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 de Cádiz	Escuela Superior de Ingeniería	11006531

NIVEL	DENOMINACIÓN CORTA
Máster	Seguridad Informática (Ciberseguridad)

DENOMINACIÓN ESPECÍFICA
Máster Universitario en Seguridad Informática (Ciberseguridad) por la Universidad de Cádiz

NIVEL MECES
3|3

RAMA DE CONOCIMIENTO	CONJUNTO
Ingeniería y Arquitectura	No

ÁMBITO DE CONOCIMIENTO
Ingeniería informática y de sistemas

HABILITA PARA EL EJERCICIO DE PROFESIONES REGULADAS	NORMA HABILITACIÓN
No	

SOLICITANTE

NOMBRE Y APELLIDOS	CARGO
Luis Lafuente Molinero	Director de la Escuela Superior de Ingeniería
Tipo Documento	**Número Documento**
NIF	75749410Z

REPRESENTANTE LEGAL

NOMBRE Y APELLIDOS	CARGO
Milagrosa Casimiro-Soriguer Escofet	Vicerrectora de Planificación, Calidad y Evaluación
Tipo Documento	**Número Documento**
NIF	30482786N

RESPONSABLE DEL TÍTULO

NOMBRE Y APELLIDOS	CARGO
Milagrosa Casimiro-Soriguer Escofet	Vicerrectora de Planificación, Calidad y Evaluación
Tipo Documento	**Número Documento**
NIF	30482786N

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
Plaza Falla, nº 8 - Hospital Real, 1ª planta	11003	Cádiz	616372141
E-MAIL	**PROVINCIA**		**FAX**
vicerrectora.planificacion@uca.es	Cádiz		956015924

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

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: Cádiz, AM 20 de julio de 2023
	Firma: Representante legal de la Universidad

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

1. DESCRIPCIÓN DEL TÍTULO

1.1. DATOS BÁSICOS

NIVEL	DENOMINACIÓN ESPECIFICA	CONJUNTO	CONVENIO	CONV. ADJUNTO
Máster	Máster Universitario en Seguridad Informática (Ciberseguridad) por la Universidad de Cádiz	No		Ver Apartado 1: Anexo 1.

LISTADO DE ESPECIALIDADES
No existen datos

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

ÁMBITO DE CONOCIMIENTO
Ingeniería informática y de sistemas

NO HABILITA O ESTÁ VINCULADO CON PROFESIÓN REGULADA ALGUNA

AGENCIA EVALUADORA
Agencia para la Calidad Científica y Universitaria de Andalucía

UNIVERSIDAD SOLICITANTE
Universidad de Cádiz

LISTADO DE UNIVERSIDADES	
CÓDIGO	UNIVERSIDAD
005	Universidad de Cádiz

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	0	10
CRÉDITOS OPTATIVOS	**CRÉDITOS OBLIGATORIOS**	**CRÉDITOS TRABAJO FIN GRADO/ MÁSTER**
0	43	7

LISTADO DE ESPECIALIDADES	
ESPECIALIDAD	CRÉDITOS OPTATIVOS
No existen datos	

1.3. Universidad de Cádiz

1.3.1. CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS	
CÓDIGO	CENTRO
11006531	Escuela Superior de Ingeniería

1.3.2. Escuela Superior de Ingeniería

1.3.2.1. Datos asociados al centro

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

PLAZAS DE NUEVO INGRESO OFERTADAS

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

PRIMER AÑO IMPLANTACIÓN	SEGUNDO AÑO IMPLANTACIÓN	
20	20	
	TIEMPO COMPLETO	
	ECTS MATRÍCULA MÍNIMA	ECTS MATRÍCULA MÁXIMA
PRIMER AÑO	60.0	60.0
RESTO DE AÑOS	0.0	0.0
	TIEMPO PARCIAL	
	ECTS MATRÍCULA MÍNIMA	ECTS MATRÍCULA MÁXIMA
PRIMER AÑO	30.0	36.0
RESTO DE AÑOS	0.0	0.0
NORMAS DE PERMANENCIA		
http://www.uca.es/secretaria/portal.do?TR=A&IDR=1&identificador=15357		
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	

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

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
CG1 - Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica
CG2 - Concebir, diseñar, poner en práctica y mantener un sistema global de ciberseguridad en un contexto definido.
CG3 - Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad.
CG4 - Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.
CG5 - Planificar, gestionar, organizar e implantar medidas de seguridad en la operación y gestión de los sistemas.
3.2 COMPETENCIAS TRANSVERSALES
CT1 - Trabajar en equipos y con equipos (del mismo ámbito o interdisciplinares) y desarrollar actitudes de participación y colaboración como miembro activo de la comunidad.
CT2 - Expresarse de forma oral y escrita en lengua inglesa
3.3 COMPETENCIAS ESPECÍFICAS
CE1 - Conocer el procedimiento de realización de una auditoría informática.
CE2 - Aplicar una metodología para el análisis y evaluación de riesgos y utilizar las herramientas para su gestión.
CE3 - Conocer y comprender el marco legal vigente europeo y español relativo a la privacidad y seguridad de la información, tanto en el ámbito privado como en el de la administración pública para satisfacer las exigencias profesionales.
CE4 - Conocer las normas y estándares de referencia y certificación relacionados con seguridad de la información.
CE5 - Conocer las técnicas y herramientas para la realización de un análisis forense con la preservación de pruebas digitales
CE6 - Aplicar los mecanismos de cifrado, esteganografía y firma digital para garantizar la confidencialidad, integridad y autenticidad de los datos en un sistema, así como el acceso y seguridad en las comunicaciones
CE7 - Implantar medidas que garanticen la seguridad de los datos en el software de sistemas.
CE8 - Aplicar técnicas para auditar y mejorar la seguridad de una aplicación.
CE9 - Diseñar aplicaciones incorporando el criterio de seguridad dentro del propio proceso de desarrollo
CE10 - Conocer, detectar y evaluar las vulnerabilidades de bajo nivel que afectan a los sistemas informáticos, así como analizar amenazas a partir de la reconstrucción de código.
CE11 - Comprender el funcionamiento y las aplicaciones de los dispositivos de seguridad TPM.
CE12 - Detectar vulnerabilidades en los distintos elementos de un sistema informático.
CE13 - Conocer y aplicar técnicas y herramientas para la realización de pruebas de penetración.
CE14 - Conocer las principales técnicas y herramientas de IA y sus aplicaciones en problemas de seguridad
CE15 - Desarrollar modelos para la resolución de problemas de seguridad con algoritmos de IA
CE16 - Diseñar mecanismos de prevención de amenazas a la seguridad, así como de detección y respuesta a las incidencias de seguridad en los sistemas críticos.

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

CE17 - Analizar las particularidades de los sistemas críticos y sus esquemas de autenticación y acceso según el ámbito de aplicación.
CE18 - Describir las amenazas de seguridad de las infraestructuras de redes modernas y aplicar técnicas para comprobar redes y mitigar dichas amenazas.
CE19 - Conocer los sistemas de detección y prevención de intrusiones en redes cableadas e inalámbricas. Discernir, seleccionar y usar el sistema de monitorización adecuado de acuerdo a la legislación vigente.
CE20 - Diseñar, desplegar y configurar redes inalámbricas seguras mediante la aplicación de políticas de seguridad apropiadas.
CE21 - Capacidad de desarrollar arquitecturas, plataformas y sistemas distribuidos seguros.
CE22 - Presentar y defender públicamente un proyecto integral de ciberseguridad de naturaleza profesional.

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

Según dispone el artículo 16 del Real Decreto 1393/2007, modificado por el Real Decreto 861/2010, para acceder a las enseñanzas oficiales de Máster será necesario estar en posesión de un título universitario oficial español u otro expedido por una institución de educación superior del Espacio Europeo de Educación Superior que facultan en el país expedidor del título para el acceso a enseñanzas de Máster. Asimismo, podrán acceder los titulados conforme a sistemas educativos ajenos al Espacio Europeo de Educación Superior sin necesidad de la homologación de 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 implica, en ningún caso, la homologación del título previo de que esté en posesión el interesado, ni su reconocimiento a otros efectos que el de cursar las enseñanzas de Máster.

Dada la naturaleza claramente disciplinar de la formación en Ingeniería Informática se dará prioridad a los graduados en Ingeniería Informática. No obstante, podrá admitirse cualesquiera titulados universitarios de grado, máster oficial, ingenierías superiores y técnicas, licenciaturas y diplomaturas afines (ingeniería telemática, etc.). También se valorará que disponga de experiencia profesional acreditada en el ámbito de la Ingeniería Informática.

De acuerdo con las previsiones del artículo 73 ~~art. 75 de la Ley 15/2003 Andaluza de Universidades~~, del Decreto legislativo 1/2013, de 8 de enero, por el que se aprueba el Texto Refundido de la Ley Andaluza de Universidades, a los únicos efectos del ingreso en los centros universitarios, todas las Universidades públicas andaluzas se constituyen en un Distrito Único, encomendando la gestión del mismo a una comisión específica, constituida en el seno del Consejo Andaluz de universidades. La composición de dicha comisión quedó establecida por el Decreto 478/1994, de 27 de diciembre, que sigue actuando tras la publicación del citado Texto Refundido de la ley Andaluza de universidades. Se establece, por tanto, un único sistema aplicable a quienes deseen iniciar cualquier Máster Universitario que se imparta en las Universidades Públicas Andaluzas, sin perjuicio de las normas propias en relación con los procesos de matriculación o de permanencia que establezca cada universidad, o de los requisitos que exija el correspondiente plan de estudios.

En consecuencia los procesos de admisión de alumnos se realizan de acuerdo con los criterios que establezca la Comisión de Distrito Único Andaluz, considerándose en los mismos la existencia de estudiantes con necesidades educativas específicas derivadas de discapacidad. A estos efectos, cada curso académico, la Dirección General de Universidades aprueba una Resolución por la que se hace público el acuerdo de la Comisión de Distrito Único Universitario de Andalucía, en la que se establece el procedimiento para el ingreso en los másteres universitarios, que vayan a ser ofertados e impartidos en el curso académico siguiente.

A la hora de establecer los criterios de admisión, se tendrá en cuenta lo establecido en el artículo 16 del RD 1393/2007, modificado por el RD 861/2010. Los requisitos de acceso a los másteres universitarios son los siguientes:

1. Estar en posesión de un título de Grado, o de Arquitecto, Ingeniero, Licenciado, Arquitecto Técnico, Diplomado, Ingeniero Técnico o Maestro, u otro expresamente declarado equivalente.

2. Estar en posesión de un título universitario extranjero expedido por una institución de educación superior del Espacio Europeo de Educación Superior que facultan en el país expedidor del título para el acceso a enseñanza de máster.

3. Estar en posesión de un título universitario extranjero, equivalente al nivel de grado en España, pero que no ha sido homologado por el Ministerio de Educación Español y que faculte en su país de origen para cursar estudios de posgrado.

Además de los requisitos de acceso generalmente establecidos en el artículo 16 RD 1393/2007, los solicitantes deberán cumplir, en su caso, los requisitos específicos que requiera cada Máster en el que desee ser admitido. En su caso, estos requisitos específicos se hacen públicos con anterioridad comienzo del plazo de presentación de solicitudes hasta la finalización del proceso en la respectiva universidad. En cualquier caso, siempre están disponibles en el punto de acceso electrónico:

http://www.juntadeandalucia.es/economiainnovacioncienciayempleo/sguit/

En cuanto al procedimiento de gestión para el ingreso en los Másteres Universitarios de las Universidades Públicas de Andalucía y de acuerdo con la Comisión del Distrito Único Universitario de Andalucía, que lo aprueba y hace público para cada curso académico, éste es estructurado del siguiente modo:

SOLICITUD DE PLAZAS: La solicitud de plaza se presentará rellenado el oportuno formulario electrónico que se habilitará en la web de Distrito Único Andaluz en los respectivos plazos de entrega de solicitudes, en la que se relacionarán todos los másteres de interés del solicitante, por orden de preferencia. Los alumnos solicitarán su preinscripción al menos en una de las siete Universidades participantes y los admitidos en el máster se matricularán en la Universidad por la que solicitaron su admisión en primer lugar.

Durante la cumplimentación del citado formulario, el sistema informático le permitirá, en su caso, aportar en formato PDF aquella documentación que cada máster le requiera. En el supuesto de que finalmente obtenga plaza, deberá presentar en el respectivo centro donde realice la matricula los documentos originales que permitan contrastar la veracidad de lo aportado al formulario.

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

FASES DEL PROCEDIMIENTO Y CUPOS: El procediendo de admisión se divide en tres fases en las que las universidades pueden repartir las plazas totales que se ofertan en cada máster. Se contempla que la primera fase sea exclusivamente para estudiantes con título extranjero con, o sin, homologación por el Ministerio de Educación Español. Así pues se establece:

Fase 1: Cupo de Extranjeros.

Fase 2: Cupo General.

Fase 3: Cupo General.

En el supuesto de que no se reserven plazas para extranjeros en la fase 1, o estos alumnos participen directamente en la fase 2 o en la fase 3, sus solicitudes se tratarán en pie de igualdad con el resto de solicitantes por el cupo general.

EVOLUCIÓN DE PLAZAS OFERTADAS: Con independencia del reparto de plazas que las universidades hagan para cada máster en cada fase, las plazas que resultasen sobrantes en cada fase, se acumularán automáticamente a la siguiente fase. A excepción de acumular desde la fase 1 a la fase 2, si la universidad ha repartido las plazas del máster de que se trate entre la fase 1 y la 3.

EVOLUCIÓN DE LAS SOLICITUDES: Todas las peticiones de másteres formuladas por un solicitante que no hayan obtenido plaza y estén en las respectivas listas de espera, serán duplicadas automáticamente, en su caso a la siguiente fase, participando en pie de igualdad con quienes han formulado su solicitud en esta ¿siguiente fase¿.

De esta manera, un solicitante no pierde sus expectativas en la fase en la que concursó -sigue estando en lista de espera de dicha fase por si se produjesen plazas vacantes-, y no necesita presentar una nueva solicitud a las siguientes fases para optar a las plazas que, en su caso, se oferte en ellas.

De igual forma, las solicitudes de plazas de la primera fase en lista de espera del cupo de extranjeros, se duplicarán automáticamente para que concurran también, en su caso, por el cupo general de la siguiente fase.

MATRÍCULA O RESERVA DE PLAZA: Cada fase de preinscripción tiene dos o tres adjudicaciones.

En la primera de cada una ella los solicitantes deberá seguir las siguientes instrucciones:

- Solicitantes que han sido admitidos en su primera petición: formalizarán la matrícula (o abonarán, en el caso de extranjeros, el correspondiente pago a cuenta de la matricula) en el máster de que se trate dentro del plazo establecido con el procedimiento que establezca la correspondiente universidad. No podrán optar a ningún otro máster donde exista lista de espera.
- Solicitantes que desean estudiar el máster actualmente asignado, rehusando estar en espera en otras peticiones de mayor preferencia: formalizarán la matrícula en el máster de que se trate dentro del plazo establecido con el procedimiento que establezca la correspondiente universidad.
- Solicitantes que desean quedar en espera de obtener plaza en másteres de mayor preferencia del asignado, deberán realizar una reserva de la plaza actualmente asignada. La citada reserva se realizará en esta misma web.
- Quienes no tengan asignada ninguna plaza, deberán esperar a figurar en las listas correspondientes a sus peticiones, y realizar matrícula en el momento en que resulten asignados en alguna de ellas, tal como se ha indicado en los apartados anteriores.

En la segunda, o en la tercera en caso de extranjeros, de las adjudicaciones todo solicitante al que se le asigne plaza deberá matricularse obligatoriamente, sin menoscabo de que si posteriormente resultasen plazas vacantes en másteres de mejor preferencia de la matriculada en las que su puntuación le permitiese la admisión, le será comunicado y podrá cambiar la matrícula a su nuevo máster.

En cualquier caso, el sistema informático le avisará al interesado cuando puede hacer matrícula o reserva de plaza.

El alumno estará vinculado, a efectos académicos y administrativos, a la Universidad en la que se haya matriculado, Así, cada Universidad asume las tareas de tramitación, custodia y emisión de certificados de los expedientes de los estudiantes relativos al Título Oficial cuya impartición es objeto de este Convenio, de conformidad con lo dispuesto en el Art. 3 del Real Decreto 1393/2007, de 29 de Octubre (modificado por el Real Decreto 861/2010, de 2 de julio), por el que se establece la ordenación de las enseñanzas universitarias oficiales. Igualmente, cada universidad emitirá el correspondiente título de Máster, que será firmado por el Rector de la Universidad en la que se ha matriculado el alumno en representación de los Rectores de las universidades participantes, indicándose esta situación junto al carácter interuniversitario del Máster y las universidades participantes.

CRITERIOS DE ADMISIÓN

Los criterios y requisitos de admisión en el Máster Universitario en Seguridad Informática (Ciberseguridad) responden al acuerdo general normativo adoptado por las autoridades académicas andaluzas que afecta a todos los másteres oficiales ofertados en la Comunidad Autónoma de Andalucía y que se plasman en los mecanismos de acceso establecidos a través del Distrito Único Universitario Andaluz, siendo éstos objetivables y ponderables.

La Comisión de Garantía de Calidad del Centro propondrá una serie de criterios de selección para el caso de que se llegue a producir una situación de acceso competitivo en un curso académico, al haber más solicitudes que plazas disponibles. Dichos criterios serán publicados en la guía docente de cada curso.

~~A título orientativo, la~~ Respecto a la selección, se seguirán los principios de objetividad, imparcialidad, mérito y capacidad. De acuerdo a la Comisión de Distrito Único Andaluz se establecerán como títulos con preferencia alta el Grado en Ingeniería Informática o títulos de Grado o Máster que cumplan el Acuerdo del Consejo de Universidades por el que se establecen recomendaciones para la propuesta por las universidades de memorias de solicitud de títulos oficiales en los ámbitos de la Ingeniería Técnica Informática e Ingeniería Informática (BOE núm. 187, de 4 de agosto de 2009), Ingeniero Técnico en Informática de Gestión, Ingeniero Técnico en Informática de Sistemas, Diplomado en Informática, Licenciado en Informática, Ingeniero en Informática. Se considerarán con preferencia media otros titulados universitarios con formación o experiencia profesional en el ámbito del máster. La ponderación inicial a establecer para los criterios de selección de los estudiantes del Máster de forma que pueda verse resuelto el exceso de demanda, y de acuerdo con los criterios que establezca la Comisión de Distrito Único Andaluz ~~(D.U.A.), puede ser la siguiente~~:

- Nota media del expediente académico, 40%
- Correspondencia de las competencias del título de acceso con el Grado en Ingeniería Informática, ~~Formación académica previa, 30%~~25%
- Experiencia profesional relacionada con el ámbito del máster, ~~20%~~25%
- Dominio de la lengua inglesa, 10%

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

La Comisión de Garantía de Calidad será la encargada de aplicar estos criterios. Estos requisitos específicos se hacen públicos desde el comienzo del plazo de presentación de solicitudes hasta la finalización del proceso. En cualquier caso, siempre están disponibles en el punto de acceso electrónico: http://www.juntadeandalucia.es/economiainnovacioncienciayempleo/sguit/

4.3 APOYO A ESTUDIANTES

4.3. Apoyo y orientación a estudiantes, una vez matriculados

4.3.1. Apoyo y orientación académica

Se tienen previstos mecanismos de apoyo y orientación a los estudiantes una vez matriculados, tal y como viene recogido en el Sistema de Garantía de Calidad de la Universidad de Cádiz.

Al igual que las actividades de acogida de los alumnos de nuevo ingreso las actividades de acción tutorial y de apoyo a la actividad académica ya tienen una larga tradición en la UCA. Los primeros antecedentes datan del curso 2000/2001 en el cual se puso en marcha el primer plan de acción tutorial de la UCA que fue galardonado con un premio nacional dentro del ¿Plan Nacional de Evaluación y Calidad de las Universidades¿.

Estas actividades tienen como objetivos generales, entre otros, los siguientes:

- Apoyar y orientar al alumno en su proceso de formación integral.
- Favorecer la integración del alumno de nuevo ingreso en el Centro y en la Universidad.
- Evitar el sentimiento de aislamiento del alumno procedente de otras universidades nacionales y extranjeras.
- Identificar las dificultades particulares que se puedan presentar en los estudios y analizar las posibles soluciones.
- Fomentar y canalizar hacia el uso de las tutorías académicas.
- Asesorar al estudiante para la toma de decisiones con respecto a las opciones de formación académica que brinda la Universidad de cara a la elección de su itinerario curricular.
- Incitar al alumno a la participación en la institución.
- Desarrollar la capacidad de reflexión, diálogo, autonomía y la crítica en el ámbito.

Adicionalmente, se prevé tener una reunión informativa con los alumnos matriculados en el Máster, previa al inicio del período lectivo, en la que se suministrará información sobre la organización y estructura del mismo, objetivos propuestos, sistema de tutorización, procedimientos, calendarios, trámites académicos, etc.

4.3.2. Apoyo a la inserción social

Por otra parte el Título dispone, en colaboración con la Dirección General de Empleo de la UCA, de un ¿Programa de Orientación Laboral¿ y de un conjunto de ¿Actividades de orientación al primer empleo¿. Estos dos programas se gestionan mediante un procedimiento común para todos los Centros de la UCA, el procedimiento para la evaluación de la inserción laboral y satisfacción con la formación recibida. El ¿Programa de orientación laboral¿ consiste en un conjunto de actuaciones con el objetivo de facilitar a los alumnos la asimilación de sus objetivos profesionales. Las ¿Actividades de orientación al primer empleo¿ es un proyecto anual regulado destinado a orientar al alumno de los últimos cursos para el acceso al primer empleo.

Más información puede obtenerse en **http://www.uca.es/vrteit/**.

4.3.3. Apoyo psicopedagógico

La Universidad de Cádiz ofrece a los estudiantes matriculados el Servicio de Atención Psicológica y Psicopedagógica (SAP). Su objetivo es atender las necesidades personales y académicas del alumnado asesorándoles en cuestiones que puedan mejorar la calidad de su estancia y el aprendizaje. Más información puede obtenerse en **http://www.uca.es/sap/**.

4.3.4. Programas específicos

Además la Universidad de Cádiz cuenta con diferentes servicios de apoyo a los estudiantes matriculados:

- Servicio de Atención a la Discapacidad: su objetivo es garantizar un tratamiento equitativo y una efectiva igualdad de oportunidades para cualquier miembro de la comunidad universitaria que presente algún tipo de discapacidad y tratar de que estos principios también se hagan realidad en la sociedad en general. Más información puede obtenerse en **http://www.uca.es/discapacidad/**.
- Servicios de asesoramiento y apoyo ofrecidos por los órganos centrales (vicerrectorados, direcciones generales, etc.). Lo más específicos son los del Vicerrectorado de Alumnos, concretamente el Área de Atención al Alumnado, que tiene como objetivo organizar y coordinar en general los procesos de gestión relacionados con los alumnos y los egresados. Entre sus funciones se encuentran: la gestión de becas y ayudas al estudio; tramitación de títulos universitarios; difusión y promoción de la oferta de titulaciones y servicios de la UCA; Información general sobre la Universidad de Cádiz mediante atención personalizada; etc. Puede consultarse específicamente la página del Vicerrectorado de Alumnado, en la siguiente dirección web: **http://www.uca.es/vralumnos/**.
- Unidad de igualdad: su objetivo es tratar de eliminar las dificultades y barreras que impiden una participación igualitaria y el desarrollo personal, académico y profesional de todos los miembros de la comunidad universitaria y de que los principios de inclusión, pluralidad, diversidad, igualdad de oportunidades y equidad se hagan realidad tanto dentro como fuera de ella. Pude consultarse al respecto la siguiente dirección web: **http://www.uca.es/igualdad/**.

4.4 SISTEMA DE TRANSFERENCIA Y RECONOCIMIENTO DE CRÉDITOS

Reconocimiento de Créditos Cursados en Enseñanzas Superiores Oficiales no Universitarias

MÍNIMO	MÁXIMO
0	0

Reconocimiento de Créditos Cursados en Títulos Propios

MÍNIMO	MÁXIMO

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

0	0

Adjuntar Título Propio
Ver Apartado 4: Anexo 2.

Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional	
MÍNIMO	**MÁXIMO**
0	9

El Real Decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales (modificado por Real Decreto 861/2010, de 2 de julio), indica en su artículo 6 que, con objeto de hacer efectiva la movilidad de estudiantes, tanto dentro del territorio nacional como fuera de él, las universidades elaborarán y harán pública su normativa sobre el sistema de reconocimiento y transferencia de créditos, con sujeción a los criterios generales establecidos en el mismo.

La Universidad de Cádiz, para dar cumplimiento al mencionado precepto, aprobó el Reglamento UCA/CG12/2010, de 28 de junio, por el que se regula el Reconocimiento y Transferencia de Créditos en las Enseñanzas Oficiales Reguladas por el Real Decreto 1393/2007, de 29 de octubre [Acuerdo del Consejo de Gobierno de 28 de junio de 2010 (BOUCA núm. 109)] y posteriormente lo modificó [Acuerdo del Consejo de Gobierno de 22 de junio de 2011 (BOUCA núm. 122)], en orden a adecuarlo a la nueva redacción del art. 6.º RD 1393/2007 dada por el RD 861/2010. Finalmente el citado Reglamento ha sido modificado recientemente en virtud de los Reglamentos UCA/CG01/2014, de 25 de febrero (BOUCA núm. 170, de 1 de abril) y UCA/CG06/2014, de 17 de junio 2014 (BOUCA núm. 173, de 27 de junio).

~~Puede consultarse el texto íntegro, ya consolidado por la referencia a la sucesión de modificaciones, de la normativa de la Universidad de Cádiz en el siguiente enlace:~~

~~http://www.uca.es/recursos/doc/Unidades/normativa/alumnos/675416340_182014121551.pdf~~

Junto a cierto articulado en el que se determinan algunos procedimientos, plazos, publicidad debida, efectos administrativos sobre el expediente académico y precios públicos, se exponen a continuación los artículos y apartados más relevantes en lo que concierte al Máster Universitario en Seguridad Informática (Ciberseguridad).

CAPÍTULO II. RECONOCIMIENTO DE CRÉDITOS

Artículo 5. Objeto.

1. El reconocimiento de créditos procede en los siguientes casos de estudios que no han conducido a la obtención de un título oficial:

a) Alumnos que hayan realizado estudios equivalentes en una escuela o facultad y desean continuar dichos estudios en otra facultad o escuela de la misma o distinta universidad, con exclusión de los supuestos de solicitudes de cambio de centro o sede donde se imparte el plan de estudios en la Universidad de Cádiz.

b) Alumnos que hayan realizado estudios en una escuela o facultad e inician nuevos estudios en el mismo centro o en otra facultad o escuela de la misma o distinta universidad.

c) Alumnos que, realizando estudios en una escuela o facultad, los simultanean con otros estudios oficiales universitarios, previa resolución favorable del Rector.

d) Alumnos que hayan realizado estudios universitarios en el extranjero y desean continuarlos en la Universidad de Cádiz, de conformidad con lo establecido en el Capítulo V.

e) Alumnos de la Universidad de Cádiz que hayan realizado parte de sus estudios universitarios en otra universidad, dentro de programas de movilidad, nacional o internacional.

2. El reconocimiento de créditos procede en los siguientes casos de estudios que han conducido a la obtención de un título oficial y con validez en todo el territorio nacional o a un título propio de la Universidad de Cádiz:

a) Alumnos con una titulación universitaria oficial que estudian una nueva titulación en la Universidad de Cádiz.

b) Estudiantes con un título propio de la Universidad de Cádiz que estudian un título oficial, en los casos especificados en el presente reglamento.

3. También podrá solicitarse reconocimiento de créditos con respecto a los estudios cursados en enseñanza superior oficial, ciclos formativos de grado superior y experiencia profesional o laboral, en los términos previstos en la presente norma.

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

4. Para créditos de Prácticas Externas, podrán reconocerse los créditos superados en la Universidad de Cádiz o en otra Universidad, cuando su extensión sea igual o superior a la exigida en la titulación de destino y cuando su tipo y naturaleza sean similares a las exigidas, a juicio de la Comisión competente en materia de reconocimiento del Centro donde se imparte la titulación de destino.

Artículo 6. Criterios generales.

1. El sistema de reconocimiento está basado en créditos y en la acreditación de competencias.

2. Las solicitudes de reconocimiento de créditos tendrán su origen en módulos, materias o asignaturas efectivamente cursadas y superadas. En ningún caso se referirán a módulos, materias o asignaturas previamente reconocidas, convalidadas o adaptadas.

3. Los créditos cursados y superados por los estudiantes podrán utilizarse más de una vez para su reconocimiento en otras titulaciones.

CAPÍTULO III. TRANSFERENCIA DE CRÉDITOS

Artículo 19. Procedimiento y anotación en el expediente académico.

1. Los créditos obtenidos por el alumno en enseñanzas oficiales de la Universidad de Cádiz o de otra universidad, que no hayan conducido a la obtención de un título oficial, ni hayan sido objeto de reconocimiento, serán transferidos a su expediente en la titulación de destino con la calificación de origen, con mención expresa de la universidad y plan de estudios en que fueron cursados y superados.

6. Los módulos, las materias o asignaturas transferidas al expediente académico de los nuevos títulos no se tendrán en cuenta para el cálculo de la baremación del expediente.

7. En los supuestos de simultaneidad de estudios, no serán objeto de transferencia los créditos obtenidos en los mismos, salvo que estos sean objeto de reconocimiento o el estudiante renuncie a dicha simultaneidad, por abandono de dichos estudios.

CAPÍTULO IV. NORMAS ESPECÍFICAS EN RELACIÓN CON LOS TÍTULOS OFICIALES DE MÁSTERES Y DOCTORADO.

Artículo 20. Materia objeto de reconocimiento.

1. Quienes accedan a las enseñanzas conducentes a la obtención de un título oficial de Máster o Doctorado podrán obtener reconocimiento de créditos por materias previamente cursadas en función de la adecuación entre las competencias y conocimientos asociados a las materias superadas y los previstos en el plan de estudios de las enseñanzas de Máster o Doctorado, siempre que se compruebe que los estudios por los que se solicita el reconocimiento han sido superados dentro de las enseñanzas universitarias conducentes a títulos de posgrado.

2. En el caso de títulos oficiales de Máster que habiliten para el ejercicio de profesiones reguladas, para los que el Gobierno haya establecido las condiciones a las que han de adecuarse los planes de estudios, se reconocerán los créditos de los módulos definidos en la correspondiente norma reguladora. En caso de no haberse superado íntegramente un determinado módulo, el reconocimiento se llevará a cabo por materias o asignaturas en función de las competencias y conocimientos asociados a las mismas.

3. Se podrá obtener reconocimiento de créditos en estudios oficiales de Máster a partir de estudios previos cursados en títulos propios universitarios, en función de la adecuación entre las competencias y conocimientos asociados a las materias superadas y los previstos en el plan de estudios de las enseñanzas de Máster, dentro los límites y porcentajes que a estos efectos pueda establecer el Real Decreto 1393/2007.

4. La resolución de reconocimiento de estudios requerirá que el interesado se encuentre previamente matriculado en el título oficial de Máster o Doctorado correspondiente.

Artículo 21. Criterios generales para el reconocimiento de créditos.

1. Las solicitudes de reconocimiento de créditos tendrán su origen en módulos, materias o asignaturas realmente cursadas y superadas. La resolución del reconocimiento se hará por el total de créditos de la asignatura de destino, por lo que no podrá reconocerse un número parcial de créditos.

2. Las materias cursadas y superadas por los estudiantes podrán utilizarse más de una vez para su reconocimiento en otras titulaciones. En ningún caso el reconocimiento se referirá a módulos, materias o asignaturas previamente reconocidas, convalidadas o adaptadas.

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

3. Todos los créditos obtenidos por el alumno en enseñanzas oficiales cursadas en cualquier Universidad, los transferidos, los reconocidos y los superados para la obtención del título serán incluidos en su expediente académico y reflejado en el Suplemento Europeo al Título, previo abono de los precios públicos que, en su caso, establezca la Comunidad Autónoma en la correspondiente norma reguladora.

4. La resolución del reconocimiento de créditos requerirá que el interesado se encuentre previamente matriculado en el plan de estudios correspondiente de la UCA.

CAPÍTULO V. ESTUDIOS EXTRANJEROS.

Artículo 24. Concepto.

A los efectos del presente Reglamento, se entenderá por convalidación parcial de estudios extranjeros, el reconocimiento oficial de la validez a efectos académicos de estudios superiores realizados en el extranjero, hayan finalizado o no con la obtención de un título, respecto de estudios universitarios españoles parciales de grado o de máster, que permitan proseguir dichos estudios en la Universidad de Cádiz.

Artículo 25. Ámbito de aplicación.

La convalidación parcial de estudios universitarios extranjeros podrá solicitarse en los siguientes supuestos:

a) Cuando los estudios universitarios realizados con arreglo a un sistema extranjero no hayan concluido con la obtención del correspondiente título.

b) Cuando los estudios universitarios hayan concluido con la obtención de un título extranjero y el interesado no haya solicitado la homologación del mismo por un título universitario oficial español.

c) Cuando habiéndose solicitado la homologación del título extranjero, ésta haya sido denegada, siempre que la denegación no se haya fundado en alguna de las causas recogidas en el artículo 5 del Real Decreto 285/2004, de 20 de febrero, por el que se regulan las condiciones de homologación y convalidación de títulos y estudios extranjeros de educación superior.

Artículo 27. Criterios generales.

1. Serán susceptibles de convalidación las materias aprobadas en un plan de estudios conducente a la obtención de un título extranjero de educación superior, cuando el contenido y carga lectiva de las mismas sean equivalentes en un 75% a los de las correspondientes asignaturas incluidas en un plan de estudios conducente a la obtención de un título oficial.

Puede consultarse el texto íntegro consolidado de la normativa de la Universidad de Cádiz en el siguiente enlace:

http://www.uca.es/recursos/doc/Unidades/normativa/alumnos/675416340_182014121551.pdf

Atendiendo a este marco normativo, se establece el siguiente sistema de transferencia y reconocimiento de créditos en el Máster Universitario en Seguridad Informática (Ciberseguridad):

Transferencia

La transferencia de créditos consiste en incluir, en los documentos académicos oficiales del o la estudiante relativos a las enseñanzas en curso, la totalidad de los créditos obtenidos en enseñanzas oficiales cursadas con anterioridad, en la misma u otra universidad, que no hayan conducido a la obtención de un título oficial y que no puedan ser reconocidos en la titulación a la que accede.

Los módulos, las materias o asignaturas transferidas al expediente académico de los nuevos títulos no se tendrán en cuenta para el cálculo de la baremación del expediente.

En los supuestos de simultaneidad de estudios, no serán objeto de transferencia los créditos obtenidos en los mismos, salvo que estos sean objeto de reconocimiento o el estudiante renuncie a dicha simultaneidad, por abandono de dichos estudios.

Reconocimiento

El reconocimiento de créditos supone la aceptación por una universidad de los créditos que, habiendo sido obtenidos en unas enseñanzas oficiales, en la misma u otra universidad, son computados en otras distintas a efectos de la obtención de un título oficial.

Asimismo, en este título de Máster podrán ser objeto de reconocimiento los créditos cursados en otras enseñanzas universitarias conducentes a la obtención de otros títulos a que hace referencia el artículo 34.1 de la Ley Orgánica

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

6/2001, de 21 de diciembre, de Universidades. Podrán obtener reconocimiento de créditos por materias previamente cursadas en función de la adecuación entre las competencias y conocimientos asociados a las materias superadas y los previstos en el plan de estudios de las enseñanzas de otros títulos universitarios, oficiales o propios, que a juicio de la Comisión de Garantía de calidad del Título procuren una formación equivalente a la que ofrece este Máster.

De la misma manera, la experiencia laboral y profesional acreditada podrá ser también reconocida en forma de créditos que computarán a efectos de la obtención de un título oficial, siempre que dicha experiencia esté relacionada con las competencias inherentes a dicho título.

El número de créditos que sean objeto de reconocimiento a partir de experiencia profesional o laboral y de enseñanzas universitarias no oficiales no podrá ser superior, en su conjunto, al 15 por ciento del total de créditos que constituyen el plan de estudios. El reconocimiento de estos créditos no incorporará calificación de los mismos por lo que no computarán a efectos de baremación del expediente.

La Comisión de Garantía de Calidad de Título será la encargada de verificar la transferencia y el reconocimiento de los créditos, atendiendo a las especialidades de los méritos que aleguen los solicitantes.

En todo caso no podrán ser objeto de reconocimiento los créditos correspondientes al Trabajo de Fin de Máster.

4.6 COMPLEMENTOS FORMATIVOS

No se contemplan

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

5. PLANIFICACIÓN DE LAS ENSEÑANZAS

5.1 DESCRIPCIÓN DEL PLAN DE ESTUDIOS		
Ver Apartado 5: Anexo 1.		
5.2 ACTIVIDADES FORMATIVAS		
Clases de teoría		
Clases Teórico-Prácticas		
Clases de problemas		
Clases de prácticas		
Seminarios y conferencias		
Actividades académicas no presenciales		
Tutorías		
Evaluación		
5.3 METODOLOGÍAS DOCENTES		
Lección magistral expositiva		
Resolución de problemas y casos prácticos		
Prácticas de laboratorio		
Prácticas de ordenador		
Realización de trabajos		
Seguimiento de TFM		
5.4 SISTEMAS DE EVALUACIÓN		
Trabajos escritos realizados por el alumno		
Exposiciones de ejercicios, temas y trabajos		
Prácticas de laboratorio		
Prácticas de informática		
Participación y trabajo realizado en actividades formativas		
Pruebas escritas u orales		
Memoria, exposición y defensa del TFM		
5.5 NIVEL 1: REGULACIÓN		
5.5.1 Datos Básicos del Nivel 1		
NIVEL 2: Regulación		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	8	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
8		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NIVEL 3: Auditoría y Análisis de Riesgos		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	4	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
4		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
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: Legislación y normativa aplicada a la seguridad informática		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	4	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
4		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
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	

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

5.5.1.2 RESULTADOS DE APRENDIZAJE

Auditoría y Análisis de Riesgos

- Distinguir entre auditoría interna, externa y control interno.
- Conocer el marco jurídico y las normas internacionales relacionadas con la auditoría informática.
- Conocer las fases de realización de una auditoría informática, las fuentes de información y procedimientos de obtención de información.
- Conocer la estructura y características que debe reunir un informe de auditoría informática.
- Conocer los objetivos y metodologías existentes para el análisis y gestión de riesgos.
- Conocer cuáles son las etapas del proceso de análisis y gestión de riesgos, y ser capaz de llevarlas a la práctica.

Legislación y Normativa aplicada a la seguridad informática

- Conocer las consideraciones legales que deben aplicarse en distintos supuestos
- Conocer las ventajas que aportan las certificaciones.
- Conocer las directivas europeas actuales
- Manejar la documentación exigida por la agencia española de protección de datos
- Identificar las principales instituciones relacionadas con la seguridad informática
- Adquirir las habilidades precisas para gestionar la seguridad legal relacionada con las TICs, anticipando así los problemas jurídicos derivados de su incumplimiento.
- Conocer los factores implicados en la ciberdelincuencia y los riesgos existentes
- Conocer la respuesta jurídico-penal a la delincuencia informática

5.5.1.3 CONTENIDOS

Auditoría y Análisis de Riesgos

- Tema 1: Auditoría
- Tema 2: Análisis y gestión de riesgos de los sistemas de información

Legislación y Normativa aplicada a la seguridad informática

- Tema 1: Legislación de protección de datos y seguridad
- Tema 2: La Agencia Española de Protección de Datos
- Tema 3: La seguridad de la información en la administración electrónica
- Tema 4: Normas y certificaciones de seguridad
- Tema 5: Documento de seguridad
- Tema 6. La interpretación jurídica de los avances tecnológicos
- Tema 7. La delincuencia en el ciberespacio: la cibercriminalidad
- Tema 8. Delitos informáticos
- Tema 9. Imputación a los proveedores de servicios (ISPS) por delitos cometidos a través de internet.

5.5.1.4 OBSERVACIONES

Algunas de las actividades podrán realizarse en inglés.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG3 - Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad.

CG4 - Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.

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 - Trabajar en equipos y con equipos (del mismo ámbito o interdisciplinares) y desarrollar actitudes de participación y colaboración como miembro activo de la comunidad.

5.5.1.5.3 ESPECÍFICAS

CE1 - Conocer el procedimiento de realización de una auditoría informática.

CE2 - Aplicar una metodología para el análisis y evaluación de riesgos y utilizar las herramientas para su gestión.

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

CE3 - Conocer y comprender el marco legal vigente europeo y español relativo a la privacidad y seguridad de la información, tanto en el ámbito privado como en el de la administración pública para satisfacer las exigencias profesionales.		
CE4 - Conocer las normas y estándares de referencia y certificación relacionados con seguridad de la información.		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Clases Teórico-Prácticas	36	100
Clases de prácticas	16	100
Seminarios y conferencias	12	100
Actividades académicas no presenciales	128	0
Evaluación	8	100
5.5.1.7 METODOLOGÍAS DOCENTES		
Lección magistral expositiva		
Resolución de problemas y casos prácticos		
Prácticas de ordenador		
Realización de trabajos		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Trabajos escritos realizados por el alumno	0.0	50.0
Exposiciones de ejercicios, temas y trabajos	0.0	30.0
Participación y trabajo realizado en actividades formativas	10.0	30.0
Pruebas escritas u orales	30.0	90.0
5.5 NIVEL 1: TECNOLOGÍAS DE SEGURIDAD		
5.5.1 Datos Básicos del Nivel 1		
NIVEL 2: Tecnologías de seguridad		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	12	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
4	8	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
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	

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

NIVEL 3: Desarrollo de aplicaciones seguras		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	4	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
4		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
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: Ingeniería inversa y arquitecturas seguras		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	4	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	4	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
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: Inteligencia artificial aplicada a la seguridad		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	4	Semestral
DESPLIEGUE TEMPORAL		

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
	4	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

5.5.1.2 RESULTADOS DE APRENDIZAJE

Desarrollo de Aplicaciones Seguras

- Ser capaz de realizar un análisis crítico de la seguridad en aplicaciones.
- Ser capaz de diseñar y desarrollar aplicaciones siguiendo un enfoque de ingeniería del software y teniendo en cuenta las recomendaciones y buenas prácticas para el aseguramiento de la seguridad en la web.

Ingeniería Inversa y Arquitecturas Seguras

- Efectuar reconstrucción de código de ficheros ejecutables.
- Conocer y detectar vulnerabilidades de bajo nivel.
- Analizar ataques por desbordamiento de buffer y comprender los diferentes mecanismos de protección.
- Realizar análisis de ficheros binarios.
- Comprender el funcionamiento y las aplicaciones de los dispositivos de seguridad TPM.

Inteligencia Artificial Aplicada a la Seguridad

- Conocer las distintas técnicas de IA y sus aplicaciones a la seguridad informática
- Valorar la aplicabilidad de estrategias de IA para distintos problemas de seguridad
- Seleccionar herramientas apropiadas basadas en IA para la resolución de problemas de seguridad informática
- Evaluar métodos de IA para el reconocimiento automático (caras, objetos, huellas, ...)
- Aplicar herramientas de IA para la detección automática de intrusos
- Usar algoritmos inteligentes para la mejora de la seguridad en software
- Abordar el problema de la denegación de servicio usando la IA

5.5.1.3 CONTENIDOS

Desarrollo de Aplicaciones Seguras

1. Construcción de aplicaciones seguras
2. Ingeniería del software de sistemas seguros
3. Seguridad en desarrollo web

Ingeniería Inversa y Arquitecturas Seguras

1. Introducción a la arquitectura del conjunto de instrucciones x86-32 y x86-64
2. Reconstrucción de código
3. Vulnerabilidades de bajo nivel
4. Ofuscación
5. Análisis de ficheros binarios
6. Trusted Platform Module (TPM)

Inteligencia Artificial Aplicada a la Seguridad

1. La inteligencia artificial y sus aplicaciones en seguridad
2. Identificación basada en parámetros biomédicos
3. Detección inteligente de intrusos
4. Mejora automática en la seguridad del software
5. Prevención de la denegación de servicio

5.5.1.4 OBSERVACIONES

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Algunas actividades podrán realizarse en inglés.

Asignatura Ingeniería Inversa y Arquitecturas Seguras

- Se recomienda poseer conocimientos básicos de lenguaje ensamblador.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica

CG2 - Concebir, diseñar, poner en práctica y mantener un sistema global de ciberseguridad en un contexto definido.

CG3 - Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad.

CG5 - Planificar, gestionar, organizar e implantar medidas de seguridad en la operación y gestión de los sistemas.

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 - Trabajar en equipos y con equipos (del mismo ámbito o interdisciplinares) y desarrollar actitudes de participación y colaboración como miembro activo de la comunidad.

5.5.1.5.3 ESPECÍFICAS

CE8 - Aplicar técnicas para auditar y mejorar la seguridad de una aplicación.

CE9 - Diseñar aplicaciones incorporando el criterio de seguridad dentro del propio proceso de desarrollo

CE10 - Conocer, detectar y evaluar las vulnerabilidades de bajo nivel que afectan a los sistemas informáticos, así como analizar amenazas a partir de la reconstrucción de código.

CE11 - Comprender el funcionamiento y las aplicaciones de los dispositivos de seguridad TPM.

CE14 - Conocer las principales técnicas y herramientas de IA y sus aplicaciones en problemas de seguridad

CE15 - Desarrollar modelos para la resolución de problemas de seguridad con algoritmos de IA

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Clases Teórico-Prácticas	96	100
Actividades académicas no presenciales	194	0
Tutorías	2	100
Evaluación	8	100

5.5.1.7 METODOLOGÍAS DOCENTES

Lección magistral expositiva

Resolución de problemas y casos prácticos

Prácticas de laboratorio

Prácticas de ordenador

Realización de trabajos

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Exposiciones de ejercicios, temas y trabajos	0.0	70.0
Prácticas de informática	25.0	100.0
Participación y trabajo realizado en actividades formativas	0.0	50.0
Pruebas escritas u orales	0.0	75.0

NIVEL 2: Prácticas Externas		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Prácticas Externas	
ECTS NIVEL 2	10	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
5	5	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
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 Análisis Forense		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Prácticas Externas	5	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
5		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
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**	

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

No	No	
NIVEL 3: Prácticas en Hacking Ético		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Prácticas Externas	5	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	5	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
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

Prácticas en Análisis Forense

- Conocer el mecanismo para obtener evidencias digitales válidas en procedimientos legales
- Desarrollar técnicas y herramientas necesarias para la investigación forense.

Prácticas en Hacking Ético

- Identificar vulnerabilidades en redes, sistemas y aplicaciones, establecer los riesgos asociados a cada vulnerabilidad y definir las acciones correctivas que sean necesarias.
- Realizar pruebas de penetración y auditorías de seguridad
- Aplicar técnicas y herramientas para las pruebas de penetración en sistemas informáticos

5.5.1.3 CONTENIDOS

Prácticas en Análisis Forense

Esta asignatura se enmarca dentro del convenio con la empresa Deloitte donde el alumnado realizará, tras una formación teórica inicial por parte del personal de Deloitte, las prácticas en los laboratorios del CyberSoc de Deloitte, a los que se accederá remotamente para la realización de las mismas. La formación que realizarán es la siguiente:

1. Introducción a la ciencia forense
2. Leyes y ciencia forense
3. Proceso de investigación
4. Laboratorio forense
5. Adquisición de evidencias
6. Recolección de evidencias volátiles en Microsoft Windows
7. Herramientas de análisis forense
8. Discos duros y sistemas de ficheros (FAT y NTFS)
9. Análisis forense en sistemas Microsoft Windows
10. Análisis forense de memoria RAM
11. Análisis forense en sistemas GNU/Linux
12. Análisis de ficheros
13. Análisis de correos electrónicos
14. Análisis de perfiles de navegación web

Prácticas en Hacking Ético

Esta asignatura se enmarca dentro del convenio con la empresa Deloitte donde el alumnado realizará, tras una formación teórica inicial por parte del personal de Deloitte, las prácticas en los laboratorios del CyberSoc de Deloitte, a los que se accederá remotamente para la realización de las mismas. La formación que realizarán es la siguiente:

1. Footprinting
2. Fingerprinting

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

3. Vulnerabilidades
4. Metasploit
5. Ataques a credenciales
6. Malware
7. Seguridad física de los equipos
8. Seguridad en aplicaciones web

5.5.1.4 OBSERVACIONES

- Algunas de las actividades podrán realizarse en inglés.
- La superación de la asignatura Prácticas en Análisis Forense con más de un 7 sobre 10 permitirá al alumno obtener el certificado D-CFIA (Deloitte Certified Forensic Investigator Associate), que se entregará a la finalización del máster.
- La superación de la asignatura Prácticas en Hacking Ético con más de un 7 sobre 10 permitirá al alumno obtener el certificado D-CEHA (Deloitte Certified Ethical Hacking Associate), que se emitirá junto al título del Máster.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica

CG2 - Concebir, diseñar, poner en práctica y mantener un sistema global de ciberseguridad en un contexto definido.

CG3 - Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad.

CG4 - Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.

CG5 - Planificar, gestionar, organizar e implantar medidas de seguridad en la operación y gestión de los sistemas.

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

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE5 - Conocer las técnicas y herramientas para la realización de un análisis forense con la preservación de pruebas digitales

CE12 - Detectar vulnerabilidades en los distintos elementos de un sistema informático.

CE13 - Conocer y aplicar técnicas y herramientas para la realización de pruebas de penetración.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Clases Teórico-Prácticas	50	100
Actividades académicas no presenciales	192	0
Evaluación	8	100

5.5.1.7 METODOLOGÍAS DOCENTES

Lección magistral expositiva

Resolución de problemas y casos prácticos

Prácticas de laboratorio

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Prácticas de laboratorio	0.0	70.0
Pruebas escritas u orales	30.0	100.0

5.5 NIVEL 1: SEGURIDAD EN SISTEMAS

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

5.5.1 Datos Básicos del Nivel 1		
NIVEL 2: Seguridad en Sistemas		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	23	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
11	12	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
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: Criptografía y Seguridad en Software de Sistemas		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
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		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	5	Semestral

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
5		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
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 e Infraestructuras Críticas		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	4	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	4	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NIVEL 3: Seguridad en Sistemas Distribuidos		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	4	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	4	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

ECTS Semestral 10	ECTS Semestral 11	ECTS Semestral 12
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	Sí
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NIVEL 3: Monitorización y Seguridad Inalámbrica		
5.5.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	4	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	4	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
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		

Seguridad en Sistemas e Infraestructuras críticas

- Diferenciar los sistemas críticos de los de misión crítica y de los no críticos
- Comprender la relación entre los errores y las amenazas a la seguridad
- Conocer los peligros que las amenazas a los sistemas críticos suponen para la seguridad de las personas
- Seleccionar esquemas de autenticación y acceso adecuados a sistemas críticos concretos
- Analizar los requisitos de seguridad de sistemas críticos concretos
- Definir las respuestas a incidencias de seguridad para sistemas críticos concretos
- Definir políticas de seguridad para sistemas críticos concretos

Criptografía aplicada y seguridad en software de sistemas

- Diseñar mecanismos y protocolos necesarios para proporcionar algunos de los servicios básicos de seguridad: autenticación, autorización, privacidad y control de acceso.
- Establecer medidas de protección para solventar los problemas de seguridad planteados en sistemas operativos y bases de datos.

Seguridad en redes

- Adquirir conocimientos básicos de seguridad.
- Configurar los dispositivos de interconexión de redes de manera segura.
- Implementar AAA (autenticación, autorización y contabilización) con dispositivos de interconexión de redes (routers y switchs).
- Implantar y configurar cortafuegos.
- Implantar y configurar IDS/IPS.
- Asegurar los nodos finales.

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

- Implementar redes privadas virtuales entre sitios.
- Configurar correctamente dispositivos de redes todo en uno.
- Gestionar la seguridad de las redes.

Monitorización y seguridad inalámbrica

- Comprender los aspectos básicos de la monitorización de la seguridad de redes y diseñar una estrategia adecuada de monitorización.
- Identificar los datos adquiridos en el proceso de monitorización.
- Distinguir y comprender los sistemas de detección y prevención de intrusiones.
- Usar aplicaciones de monitorización de seguridad.
- Identificar las amenazas y riesgos de seguridad que afectan a las redes inalámbricas.
- Conocer los mecanismos de autenticación y cifrado de las redes inalámbricas.
- Diseñar e implementar servicios de acceso inalámbricos seguros.
- Conocer los principales métodos utilizados para proteger el anonimato en redes ad-hoc.

Seguridad en Sistemas Distribuidos

- Ser capaz de elegir el sistema de seguridad más adecuado para asegurar arquitecturas, plataformas y sistemas distribuidos.
- Ser capaz de diseñar e implementar arquitecturas, plataformas y sistemas distribuidos seguros.

5.5.1.3 CONTENIDOS

Seguridad en Sistemas e Infraestructuras críticas

1. Seguridad en sistemas críticos
2. Casos de estudio
3. Esquemas de autenticación y control de acceso a sistemas críticos
4. Amenazas a los sistemas críticos

Criptografía aplicada y seguridad en software de sistemas

1. Cifrado y ocultación de la información
2. Autentificación basada en claves e infraestructura de clave pública
3. Firma digital y DNIe
4. Seguridad en sistemas operativos
5. Seguridad en bases de datos

Seguridad en redes

1. Amenazas de seguridad
2. Seguridad en dispositivos de interconexión
3. Seguridad en el acceso a la red
4. Seguridad perimetral
5. Implementación de la prevención
6. Lan segura
7. Redes privadas virtuales
8. Dispositivos todo en uno
9. Gestión de redes seguras

Monitorización y seguridad inalámbrica

Bloque 1: Monitorización de la seguridad en redes

1. Introducción a la monitorización de la seguridad en redes
2. Análisis de datos en la monitorización de redes
3. Sistemas de detección y prevención de intrusiones (IPS & IDS)
4. Herramientas de monitorización

Bloque 2: Seguridad en redes inalámbricas

1. Topologías de redes inalámbricas
2. Amenazas y riesgos de seguridad
3. Métodos de cifrado utilizados en las comunicaciones inalámbricas
4. Métodos de autenticación
5. Infraestructuras de seguridad
6. Seguridad en redes Ad-Hoc

Seguridad en Sistemas Distribuidos

1. Seguridad en Arquitecturas Orientadas a Servicios y Dirigidas por Eventos
2. Seguridad en Internet de las Cosas
3. Seguridad en Cloud

5.5.1.4 OBSERVACIONES

- Algunas de las actividades podrán realizarse en inglés.
- En la medida que sea posible se ofrecerá al alumnado, en paralelo a la asignatura de Seguridad en Redes, la realización del curso CCNA Security de Cisco.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica

CG2 - Concebir, diseñar, poner en práctica y mantener un sistema global de ciberseguridad en un contexto definido.

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

CG3 - Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad.
CG4 - Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.
CG5 - Planificar, gestionar, organizar e implantar medidas de seguridad en la operación y gestión de los sistemas.
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 - Trabajar en equipos y con equipos (del mismo ámbito o interdisciplinares) y desarrollar actitudes de participación y colaboración como miembro activo de la comunidad.
CT2 - Expresarse de forma oral y escrita en lengua inglesa
5.5.1.5.3 ESPECÍFICAS
CE6 - Aplicar los mecanismos de cifrado, esteganografía y firma digital para garantizar la confidencialidad, integridad y autenticidad de los datos en un sistema, así como el acceso y seguridad en las comunicaciones
CE7 - Implantar medidas que garanticen la seguridad de los datos en el software de sistemas.
CE16 - Diseñar mecanismos de prevención de amenazas a la seguridad, así como de detección y respuesta a las incidencias de seguridad en los sistemas críticos.
CE17 - Analizar las particularidades de los sistemas críticos y sus esquemas de autenticación y acceso según el ámbito de aplicación.
CE18 - Describir las amenazas de seguridad de las infraestructuras de redes modernas y aplicar técnicas para comprobar redes y mitigar dichas amenazas.
CE19 - Conocer los sistemas de detección y prevención de intrusiones en redes cableadas e inalámbricas. Discernir, seleccionar y usar el sistema de monitorización adecuado de acuerdo a la legislación vigente.
CE20 - Diseñar, desplegar y configurar redes inalámbricas seguras mediante la aplicación de políticas de seguridad apropiadas.
CE21 - Capacidad de desarrollar arquitecturas, plataformas y sistemas distribuidos seguros.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Clases de teoría	8	100
Clases Teórico-Prácticas	132	100
Clases de prácticas	40	100
Seminarios y conferencias	4	100
Actividades académicas no presenciales	375	0
Evaluación	16	100

5.5.1.7 METODOLOGÍAS DOCENTES

Lección magistral expositiva
Resolución de problemas y casos prácticos
Prácticas de laboratorio
Prácticas de ordenador
Realización de trabajos

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Trabajos escritos realizados por el alumno	0.0	50.0
Exposiciones de ejercicios, temas y trabajos	0.0	80.0
Prácticas de laboratorio	0.0	50.0
Prácticas de informática	0.0	80.0
Participación y trabajo realizado en actividades formativas	0.0	75.0
Pruebas escritas u orales	25.0	100.0

5.5 NIVEL 1: TRABAJO FIN DE MÁSTER		
5.5.1 Datos Básicos del Nivel 1		
NIVEL 2: Trabajo Fin de Máster		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Trabajo Fin de Grado / Máster	
ECTS NIVEL 2	7	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	7	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
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	7	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	7	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

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

- Capacidad para la realización por parte del alumno de un proyecto en el ámbito de la ciberseguridad, de naturaleza profesional o investigadora, en el que se sinteticen e integren las competencias adquiridas en las enseñanzas del título.
- Realizar una presentación escrita y oral de su trabajo.
- Adquirir conciencia de los aspectos sociales y éticos de la ciberseguridad para su incorporación al mercado laboral.

5.5.1.3 CONTENIDOS

Realización, presentación y defensa, una vez obtenidos todos los créditos del plan de estudios, de un ejercicio original realizado individualmente ante un tribunal universitario, consistente en un proyecto integral de ciberseguridad de naturaleza profesional en el que se sinteticen las competencias adquiridas en las enseñanzas.

5.5.1.4 OBSERVACIONES

Para poder ser evaluado de este módulo el alumno debe haber cursado y superado el resto de módulos del título.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica

CG2 - Concebir, diseñar, poner en práctica y mantener un sistema global de ciberseguridad en un contexto definido.

CG3 - Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad.

CG4 - Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.

CG5 - Planificar, gestionar, organizar e implantar medidas de seguridad en la operación y gestión de los sistemas.

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

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE22 - Presentar y defender públicamente un proyecto integral de ciberseguridad de naturaleza profesional.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Actividades académicas no presenciales	170	0
Tutorías	4	100
Evaluación	1	100

5.5.1.7 METODOLOGÍAS DOCENTES

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Seguimiento de TFM		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Memoria, exposición y defensa del TFM	100.0	100.0

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

6. PERSONAL ACADÉMICO

6.1 PROFESORADO Y OTROS RECURSOS HUMANOS				
Universidad	**Categoría**	**Total %**	**Doctores %**	**Horas %**
Universidad de Cádiz	Profesor Titular de Universidad	38.9	100	32,5
Universidad de Cádiz	Otro personal docente con contrato laboral	5.6	100	4,7
Universidad de Cádiz	Profesor Contratado Doctor	11.1	100	9,3
Universidad de Cádiz	Profesor colaborador Licenciado	5.6	0	11,6
Universidad de Cádiz	Ayudante Doctor	22.2	100	32,5
Universidad de Cádiz	Profesor Titular de Escuela Universitaria	16.7	33.3	9,3

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 %**
65	10	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

Una parte esencial para el desarrollo de este máster en Seguridad Informática y sus posibilidades de mejora, estriba en disponer de un procedimiento general, para la planificación y despliegue del programa formativo, así como para la evaluación de los resultados del aprendizaje, con el fin de valorar si los estudiantes alcanzan los objetivos y competencias definidas en el título.

La Universidad de Cádiz cuenta con un procedimiento general para todas sus titulaciones, que se recoge en el Sistema de Garantía de Calidad de la UCA (SGC-UCA), *Proceso Procedimiento de Planificación, Desarrollo y Medición de los Resultados de las enseñanzas* (http://sgc.uca.es), aprobado por Acuerdo de Consejo de Gobierno de 21 de noviembre de 2012, revisado y ratificado en diciembre 2014, publicado en el BOUCA 179 (23 de diciembre de 2014), en cumplimiento de lo preceptuado en el Anexo I (Memoria para la solicitud de verificación de Títulos oficiales, epígrafe 8.2. Resultados previstos) del RD 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales.

Este procedimiento recoge el proceso de Planificación Docente de la Universidad de Cádiz regulado a través de una instrucción anual, emitida por el Vicerrectorado competente en materia de ordenación académica, para elaborar y coordinar los Planes de Ordenación Docente de Centros y Departamentos. El desarrollo de la docencia es responsabilidad de los Departamentos, en coordinación con los Centros, debiendo velar por el cumplimiento de la planificación y la calidad de la docencia encomendada.

Con relación a la evaluación de los aprendizajes, ésta se realiza por parte del equipo docente, de forma coordinada, conforme a lo establecido en el programa formativo o programa docente de la asignatura (criterios de evaluación e instrumentos que el profesorado utilizará para evaluar el progreso en el aprendizaje y grado de adquisición de competencias: exámenes, presentación de trabajos, seminarios, defensa del TFM, etc.). La Comisión de Garantía de Calidad del Centro será la encargada de revisar y realizar el control y seguimiento de la planificación, desarrollo de la enseñanza y resultados del aprendizaje.

Una vez finalizado el curso académico, la Universidad facilita a los responsables de cada título un informe con los resultados de este procedimiento. Estos resultados incluyen los indicadores establecidos en el Real Decreto 1393/2007 y el Real Decreto 861/2010, los indicadores reflejados en el protocolo para el proceso de seguimiento de títulos universitarios oficiales (CURSA), indicadores de satisfacción de los estudiantes con la planificación, desarrollo y resultados del aprendizaje y otros indicadores contemplados en el Sistema Integrado de Información de las Universidades Públicas Españolas (SIIU).

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

En el Procedimiento de planificación, desarrollo y medición de los Resultados se detallan los indicadores, herramientas y formatos utilizados para la valoración de los siguientes indicadores:

- Porcentaje de asignaturas del título que tienen su Programa Docente validado y publicado en red.
- Satisfacción global de los estudiantes con la planificación de la enseñanza y aprendizaje.
- Satisfacción global de los estudiantes con el desarrollo de la docencia.
- Satisfacción del profesorado con la organización y el desarrollo de la docencia.
- Tasa de rendimiento.
- Tasa de éxito.
- Tasa de evaluación.
- Tasa de abandono.
- Tasa de graduación.
- Tasa de eficiencia.

Adicionalmente también se dispone de las siguientes herramientas:

- Encuesta opinión de los estudiantes sobre la labor docente del profesorado.
- Cuestionario de evaluación de la satisfacción sobre el título: Profesorado.

Considerando que la mejora continua es uno de los fundamentos clave sobre los que se asienta la gestión de la calidad, se presenta toda la información extraída de los análisis de cada procedimiento, no sólo a los distintos órganos de gobierno del Centro, sino a todos los profesores en general y de cada sede en particular. Su objetivo es implementar un espíritu de mejora continua en todas y cada una de las partes implicadas en ello, creando un equipo que trabaje por un fin compartido. En este sentido, tras haber detectado posibles deficiencias o indicadores a mantener, cada curso académico, el Centro pondrá en conocimiento de los distintos grupos de interés información sobre la calidad obtenida en los distintos programas formativos conforme a lo indicado en el Procedimiento para garantizar la calidad del personal docente, el grado en el que el profesorado participa en Proyectos de Innovación Docente, Acciones Avaladas, Cursos de Formación, etc. Al mismo tiempo, se trabaja en identificar las distintas reclamaciones y propuestas de mejora que son recabadas mediante el Procedimiento para tratar las incidencias, reclamaciones y sugerencias de los grupos de interés internos del Centro.

De manera análoga el SGC incluye procedimientos destinados a medir y analizar los resultados de prácticas externas y movilidad de estudiantes. La normativa que rige dicho programa de prácticas es el R.D. 592/2014, de 11 de julio. Cada alumno que se acoge al programa tiene designado un tutor de empresa y un tutor académico, que velan por el cumplimiento de cada convenio individual en los términos de duración y actividades formativas pactados. Finalizado el periodo de prácticas, ambos tutores emiten un informe al respecto que es remitido a través de la aplicación informática practicas.uca.es al Vicedecanato que, a la luz de dichos informes, se emite un Certificado Oficial de Prácticas con el que el alumno solicitara# el reconocimiento de los ECTS correspondientes a la asignatura Prácticas de Empresas.

Resaltar que, al planificar las enseñanzas, la Comisión responsable del diseño del título distribuye las competencias generales y específicas del mismo en los diferentes módulos, materias y asignaturas. Los métodos para evaluar la consecución de estas competencias se concretan en el plan de estudios y en las guías docentes de las asignaturas elaboradas, cada curso académico, por parte del profesorado responsable.

Entre los métodos de evaluación de competencias se combinan actividades de evaluación, que se aplican durante todo el proceso formativo (trabajos en grupo, trabajos individuales, actividades a realizar en el campus virtual, etc.), y se suman al final del mismo. Esta combinación permite, tanto al profesorado como al alumnado, aprehender de manera mucho más centrada las competencias objetivo de cada asignatura. La superación de las diferentes asignaturas, implica la demostración de la adquisición de las competencias que tenía asignadas, y al completar los diferentes módulos y materias, el estudiante esta# en disposición de recibir el título.

No obstante, para la asignatura Trabajo Fin de Máster, siguiendo la Normativa general de la Universidad de Cádiz, los profesores de distintas ramas de conocimiento con docencia en la titulación junto a los estudiantes proponen cada año una oferta que es aprobada por la Comisión de Trabajos Fin de Máster. También es responsabilidad de esta Comisión la aprobación del tribunal que evalúa dicho trabajo siendo obligatoria su defensa oral.

9. SISTEMA DE GARANTÍA DE CALIDAD

ENLACE	http://sgc.uca.es/

10. CALENDARIO DE IMPLANTACIÓN

10.1 CRONOGRAMA DE IMPLANTACIÓN	
CURSO DE INICIO	2017
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**
30482786N	Milagrosa	Casimiro-Soriguer	Escofet
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Plaza Falla, nº 8 - Hospital Real, 1ª planta	11003	Cádiz	Cádiz
EMAIL	**MÓVIL**	**FAX**	**CARGO**

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

vicerrectora.planificacion@uca.es	616372141	956015924	Vicerrectora de Planificación, Calidad y Evaluación
11.2 REPRESENTANTE LEGAL			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
30482786N	Milagrosa	Casimiro-Soriguer	Escofet
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Plaza Falla, nº 8 - Hospital Real, 1ª planta	11003	Cádiz	Cádiz
EMAIL	**MÓVIL**	**FAX**	**CARGO**
vicerrectora.planificacion@uca.es	616372141	956015924	Vicerrectora de Planificación, Calidad y Evaluación
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**
75749410Z	Luis	Lafuente	Molinero
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Avenida de la Universidad de Cádiz, nº 10	11519	Cádiz	Puerto Real
EMAIL	**MÓVIL**	**FAX**	**CARGO**
direccion.esi@uca.es	636746952	956483202	Director de la Escuela Superior de Ingeniería

RESOLUCIÓN AGENCIA DE CALIDAD / INFORME DEL SIGC

Resolución Agencia de calidad / Informe del SIGC: Ver Apartado Resolución Agencia de calidad/Informe del SIGC: Anexo 1.

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 2: Anexo 1

Nombre : M Seguridad Inf_Alegac y 2.pdf

HASH SHA1 : C43B5064A0C406FBA45297EC537672CCCC6BD766

Código CSV : 248194592824359661830076

Ver Fichero: M Seguridad Inf_Alegac y 2.pdf

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 4: Anexo 1

Nombre : M Seguridad Inf_4_1_Alegac.pdf

HASH SHA1 : 090F81A8A5CF015A5FB9EF8F16D9B5C861FC69AE

Código CSV : 248172742841951849315285

Ver Fichero: M Seguridad Inf_4_1_Alegac.pdf

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 5: Anexo 1

Nombre : M Seguridad Inf_5_Alegac.pdf

HASH SHA1 : 1917A80635CF59B34377CDC0D0B985A81383EEF5

Código CSV : 248175914626470409198298

Ver Fichero: M Seguridad Inf_5_Alegac.pdf

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 6: Anexo 1

Nombre : M Seguridad Inf_6.1.pdf

HASH SHA1 : B105861EEFDF6CC6E19C72F4DB45640212DF5572

Código CSV : 234121425294477345538016

Ver Fichero: M Seguridad Inf_6.1.pdf

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 6: Anexo 2

Nombre : M Seguridad Inf_6.2.pdf

HASH SHA1 : F8CECE9714536EAFF2C629EA276194D980C5D5DB

Código CSV : 234122623917518017487722

Ver Fichero: M Seguridad Inf_6.2.pdf

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 7: Anexo 1

Nombre : M Seguridad Inf_7_1_Alegac.pdf

HASH SHA1 : 43838BC30E8F499A76B2BE69B3540C1F6C10B811

Código CSV : 248177241756819877999258

Ver Fichero: M Seguridad Inf_7_1_Alegac.pdf

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 8: Anexo 1

Nombre : M Seguridad Inf_8_1_Alegac.pdf

HASH SHA1 : ADCD7700A06737891B54918473121BAE5DDABA37

Código CSV : 248177631588848348416815

Ver Fichero: M Seguridad Inf_8_1_Alegac.pdf

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 10: Anexo 1

Nombre : M Seguridad Inf_10.1.pdf

HASH SHA1 : EB94717E3E4F32F6AB236F45986AE10C19B20159

Código CSV : 234125347393041241267407

Ver Fichero: M Seguridad Inf_10.1.pdf

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 11: Anexo 1

Nombre : ACREDITACION_delegfirma_VPCE.pdf

HASH SHA1 : D05D2A294A71FF1985035D68D8E40336E86AD8C9

Código CSV : 632698807659420443962788

Ver Fichero: ACREDITACION_delegfirma_VPCE.pdf

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado Resolución Agencia de calidad/Informe del SIGC: Anexo 1

Nombre : 25. Resol. M Inv Ing Sist_M Ciberseguridad.pdf

HASH SHA1 : 058E6673DDE63CAFBE24A94E92D78EA01D9CC38C

Código CSV : 631103754030283380481280

Ver Fichero: 25. Resol. M Inv Ing Sist_M Ciberseguridad.pdf

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

CSV: 633985552627631345496327 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es