IMPRESO SOLICITUD PARA VERIFICACIÓN DE TÍTULOS OFICIALES

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

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

UNIVERSIDAD SOLICITANTE	CENTRO	CÓDIGO CENTRO
Universidad 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|3		
RAMA DE CONOCIMIENTO	**CONJUNTO**	
Ingeniería y Arquitectura	No	
HABILITA PARA EL EJERCICIO DE PROFESIONES REGULADAS	**NORMA HABILITACIÓN**	
No		
SOLICITANTE		
NOMBRE Y APELLIDOS	**CARGO**	
Virginia Montiel Martín	Responsable de programas ANECA	
Tipo Documento	**Número Documento**	
NIF	16609588T	
REPRESENTANTE LEGAL		
NOMBRE Y APELLIDOS	**CARGO**	
Juan Pablo Guzmán Palomino	Secretario General de la Universidad	
Tipo Documento	**Número Documento**	
NIF	24236227T	
RESPONSABLE DEL TÍTULO		
NOMBRE Y APELLIDOS	**CARGO**	
Manuel Sánchez Rubio	Director del Máster	
Tipo Documento	**Número Documento**	
NIF	08978689H	

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 5/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa que los datos solicitados en este impreso son necesarios para la tramitación de la solicitud y podrán ser objeto de tratamiento automatizado. La responsabilidad del fichero automatizado corresponde al Consejo de Universidades. Los solicitantes, como cedentes de los datos podrán ejercer ante el Consejo de Universidades los derechos de información, acceso, rectificación y cancelación a los que se refiere el Título III de la citada Ley 5-1999, sin perjuicio de lo dispuesto en otra normativa que ampare los derechos como cedentes de los datos de carácter personal.	
El solicitante declara conocer los términos de la convocatoria y se compromete a cumplir los requisitos de la misma, consintiendo expresamente la notificación por medios telemáticos a los efectos de lo dispuesto en el artículo 59 de la 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en su versión dada por la Ley 4/1999 de 13 de enero.	
	En: La Rioja, AM 28 de abril de 2023
	Firma: Representante legal de la Universidad

1. DESCRIPCIÓN DEL TÍTULO

1.1. DATOS BÁSICOS

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

LISTADO DE ESPECIALIDADES
No existen datos

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

NO HABILITA O ESTÁ VINCULADO CON PROFESIÓN REGULADA ALGUNA

AGENCIA EVALUADORA
Agencia Nacional de Evaluación de la Calidad y Acreditación

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	

LISTADO DE INSTITUCIONES PARTICIPANTES
No existen datos

1.2. DISTRIBUCIÓN DE CRÉDITOS EN EL TÍTULO

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

LISTADO DE ESPECIALIDADES	
ESPECIALIDAD	CRÉDITOS OPTATIVOS
No existen datos	

1.3. Universidad Internacional de La Rioja

1.3.1. CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS	
CÓDIGO	CENTRO
26004007	Escuela Superior de Ingeniería y Tecnología

1.3.2. Escuela Superior de Ingeniería y Tecnología

1.3.2.1. Datos asociados al centro

TIPOS DE ENSEÑANZA QUE SE IMPARTEN EN EL CENTRO		
PRESENCIAL	SEMIPRESENCIAL	VIRTUAL
No	No	Sí

PLAZAS DE NUEVO INGRESO OFERTADAS	
PRIMER AÑO IMPLANTACIÓN	SEGUNDO AÑO IMPLANTACIÓN
750	750
	TIEMPO COMPLETO

	ECTS MATRÍCULA MÍNIMA	ECTS MATRÍCULA MÁXIMA
PRIMER AÑO	60.0	60.0
RESTO DE AÑOS	49.0	60.0
	TIEMPO PARCIAL	
	ECTS MATRÍCULA MÍNIMA	ECTS MATRÍCULA MÁXIMA
PRIMER AÑO	22.0	48.0
RESTO DE AÑOS	22.0	48.0
NORMAS DE PERMANENCIA		
http://static.unir.net/documentos/normativa_permanencia_estudiante.pdf		
LENGUAS EN LAS 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	

2. JUSTIFICACIÓN, ADECUACIÓN DE LA PROPUESTA Y PROCEDIMIENTOS

Ver Apartado 2: Anexo 1.

3. COMPETENCIAS

3.1 COMPETENCIAS BÁSICAS Y GENERALES
BÁSICAS
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
GENERALES
CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarollarlos mediante los métodos y procesos adecuados.
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.
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.
CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación contínua en su futuro desempeño profesional como experto en seguridad informática.
CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de la entidades de TI.
CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática.
CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes.
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.
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.
3.2 COMPETENCIAS TRANSVERSALES
CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line.
CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc.
CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento.
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.
CT5 - Capacidad de investigar y comunicar los resultados de la investigación.
3.3 COMPETENCIAS ESPECÍFICAS
CE18 - Optimizar las políticas de seguridad de la infraestructura de la red de la entidad.
CE19 - Proteger la integridad de las bases de datos para asegurar la confidencialidad de la información sensible contenida.
CE20 - Asesorar sobre las distintas medidas de seguridad aplicables a los sistemas informáticos para disminuir el empacto de sus posibles fallos.

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.
CE22 - Diseñar las políticas de recuperación de datos más adecuadas par disminuir el impacto ante incidentes.
CE23 - Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones.
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención.
CE25 - Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, infraestructuras críticas y principales conceptos de auditoría de sistemas.
CE26 - Implantar procesos de análisis forense de cualquier sistema informático.
CE27 - Diseñar, implantar e institucionalizar un proceso de análisis y gestión de riesgos de los sistemas de información en cualquier organización.
CE1 - Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles.
CE2 - Adquirir una visión general e integrada del asesoramiento en seguridad que permita la colaboración con otros departamentos de la entidad.
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.
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.
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.
CE6 - Analizar el funcionamiento de herramientas de seguridad y su uso conjugado.
CE7 - Identificar y proceder contra aquellas conductas tipificadas como delito informático en el marco jurídico actual.
CE8 - Tomar decisiones proactivas y reactivas frente los posibles fallos de seguridad, investigando las causas que las originan.
CE9 - Comprender el funcionamiento, características y nevel de riesgo de los servicios de las empresas y establecer mecanismos de protección.
CE10 - Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos.
CE11 - Conocer todos los activos del negocio de la empresa y las variables necesarias para poder implementar un SGSI.
CE12 - Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa.
CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada inmplantación en su infraestructura.
CE14 - Diseñar las correctas políticas para analizar y reproducir los hechos ante un incidente de seguridad informática.
CE15 - Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad.
CE16 - Conocer y comprender la legislación europea en materia de seguridad, para poder emitir juicios sobre su aplicabilidad y relevancia en cada ámbito.
CE17 - Discernir los distintos mecanismos criptográficos para seleccionar el óptimo en cada ámbito de aplicación.

4. ACCESO Y ADMISIÓN DE ESTUDIANTES

4.1 SISTEMAS DE INFORMACIÓN PREVIO

Ver Apartado 4: Anexo 1.

4.2 REQUISITOS DE ACCESO Y CRITERIOS DE ADMISIÓN

4.2.1. 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.

4.2.2. 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 TICs. También profesionales con grado de diplomados, ingenieros técnicos, licenciados o ingenieros con amplia y constatable experiencia laboral en TICs.

4.2.3. Criterios de admisión

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

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

- 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 necesario seguir los requisitos de acceso establecidos en el artículo 18 del RD 822/20221, de 28 de septiembre. ~~contar con Titulación Universitaria. Este requisito se corresponde con los criterios de acceso establecidos en el artículo 16 del Real Decreto 1393/2007 de 29 de octubre, sobre Organización de las Enseñanzas Universitarias Oficiales, modificado por el Real Decreto 861/2010, de 2 de julio:~~

~~· Estar en posesión de un título universitario oficial español u otro expedido por una institución de educación superior perteneciente a otro estado integrante del Espacio Europeo de Educación Superior que faculte en el mismo para el acceso a enseñanzas de máster.~~

~~· Para los titulados conforme a sistemas educativos ajenos al Espacio Europeo de Educación Superior sin necesidad de homologar sus Títulos, previa comprobación por la Universidad de que aquellos acreditan un nivel de formación equivalente a los correspondientes Títulos universitarios oficiales españoles y que facultan en el país expedidor del Título para el acceso a enseñanzas de postgrado. El acceso por esta vía no implicará en ningún caso, la homologación del Título previo de que esté en posesión el interesado, ni su reconocimiento a otros efectos que el cursar las enseñanzas del 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.

4.2.4. Atención a estudiantes con necesidades especiales

Existe en UNIR el Servicio de Atención a las Necesidades Especiales que presta apoyo a los estudiantes en situación de diversidad funcional, temporal o permanente, aportando las soluciones más adecuadas a cada caso. Su objetivo prioritario es conseguir la plena integración en la vida universitaria de todos los estudiantes buscando los medios y recursos necesarios para hacer una universidad para todos.

La detección de dichas necesidades se realiza a través de diversos mecanismos:

- Estudiantes con certificado de discapacidad: siguiendo la idea central de proactividad se llama a todos los estudiantes.
- Desde tutorías: los tutores remiten al Servicio los casos de estudiantes sin certificado de discapacidad.
- Admisiones: los asesores remiten las dudas de los posibles futuros estudiantes con discapacidad, el Servicio se pone en contacto directamente con ellos.
- Otros departamentos: SOA (Servicio de Orientación Académica), Defensor Universitario, Solicitudes, etc.

En el contacto con el estudiante se definen los ámbitos de actuación: diagnóstico de necesidades, identificación de barreras, asesoramiento personalizado, etc.

Entre los servicios que presta se encuentran adaptaciones de materiales, curriculares, en los exámenes, asesoramiento pedagógico, etc., involucrando en cada caso a los departamentos implicados (Departamento de Exámenes, Dirección Académica, Profesorado, etc.).

ANEXO: 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).

4.3 APOYO A ESTUDIANTES

El Departamento de Educación en Internet es el encargado de garantizar el seguimiento y orientación de los estudiantes. Sus funciones se materializan en dos tipos de procedimientos referidos a:

1. Seguimiento y comprobación de la calidad de la orientación de los estudiantes a través del **Curso de introducción al campus virtual** que realizan la primera semana en cualquier titulación: incluye orientación relativa a la metodología docente de UNIR, papel de los tutores personales, modos de comunicación con el profesorado y con las autoridades académicas y, especialmente, el uso de las herramientas del aula virtual.

2. Seguimiento y comprobación de la calidad de la orientación de los estudiantes a través del **plan de acción tutorial personalizado**, que pretende garantizar la calidad de la orientación de los estudiantes a lo largo de todo el proceso formativo.

4.3.1. Primer contacto con el campus virtual

Cuando los estudiantes se enfrentan por primera vez a una herramienta como es una plataforma de formación en Internet pueden surgir muchas dudas de funcionamiento.

Este problema se soluciona en UNIR mediante un periodo de adaptación previo al comienzo del curso denominado "Curso de introducción al campus virtual", en el que el alumno dispone de un aula de información general que le permite familiarizarse con el campus virtual.

En esta aula se explica mediante vídeos y textos el concepto de UNIR como universidad en Internet. Incluye la metodología empleada, orientación para el estudio y la planificación del trabajo personal y sistemas de evaluación. El estudiante tiene un primer contacto con el uso de foros y envío de tareas a través del aula virtual.

Durante esta semana, el Departamento de Educación en Internet se encarga de:

1. **Revisión diaria de la actividad de los estudiantes en el campus virtual** a través de: correos electrónicos, llamadas de teléfono y del propio desarrollo de las actividades formativas. Los tutores personales realizan esta comprobación y si detectan alguna dificultad se ponen en contacto con el estudiante y le recomiendan que vuelva a los puntos que presentan mayor debilidad. Si persisten, el tutor personal resuelve de manera personal. Si aún persisten se pondrá en conocimiento de la dirección académica. Dicha incidencia será tomada en cuenta y tendrá un seguimiento especial durante los siguientes meses de formación.
2. **Test de autoaprendizaje al finalizar el curso de introducción al campus virtual.** Los tutores personales evalúan los resultados y en el caso de detectar alguna dificultad se ponen en contacto con el estudiante.

4.3.2. Seguimiento diario del alumnado

UNIR aplica un Plan de Acción Tutorial, que consiste en el acompañamiento y seguimiento del alumnado a lo largo del proceso educativo. Con ello se pretende lograr los siguientes objetivos:

- Favorecer la educación integral de los alumnos.
- Potenciar una educación lo más personalizada posible y que tenga en cuenta las necesidades de cada alumno y recurrir a los apoyos o actividades adecuadas.
- Promover el esfuerzo individual y el trabajo en equipo.

Para llevar a cabo el plan de acción tutorial, UNIR cuenta con un grupo de tutores personales. **Es personal no docente** que tiene como función la guía y asesoramiento del estudiante durante el curso. Todos ellos están en posesión de títulos superiores. Se trata de un sistema muy bien valorado por el alumnado, como se deduce de los resultados de las encuestas realizadas a los estudiantes.

A cada tutor personal se le asigna un grupo de alumnos para que realice su seguimiento. Para ello cuenta con la siguiente información:

- El acceso de cada usuario a los contenidos teóricos del curso además del tiempo de acceso.
- La utilización de las herramientas de comunicación del campus (foros, grupos de discusión, etc.).
- Los resultados de los test y actividades enviadas a través del campus.

Estos datos le permiten conocer el nivel de participación de cada estudiante para ofrecer la orientación adecuada.

4.3.3. Proceso para evitar abandonos

Dentro de las actuaciones del SOA (Servicio de Orientación Académica), las herramientas de organización y planificación, así como las metodologías de estudio que se les aporta a los estudiantes atendidos en este departamento, conducen a reducir posibles abandonos de los estudios. Por un lado, se mejora el aprendizaje y, por otro, se ayuda a los alumnos a valorar su disponibilidad de tiempo, de tal manera que la matriculación en el siguiente periodo se adapte verdaderamente a la carga lectiva que puedan afrontar.

4.4 SISTEMA DE TRANSFERENCIA Y RECONOCIMIENTO DE CRÉDITOS

Reconocimiento de Créditos Cursados en Enseñanzas Superiores Oficiales no Universitarias

MÍNIMO	MÁXIMO
0	9

Reconocimiento de Créditos Cursados en Títulos Propios

MÍNIMO	MÁXIMO
0	9

Adjuntar Título Propio

Ver Apartado 4: Anexo 2.

Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional

MÍNIMO	MÁXIMO
0	9

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).

4.6 COMPLEMENTOS FORMATIVOS

5. PLANIFICACIÓN DE LAS ENSEÑANZAS

5.1 DESCRIPCIÓN DEL PLAN DE ESTUDIOS
Ver Apartado 5: Anexo 1.
5.2 ACTIVIDADES FORMATIVAS
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
5.3 METODOLOGÍAS DOCENTES
No existen datos
5.4 SISTEMAS DE EVALUACIÓN
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
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
5.5 SIN NIVEL 1
NIVEL 2: GESTIÓN Y REGULACIÓN DE LA CIBERSEGURIDAD
5.5.1.1 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**
LENGUAS EN LAS 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	
NIVEL 3: Ciberdelitos y Regulación de la Ciberseguridad		
5.5.1.1.1 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**
LENGUAS EN LAS 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	
NIVEL 3: Gobierno de la Ciberseguridad y Análisis de Riesgos		
5.5.1.1.1 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**
LENGUAS EN LAS 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	

5.5.1.2 RESULTADOS DE APRENDIZAJE

Los resultados del aprendizaje esperados para esta materia pasan por la correcta comprensión de los aspectos relacionados con la legislación reguladora y su ámbito de aplicación, la protección de datos, la gestión de la seguridad, los delitos informáticos y los análisis de riesgos ~~legales~~ de los sistemas de información.

5.5.1.3 CONTENIDOS

~~**Aspectos Legales y Regulatorios.** Estudio genérico del marco legal vigente en materia de bienes y servicios informáticos, centrado en aspectos clave tales como propiedad industrial e intelectual, protección de datos o regulación de mercados.~~

~~**Análisis de Riesgos Legales**. Metodología para una gestión proactiva de los riesgos legales inherentes al desarrollo, implantación y despliegue de actividad informática~~

~~**Delitos Informáticos** **Ciberdelitos y Regulación de la Ciberseguridad.** Estudio de la legisación penal en materia de infracciones cuyo medio de comisión u objeto de la misma sean bienes o servicios informáticos, de tal manera que se permita su identificación, su denuncia y correspondiente seguimiento procesal. La presente asignatura posee también un estudio genérico del marco legal vigente en materia de bienes y servicios informáticos, centrado en aspectos clave tales como propiedad industrial e intelectual, protección de datos o regulación de mercados.

Gobierno de la Ciberseguridad y Análisis de Riesgos. Metodología para una gestión proactiva de los riesgos ~~legales~~ de los sistemas de información inherentes al desarrollo, implantación y despliegue de actividad informática, con especial atención a la industria del software, especialmente relevante en esta materia. Identificación de los problemas relacionados con la gestión de sistemas informáticos de seguridad, diseño de planes de auditoría, políticas de recuperación de datos, implantación de SGSI, grado de implantación de las normativas de seguridad, seguridad en la nube, infraestructuras críticas y diseño de planes de seguridad proactivos.

~~Esta materia da una visión de conjunto sobre los aspectos legales y el marco jurídico institucional en relación a la seguridad informática. También se estudia cómo analizar y recomendar diversas estrategias en dicho ámbito.~~

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarollarlos mediante los métodos y procesos adecuados.
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.
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.
CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación contínua en su futuro desempeño profesional como experto en seguridad informática.
CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de la entidades de TI.
CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática.
CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes.
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.
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.

CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
5.5.1.5.2 TRANSVERSALES
CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line.
CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc.
CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento.
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.
CT5 - Capacidad de investigar y comunicar los resultados de la investigación.
5.5.1.5.3 ESPECÍFICAS
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.
CE22 - Diseñar las políticas de recuperación de datos más adecuadas par disminuir el impacto ante incidentes.
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención.
CE25 - Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, infraestructuras críticas y principales conceptos de auditoría de sistemas.
CE27 - Diseñar, implantar e institucionalizar un proceso de análisis y gestión de riesgos de los sistemas de información en cualquier organización.
CE1 - Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles.
CE2 - Adquirir una visión general e integrada del asesoramiento en seguridad que permita la colaboración con otros departamentos de la entidad.
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.
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.
CE7 - Identificar y proceder contra aquellas conductas tipificadas como delito informático en el marco jurídico actual.
CE9 - Comprender el funcionamiento, características y nevel de riesgo de los servicios de las empresas y establecer mecanismos de protección.
CE10 - Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos.
CE11 - Conocer todos los activos del negocio de la empresa y las variables necesarias para poder implementar un SGSI.
CE12 - Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa.
CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada inmplantación en su infraestructura.
CE15 - Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad.
CE16 - Conocer y comprender la legislación europea en materia de seguridad, para poder emitir juicios sobre su aplicabilidad y relevancia en cada ámbito.

5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Sesiones presenciales virtuales	30	100
Recursos didácticos audiovisuales	12	0
Estudio del material básico	120	0
Lectura del material complementario	90	0
Proyectos y casos prácticos	34	0
Prácticas informáticas	20	0
Test de autoevaluación	8	0
Tutorías	32	30
Trabajo colaborativo	14	0
5.5.1.7 METODOLOGÍAS DOCENTES		
No existen datos		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Participación en foros y otros medios participativos	0.0	10.0
Realización de proyectos y casos prácticos	10.0	20.0
Prácticas informáticas	20.0	30.0
Test de autoevaluación	0.0	10.0
Prueba de evaluación final	60.0	60.0
NIVEL 2: AUDITORÍA Y ANÁLISIS FORENSE		
5.5.1.1 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**
LENGUAS EN LAS 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	
NIVEL 3: Informática Forense y Respuesta ante Incidentes		
5.5.1.1.1 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**
LENGUAS EN LAS 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	
NIVEL 3: Hacking Ético y Análisis de Malware		
5.5.1.1.1 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**
LENGUAS EN LAS 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	
NIVEL 3: Desarrollo Seguro de Software y Auditoría de la Ciberseguridad		
5.5.1.1.1 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
LENGUAS EN LAS 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	

5.5.1.2 RESULTADOS DE APRENDIZAJE

Los resultados del aprendizaje esperados para esta materia pasan por la correcta comprensión de los aspectos relacionados con los análisis de ~~ries-gos~~ vulnerabilidades en los sistemas, la securización del software, definir y desarrollar unos procesos correctos de auditoría de la seguridad, ~~los meca-nismos de protección, el diseño~~ comprensión y ejecución de ~~planes~~ de una forma correcta de un análisis forense y la respuesta ante incidentes de se-guridad~~, los SGSI, y la auditoría de sistemas en entornos sensibles~~.

5.5.1.3 CONTENIDOS

~~**Gestión de la Seguridad**. Identificación de los problemas relacionados con la gestión de sistemas informáticos de seguridad, diseño de planes de au-ditoría, implantación de SGSI, grado de implantación de las normativas de seguridad, diseño de planes de seguridad proactivos, desarrollo de políticas de seguridad, despliegue de políticas de seguridad, seguimiento de políticas de seguridad, autenticación, control de accesos, pruebas de conocimiento nulo.~~

Informática Forense y Respuesta ante Incidentes. Diseño y desarrollo de un plan de respuesta ante incidentes para minimizar su impacto, contem-plado en el diseño de los planes de seguridad y los planes de auditoría, durante el que se va a trabajar la recuperación de información, adquisición de datos, metodología de análisis forense, investigación de datos, documentación de procesos, herramientas de recuperación de información, medidas reactivas, protección ante desastres, redundancia de sistemas de ficheros, sistemas de ficheros avanzados.

Hacking Ético y Análisis de ~~Vulnerabilidades~~ Malware. Estudio de los fallos de seguridad, tipos de vulnerabilidades, explotación de vulnerabilida-des, gestión de memoria, mecanismos de protección de memoria, espacio de usuario y de sistema, exploits locales, exploits remotos, alteraciones bá-sicas, explotaciones de memoria, shellcodes, escalada de privilegios, integer overflow, buffer overflow, heap overflow, inyección de código, puertas tra-seras, rootkits, protección de ejecutables. También se estudian las recomendaciones a tener en cuenta a la hora de desarrollar software y técnicas de análisis y reingeniería de *malware* aplicadas al análisis de *malware* para poder comprender el funcionamiento del código malicioso.

Desarrollo Seguro de Software y Auditoría de la Ciberseguridad. Sistemas de memoria, fortificación de aplicaciones, prevención de desbordamien-tos de memoria, prevención de ataques basados en cadenas, condiciones de carrera, inducción de fallos, política de mínimos privilegios, autentica-ción, control de acceso. Planes de auditoría, ~~auditoría técnica y de certificación,~~ tipos de auditorías, ~~auditorías de SGSI,~~ aspectos documentales, meto-dologías de auditoría, ejecución de auditorías, herramientas de auditoría, ~~ISO 27000,~~ estudio comparativo de auditorías.

~~Esta materia se centra en el estudio de los Sistemas de Gestión de la Seguridad que permitirán diseñar e implementar medidas y planes para mejorar la seguridad informática en una organización. Del mismo modo, se estudiarán las vulnerabilidades más utilizadas para desestabilizar sistemas informá-ticos permitiendo interrumpir su funcionamiento e incluso tomar control sobre ellos de forma no autorizada. El estudio de estos dos temas se comple-mentará con la auditoría de seguridad, que servirá para comprender los procesos más avanzados utilizados en dicha disciplina.~~

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarollarlos mediante los métodos y procesos adecuados.

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.

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.

CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación contínua en su futuro desempeño profesional como experto en seguridad informática.

CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de la entidades de TI.

CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática.

CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes.
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.
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.
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
5.5.1.5.2 TRANSVERSALES
CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line.
CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc.
CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento.
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.
CT5 - Capacidad de investigar y comunicar los resultados de la investigación.
5.5.1.5.3 ESPECÍFICAS
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.
CE22 - Diseñar las políticas de recuperación de datos más adecuadas par disminuir el impacto ante incidentes.
CE23 - Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones.
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención.
CE25 - Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, infraestructuras críticas y principales conceptos de auditoría de sistemas.
CE26 - Implantar procesos de análisis forense de cualquier sistema informático.
CE1 - Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles.
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.
CE6 - Analizar el funcionamiento de herramientas de seguridad y su uso conjugado.
CE8 - Tomar decisiones proactivas y reactivas frente los posibles fallos de seguridad, investigando las causas que las originan.
CE9 - Comprender el funcionamiento, características y nevel de riesgo de los servicios de las empresas y establecer mecanismos de protección.
CE12 - Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa.
CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada inmplantación en su infraestructura.
CE14 - Diseñar las correctas políticas para analizar y reproducir los hechos ante un incidente de seguridad informática.
5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	45	100
Recursos didácticos audiovisuales	18	0
Estudio del material básico	180	0
Lectura del material complementario	135	0
Proyectos y casos prácticos	51	0
Prácticas informáticas	30	0
Test de autoevaluación	12	0
Tutorías	48	30
Trabajo colaborativo	21	0
5.5.1.7 METODOLOGÍAS DOCENTES		
No existen datos		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Participación en foros y otros medios participativos	0.0	10.0
Realización de proyectos y casos prácticos	10.0	20.0
Prácticas informáticas	20.0	30.0
Test de autoevaluación	0.0	10.0
Prueba de evaluación final	60.0	60.0
NIVEL 2: TÉCNICAS AVANZADAS DE SEGURIDAD		
5.5.1.1 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**
LENGUAS EN LAS 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	
NIVEL 3: Seguridad en Redes y Análisis Inteligente de Amenazas		
5.5.1.1.1 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**
LENGUAS EN LAS 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	
NIVEL 3: Seguridad en Sistemas, Aplicaciones y el Big Data		
5.5.1.1.1 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**
LENGUAS EN LAS 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	

5.5.1.2 RESULTADOS DE APRENDIZAJE

Los resultados del aprendizaje esperados para esta materia pasan por ~~la correcta comprensión de~~ proteger los ~~aspectos relacionados con las distintas herramientas de~~ principales sistemas operativos que hoy en día existen en el mundo de la informática, aplicar una seguridad~~,~~ lo más óptima posible de una aplicación desplegada en online y de sus repositorios de datos asociados, como son los ~~mecanismos de seguridad,~~ Sistemas Gestores de Bases de Datos o los ~~informes técnicos de seguridad,~~ Servicios de Directorio Activo y describir las tecnologías de protección de los ~~mecanismos criptográficos y los elementos involucrados en un entorno de seguridad~~ sistemas de información distribuidos.

5.5.1.3 CONTENIDOS

Seguridad en Redes y Análisis Inteligente de Amenazas. Aspectos avanzados sobre redes TCP/IP, seguridad en redes, ataques contra redes, denegaciones de servicio, analizadores de tráfico, zonas desmilitarizadas, características avanzadas de los sistemas de cortafuegos, redes privadas virtuales, sistemas remotos seguros, TLS/SSL, IPSec, algoritmos criptográficos usados en los protocolos de seguridad, sistemas de detección de intrusos, detección de ataques distribuidos, medidas de protección proactivas, escaneo de vulnerabilidades en redes, sistemas de gestión de identidades y control de acceso, búsqueda de patrones de ataque dinámicos, que van aprendiendo y evolucionando con el tiempo de forma autónoma.

Seguridad en Sistemas ~~operativos~~, Aplicaciones y el Big Data. Administración de servidores, estudio avanzado de servicios, estudio avanzado de sistemas de memoria, mecanismos de protección de memoria, sistemas de protección del espacio de núcleo, monitorización de procesos, ~~sistemas de~~

detección de intrusiones en sistemas de ficheros, cuotas de disco, monitorización de usuarios, gestión de permisos, políticas de sistemas operativos en organizaciones, y administración de discos, denegaciones de servicio. Principales arquitecturas de bases de datos, inyección SQL, inyección SQL a ciegas, desbordamiento de memoria en bases de datos, Cross-site scripting, Cross-site request forgery, form tampering, clickjacking, remote file inclusión, escalada de directorios, escalada transversal de directorios, ataques a ciegas, acceso remoto a sistemas, protección de servidores web, medidas de seguridad en servidores tanto locales como en la nube, ataques a sistemas desplegados sobre infraestructuras de red, autenticación, control de acceso. Análisis de información de los sistemas y aplicaciones mediante el uso de técnicas de Big Data para alertar de posibles ataques.

Criptografía y mecanismos de seguridad. Fundamentos matemáticos avanzados sobre sistemas criptográficos, criptografía clásica, criptografía de clave secreta, criptografía de clave pública, sistemas criptográficos híbridos, funciones de resumen criptográfico hash, funciones de resumen criptográfico HMAC, autenticación de mensajes, firma digital, protocolos criptográficos seguros, transmisión segura de información, criptoanálisis, ataques de diccionario, ataques de fuerza bruta.

Esta materia da una visión de conjunto sobre los aspectos más avanzados de la seguridad en redes, tratando temas que resultarán decisivos a la hora de proteger correctamente una red desde el punto de vista de la seguridad informática. Igualmente, se aprenderán las técnicas más avanzadas de seguridad en los distintos sistemas operativos y los sistemas criptográficos más modernos y seguros, que sustentan la arquitectura de seguridad de todos los sistemas críticos en Internet.

5.5.1.4 OBSERVACIONES

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarollarlos mediante los métodos y procesos adecuados.

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.

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.

CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación contínua en su futuro desempeño profesional como experto en seguridad informática.

CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de la entidades de TI.

CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática.

CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes.

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.

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.

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

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

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

5.5.1.5.2 TRANSVERSALES

CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line.

CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc.

CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento.

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.

CT5 - Capacidad de investigar y comunicar los resultados de la investigación.
5.5.1.5.3 ESPECÍFICAS
CE18 - Optimizar las políticas de seguridad de la infraestructura de la red de la entidad.
CE19 - Proteger la integridad de las bases de datos para asegurar la confidencialidad de la información sensible contenida.
CE20 - Asesorar sobre las distintas medidas de seguridad aplicables a los sistemas informáticos para disminuir el empacto de sus posibles fallos.
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.
CE23 - Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones.
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención.
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.
CE6 - Analizar el funcionamiento de herramientas de seguridad y su uso conjugado.
CE9 - Comprender el funcionamiento, características y nevel de riesgo de los servicios de las empresas y establecer mecanismos de protección.
CE10 - Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos.
CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada inmplantación en su infraestructura.
CE15 - Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad.
CE17 - Discernir los distintos mecanismos criptográficos para seleccionar el óptimo en cada ámbito de aplicación.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	30	100
Recursos didácticos audiovisuales	12	0
Estudio del material básico	120	0
Lectura del material complementario	90	0
Proyectos y casos prácticos	34	0
Prácticas informáticas	20	0
Test de autoevaluación	8	0
Tutorías	32	30
Trabajo colaborativo	14	0

5.5.1.7 METODOLOGÍAS DOCENTES

No existen datos

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Participación en foros y otros medios participativos	0.0	10.0
Realización de proyectos y casos prácticos	10.0	20.0
Prácticas informáticas	20.0	30.0
Test de autoevaluación	0.0	10.0
Prueba de evaluación final	60.0	60.0

NIVEL 2: PRÁCTICAS EN EMPRESA

5.5.1.1 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**
LENGUAS EN LAS 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	
NIVEL 3: Prácticas en Empresa		
5.5.1.1.1 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**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS 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	
5.5.1.2 RESULTADOS DE APRENDIZAJE		
Los resultados del aprendizaje esperados para esta materia pasan por la correcta aplicación de los conocimientos adquiridos durante el estudio del resto de materias del plan de estudios.		
5.5.1.3 CONTENIDOS		
Prácticas en empresas Realización labores básicas de seguridad informática, tuteladas por un profesional que supervisa el correcto desarrollo de las tareas que se le asignen y mantiene las relaciones pertinentes con el tutor designado por la UNIR quienes, en régimen de colaboración, velan por la óptima formación del alumno. Los detalles de las tareas a desarrollar por el alumno durante la ~~estancia~~ realización de las prácticas en la empresa serán fijadas por el Tutor de Prácticas Externas y se adaptarán a las peculiaridades propias de cada centro.		
5.5.1.4 OBSERVACIONES		

En relación a la actividad formativa "Realización de prácticas en el centro", se entiende por presencialidad, las tareas o proyectos realizados por el alumno en el centro de prácticas, ya sea de forma presencial o en la modalidad teletrabajo.
5.5.1.5 COMPETENCIAS
5.5.1.5.1 BÁSICAS Y GENERALES
CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarollarlos mediante los métodos y procesos adecuados.
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.
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.
CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación contínua en su futuro desempeño profesional como experto en seguridad informática.
CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de la entidades de TI.
CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática.
CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes.
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.
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.
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
5.5.1.5.2 TRANSVERSALES
CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line.
CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc.
CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento.
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.
CT5 - Capacidad de investigar y comunicar los resultados de la investigación.
5.5.1.5.3 ESPECÍFICAS
CE18 - Optimizar las políticas de seguridad de la infraestructura de la red de la entidad.
CE19 - Proteger la integridad de las bases de datos para asegurar la confidencialidad de la información sensible contenida.
CE20 - Asesorar sobre las distintas medidas de seguridad aplicables a los sistemas informáticos para disminuir el empacto de sus posibles fallos.
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.

CE22 - Diseñar las políticas de recuperación de datos más adecuadas par disminuir el impacto ante incidentes.
CE23 - Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones.
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención.
CE25 - Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, infraestructuras críticas y principales conceptos de auditoría de sistemas.
CE26 - Implantar procesos de análisis forense de cualquier sistema informático.
CE27 - Diseñar, implantar e institucionalizar un proceso de análisis y gestión de riesgos de los sistemas de información en cualquier organización.
CE1 - Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles.
CE2 - Adquirir una visión general e integrada del asesoramiento en seguridad que permita la colaboración con otros departamentos de la entidad.
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.
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.
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.
CE6 - Analizar el funcionamiento de herramientas de seguridad y su uso conjugado.
CE7 - Identificar y proceder contra aquellas conductas tipificadas como delito informático en el marco jurídico actual.
CE8 - Tomar decisiones proactivas y reactivas frente los posibles fallos de seguridad, investigando las causas que las originan.
CE9 - Comprender el funcionamiento, características y nevel de riesgo de los servicios de las empresas y establecer mecanismos de protección.
CE10 - Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos.
CE11 - Conocer todos los activos del negocio de la empresa y las variables necesarias para poder implementar un SGSI.
CE12 - Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa.
CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada inmplantación en su infraestructura.
CE14 - Diseñar las correctas políticas para analizar y reproducir los hechos ante un incidente de seguridad informática.
CE15 - Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad.
CE16 - Conocer y comprender la legislación europea en materia de seguridad, para poder emitir juicios sobre su aplicabilidad y relevancia en cada ámbito.
CE17 - Discernir los distintos mecanismos criptográficos para seleccionar el óptimo en cada ámbito de aplicación.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesiones presenciales virtuales	3	100
Realización de prácticas en el centro	126	100
Redacción de la memoria de prácticas	36	0
Tutorías (Prácticas)	15	0

5.5.1.7 METODOLOGÍAS DOCENTES

No existen datos

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Evaluación con base en el informe del tutor externo	40.0	40.0

Memoria de prácticas	60.0	60.0
NIVEL 2: TRABAJO FIN DE MÁSTER		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Trabajo Fin de Grado / Máster	
ECTS NIVEL 2	12	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	12	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NIVEL 3: Trabajo Fin de Máster		
5.5.1.1.1 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**
LENGUAS EN LAS 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	
5.5.1.2 RESULTADOS DE APRENDIZAJE		

Los resultados del aprendizaje esperados para esta materia pasan por la correcta aplicación de los conocimientos adquiridos durante el estudio del resto de materias del plan de estudios

5.5.1.3 CONTENIDOS

Trabajo Fin de Máster

Se realiza bajo el asesoramiento y orientación del Profesor, siguiendo las directrices marcadas por el Reglamento de Trabajos de Fin de Grado (TFG) y de Fin de Máster (TFM) en los programas de enseñanzas oficiales de la Universidad Internacional de La Rioja (UNIR).

Elaboración, diseño y defensa pública de un caso teórico o práctico sobre seguridad informática, donde el estudiante deberá demostrar sus habilidades y conocimientos en relación a uno o varios de los siguientes aspectos:

- Análisis exhaustivo de sistemas informáticos complejos, en los que la seguridad resulte un elemento crítico para su correcto funcionamiento.
- Identificación de las potenciales amenazas, debilidades y elementos inseguros, tanto externos como internos. Estos pueden pertenecer tanto al plano técnico, como administrativo, legal, o una combinación de los mismos.
- Realización de un análisis detallado de las amenazas, debilidades y elementos inseguros; para la posterior realización de un informe con posibles soluciones, así como con recomendaciones para mejorar el sistema desde el punto de vista de la seguridad informática.
- Presentación del plan de implantación para las soluciones anteriormente descritas.

5.5.1.4 OBSERVACIONES

De acuerdo con el Real Decreto 1393/2007, derogado y sustituido por el RD 822/2021, de 28 de septiembre, la defensa pública del Trabajo Fin de Máster tiene carácter obligatorio.

El trabajo fin de máster se realiza individualmente o de manera grupal, con el seguimiento continuo por parte de un profesor-director de TFM, durante la elaboración del mismo. En este máster se justifica la inclusión de la posibilidad de realizar el Trabajo Fin de Máster de manera grupal, debido a debido a que en el mundo laboral dentro del sector de la ciberseguridad los trabajos se conciben en equipos multidisciplinares en los que deben trabajar en conjunto para poder afrontar los problemas/proyectos. Por ello, es necesario que los estudiantes de nuestra titulación desarrollen esta capacidad de trabajo en grupo, aprendiendo a justificar sus decisiones frente a sus compañeros, creando un entorno lo más similar posible a lo que será el ambiente laboral al que se van a tener que enfrentar al completar la titulación.

Elaboración, defensa y evaluación de trabajos grupales de fin de máster

Elaboración

En el caso de que el trabajo de fin de máster se realice en grupo, se deberá incluir un apartado específico sobre la organización del grupo dónde se especifiquen las partes en las que se ha dividido el trabajo, los objetivos y responsables de cada una de ellas y los mecanismos de coordinación entre los miembros del grupo.

El director del TFM asegurará un correcto **seguimiento individual** de cada uno de los integrantes del grupo a través de **tutorías individuales (4 horas)**. Prestará especial atención a verificar las tareas individualmente realizadas por cada uno de los miembros y su evolución para asegurar que cada uno de los miembros del grupo avanza adecuadamente. **Además**, se realizarán **tutorías grupales (4 horas)** con todos los componentes de modo que se pueda garantizar el avance adecuado (tanto individual como grupal) y ajustes del proceso. Estas tutorías servirán de mecanismo corrector para los obstáculos que se puedan observar pudiendo el director del TFM reasignar tareas si el trabajo final se pudiese ver comprometido.

El estudiante que no cumpla la planificación de trabajo comprometida, podrá ser objeto de apercibimiento de expulsión del grupo por parte de su director del trabajo. La persistente falta de colaboración e incumplimiento por parte de alguno de los integrantes del grupo, previamente constatada por el director de TFM y después del correspondiente apercibimiento, podrá tener como consecuencia la expulsión del equipo. El estudiante que resulte expulsado pasará a la realización de un trabajo realizado de manera individual.

En caso de que un estudiante por, cualquiera que sea la causa, hubiera de abandonar un TFM grupal y con el fin de no generar daños al resto del grupo, el Director/Coordinador del título o la Comisión Académica del título, será la encargada de gestionar la reorganización del grupo y de las tareas que queden pendientes de entrega. Así mismo, deberán garantizar la asignación de un nuevo director para el estudiante que hubo de abandonar el grupo, pudiendo encomendarse esta tarea a la propia Comisión Académica o Director/Coordinador del título.

Defensa y evaluación

El director de un TFM en grupo debe realizar el informe de autorización de forma individual para cada uno de los componentes del grupo, teniendo en cuenta para ello el seguimiento individual que haya realizado de cada uno de ellos. Por ello, cabe la posibilidad de que no todos los miembros del equipo obtengan autorización para defensa.

Durante la defensa cada miembro del grupo presentará una de las partes, aunque se podrá dirigir las cuestiones que se considere oportunas a cualquiera de sus componentes o solicitar a cualquier miembro que defienda y explique cualquier parte.

La calificación final se hará de manera individual a cada uno de los componentes del grupo, teniendo en cuenta sus aportaciones al trabajo final y la defensa individual de la parte que haya defendido y las contestaciones a las cuestiones planteadas.

Cabe recordar, según se indica en la ficha de la materia y en el apartado 5.1, que para el trabajo grupal de fin de máster la ponderación de los sistemas de evaluación, es la siguiente:

SISTEMA DE EVALUACIÓN	PONDERACIÓN
Evaluación de la estructura del Trabajo Fin de Máster	20 %
Evaluación de la exposición del Trabajo Fin de Máster	30 %
Evaluación del contenido individual del Trabajo Fin de Máster	50 %

La **evaluación final**, por tanto, tiene dos componentes: uno individual y otro grupal.

Individual:

"Evaluación de la exposición del Trabajo Fin de Máster". Representa el 30 % de la calificación final y refleja la exposición y defensa individual que el miembro del grupo realice.

"Evaluación del contenido individual del Trabajo Fin de Máster". Representa el 50 % de la calificación final y refleja la calificación que la Comisión evaluadora realiza de la parte del trabajo bajo responsabilidad del estudiante.

De este modo, la calificación individualizada supone el 80 % de la evaluación final.

Grupal:

"Evaluación de la estructura del Trabajo Fin de Máster". Representa el 20 % de la calificación final y, dado que, la estructura del TFM es única, será la misma calificación para todos los miembros del grupo.

De este modo, la calificación grupal supone el 20 % de la evaluación final.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarollarlos mediante los métodos y procesos adecuados.

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.

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.

CG3 - Mantener una actitud que les permita estudiar de manera autónoma y promover la formación contínua en su futuro desempeño profesional como experto en seguridad informática.

CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de la entidades de TI.

CG6 - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática.

CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes.

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.

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.

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

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

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

5.5.1.5.2 TRANSVERSALES

CT1 - Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line.

CT2 - Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc.

CT3 - Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento.

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.

CT5 - Capacidad de investigar y comunicar los resultados de la investigación.
5.5.1.5.3 ESPECÍFICAS
CE18 - Optimizar las políticas de seguridad de la infraestructura de la red de la entidad.
CE19 - Proteger la integridad de las bases de datos para asegurar la confidencialidad de la información sensible contenida.
CE20 - Asesorar sobre las distintas medidas de seguridad aplicables a los sistemas informáticos para disminuir el empacto de sus posibles fallos.
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.
CE22 - Diseñar las políticas de recuperación de datos más adecuadas par disminuir el impacto ante incidentes.
CE23 - Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones.
CE24 - Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención.
CE25 - Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, infraestructuras críticas y principales conceptos de auditoría de sistemas.
CE26 - Implantar procesos de análisis forense de cualquier sistema informático.
CE27 - Diseñar, implantar e institucionalizar un proceso de análisis y gestión de riesgos de los sistemas de información en cualquier organización.
CE1 - Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles.
CE2 - Adquirir una visión general e integrada del asesoramiento en seguridad que permita la colaboración con otros departamentos de la entidad.
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.
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.
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.
CE6 - Analizar el funcionamiento de herramientas de seguridad y su uso conjugado.
CE7 - Identificar y proceder contra aquellas conductas tipificadas como delito informático en el marco jurídico actual.
CE8 - Tomar decisiones proactivas y reactivas frente los posibles fallos de seguridad, investigando las causas que las originan.
CE9 - Comprender el funcionamiento, características y nevel de riesgo de los servicios de las empresas y establecer mecanismos de protección.
CE10 - Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos.
CE11 - Conocer todos los activos del negocio de la empresa y las variables necesarias para poder implementar un SGSI.
CE12 - Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa.
CE13 - Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada inmplantación en su infraestructura.
CE14 - Diseñar las correctas políticas para analizar y reproducir los hechos ante un incidente de seguridad informática.
CE15 - Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad.
CE16 - Conocer y comprender la legislación europea en materia de seguridad, para poder emitir juicios sobre su aplicabilidad y relevancia en cada ámbito.
CE17 - Discernir los distintos mecanismos criptográficos para seleccionar el óptimo en cada ámbito de aplicación.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Sesión Inicial de presentación de TFM	2	100
Lectura de material en el aula virtual (TFM)	5	0

Seminarios de TFM	2	100
Tutorías (TFM)	8	100
Sesiones grupales de TFM	3	100
Elaboración del Trabajo Fin de Máster	340	0
5.5.1.7 METODOLOGÍAS DOCENTES		
No existen datos		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Evaluación de la Estructura del Trabajo Fin de Máster	20.0	20.0
Evaluación de la Exposición del Trabajo Fin de Máster	30.0	30.0
Evaluación del Contenido individual del Trabajo Fin de Máster	50.0	50.0

6. PERSONAL ACADÉMICO

6.1 PROFESORADO Y OTROS RECURSOS HUMANOS				
Universidad	**Categoría**	**Total %**	**Doctores %**	**Horas %**
Universidad Internacional de La Rioja	Ayudante	36.5	0	36,5
Universidad Internacional de La Rioja	Profesor Adjunto	18.9	100	18,9
Universidad Internacional de La Rioja	Profesor Asociado (incluye profesor asociado de C.C.: de Salud)	44.6	100	44,6

PERSONAL ACADÉMICO

Ver Apartado 6: Anexo 1.

6.2 OTROS RECURSOS HUMANOS

Ver Apartado 6: Anexo 2.

7. RECURSOS MATERIALES Y SERVICIOS

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

8. RESULTADOS PREVISTOS

8.1 ESTIMACIÓN DE VALORES CUANTITATIVOS

TASA DE GRADUACIÓN %	TASA DE ABANDONO %	TASA DE EFICIENCIA %
60	25	80

CODIGO	TASA	VALOR %
No existen datos		

Justificación de los Indicadores Propuestos:

Ver Apartado 8: Anexo 1.

8.2 PROCEDIMIENTO GENERAL PARA VALORAR EL PROCESO Y LOS RESULTADOS

8.2. Procedimiento general para valorar el progreso y los resultados de aprendizaje

La Política de Calidad de la UNIR fue definida para promover y garantizar el logro de la misión de la organización. El despliegue de la Política de Calidad se evidencia en la implantación de un Sistema de Aseguramiento Interno de Calidad (SAIC), que es de aplicación en cada Centro y Departamento responsables de los Títulos de Grado, Máster, y Doctorado. Dicho sistema queda recogido en el criterio 9 de esta guía y aparece desarrollado en el Manual de Calidad y sus procedimientos. La estructura definida en el Manual de Calidad establece que la Unidad de Calidad, UNICA, será el órgano responsable del seguimiento y la toma de decisiones generales sobre el SAIC y de cada titulación, en este último caso recibe la asistencia y colaboración de las Unidades de Calidad de Titulación (en adelante UCT).

Para garantizar el adecuado funcionamiento del SAIC se han establecido diferentes instrumentos de seguimiento que aparecen recogidos en el procedimiento PC-6-1.2 donde se describe cómo se realiza la medición, el análisis de los resultados y la mejora continua.

- Las unidades de calidad que realizan el análisis **del progreso, de los resultados de aprendizaje y del logro de los objetivos establecidos inicialmente**, elaboran un informe anual de conclusiones indicando las posibles medidas correctivas, en su caso, y el correspondiente informe de propuestas de mejora (DC_6.1.2-1 Informe Anual de la Unidad de Calidad de titulación y DC_6.1.2-3 Informe de Propuestas de Mejora).
- **La UNICA** recibe y analiza la información de cada Titulación y de cada Departamento involucrado en la calidad del proceso de enseñanza-aprendizaje realizando, en su caso, las sugerencias que considere oportunas al Plan de Mejora.

En particular, y adaptado a esta titulación y a estos resultados el procedimiento es el siguiente:

Tras cada periodo de evaluación, a través de la aplicación informática de informes de calidad, Dirección Académica del Título comprueba si los resultados obtenidos se adecúan a las expectativas, o si por el contrario, es necesario definir alguna medida (en la mayoría de los casos, estas medidas vendrán sugeridas por profesores, alumnos y la propia coordinación).

La Coordinación Académica es la encargada de custodiar los datos y los registros necesarios. Para su custodia y comunicación dispone de un espacio compartido, el REPOSITORIO DOCUMENTAL, donde son controlados los documentos por parte del Departamento de Calidad, pero accesibles para su consulta por parte de todos los usuarios autorizados (PC-6-3 Procedimiento para la aprobación, modificación de procedimientos y control de la documentación).

Con los datos obtenidos, la coordinación Académica realiza un análisis de los mismos y del logro de los objetivos establecidos inicialmente. Elabora un informe anual de conclusiones indicando las posibles medidas correctivas, en su caso, y el correspondiente informe de propuestas de mejora (DC_6.1.2-1 Informe Anual de la Unidad de Calidad de titulación y DC_6.1.2-3 Informe de Propuestas de Mejora).

UNICA recibe y analiza la información de cada Titulación realizando, en su caso, sugerencias al Plan de Mejora que se haya establecido en el informe.

UNICA traslada la información a la Comisión Permanente del Consejo Directivo para la aprobación de las medidas propuestas o su desestimación.

Toda información relevante se hace saber a los grupos implicados (ver Plan de comunicación y PA-5.2 de Comunicación Interna.)

De este modo la UNICA, tiene una visión conjunta de todas las titulaciones y propone en el Pleno de la UNICA, que se reúne al inicio y al final del curso, las acciones de mejora que son necesarias a nivel global de Universidad y ratifica las propuestas de cada UCT para su titulación.

9. SISTEMA DE GARANTÍA DE CALIDAD

ENLACE	http://www.unir.net/universidad-online/manual-calidad-procedimientos/

10. CALENDARIO DE IMPLANTACIÓN

10.1 CRONOGRAMA DE IMPLANTACIÓN	
CURSO DE INICIO	2011
Ver Apartado 10: Anexo 1.	
10.2 PROCEDIMIENTO DE ADAPTACIÓN	
No procede	
10.3 ENSEÑANZAS QUE SE EXTINGUEN	
CÓDIGO	**ESTUDIO - CENTRO**

11. PERSONAS ASOCIADAS A LA SOLICITUD

11.1 RESPONSABLE DEL TÍTULO			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
08978689H	Manuel	Sánchez	Rubio
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Avenida de la Paz, 137	26006	La Rioja	Logroño
EMAIL	**MÓVIL**	**FAX**	**CARGO**
virginia.montiel@unir.net	676614276	902877037	Director del Máster
11.2 REPRESENTANTE LEGAL			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
24236227T	Juan Pablo	Guzmán	Palomino
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Avenida de la Paz, 137	26006	La Rioja	Logroño
EMAIL	**MÓVIL**	**FAX**	**CARGO**
virginia.montiel@unir.net	676614276	902877037	Secretario General de la Universidad
El Rector de la Universidad no es el Representante Legal			
Ver Apartado 11: Anexo 1.			
11.3 SOLICITANTE			
El responsable del título no es el solicitante			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
16609588T	Virginia	Montiel	Martín
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Avenida de la Paz, 137	26006	La Rioja	Logroño
EMAIL	**MÓVIL**	**FAX**	**CARGO**
virginia.montiel@unir.net	676614276	902877037	Responsable de programas ANECA

Apartado 2: Anexo 1

Nombre : 2_Justificacion_completo2.pdf

HASH SHA1 : 9883F20C47451BF09E0EA8FA0AAA4788522446CD

Código CSV : 631962648643515748939571

Ver Fichero: 2_Justificacion_completo2.pdf

Apartado 4: Anexo 1

Nombre : 4.1_Sistemas_de_información_previo.pdf

HASH SHA1 : 3C4A29E8874F0A7A0BC5C861FFD3468479A2A7A0

Código CSV : 44624606524150224715382 3

Ver Fichero: 4.1_Sistemas_de_información_previo.pdf

Apartado 5: Anexo 1

Nombre : 5_1_Planificación de las Enseñanzas.pdf

HASH SHA1 : F542B7F932FC70184B0A13250E5664BD7D36DC9D

Código CSV : 615036947033634270784222

Ver Fichero: 5_1_Planificación de las Enseñanzas.pdf

Apartado 6: Anexo 1

Nombre : 6_1_Personal Académico_v2.pdf

HASH SHA1 : 4560D6F7EE5354A27DE545BA99EE19A82250E93B

Código CSV : 616608724750905973228401

Ver Fichero: 6_1_Personal Académico_v2.pdf

Apartado 6: Anexo 2

Nombre : 6_2_Otros RRHH.pdf

HASH SHA1 : 0FA8E9067DF65E011E59F7DE81416A89792A99C6

Código CSV : 615042511407072414962775

Ver Fichero: 6_2_Otros RRHH.pdf

Apartado 7: Anexo 1

Nombre : 7_Recursos Materiales.pdf

HASH SHA1 : 2BBDFBF3B53132F2C25BCC141C288AF3BF44E844

Código CSV : 616744519526702154332418

Ver Fichero: 7_Recursos Materiales.pdf

Apartado 8: Anexo 1

Nombre : 8.1_Estimacion_valores_cuantitativos.pdf

HASH SHA1 : 247FA6A127CCF89990ACCED571E462471F9DC030

Código CSV : 446687851065124944082745

Ver Fichero: 8.1_Estimacion_valores_cuantitativos.pdf

Apartado 10: Anexo 1

Nombre : 10_Calendario de Implantación.pdf

HASH SHA1 : 622F36B903D9B3802D05D8D33673D157A7B56AA4

Código CSV : 615069808402473294460299

Ver Fichero: 10_Calendario de Implantación.pdf

Apartado 11: 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