos y sociales y con el máximo respeto a la legalidad vigente. TIPO: Habilidades o destrezas
CG9 - Manejar adecuadamente información relativa al sector de la seguridad informática. Atendiendo a la legislación vigente, notas técnicas, revistas especializadas, Internet, documentos internos de la empresa, etc. TIPO: Habilidades o destrezas
CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line. TIPO: Habilidades o destrezas
CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc. TIPO: Habilidades o destrezas
CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento. TIPO: Habilidades o destrezas
CT4 - Capacidad para realizar una enseñanza personalizada adaptada al espacio (aula virtual multicultural y multirracial) a los recursos y a las situaciones y necesidades personales de los alumnos. TIPO: Competencias
CT5 - Capacidad de investigar y comunicar los resultados de la investigación. TIPO: Habilidades o destrezas

3. ADMISIÓN, RECONOCIMIENTO Y MOVILIDAD

3.1 REQUISITOS DE ACCESO Y PROCEDIMIENTOS DE ADMISIÓN

3.1. Requisitos de acceso y procedimientos de admisión de estudiantes

Requisitos de acceso con carácter general

Las enseñanzas de los diversos Másteres de la UNIR se ofrecen a cualquier persona que reuniendo las condiciones de acceso que expresa la ley desea tener una enseñanza a distancia ofrecida en un entorno virtual.

Los motivos que suelen llevar a esa elección están relacionados con algún tipo de dificultad para cursar estudios presenciales. Entre estos destacan los de aquellos que ya desempeñan una ocupación laboral o que ya tienen trabajo, que quieren iniciar o reanudar estudios universitarios.

Requisitos de acceso con carácter específico

Ingenieros o ingenieros técnicos en Informática, Telecomunicaciones o Telemática fundamentalmente, así como en cualquier otra ingeniería relacionada con las TIC. También profesionales con grado de diplomados, ingenieros técnicos, licenciados o ingenieros con amplia y constatable experiencia laboral en TIC.

Criterios de admisión

El órgano encargado de la gestión del proceso de admisión es el Departamento de Admisiones en su vertiente nacional e internacional.

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

La admisión definitiva en el título es competencia de la Comisión de Admisiones del mismo, que está formada por, al menos:

- Responsable del título (que puede delegar en un profesor del título)
- Responsable de Acceso y Verificaciones

Para poder acceder al Máster Universitario en Ciberseguridad, es necesarioseguir los requisitos de acceso establecidos en el artículo 18 del RD 822/2021, de 28 de septiembre:

1. La posesión de un título universitario oficial de Graduada o Graduado español o equivalente es condición para acceder a un Máster Universitario, o en su caso disponer de otro título de Máster Universitario, o títulos del mismo nivel que el título español de Grado o Máster expedidos por universidades e instituciones de educación superior de un país del EEES que en dicho país permita el acceso a los estudios de Máster.

2. De igual modo, podrán acceder a un Máster Universitario del sistema universitario español personas en posesión de títulos procedentes de sistemas educativos que no formen parte del EEES, que equivalgan al título de Grado, sin necesidad de homologación del título, pero sí de comprobación por parte de la universidad del nivel de formación que implican, siempre y cuando en el país donde se haya expedido dicho título permita acceder a estudios de nivel de postgrado universitario. En ningún caso el acceso por esta vía implicará la homologación del título previo del que disponía la persona interesada ni su reconocimiento a otros efectos que el de realizar los estudios de Máster.

Satisfechos los requisitos de admisión previamente mencionados, y solo en el caso de que el número de solicitudes de plaza que cumplen con los requisitos recogidos en las vías de acceso exceda al número de plazas ofertadas, en la resolución de las solicitudes de admisión se tendrá en cuenta los siguientes criterios de valoración:

- Nota media del expediente en la titulación que otorga el acceso al máster (100 %).

En caso de empate en puntuaciones, se elegirá al que tenga mayor número de matrículas de honor y, en su caso, sobresalientes y así sucesivamente.

Normativa aplicable:

REGLAMENTO DE ACCESO Y ADMISIÓN A ESTUDIOS OFICIALES DE LA UNIVERSIDAD INTERNACIONAL DE LA RIOJA:

Se aporta el enlace que consta en la página web de la Universidad:
https://static.unir.net/documentos/reglamento_acceso_admision_e_o_unir.pdf

(La limitación de 10000 palabras incluida en el aplicativo del Ministerio no nos permite aportar el texto completo, por ello se aporta el enlace de descarga).

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

Ver Apartado 3: Anexo 2.	

Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional

MÍNIMO	MÁXIMO
0	9

DESCRIPCIÓN

Normativa aplicable:

NORMATIVA DE RECONOCIMIENTO Y TRANSFERENCIA DE CRÉDITOS DE LA UNIVERSIDAD INTERNACIONAL DE LA RIOJA:

Se aporta el enlace que consta en la página web de la Universidad:
https://static.unir.net/documentos/normativa-RTC.pdf

(La limitación de 10000 palabras incluida en el aplicativo del Ministerio no nos permite aportar el texto completo, por ello se aporta el enlace de descarga).

3.3 MOVILIDAD DE LOS ESTUDIANTES PROPIOS Y DE ACOGIDA

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Información indicada en el apartado de Anexos de la presente memoria; en concreto, en el Anexo I.

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: GESTIÓN Y REGULACIÓN DE LA CIBERSEGURIDAD		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	12	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
12		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
NIVEL 3: Ciberdelitos y Regulación de la Ciberseguridad		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
6		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
NIVEL 3: Gobierno de la Ciberseguridad y Análisis de Riesgos		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
6		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada implantación en su infraestructura. TIPO: Habilidades o destrezas		
CE16 - Conocer y comprender la legislación europea en materia de seguridad, para poder emitir juicios sobre su aplicabilidad y relevancia en cada ámbito. TIPO: Conocimientos o contenidos		
CE21 - Analizar la infraestructura de red para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas, tanto en entorno local como en la nube. TIPO: Competencias		

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

CE22 - Diseñar las políticas de recuperación de datos más adecuadas para disminuir el impacto ante incidentes. TIPO: Competencias
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención. TIPO: Competencias
CE25 - Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, infraestructuras críticas y principales conceptos de auditoría de sistemas. TIPO: Conocimientos o contenidos
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación. TIPO: Conocimientos o contenidos
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. TIPO: Competencias
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades. TIPO: Habilidades o destrezas
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo. TIPO: Habilidades o destrezas
CG1 - Aplicar los conocimientos adquiridos y ser capaces de resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con el área de la seguridad informática. TIPO: Habilidades o destrezas
CG2 - Integrar conocimientos para formular juicios a partir de determinada información. A la vez, incluir reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios en materia de asesoramiento en seguridad informática. TIPO: Competencias
CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación continua en su futuro desempeño profesional como experto en seguridad informática TIPO: Habilidades o destrezas
CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarrollarlos mediante los métodos y procesos adecuados. TIPO: Competencias
CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de las entidades de TI. TIPO: Competencias
CG8 - Tener la capacidad analítica y de resolución para atender a los problemas reales de acuerdo con los valores éticos y sociales y con el máximo respeto a la legalidad vigente. TIPO: Habilidades o destrezas
CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc. TIPO: Habilidades o destrezas
CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento. TIPO: Habilidades o destrezas
CE9 - Comprender el funcionamiento, características y nivel de riesgo de los servicios de las empresas y establecer mecanismos de protección. TIPO: Conocimientos o contenidos
CE12 - Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa. TIPO: Habilidades o destrezas
CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line. TIPO: Habilidades o destrezas
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio. TIPO: Habilidades o destrezas
CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática. TIPO: Habilidades o destrezas
CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes. TIPO: Habilidades o destrezas
CG9 - Manejar adecuadamente información relativa al sector de la seguridad informática. Atendiendo a la legislación vigente, notas técnicas, revistas especializadas, Internet, documentos internos de la empresa, etc. TIPO: Habilidades o destrezas
CT4 - Capacidad para realizar una enseñanza personalizada adaptada al espacio (aula virtual multicultural y multirracial) a los recursos y a las situaciones y necesidades personales de los alumnos. TIPO: Competencias
CT5 - Capacidad de investigar y comunicar los resultados de la investigación. TIPO: Habilidades o destrezas
CE1 - Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles TIPO: Competencias

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

CE2 - Adquirir una visión general e integrada del asesoramiento en seguridad que permita la colaboración con otros departamentos de la entidad. TIPO: Habilidades o destrezas
CE3 - Identificar, analizar y definir los riesgos de los servicios de las empresas para poder gestionarlos con criterio y de manera efectiva, en función de sus perfiles de seguridad. TIPO: Competencias
CE4 - Asesorar sobre el cumplimiento de la legislación reguladora de la protección de datos en materia de seguridad, en especial sobre la adopción de las medidas de índole técnica y organizativas necesarias considerando la problemática de los datos almacenados en la nube. TIPO: Competencias
CE7 - Identificar y proceder contra aquellas conductas tipificadas como delito informático en el marco jurídico actual. TIPO: Competencias
CE10 - Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos. TIPO: Competencias
CE11 - Conocer todos los activos del negocio de la empresa y las variables necesarias para poder implementar un SGSI. TIPO: Conocimientos o contenidos
CE15 - Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad. TIPO: Competencias
CE27 - Diseñar, implantar e institucionalizar un proceso de análisis y gestión de riesgos de los sistemas de información en cualquier organización. TIPO: Competencias

NIVEL 2: AUDITORÍA Y ANÁLISIS FORENSE		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	18	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
6	12	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
NIVEL 3: Informática Forense y Respuesta ante Incidentes		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
6		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
NIVEL 3: Hacking Ético y Análisis de Malware		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	6	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
NIVEL 3: Desarrollo Seguro de Software y Auditoría de la Ciberseguridad		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	6	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada implantación en su infraestructura. TIPO: Habilidades o destrezas		
CE14 - Diseñar las correctas políticas para analizar y reproducir los hechos ante un incidente de seguridad informática. TIPO: Competencias		
CE21 - Analizar la infraestructura de red para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas, tanto en entorno local como en la nube. TIPO: Competencias		
CE22 - Diseñar las políticas de recuperación de datos más adecuadas para disminuir el impacto ante incidentes. TIPO: Competencias		
CE23 - Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones. TIPO: Habilidades o destrezas		
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención. TIPO: Competencias		
CE25 - Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, infraestructuras críticas y principales conceptos de auditoría de sistemas. TIPO: Conocimientos o contenidos		
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación. TIPO: Conocimientos o contenidos		
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. TIPO: Competencias		
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades. TIPO: Habilidades o destrezas		
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo. TIPO: Habilidades o destrezas		
CG1 - Aplicar los conocimientos adquiridos y ser capaces de resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con el área de la seguridad informática. TIPO: Habilidades o destrezas		
CG2 - Integrar conocimientos para formular juicios a partir de determinada información. A la vez, incluir reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios en materia de asesoramiento en seguridad informática. TIPO: Competencias		
CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación continua en su futuro desempeño profesional como experto en seguridad informática TIPO: Habilidades o destrezas		
CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarrollarlos mediante los métodos y procesos adecuados. TIPO: Competencias		
CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de las entidades de TI. TIPO: Competencias		
CG8 - Tener la capacidad analítica y de resolución para atender a los problemas reales de acuerdo con los valores éticos y sociales y con el máximo respeto a la legalidad vigente. TIPO: Habilidades o destrezas		

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc. TIPO: Habilidades o destrezas
CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento. TIPO: Habilidades o destrezas
CE9 - Comprender el funcionamiento, características y nivel de riesgo de los servicios de las empresas y establecer mecanismos de protección. TIPO: Conocimientos o contenidos
CE12 - Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa. TIPO: Habilidades o destrezas
CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line. TIPO: Habilidades o destrezas
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio. TIPO: Habilidades o destrezas
CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática. TIPO: Habilidades o destrezas
CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes. TIPO: Habilidades o destrezas
CG9 - Manejar adecuadamente información relativa al sector de la seguridad informática. Atendiendo a la legislación vigente, notas técnicas, revistas especializadas, Internet, documentos internos de la empresa, etc. TIPO: Habilidades o destrezas
CT4 - Capacidad para realizar una enseñanza personalizada adaptada al espacio (aula virtual multicultural y multirracial) a los recursos y a las situaciones y necesidades personales de los alumnos. TIPO: Competencias
CT5 - Capacidad de investigar y comunicar los resultados de la investigación. TIPO: Habilidades o destrezas
CE1 - Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles TIPO: Competencias
CE3 - Identificar, analizar y definir los riesgos de los servicios de las empresas para poder gestionarlos con criterio y de manera efectiva, en función de sus perfiles de seguridad. TIPO: Competencias
CE6 - Analizar el funcionamiento de herramientas de seguridad y su uso conjugado. TIPO: Competencias
CE8 - Tomar decisiones proactivas y reactivas frente los posibles fallos de seguridad, investigando las causas que las originan. TIPO: Competencias
CE26 - Implantar procesos de análisis forense de cualquier sistema informático. TIPO: Competencias

NIVEL 2: TÉCNICAS AVANZADAS DE SEGURIDAD		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	12	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
12		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
NIVEL 3: Seguridad en Redes y Análisis Inteligente de Amenazas		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
6		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
NIVEL 3: Seguridad en Sistemas, Aplicaciones y el Big Data		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
6		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada implantación en su infraestructura. TIPO: Habilidades o destrezas		
CE17 - Discernir los distintos mecanismos criptográficos para seleccionar el óptimo en cada ámbito de aplicación. TIPO: Habilidades o destrezas		
CE18 - Optimizar las políticas de seguridad de la infraestructura de la red de la entidad. TIPO: Competencias		
CE19 - Proteger la integridad de las bases de datos para asegurar la confidencialidad de la información sensible contenida. TIPO: Competencias		
CE20 - Asesorar sobre las distintas medidas de seguridad aplicables a los sistemas informáticos para disminuir el impacto de sus posibles fallos. TIPO: Competencias		
CE21 - Analizar la infraestructura de red para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas, tanto en entorno local como en la nube. TIPO: Competencias		
CE23 - Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones. TIPO: Habilidades o destrezas		
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención. TIPO: Competencias		
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación. TIPO: Conocimientos o contenidos		
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. TIPO: Competencias		
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades. TIPO: Habilidades o destrezas		
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo. TIPO: Habilidades o destrezas		
CG1 - Aplicar los conocimientos adquiridos y ser capaces de resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con el área de la seguridad informática. TIPO: Habilidades o destrezas		
CG2 - Integrar conocimientos para formular juicios a partir de determinada información. A la vez, incluir reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios en materia de asesoramiento en seguridad informática. TIPO: Competencias		
CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación continua en su futuro desempeño profesional como experto en seguridad informática TIPO: Habilidades o destrezas		
CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarrollarlos mediante los métodos y procesos adecuados. TIPO: Competencias		
CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de las entidades de TI. TIPO: Competencias		

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

CG8 - Tener la capacidad analítica y de resolución para atender a los problemas reales de acuerdo con los valores éticos y sociales y con el máximo respeto a la legalidad vigente. TIPO: Habilidades o destrezas
CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc. TIPO: Habilidades o destrezas
CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento. TIPO: Habilidades o destrezas
CE9 - Comprender el funcionamiento, características y nivel de riesgo de los servicios de las empresas y establecer mecanismos de protección. TIPO: Conocimientos o contenidos
CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line. TIPO: Habilidades o destrezas
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio. TIPO: Habilidades o destrezas
CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática. TIPO: Habilidades o destrezas
CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes. TIPO: Habilidades o destrezas
CG9 - Manejar adecuadamente información relativa al sector de la seguridad informática. Atendiendo a la legislación vigente, notas técnicas, revistas especializadas, Internet, documentos internos de la empresa, etc. TIPO: Habilidades o destrezas
CT4 - Capacidad para realizar una enseñanza personalizada adaptada al espacio (aula virtual multicultural y multirracial) a los recursos y a las situaciones y necesidades personales de los alumnos. TIPO: Competencias
CT5 - Capacidad de investigar y comunicar los resultados de la investigación. TIPO: Habilidades o destrezas
CE5 - Discernir sobre los distintos entornos de seguridad existentes, tanto en local como en la nube, para poder seleccionar el óptimo siguiendo un razonamiento profesional y completo. TIPO: Competencias
CE6 - Analizar el funcionamiento de herramientas de seguridad y su uso conjugado. TIPO: Competencias
CE10 - Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos. TIPO: Competencias
CE15 - Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad. TIPO: Competencias

NIVEL 2: PRÁCTICAS EN EMPRESA		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Prácticas Externas	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	6	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
NIVEL 3: Prácticas en Empresa		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Prácticas Externas	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	6	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

ECTS Cuatrimestral 10	ECTS Cuatrimestral 11	ECTS Cuatrimestral 12
4.1.1.2 RESULTADOS DE APRENDIZAJE		
CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada implantación en su infraestructura. TIPO: Habilidades o destrezas		
CE14 - Diseñar las correctas políticas para analizar y reproducir los hechos ante un incidente de seguridad informática. TIPO: Competencias		
CE16 - Conocer y comprender la legislación europea en materia de seguridad, para poder emitir juicios sobre su aplicabilidad y relevancia en cada ámbito. TIPO: Conocimientos o contenidos		
CE17 - Discernir los distintos mecanismos criptográficos para seleccionar el óptimo en cada ámbito de aplicación. TIPO: Habilidades o destrezas		
CE18 - Optimizar las políticas de seguridad de la infraestructura de la red de la entidad. TIPO: Competencias		
CE19 - Proteger la integridad de las bases de datos para asegurar la confidencialidad de la información sensible contenida. TIPO: Competencias		
CE20 - Asesorar sobre las distintas medidas de seguridad aplicables a los sistemas informáticos para disminuir el impacto de sus posibles fallos. TIPO: Competencias		
CE21 - Analizar la infraestructura de red para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas, tanto en entorno local como en la nube. TIPO: Competencias		
CE22 - Diseñar las políticas de recuperación de datos más adecuadas para disminuir el impacto ante incidentes. TIPO: Competencias		
CE23 - Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones. TIPO: Habilidades o destrezas		
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención. TIPO: Competencias		
CE25 - Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, infraestructuras críticas y principales conceptos de auditoría de sistemas. TIPO: Conocimientos o contenidos		
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación. TIPO: Conocimientos o contenidos		
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. TIPO: Competencias		
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades. TIPO: Habilidades o destrezas		
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo. TIPO: Habilidades o destrezas		
CG1 - Aplicar los conocimientos adquiridos y ser capaces de resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con el área de la seguridad informática. TIPO: Habilidades o destrezas		
CG2 - Integrar conocimientos para formular juicios a partir de determinada información. A la vez, incluir reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios en materia de asesoramiento en seguridad informática. TIPO: Competencias		
CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación continua en su futuro desempeño profesional como experto en seguridad informática TIPO: Habilidades o destrezas		
CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarrollarlos mediante los métodos y procesos adecuados. TIPO: Competencias		
CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de las entidades de TI. TIPO: Competencias		
CG8 - Tener la capacidad analítica y de resolución para atender a los problemas reales de acuerdo con los valores éticos y sociales y con el máximo respeto a la legalidad vigente. TIPO: Habilidades o destrezas		
CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc. TIPO: Habilidades o destrezas		
CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento. TIPO: Habilidades o destrezas		

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

CE9 - Comprender el funcionamiento, características y nivel de riesgo de los servicios de las empresas y establecer mecanismos de protección. TIPO: Conocimientos o contenidos
CE12 - Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa. TIPO: Habilidades o destrezas
CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line. TIPO: Habilidades o destrezas
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio. TIPO: Habilidades o destrezas
CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática. TIPO: Habilidades o destrezas
CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes. TIPO: Habilidades o destrezas
CG9 - Manejar adecuadamente información relativa al sector de la seguridad informática. Atendiendo a la legislación vigente, notas técnicas, revistas especializadas, Internet, documentos internos de la empresa, etc. TIPO: Habilidades o destrezas
CT4 - Capacidad para realizar una enseñanza personalizada adaptada al espacio (aula virtual multicultural y multirracial) a los recursos y a las situaciones y necesidades personales de los alumnos. TIPO: Competencias
CT5 - Capacidad de investigar y comunicar los resultados de la investigación. TIPO: Habilidades o destrezas
CE1 - Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles TIPO: Competencias
CE2 - Adquirir una visión general e integrada del asesoramiento en seguridad que permita la colaboración con otros departamentos de la entidad. TIPO: Habilidades o destrezas
CE3 - Identificar, analizar y definir los riesgos de los servicios de las empresas para poder gestionarlos con criterio y de manera efectiva, en función de sus perfiles de seguridad. TIPO: Competencias
CE4 - Asesorar sobre el cumplimiento de la legislación reguladora de la protección de datos en materia de seguridad, en especial sobre la adopción de las medidas de índole técnica y organizativas necesarias considerando la problemática de los datos almacenados en la nube. TIPO: Competencias
CE5 - Discernir sobre los distintos entornos de seguridad existentes, tanto en local como en la nube, para poder seleccionar el óptimo siguiendo un razonamiento profesional y completo. TIPO: Competencias
CE6 - Analizar el funcionamiento de herramientas de seguridad y su uso conjugado. TIPO: Competencias
CE7 - Identificar y proceder contra aquellas conductas tipificadas como delito informático en el marco jurídico actual. TIPO: Competencias
CE8 - Tomar decisiones proactivas y reactivas frente los posibles fallos de seguridad, investigando las causas que las originan. TIPO: Competencias
CE10 - Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos. TIPO: Competencias
CE11 - Conocer todos los activos del negocio de la empresa y las variables necesarias para poder implementar un SGSI. TIPO: Conocimientos o contenidos
CE15 - Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad. TIPO: Competencias
CE26 - Implantar procesos de análisis forense de cualquier sistema informático. TIPO: Competencias
CE27 - Diseñar, implantar e institucionalizar un proceso de análisis y gestión de riesgos de los sistemas de información en cualquier organización. TIPO: Competencias

NIVEL 2: TRABAJO FIN DE MÁSTER		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Trabajo Fin de Grado / Máster	
ECTS NIVEL 2	12	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	12	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
NIVEL 3: Trabajo Fin de Máster		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Trabajo Fin de Grado / Máster	12	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	12	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada implantación en su infraestructura. TIPO: Habilidades o destrezas		
CE14 - Diseñar las correctas políticas para analizar y reproducir los hechos ante un incidente de seguridad informática. TIPO: Competencias		
CE16 - Conocer y comprender la legislación europea en materia de seguridad, para poder emitir juicios sobre su aplicabilidad y relevancia en cada ámbito. TIPO: Conocimientos o contenidos		
CE17 - Discernir los distintos mecanismos criptográficos para seleccionar el óptimo en cada ámbito de aplicación. TIPO: Habilidades o destrezas		
CE18 - Optimizar las políticas de seguridad de la infraestructura de la red de la entidad. TIPO: Competencias		
CE19 - Proteger la integridad de las bases de datos para asegurar la confidencialidad de la información sensible contenida. TIPO: Competencias		
CE20 - Asesorar sobre las distintas medidas de seguridad aplicables a los sistemas informáticos para disminuir el impacto de sus posibles fallos. TIPO: Competencias		
CE21 - Analizar la infraestructura de red para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas, tanto en entorno local como en la nube. TIPO: Competencias		
CE22 - Diseñar las políticas de recuperación de datos más adecuadas para disminuir el impacto ante incidentes. TIPO: Competencias		
CE23 - Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones. TIPO: Habilidades o destrezas		
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención. TIPO: Competencias		
CE25 - Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, infraestructuras críticas y principales conceptos de auditoría de sistemas. TIPO: Conocimientos o contenidos		
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación. TIPO: Conocimientos o contenidos		
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. TIPO: Competencias		
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades. TIPO: Habilidades o destrezas		
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo. TIPO: Habilidades o destrezas		
CG1 - Aplicar los conocimientos adquiridos y ser capaces de resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con el área de la seguridad informática. TIPO: Habilidades o destrezas		

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

CG2 - Integrar conocimientos para formular juicios a partir de determinada información. A la vez, incluir reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios en materia de asesoramiento en seguridad informática. TIPO: Competencias
CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación continua en su futuro desempeño profesional como experto en seguridad informática TIPO: Habilidades o destrezas
CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarrollarlos mediante los métodos y procesos adecuados. TIPO: Competencias
CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de las entidades de TI. TIPO: Competencias
CG8 - Tener la capacidad analítica y de resolución para atender a los problemas reales de acuerdo con los valores éticos y sociales y con el máximo respeto a la legalidad vigente. TIPO: Habilidades o destrezas
CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc. TIPO: Habilidades o destrezas
CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento. TIPO: Habilidades o destrezas
CE9 - Comprender el funcionamiento, características y nivel de riesgo de los servicios de las empresas y establecer mecanismos de protección. TIPO: Conocimientos o contenidos
CE12 - Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa. TIPO: Habilidades o destrezas
CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line. TIPO: Habilidades o destrezas
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio. TIPO: Habilidades o destrezas
CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática. TIPO: Habilidades o destrezas
CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes. TIPO: Habilidades o destrezas
CG9 - Manejar adecuadamente información relativa al sector de la seguridad informática. Atendiendo a la legislación vigente, notas técnicas, revistas especializadas, Internet, documentos internos de la empresa, etc. TIPO: Habilidades o destrezas
CT4 - Capacidad para realizar una enseñanza personalizada adaptada al espacio (aula virtual multicultural y multirracial) a los recursos y a las situaciones y necesidades personales de los alumnos. TIPO: Competencias
CT5 - Capacidad de investigar y comunicar los resultados de la investigación. TIPO: Habilidades o destrezas
CE1 - Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles TIPO: Competencias
CE2 - Adquirir una visión general e integrada del asesoramiento en seguridad que permita la colaboración con otros departamentos de la entidad. TIPO: Habilidades o destrezas
CE3 - Identificar, analizar y definir los riesgos de los servicios de las empresas para poder gestionarlos con criterio y de manera efectiva, en función de sus perfiles de seguridad. TIPO: Competencias
CE4 - Asesorar sobre el cumplimiento de la legislación reguladora de la protección de datos en materia de seguridad, en especial sobre la adopción de las medidas de índole técnica y organizativas necesarias considerando la problemática de los datos almacenados en la nube. TIPO: Competencias
CE5 - Discernir sobre los distintos entornos de seguridad existentes, tanto en local como en la nube, para poder seleccionar el óptimo siguiendo un razonamiento profesional y completo. TIPO: Competencias
CE6 - Analizar el funcionamiento de herramientas de seguridad y su uso conjugado. TIPO: Competencias
CE7 - Identificar y proceder contra aquellas conductas tipificadas como delito informático en el marco jurídico actual. TIPO: Competencias
CE8 - Tomar decisiones proactivas y reactivas frente los posibles fallos de seguridad, investigando las causas que las originan. TIPO: Competencias
CE10 - Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos. TIPO: Competencias
CE11 - Conocer todos los activos del negocio de la empresa y las variables necesarias para poder implementar un SGSI. TIPO: Conocimientos o contenidos

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

CE15 - Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad. TIPO: Competencias
CE26 - Implantar procesos de análisis forense de cualquier sistema informático. TIPO: Competencias
CE27 - Diseñar, implantar e institucionalizar un proceso de análisis y gestión de riesgos de los sistemas de información en cualquier organización. TIPO: Competencias
NO CONSTAN ELEMENTOS DE NIVEL 2

4.2 ACTIVIDADES Y METODOLOGÍAS DOCENTES

ACTIVIDADES FORMATIVAS

Denominación de las actividades formativas según las definiciones y datos aportados en el apartado 4.1.
Sesiones presenciales virtuales
Recursos didácticos audiovisuales
Estudio del material básico
Lectura del material complementario
Proyectos y casos prácticos
Prácticas informáticas
Test de autoevaluación
Tutorías
Trabajo colaborativo
Realización de prácticas en el centro
Redacción de la memoria de prácticas
Tutorías (Prácticas)
Sesión Inicial de presentación de TFM
Lectura de material en el aula virtual (TFM)
Seminarios de TFM
Tutorías (TFM)
Sesiones grupales de TFM
Elaboración del Trabajo Fin de Máster

Adicionalmente, en el PDF del apartado 4.1. se indican las definiciones de las actividades formativas, así como su asignación en horas y porcentaje de interacción virtual síncrona, o porcentaje de presencialidad física en su caso, en las diferentes materias del título.

METODOLOGÍAS DOCENTES

Metodologías docentes	
MD1	**Métodos de enseñanza magistral con mediación tecnológica:** aquí se incluirían las clases presenciales virtuales, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.
MD2	**Métodos activos:** son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje - servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.
MD3	**Métodos fundamentados en el aprendizaje individual:** estudio personal, aprendizaje acompañado a través de lecturas de material complementario, realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.

Adicionalmente, en el PDF del apartado 4.1. se indica la asignación de las metodologías docentes a las diferentes materias del título.

4.3 SISTEMAS DE EVALUACIÓN

Denominación de los sistemas de evaluación según las definiciones y datos aportados en el apartado 4.1.
Participación en foros y otros medios participativos
Realización de proyectos y casos prácticos
Prácticas informáticas
Test de autoevaluación
Prueba de evaluación final
Evaluación con base en el informe del tutor externo
Memoria de prácticas

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Evaluación de la Estructura del Trabajo Fin de Máster
Evaluación de la Exposición del Trabajo Fin de Máster
Evaluación del Contenido individual del Trabajo Fin de Máster

Adicionalmente, en el PDF del apartado 4.1. se indican las definiciones de los sistemas de evaluación, así como su asignación a las diferentes materias del título y sus ponderaciones mínimas y máximas correspondientes.

4.4 ESTRUCTURAS CURRICULARES ESPECÍFICAS

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

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	2011
Ver Apartado 7: Anexo 1.	
7.2 PROCEDIMIENTO DE ADAPTACIÓN	
No procede	
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	http://www.unir.net/universidad-online/manual-calidad-procedimientos/
8.2 INFORMACIÓN PÚBLICA	

8.2. Medios de información pública relevante

8.2.1. Canales de difusión de la información y su gestión

Para informar tanto al estudiantado, previamente a su matriculación y durante el proceso de formación y aprendizaje, como al profesorado, a los empleadores y a la sociedad en su conjunto se dispone de la **página web oficial de la Universidad Internacional de La Rioja** donde se aporta la información sobre las características del título (resultados de aprendizaje, temporalización del plan de estudios que incluye asignaturas, actividades formativas y sistemas de evaluación), sistemas de acceso y admisión, idioma de impartición, etc.

La Universidad dispone de sistemas para el **control periódico de la información** disponible en la página web. Por ello, se verifica periódicamente que la información disponible en la página web del título es suficientemente completa, adecuada y relevante para el estudiantado. El coordinador académico del título hace constar en el informe anual de la Unidad de Calidad de Titulación (UCT) esta revisión periódica.

Información pública relevante del plan de estudios

UNIR pone a disposición del estudiantado, el profesorado, los empleadores y la sociedad en su conjunto toda la información actualizada del plan de estudios a través de las guías docentes disponibles en la página web de la Universidad. Así, a través de la guía docente de cada una de las asignaturas que forman el plan de estudios, se puede acceder a la siguiente información:

- **Presentación**: describe el objetivo de la asignatura y cómo su contenido es relevante para el desarrollo del plan de estudios.
- **Competencias**: se enumeran y describen las competencias y/o resultados de aprendizaje desarrollados en el título.
- **Contenidos**: se detalla por temas el contenido desarrollado en la asignatura.
- **Metodología**: se describen las actividades formativas de la asignatura especificando las horas de dedicación indicadas en la memoria para cada actividad formativa, así como su presencialidad.
- Además, se incluye la distribución temporal prevista para la asignatura.
- **Bibliografía**: se detalla la bibliografía básica, considerada imprescindible para el estudio de la asignatura, así como, en su caso, la bibliografía complementaria, para ayudar a profundizar más en los temas de mayor interés.
- **Evaluación y calificación**: se detallan los sistemas de evaluación y sus porcentajes de evaluación, así como los requisitos específicos, en su caso, para aprobar la asignatura.
- **Profesorado**: se presentan los datos básicos del profesor encargado de impartir la asignatura.
- **Orientaciones para el estudio**: se dan orientaciones al estudiante de cómo organizar el estudio de la asignatura, así como diferentes consejos para un adecuado seguimiento de la asignatura.

8.2.2. Sistemas de información previa: información transparente y accesible

Con carácter general, por parte de UNIR se pondrá a disposición de los potenciales estudiantes toda la información necesaria para que puedan realizar la elección de su titulación con los mayores elementos de juicio posibles. **Se garantiza una información transparente y accesible sobre los requisitos de acceso específicos para el título y los procedimientos de admisión, descritos en la presente memoria**, estando disponibles a través de la página web de la Universidad para todos los grupos de interés del título.

En las condiciones de matrícula, disponibles en el apartado normativa de la página web de la universidad se alude a los requisitos tecnológicos e informáticos precisos para seguir el curso adecuadamente, dichas condiciones son conocidas y firmadas por el estudiante al matricularse de sus estudios.

En relación a las competencias y conocimientos digitales para seguir la actividad docente programada:

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Las competencias digitales que los estudiantes de UNIR precisarán tener para el manejo del campus y correcto desarrollo en la plataforma, serán conocimientos a nivel de usuario de distintos programas (esencialmente del paquete Office), así como nociones básicas sobre navegación por internet.

El estudiante que se matricula en UNIR además cuenta con un período de adecuación a la metodología virtual con apoyo de su personal no docente de asistencia.

Por último, desde UNIR se ofrecerá a todos los estudiantes los programas adicionales necesarios que sean específicos para cada titulación que podrán descargar fácilmente desde su campus virtual o a través de cualquier otro enlace accesible o usarse desde las máquinas virtuales habilitadas para tal fin.

8.2.3. Procedimientos de orientación para la admisión y matriculación de estudiantes de nuevo ingreso

UNIR cuenta con una oficina de Atención al Estudiante que centraliza y contesta todas las solicitudes de información (llamadas y correos electrónicos) y un Servicio Técnico de Orientación (*contact center*) que gestiona y soluciona todas las preguntas y posibles dudas de los futuros estudiantes referidas a:

- Descripción de la metodología de UNIR. Para ello, los alumnos tendrán acceso a una demo donde se explica paso por paso.
- Niveles de dificultad y horas de estudio estimadas para poder llevar a cabo un itinerario formativo ajustado a las posibilidades reales del estudiante para poder planificar adecuadamente su matrícula.
- Descripción de los estudios.
- Convalidaciones de las antiguas titulaciones.
- Preguntas sobre el Espacio Europeo de Educación Superior.

Finalmente, el personal de gestión y administración (PGA) a través del Servicio de Admisiones proporcionará al estudiante todo el apoyo administrativo necesario para realizar de manera óptima todo el proceso de admisión y matriculación por medio de atención telefónica o por correo electrónico, con información guiada en la web para la realización de la matrícula *online*.

8.2.4. Perfil de ingreso recomendado

Se recomienda que el estudiante que pretenda realizar el Máster Universitario en Ciberseguridad, además de los requisitos de acceso que señala la ley reúna el siguiente perfil:

- Actitud abierta y capacidad de análisis.
- Capacidad de comunicación, relación social y trabajo en equipo.
- Autodisciplina.

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	Manuel	Sánchez	Rubio
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Avenida de la Paz, 137	26006	La Rioja	Logroño
EMAIL	**FAX**		
virginia.montiel@unir.net	902877037		

REPRESENTANTE LEGAL			
CARGO	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
Secretario General de la Universidad	Juan Pablo	Guzmán	Palomino
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Avenida de la Paz, 137	26006	La Rioja	Logroño
EMAIL	**FAX**		
virginia.montiel@unir.net	902877037		

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**

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Responsable de programas ANECA	Virginia	Montiel	Martín
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Avenida de la Paz, 137	26006	La Rioja	Logroño
EMAIL	**FAX**		
virginia.montiel@unir.net	902877037		

INFORME DEL SIGC

Informe del SIGC: Ver Apartado del SIGC: Anexo 1.

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 1: Anexo 6

Nombre :1.10_completo.pdf

HASH SHA1 :A3340E20865DBE6AFE3254EA583CD8B2D5EA6947

Código CSV :836813624857824940226581

Ver Fichero: 1.10_completo.pdf

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 4: Anexo 1

Nombre :4.pdf

HASH SHA1 :2A51835A291AE6D325797998003D47094E317970

Código CSV :836814087522649329706561

Ver Fichero: 4.pdf

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 5: Anexo 1

Nombre :5.1_MU_Ciberseguridad.pdf

HASH SHA1 :95E5CF7F88D8BCEFA48F0E84A68D0B082F4AF635

Código CSV :836926531243909816895513

Ver Fichero: 5.1_MU_Ciberseguridad.pdf

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 5: Anexo 2

Nombre :5.2.pdf

HASH SHA1 :C33DC726BC18ADFA16E05072EBCF1269765C1E68

Código CSV :836807418595456725671524

Ver Fichero: 5.2.pdf

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 6: Anexo 1

Nombre :6.pdf

HASH SHA1 :3ACEEF879E19CDFD8878C54ED565BC807E5FC729

Código CSV :836807651017928769475278

Ver Fichero: 6.pdf

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 7: Anexo 1

Nombre :7.pdf

HASH SHA1 :30565FA2DCB620238AD9F2252F9E04E86F1D913D

Código CSV :836807755222090973400647

Ver Fichero: 7.pdf

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 8: Anexo 1

Nombre : Anexo 8.3.pdf

HASH SHA1 :BA94ABFCBF188EA5AA7BCBB7D870C70DDA5E5FE6

Código CSV :836808005584878383523349

Ver Fichero: Anexo 8.3.pdf

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado Personas asociadas a la solicitud: Anexo 1

Nombre : Delegacion_Representante_Legal_PABLO_GUZMAN_18052016.pdf

HASH SHA1 :7D3DB15AB0D5DEAA1F83FB17B840A52C57F227EF

Código CSV :243173502221459213834102

Ver Fichero: Delegacion_Representante_Legal_PABLO_GUZMAN_18052016.pdf

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado Informe del SIGC: Anexo 1

Nombre : Informe_SGIC_20240522_MU_C_aplicacion.pdf

HASH SHA1 :2059B864148AFAB1702F41998C97928C230D188B

Código CSV :836809178049024240449743

Ver Fichero: Informe_SGIC_20240522_MU_C_aplicacion.pdf

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

CSV: 880376398776229179316798 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es