MEMORIA DEL TÍTULO DE:
MÁSTER UNIVERSITARIO EN SEGURIDAD INFORMÁTICA (CIBERSEGURIDAD) POR LA UNIVERSIDAD DE CÁDIZ

FECHA DE LA MEMORIA:		VERSIÓN:	

RESUMEN DE MODIFICACIONES		
NÚMERO	**FECHA**	**MODIFICACIÓN**

Avda. de la Universidad de Cádiz, 10, 11519. Puerto Real (Cádiz)
E-mail: direccion.esi@uca.es

CONTENIDO

Escuela Superior de Ingeniería.
Avda. de la Universidad de Cádiz, 10, 11519. Puerto Real (Cádiz)
E-mail: direccion.esi@uca.es

1. Descripción del Título.

1.1. Datos básicos del título.

DATOS GENERALES DEL TÍTULO	
Denominación del Título:	Máster Universitario en Seguridad Informática (Ciberseguridad)
Especialidades:	
Universidad solicitante:	Universidad de Cádiz

Título Conjunto:		**Convenio** ***(archivo.pdf):***	
Universidades participantes: ***(únicamente si es de un título conjunto)***			

Rama de Conocimiento:	Ingeniería y Arquitectura		
Código ISCED1:	481	**Código ISCED2:**	520

Orientación del título de Máster:	Profesional		
Habilita para profesión regulada:	N	**Profesión Regulada:** ***(en caso afirmativo, indicar Resolución)***	N
Resolución:			
Vincula con profesión Regulada:		**Profesión Vinculada:**	

RESPONSABLE DEL TÍTULO			
1er. Apellido:	Domínguez	**2º Apellido:**	Jiménez
Nombre:	Juan José	**NIF:**	31266075J
Domicilio:	Escuela Superior de Ingeniería. Avda. de la Universidad, 10		
Localidad:	Puerto Real (Cádiz)	**Código Postal:**	11519
E-mail:	direccion.esi@uca.es		
Centro responsable del título:	Escuela Superior de Ingeniería		

1.2. Distribución de créditos en el título.

DISTRIBUCIÓN GENERAL DE CRÉDITOS EN EL TÍTULO	
Créditos totales:	60
Número de créditos en Prácticas Externas:	0
Número de créditos Optativos:	0
Número de créditos Obligatorios:	53
Número de créditos Trabajo Fin de Máster:	7
Número de créditos de Complementos Formativos:	0

1.3. Datos asociados al Centro.

CENTROS EN EL/LOS QUE SE IMPARTE
Escuela Superior de Ingeniería

PLAZAS DE NUEVO INGRESO OFERTADAS	
Primer Año de Implantación:	20
Segundo Año de Implantación:	20

NÚMERO ECTS DE MATRÍCULAS				
	Tiempo Completo		**Tiempo Parcial**	
	ECTS Matrícula mínima	**ECTS Matrícula máxima**	**ECTS Matrícula mínima**	**ECTS Matrícula máxima**
Primer año	60	60	30	36
Resto de años	60	60	24	30

OTROS DATOS:	
Tipo de Enseñanza ***(presencial, semipresencial, a distancia):***	Semipresencial
Normas de permanencia:	http://www.uca.es/secretaria/normativa/disposiciones-generales/alumnos/reglamento-permanencia-uca
Lenguas en las que se imparte:	Español
	Algunasactividades podrán realizarse en inglés.

2. Justificación del Título Propuesto.

2.1. Interés académico, científico o profesional del mismo.

La creciente preocupación por la ciberseguridad es un hecho en cada vez más empresas. En 2014, el número de empresas que han invertido en protegerse de amenazas cibernéticas ha aumentado un 33%, y solo en España se necesitan hasta 20.000 profesionales dedicados a esta ciencia y sus puestos no se cubren por falta de formación y especialización en la materia. Según varios informes, el mercado laboral en torno a la seguridad informática se estima que crezca exponencialmente en los próximos años. De acuerdo con el Informe de Seguridad Anual 2014 de Cisco, la falta de casi un millón de profesionales expertos en seguridad informática a nivel mundial está impactando las habilidades de las organizaciones de monitorizar y asegurar las redes, mientras las vulnerabilidades y amenazas en general alcanzaron sus niveles más altos desde el año 2000.

En el año 2010, la consultora Deloitte, en un informe-encuesta a nivel mundial sobre la seguridad de la información (realizado sobre el 27%, el 26% y el 28% de las principales instituciones financieras, bancos y aseguradoras respectivamente), indicaba que un 56% de encuestados a nivel mundial (y un 53% de los europeos) pensaban incrementar su presupuesto en seguridad de la información y la consultora Ernst & Young señalaba que las organizaciones estaban aumentando el nivel de inversión en seguridad de la información relacionada con sus cinco principales áreas de riesgos de Tecnologías de la Información [3] .

La Ley de Protección de Infraestructuras Críticas [4] y su desarrollo normativo (con la obligación impuesta a los operadores críticos de nombramiento de Responsables de seguridad y enlace, además de delegado de seguridad por cada una de sus infraestructura críticas o críticas europeas), la aprobación del Esquema Nacional de Seguridad (de obligado cumplimiento para todos los organismos públicos), etc., auguran una fuerte demanda de profesionales en ciberseguridad.

Por otro lado, la Estrategia Española de Seguridad de 2011 [5] refleja el incremento de ciberataques, haciendo hincapié en la necesidad de garantizar el uso seguro del ciberespacio. En este sentido, el Ministerio de Defensa creó el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas [6]. Por su parte, el Plan Estratégico 2013-2016 de la Policía Nacional indica que el tercer delito más lucrativo a nivel mundial es el cibercrimen, después de la prostitución

y el tráfico de drogas, por lo que califica por primera a vez a la lucha contra este delito como una "prioridad estratégica". Así pues, no puede extrañar que según un informe de la multinacional IDG Communications centrado en España, la seguridad sea una de las diez áreas de las TIC con mayor demanda profesional [6]. A nivel estadounidense, en un sondeo realizado por CompTIA (Computing Technology Industry Association) [7] la seguridad aparece como la principal prioridad para las tres cuartas partes de los 3.578 directores de contratación de TI entrevistados. Es un dato relativo al mercado laboral de Estados Unidos, pero en buena medida sirve de indicador de tendencias también para España.

Por lo que atañe a la formación en seguridad, ya en el año 2002 el Consejo de Europa en su Resolución de 28 de enero de ese mismo año "Relativa a un enfoque común y a acciones específicas en materia de seguridad de las redes y de la información", pedía a los Estados Miembros que: "para finales del año 2002, refuercen o promuevan la importancia de los conceptos de seguridad como componentes de la educación y formación en informática e insistía: "en la necesidad de aumentar las actividades de investigación, especialmente en lo que se refiere a los mecanismos de seguridad y su interoperabilidad, la fiabilidad y protección de las redes, una criptografía avanzada, las tecnologías que refuerzan la protección de la vida privada y la seguridad de las comunicaciones inalámbricas." En particular, en los informes y encuestas anteriormente señalados los perfiles profesionales más demandados comprenden, entre otras: jefe de seguridad, administrador o gestor de ciberseguridad, arquitecto de ciberseguridad, analista de operaciones de ciberseguridad, ingeniero de ciberseguridad, auditor de ciberseguridad, ingeniero de garantía de software seguro, o planificador de ciberoperaciones, y forense informático. Los contratantes potenciales se esperan fundamentalmente en los sectores de la banca, energía y consultoría tecnológicas.

El Máster en Seguridad Informática nace con la vocación de dar respuesta a esta necesidad empresarial y formar expertos en la seguridad de las tecnologías de la información y la comunicación. Es un Máster que está diseñado para:

- Formar profesionales en la seguridad de las tecnologías de la información y la comunicación capaces de realizar auditorías de seguridad, analizar los hechos y la información de seguridad recopilada, aplicar la ingeniería inversa y la ciberinteligencia, así como llevar a cabo un correcto análisis forense.
- Garantizar el desarrollo seguro de aplicaciones, ya sea tanto en plataformas web como en entornos móviles.
- Capacitar para aplicar la seguridad defensiva desde el punto de vista del administrador de sistemas o de la arquitectura web.

- Saber aplicar la seguridad ofensiva desde las metodologías de ataque.

Respecto a los grados de referencia en los perfiles de acceso previsto, la Escuela Superior de Ingeniería imparte actualmente el título de Grado en Ingeniería Informática desde el curso 2010-2011, donde los egresados del mismo constituyen la fuente natural de entrada al Máster solicitado. Previamente, el centro había impartido las titulaciones de I. T. Informática de Gestión y la I. T. Informática de Sistemas, titulaciones que fueron sustituidas con la entrada del mencionado Grado. En relación a la demanda potencial, considerando al Grado en Ingeniería Informática como título de referencia para los admitidos al Máster, la Tabla 3 muestra el número de egresados en las Titulaciones de primer ciclo de Ingeniería Técnica en Informática junto al Grado en Ingeniería Informática durante los últimos cinco cursos académicos, así como del extinto segundo ciclo de Ingeniería en Informática, titulaciones que proporcionan potenciales estudiantes para el Máster solicitado.

Curso	Ingeniería Técnica en Informática	Ingeniería Informática	Grado Ingeniería Informática	TOTAL
11-12	66	11	..	77
12-13	51	9	--	60
13-14	53	19	7	79
14-15	40	13	33	86
15-16	20	16	20	56

Tabla 3. Evolución del número de estudiantes egresados de titulaciones de informática

Esta previsión es muy conservadora, esperando atraer alumnos de fuera de la provincia de Cádiz así como de otros títulos afines, al no disponer de un máster oficial de carácter similar en la Comunidad Andaluza. Actualmente sólo la Universidad de Sevilla y la Universidad de Granada ofertan un título propio relacionado con la seguridad informática. Además, se cuenta

con la participación en el máster de la empresa Deloitte y se entregarán certificaciones profesionales de dicha empresa a los alumnos que superen el máster, lo que supone un valor añadido, además de contar con la posibilidad de atraer a profesionales del sector de las TIC que vean la ciberseguridad como una oportunidad de progreso en su vida profesional.

[1].VisiongainCyber Security Market 2013-2023 Report: https://www.visiongain.com/Report/951/Global-Cyber-Security-Market-2013-2023.
[2]. Deloitte. 2010 Financial services. Global Security study.
[3]. Borderless security: Ernst & Young's 2010 Global Information Security Survey [4]. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas
[5] Estrategia Española de Seguridad 2011 http://www.lamoncloa.gob.es
[6]. Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas
[7]. http://www.idg.es/cio/estructura/imprimir.asp?id=193751&cat=art
[8]. http://www.comptia.org/home.aspx

2.2. Referentes externos a la universidad proponente que avalen la adecuación de la propuesta a criterios nacionales o internacionales para títulos de similares características académicas.

El reciente interés de la ciberseguridad ha producido la aparición de los primeros títulos oficiales de Máster en materia de seguridad informática. Los referentes nacionales similares en materia al propuesto son los siguientes:

- Máster Universitario en Ingeniería de Seguridad de la Información y las Comunicaciones por la Universidad Alfonso X El Sabio
- Máster Universitario en Ingeniería Informática: Seguridad Informática y Sistemas Inteligentes por la Universidad Rovira i Virgili
- Máster Universitario en Investigación en Ciberseguridad por la Universidad de León
- Máster Universitario en Seguridad de la Información por la Universidad de Deusto
- Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones por la Universidad Autónoma de Barcelona; la Universidad Rovira i Virgili y la Universitat Oberta de Catalunya
- Máster Universitario en Seguridad de las Tecnologías de la Información y las Comunicaciones por la Universidad Europea de Madrid

- Máster Universitario en Seguridad Informática por la Universidad Internacional de La Rioja
- Máster Universitario en Seguridad Informática y Sistemas Inteligentes
- Máster Universitario en Tecnologías de Protección para Sistemas de Seguridad y Defensa por la Universidad Rey Juan Carlos
- Máster Universitario en Cómputo de Altas Prestaciones, Teoría de la Información y Seguridad / High Performance Computing, Information Theory and Security por la Universidad Autónoma de Barcelona
- Máster Universitario en Gestión de la Seguridad de la Información
- Máster Universitario en Ciberseguridad por la Universidad Carlos III de Madrid

No obstante, muchos de esos másteres están orientados a gestores y jefes de seguridad, por lo que se centran en aspectos de gestión de la seguridad y auditoría. Por el contrario, el máster propuesto tiene una vocación más técnica y práctica, centrada en la aplicación directa de las medidas de seguridad ante un ciberataque.

En la Comunidad de Andalucía, sólo se imparten dos títulos propios en materia de seguridad informática, que se encuentran en la Universidad de Sevilla y la Universidad de Granada.

En el ámbito europeo, la agencia europea por la ciberseguridad ENISA [http://www.enisa.europa.eu/] no ha hecho una apuesta tan decidida por la educación reglada en ciberseguridad como la que encontramos en EEUU, que ha creado un programa estratégico destinado a aumentar el personal cualificado en ciberseguridad en las empresas y en la administración. A través de dicho programa, la Agencia Nacional de Seguridad de EEUU (NSA) dentro del programa estratégico cyber-ops reconoce y financia cuatro centros de excelencia que imparten estudios de Máster dirigidos a fundamentalmente a Graduados en Informática e Ingeniería, como el que aquí proponemos. Sus planes de estudio nos han servido para orientarnos en el diseño del Plan de Estudios, además de la colaboración del Comité Elaborador que mencionamos en el apartado siguiente, con fuerte participación de los agentes sociales.

En este sentido, es de destacar la colaboración con la empresa Deloitte, que ha participado activamente en la elaboración del máster, teniendo experiencia en la impartición de otros másteres propios repartidos por el territorio nacional como el Máster en Ciberseguridad de la Universitat Ramon Llull o el Máster en Ciberseguridad de la Universidad Católica de Ávila.

Los centros y programas de Estados Unidos más relevantes son:

- Dakota State University, South Dakota [http://www.dsu.edu/majors-programs/computernetwork-security.aspx];
- Naval Postgraduate School, California [http://www.cisr.us/sfscourses.STEM.html];
- Northeastern University, Massachusetts [http://www.ccs.neu.edu/graduate/degreeprograms/m-s-in-information-assurance/];
- Tulsa University, Oklahoma [http://isec.utulsa.edu/education/].

Aparte de esta iniciativa, también nos ha ayudado el análisis de los diferentes planes de estudios de alguno de los programas más renombrados en seguridad, aunque no estén específicamente centrados en ciberseguridad:

- University of Maryland UniversityCollege: http://www.umuc.edu/grad/gradprograms/csec.cfm
- Georgia Institue of Technology: http://www.gtisc.gatech.edu
- Purdue University: http://www.cerias.purdue.edu

Por último, en Europa la oferta de másteres incluye aspectos de ciberseguridad, aunque no están centrados en ella, es más habitual encontrar estudios más tradicionales de seguridad y análisis forense, como:

- M.Sc. in ComputerScience and Forensics de la Universidad de Bedfordshire [http://www.beds.ac.uk/howtoapply/courses/postgraduate/current-year/computer-security-andforensics]
- M.Sc. in Security and Forensic Computing de la Ciudad de Dublín [http://www.dcu.ie/prospective/deginfo.php?classname=MSSF]
- Master in Cibersecurity, oferta conjunta de Ecole Royale Militaire, Université Libre de Bruxelles, Université Catholique de Louvain, Université de Namur, Haute Ecole de Bruxelles, Haute Ecole Libre de Bruxelles [https://masterincybersecurity.ulb.ac.be/]

2.3. Descripción de los procedimientos de consulta internos utilizados para la elaboración del plan de estudios.

Con la finalidad de intercambiar información y experiencias académicas, promover el debate y la reflexión para la preparación del Plan de Estudios del Máster Universitario en Seguridad Informática (Ciberseguridad) por la Universidad de Cádiz, se realizó un análisis de los colectivos que podrían aportar información relevante para el diseño del mismo y de los

posibles procedimientos de consulta más adecuados. Como resultado de este análisis, el 3 de junio de 2 016, y de acuerdo al marco del Reglamento UCA/CG02/2012, de 30 de marzo de 2012, por el que se aprueban los criterios generales y el procedimiento para la definición del Mapa de Másteres de la Universidad de Cádiz y la reordenación de los títulos de másteres, se aprueba por la Junta de Escuela de la ESI la Propuesta de la Comisión para la elaboración de la Memoria del Máster Universitario en Seguridad Informática (Ciberseguridad) que se constituyó oficialmente en la sesión celebrada el día 19 de julio de 2016. Para conformar esta Comisión, se solicitó la designación de representantes a los Departamentos vinculados a la Ingeniería informática. En concreto, dos representantes del área de Lenguajes y Sistemas Informáticos, dos representantes del área de Arquitectura de Computadores y dos representantes del área de Ciencias de la Computación e Inteligencia Artificial. Se realizó la invitación a un miembro del departamento de Matemáticas y a otro miembro del departamento de Estadística e Investigación Operativa. Además, se incorporó a dos profesionales expertos de reconocido prestigio en el ámbito de la ingeniería informática, uno de ellos representando al Colegio de Ingenieros Informáticos de Andalucía y otro en representación de la empresa Deloitte. Esta Comisión estuvo elaborando, en varias sesiones de trabajo, la estructura académica del plan de estudios, con el establecimiento de las asignaturas obligatorias y la oferta de asignaturas optativas a partir de las propuestas realizadas por los Departamentos de la UCA.

Paralelamente se han llevado a cabo una serie de reuniones de coordinación y consultas con los responsables de calidad y oficina de posgrado.

Finalmente, esta Memoria elaborada por la Comisión se somete al proceso de exposición pública y aprobación definido en la Instrucción **UCA/I01VDF/2012, de 5 de noviembre de 2012,** del Vicerrector de Docencia y Formación de la Universidad de Cádiz, por la que se dicta el calendario para la elaboración y la aprobación de las memorias de los títulos que conformarán el Mapa de Másteres de la Universidad de Cádiz, con vistas a su verificación para el Curso académico 2017/2018. Las evidencias y documentos relacionados con los procedimientos de consulta están disponibles en las actas de la comisión que se conservan en la Secretaría del Centro. También se conservan los espacios de trabajo colaborativo en red que se usaron como foro de intercambio de información y opiniones

2.4. Descripción de los procedimientos de consulta externos utilizados para la elaboración del plan de estudios

Como punto de partida se realizó una encuesta a los alumnos de la Escuela Superior de Ingeniería sobre la impartición de un futuro máster, siendo el máster en seguridad informática el más demandado por los futuros egresados.

La Escuela Superior de Ingeniería ha participado en la estrategia de definición de másteres de la Universidad de Cádiz. En paralelo, desde la dirección de la Escuela Superior de Ingeniería se propuso la creación de un grupo de trabajo para la elaboración de la estrategia del mapa de másteres del centro, creándose en la Junta de Escuela del pasado día 3 de junio de 2016. En la estrategia que se plantea por dicho grupo de trabajo se establece como una de las líneas prioritaria la seguridad informática.

En las sesiones de trabajo de la Comisión han participado en el análisis y debate de esta propuesta de grado, representantes del mundo empresarial así como del colegio de Ingenieros Informáticos, que han aportado sus comentarios y puntos de vista sobre determinados aspectos.

Asimismo, han sido consultados diversos profesionales de la ingeniería informática. Las consultas se han realizado a través de reuniones con las personas implicadas y durante la participación en congresos.

Además de los procedimientos anteriores nuestro centro ha participado en todas las reuniones llevadas a cabo por la Conferencia de Decanos y Directores de Ingeniería Informática de España (CODDII) y se ha mantenido informado de todos los acuerdos realizados por dicha Conferencia.

3. Objetivos y Competencias.

3.1. Objetivos generales del título.

El Máster en Seguridad Informática tiene como objetivo general la formación de expertos en la seguridad de las tecnologías de la información y la comunicación, y muy especialmente en la ciberseguridad. Así, se marca como objetivos generales:

- Formar profesionales en la seguridad de las tecnologías de la información y la comunicación capaces de realizar auditorías de seguridad, analizar los hechos y la información de seguridad recopilada, aplicar la ingeniería inversa y la ciberinteligencia, así como llevar a cabo un correcto análisis forense.
- Garantizar el desarrollo seguro de aplicaciones, ya sea tanto en plataformas web como en entornos móviles.
- Capacitar para aplicar la seguridad defensiva desde el punto de vista del administrador de sistemas o de la arquitectura web.
- Saber aplicar la seguridad ofensiva desde las metodologías de ataque.

3.2. Competencias básicas.

CÓDIGO	COMPETENCIA BÁSICA
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.

3.3. Competencias generales.

CÓDIGO	COMPETENCIA GENERAL

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.

3.4. Competencias específicas.

CÓDIGO	COMPETENCIA ESPECÍFICA
CE1	Conocer el procedimiento de realización de una auditoría informática.
CE2	Ser capaces de aplicar una metodología para el análisis y evaluación de riesgos, así como saber utilizar las herramientas para su gestión.
CE3	Conocer 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, que posibilite al alumno su comprensión, y a satisfacer de manera óptima las exigencias profesionales.
CE4	Conocer las normas y estándares de referencia y certificación relacionados con seguridad de la información.
CE5	Poder ejercer la actividad profesional de acuerdo con los aspectos legales actuales en el entorno de las TIC.
CE6	Conocer las técnicas y herramientas para la realización de un análisis forense con la preservación de pruebas digitales
CE7	Conocer y aplicar los mecanismos de cifrado y esteganografiado pertinentes para proteger los datos residentes en un sistema o en tránsito por una red.
CE8	Asegurar las comunicaciones para garantizar la integridad, autenticidad y confidencialidad.

CE9	Elaborar técnicas para incrementar la seguridad de sistemas web.
CE10	Analizar el código de una aplicación para reconocer posibles errores de seguridad.
CE11	Diseñar aplicaciones incorporando el criterio de seguridad dentro del propio proceso de desarrollo
CE12	Capacidad para reconstruir el código de las aplicaciones a partir de los ficheros ejecutables.
CE13	Conocimiento, detección y evaluación de las vulnerabilidades de bajo nivel que afectan a los sistemas informáticos.
CE14	Capacidad para analizar ataques stack overflow.
CE15	Conocimiento de las diferentes medidas de prevención contra ataques stack overflow.
CE16	Conocimiento del funcionamiento y de los dispositivos de seguridad TPM
CE17	Capacidad para la detección de vulnerabilidades en los distintos elementos de un sistema informático.
CE18	Conocer y aplicar técnicas y herramientas para la realización de pruebas de penetración
CE19	Conocimiento de las principales técnicas de IA y sus aplicaciones en seguridad
CE20	Capacidad para identificar herramientas de IA apropiadas para distintos problemas de seguridad
CE21	Capacidad de modelar problemas de seguridad para su resolución con algoritmos de IA
CE22	Desarrollo de habilidades para la elaboración y evaluación de nuevos diseños de IA
CE23	Capacidad para el establecimiento de medidas de seguridad de los datos en sistemas abiertos a nivel de sistemas operativos, bases de datos y aplicaciones
CE24	Describir las amenazas de seguridad de las infraestructuras de red modernas.
CE25	Asegurar los dispositivos de interconexión de redes.

CE26	Describir funcionalidades AAA (autenticación, autorización y contabilización) e implementarlas en los dispositivos de interconexión de redes.
CE27	Mitigar las amenazas a las redes utilizando dispositivos de filtrado de paquetes.
CE28	Implementar sistemas de detección/prevención de intrusos para asegurar las redes contra ataques en proceso.
CE29	Mitigar las amenazas al correo electrónico, las basadas en web, los ataques a nodos finales y los ataques comunes de capa 2.
CE30	Describir el propósito de las VPNs, e implementar acceso remoto y VPN de sitio a sitio.
CE31	Asegurar redes utilizando dispositivos todo en uno.
CE32	Comprobar la seguridad de la red mediante pruebas.
CE33	Generar documentación técnica de políticas de seguridad.
CE34	Capacidad para identificar los métodos y la estrategia de monitorización de la seguridad a seguir de acuerdo a la legislación vigente.
CE35	Análisis de los contenidos de los paquetes de red. Capacidad para detectar información sensible en materia de seguridad.
CE36	Conocimiento de los sistemas de detección y prevención de intrusiones. Capacidad para discernir y seleccionar el sistema adecuado.
CE37	Uso de las herramientas de monitorización de la seguridad.
CE38	Analizar las particularidades de los sistemas críticos y de los distintos ámbitos en los que se utilizan
CE39	Analizar los esquemas de autenticación y acceso que se emplean en los sistemas críticos según el ámbito de aplicación
CE40	Diseñar soluciones de autenticación y control de acceso adaptadas a un sistema crítico concreto
CE41	Diseñar mecanismos de prevención de amenazas a la seguridad, así como de detección y respuesta a las incidencias de seguridad en los sistemas críticos

CE42	Capacidad de dotar de sistemas de seguridad a implementaciones basadas en arquitecturas orientadas a servicios y dirigidas por eventos, en particular arquitecturas con servicios web REST, SOAP y buses de servicios empresariales.
CE43	Capacidad de elegir el mecanismo de seguridad más adecuado para una arquitectura orientada a servicios y dirigidas por eventos en función de sus características particulares y la finalidad de uso.
CE44	Capacidad de seleccionar dispositivos y plataformas IoT seguros para la obtención de datos reales provenientes de fuentes heterogéneas.
CE45	Capacidad de integrar estos dispositivos y plataformas IoT con buses de servicios empresariales para filtrar, transformar, enriquecer, correlacionar, anonimizar, securizar y almacenar los datos sensorizados.
CE46	Capacidad para diseñar, desplegar y configurar redes inalámbricas seguras mediante la aplicación de políticas de seguridad apropiadas.
CE47	Conocimiento y evaluación de las amenazas y riesgos de seguridad que afectan a las redes inalámbricas.
CTFM	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.

3.5. Competencias transversales.

CÓDIGO	COMPETENCIA TRANSVERSAL
CT1	Trabajo en equipo: capacidad de asumir las labores asignadas dentro de un equipo, así como de integrarse en él y trabajar de forma eficiente con el resto de sus integrantes.
CT2	Expresión oral y escrita en lengua inglesa

3.6. Relación entre las competencias y las asignaturas.

RELACIÓN ENTRE LAS COMPETENCIAS Y LAS ASIGNATURAS O MATERIAS															
COMPETENCIAS	ASIGNATURAS														
	AAR	LEG	AF	CRIP	DAS	IIAS	HE	IAAS	SSA	SR	MSR	SSIC	SSD	SSI	TFM
CB6	X		X		X	X		X		X	X		X	X	X
CB7			X	X		X	X	X	X	X	X	X	X	X	X

CB8		X	X	X	X	X	X		X	X	X			X	X
CB9	X	X	X			X					X	X	X	X	X
CB10	X	X	X	X	X	X	X	X	X		X	X	X		X
CG1			X	X		X	X	X	X	X				X	X
CG2			X	X	X	X	X	X	X	X	X	X	X	X	X
CG3	X	X	X			X				X	X		X	X	X
CG4		X	X						X		X	X			X
CG5					X	X	X		X	X	X	X		X	X
CE1	X													X	
CE2	X													X	
CE3		X													
CE4		X													
CE5		X													
CE6			X												
CE7				X											
CE8				X											
CE9					X										
CE10					X										
CE11					X										
CE12						X									
CE13						X									
CE14						X									
CE15						X									
CE16						X									
CE17							X								
CE18							X								
CE19								X							
CE20								X							
CE21								X							
CE22								X							
CE23									X						
CE24										X					
CE25										X					
CE26										X					
CE27										X					
CE28										X					
CE29										X					
CE30										X					
CE31										X					
CE32										X					
CE33										X					
CE34											X				
CE35											X				
CE36											X				
CE37											X				
CE38												X			

CE39													X			
CE40													X			
CE41													X			
CE42														X		
CE43														X		
CE44														X		
CE45														X		
CTFM																X
CT1	X			X	X	X		X					X	X	X	
CT2													X			

donde:

Auditoría y análisis de riesgos	AAR
Legislación y normativa aplicada a la seguridad informática	LEG
Análisis forense	AF
Criptografía aplicada a la protección de datos	CRIP
Desarrollo de aplicaciones seguras	DAS
Ingeniería inversa y arquitecturas seguras	IIAS
Hacking ético	HE
Inteligencia artificial aplicada a la seguridad	IAAS
Seguridad en sistemas abiertos	SSA
Seguridad en redes	SR
Monitorización de la seguridad de redes	MSR
Seguridad en sistemas e infraestructuras críticas	SSIC
Seguridad en sistemas distribuidos	SSD
Seguridad inalámbrica	SSI

4. Acceso y Admisión de Estudiantes.

4.1. Sistemas de Información previo a la matriculación y procedimientos de acogida accesibles y orientación a los estudiantes de nuevo ingreso para facilitar su incorporación a la universidad y a la titulación.

Se tienen previstos varios mecanismos para hacer llegar información básica y complementaria a los posibles alumnos de nuevo ingreso. En el Sistema de Garantía de Calidad se incluye un procedimiento sobre el proceso de difusión e información pública del título. El principal canal de difusión e información sobre la titulación y sobre el proceso de matriculación es el espacio web de la UCA (http://www.uca.es/posgrado/presentacion/), así como la documentación específica entregada por la Dirección General de Acceso a cada futuro estudiante. Se mantiene en el espacio web de la UCA un portal accesible con toda la información necesaria para la matriculación.

Las fechas de preinscripción y matriculación, así como otros procesos administrativos, vienen regulados en el seno del Distrito Único Andaluz (DUA). Buena parte de los aspirantes encuentran en esta instancia los canales de información que le conducen al conocimiento de estos estudios en la UCA. Por su parte, los responsables de la titulación, canalizarán diversas acciones destinadas a la divulgación de los estudios en el entorno social y económico del Centro.

El apoyo a la matriculación se realizará de manera coordinada desde diferentes instancias: la Oficina de Posgrado de la UCA, la secretaría de la Escuela responsable del Título y la Dirección de los mismos. Todo ello basado en los recursos propios de las TIC, sin desatender la comunicación directa y personal en los casos necesarios.

Para la acogida de los alumnos de nuevo ingreso, la titulación dispone de un procedimiento específico común para todos los Centros de la UCA. Dentro del Plan de acogida se proponen actividades de información y orientación específica para los alumnos de nuevo ingreso. Estas actividades de acogida están orientadas a facilitar la incorporación a la Universidad de Cádiz y ya tienen una larga tradición en la UCA. Con estas actividades se pretende que el estudiante conozca el Plan de Estudios, sus características y particularidades al igual que tenga información sobre los distintos servicios de la Universidad prestando un especial interés a los servicios de biblioteca, deportes y gestión administrativa de secretaría.

4.2. Requisitos de Acceso y Criterios de Admisión.

Según 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 art. 75 de la Ley 15/2003, Andaluza de Universidades, a los únicos efectos del ingreso en los centros universitarios, todas las Universidades públicas andaluzas se constituyen en un distrito único. 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 la hora de establecer los criterios de admisión, se tendrá en cuenta lo establecido en el artículo 17 del Real decreto 1393/2007, modificado por el Real Decreto 861/2010. Los criterios y requisitos de admisión en el Máster universitario en Seguridad Informática 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 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%
- Formación académica previa, 30%
- Experiencia profesional relacionada con el ámbito del máster, 20%
- Dominio de la lengua inglesa, 10%

4.3. Sistemas de apoyo y orientación a los estudiantes una vez matriculados.

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.

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**.**

4.4. Sistema de transferencia y reconocimiento de créditos.

La transferencia y el reconocimiento de créditos se realizarán según la normativa vigente de la Universidad de Cádiz establecida en cada momento, constituyendo tal normativa en el momento presente el Reglamento UCA/CG12/2010, de 28 de junio de 2010, 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 (BOUCA, nº 109 de julio de 2010).

RECONOCIMIENTO DE CRÉDITOS			
CURSADOS EN ENSEÑANZAS SUPERIORES OFICIALES NO UNIVERSITARIAS:			
Mínimo:	0	**Máximo:**	0
CURSADOS EN TÍTULOS PROPIOS:			
Mínimo:	0	**Máximo:**	0
CURSADOS POR ACREDITACIÓN DE EXPERIENCIA LABORAL Y PROFESIONAL:			
Mínimo:	0	**Máximo:**	9

4.5. Descripción de los Complementos Formativos.

No se contemplan

5. Planificación de las enseñanzas.

5.1. Estructura general del plan de estudios.

Se propone un Máster semipresencial con apoyo de la plataforma de docencia virtual de la UCA (http://campusvirtual.uca.es/). El plan de estudios propuesto consta de 60 ECTS en un curso académico, que se estructuran en 4 módulos obligatorios de más un Trabajo Fin de Máster, también obligatorio. Cada crédito ECTS equivale a 25 horas de trabajo del alumnado para la adquisición de los conocimientos, capacidades y destrezas. En esta equivalencia se incluyen las horas teóricas o prácticas, las horas de estudio, las dedicadas a la realización de seminarios, trabajos dirigidos o prácticas, y las necesarias para la preparación y realización de las pruebas de evaluación. Con carácter general, la presencialidad en las diferentes actividades formativas se establece en 10 horas por crédito ECTS. La siguiente tabla muestra el número de créditos por cada tipo de materia.

DISTRIBUCIÓN DEL PLAN DE ESTUDIOS EN CRÉDITOS ECTS POR MATERIA	
Créditos totales:	60
Número de créditos en Prácticas Externas:	0
Número de créditos Optativos:	0
Número de créditos Obligatorios:	53
Número de créditos Trabajo Fin de Máster:	7
Número de créditos de Complementos Formativos:	0

Las materias están organizadas de tal forma que se garantice la adquisición de las competencias generales y específicas indicadas en el capítulo 3. El programa de estudios de este Máster pretende que los alumnos adquieran conocimientos científicos y tecnológicos avanzados sobre la Seguridad Informática, especialmente en el ámbito de la Ciberseguridad. Para ello, se les dotará de un conjunto de habilidades, aptitudes y conocimientos en un conjunto de aspectos avanzados de la ciberseguridad que les capaciten para llevar a cabo trabajos de investigación, desarrollo e innovación en esta área, además de facilitar su adaptación a un entorno tan rápidamente cambiante como este.
La estructura del Máster se corresponde con los siguientes módulos:

DISTRIBUCIÓN EN MÓDULOS		
Módulo	**ECTS**	**Carácter**

Regulación	8	Obligatorio
Tecnologías de seguridad	24	Obligatorio
Seguridad en sistemas	21	Obligatorio
Trabajo Fin de Máster	7	Obligatorio

5.2. Descripción y justificación académica del plan de estudios.

A continuación especificamos la relación de créditos y asignaturas que componen cada uno de los módulos y materias que componen este Máster.

MÓDULO	MATERIA	CRÉDITOS	ASIGNATURA	CRÉDITOS	CURSO	SEMESTRE
Regulación	Regulación	8	Auditoría y análisis de riesgos	4	1	1
			Legislación y normativa aplicada a la seguridad informática	4	1	1
Tecnologías de seguridad	Tecnologías de seguridad	24	Análisis forense	5	1	1
			Criptografía aplicada a la protección de datos	2	1	1
			Desarrollo de aplicaciones seguras	4	1	1
			Ingeniería inversa y arquitecturas seguras	4	1	1
			Hacking ético	5	1	2
			Inteligencia artificial aplicada a la seguridad	4	1	2
Seguridad en sistemas	Seguridad en sistemas	21	Seguridad en sistemas abiertos	4	1	1
			Seguridad en redes	5	1	1
			Monitorización de la seguridad de redes	2	1	2
			Seguridad en sistemas e infraestructuras críticas	4	1	2

			Seguridad en sistemas distribuidos	4	1	2
			Seguridad inalámbrica	2	1	2
Trabajo fin de máster	Trabajo fin de máster	7	Trabajo de fin de máster	7	1	2

Respecto de la organización temporal, el máster se imparte en un curso académico, teniendo el primer semestre una carga asociada de 32 créditos ECTS, mientras que en el segundo es de 28 créditos ECTS. El Trabajo Fin de Máster, de 7 créditos ECTS, se realiza a lo largo de todo el curso, aunque en la práctica es razonable suponer una mayor carga de trabajo para el alumno durante el segundo semestre, de ahí la asimetría en ambos semestres.

5.2.1. Actividades Formativas *(enumerar todas las del Plan de Estudios).*

La lengua utilizada a lo largo del proceso formativo es el español, aunque pueden desarrollarse actividades en otro idioma, preferentemente inglés.

La carga total de trabajo del estudiante será de 25 horas totales por cada crédito ECTS y, con carácter general, la presencialidad en las diferentes actividades formativas se establece en 10 horas por crédito ECTS.

Considerando las competencias a desarrollar en los diferentes módulos del plan de estudios, se ha incluido una propuesta de actividades formativas por materia, así como una estimación de la dedicación establecida a las diferentes actividades formativas en cada ficha de materia, sin menoscabo de que anualmente las actividades formativas y metodología de cada materia deba ser aprobada en la planificación docente de cada curso académico, siguiendo las directrices establecidas en el Sistema de Garantía de Calidad y en el procedimiento de Planificación Docente en coordinación con el Vicerrectorado competente en materia de Ordenación Académica.

ACTIVIDADES FORMATIVAS DEL PLAN DE ESTUDIOS	
NÚMERO	**DESCRIPCIÓN DE LA ACTIVIDAD FORMATIVA**
1	Clases de teoría
2	Clases teórico-prácticas
3	Clases de problemas

4	Clases de prácticas
5	Seminarios y conferencias
6	Actividades académicas no presenciales
7	Tutorías
8	Evaluación

5.2.2. Metodologías Docentes. *Enumerar todas las del Plan de Estudios).*

El Sistema Europeo de Transferencia y Acumulación de Créditos (ECTS) centra la medición de los créditos en la carga global de trabajo del estudiante. Constituye la base sobre la que construir un programa de aprendizaje centrado en la adquisición de competencias, que comprenda, no sólo clases presenciales, sino también otro tipo de actividades docentes, dirigidas o no por el profesor y que pueden desarrollarse dentro o fuera del aula.

La Universidad de Cádiz adoptó como referencia que un crédito ECTS equivale a 25 horas de trabajo del alumno que habrán de comprender, entre otras, las siguientes modalidades organizativas:

- Docencia presencial.
- Trabajos académicamente dirigidos, en grupo y/o individuales, realizados fuera del aula.
- Trabajos académicamente dirigidos, en grupo y/o individuales, dentro del aula.
- Estudio autónomo y preparación de exámenes y/o pruebas
- Celebración de exámenes y/o pruebas de evaluación en su caso.

La metodología docente tomará como referente los modelos de innovación docente propuestos para las universidades andaluzas. De acuerdo con el Procedimiento anual de Planificación Docente se ajustarán los grupos de docencia teórica y práctica de las distintas materias y asignaturas en atención a los recursos disponibles, a las propuestas de los departamentos y a los criterios de ordenación que se establezcan por el Centro, en coordinación con el Vicerrectorado competente en materia de Ordenación Académica.

METODOLOGÍAS DOCENTES DEL PLAN DE ESTUDIOS	
NÚMERO	**DESCRIPCIÓN DE LA METODOLOGÍA DOCENTE**
1	Lección magistral expositiva
2	Resolución de problemas y casos prácticos
3	Prácticas de laboratorio
4	Prácticas de ordenador
5	Realización de trabajos
6	Seguimiento de TFG

5.2.3. Sistemas de Evaluación. *Enumerar todas las del Plan de Estudios).*

El sistema de calificaciones de las materias del Título será el vigente en cada momento, quedando definido actualmente de acuerdo con el RD 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y validez en todo el territorio nacional.

Los créditos obtenidos por reconocimiento de créditos correspondientes a actividades formativas no integradas en el plan de estudios no serán calificados numéricamente ni computarán a efectos de cómputo de la media del expediente académico.

El sistema de evaluación estará basado en pruebas que permitan evaluar de manera objetiva el nivel de competencias, conocimientos y capacidades adquiridas por los alumnos. De entre las estrategias de evaluación disponibles, las que se contemplan en las materias son las siguientes:

SISTEMAS DE EVALUACIÓN DEL PLAN DE ESTUDIOS	
NÚMERO	**DESCRIPCIÓN DE LOS SISTEMAS DE EVALUACIÓN**
1	Trabajos escritos realizados por el alumno
2	Exposiciones de ejercicios, temas y trabajos
3	Prácticas de laboratorio
4	Prácticas de informática
5	Participación y trabajo realizado en actividades formativas
6	Pruebas escritas u orales
7	Memoria, exposición y defensa del TFM

El sistema de evaluación concreto de cada asignatura deberá ser descrito en detalle en la correspondiente guía docente, como recoge el Reglamento General de Actividades Docentes de la Universidad de Cádiz. De entre las estrategias de evaluación disponibles, las que se contemplan en las materias son las siguientes:

1) Trabajos escritos realizados por el alumno.

Consiste en el diseño y desarrollo de un trabajo o proyecto que puede entregarse durante o al final de la docencia de la asignatura. Este tipo de evaluación también puede implementarse en grupos con un número reducido de estudiantes en el

que cada uno de ellos se haga cargo de un proyecto o en grupos con un mayor número de estudiantes que quede dividido en pequeños equipos, cada uno de los cuales se responsabilice de un proyecto. Este formato puede ser especialmente interesante para fomentar el trabajo en equipo de los estudiantes.

2) Exposiciones de ejercicios, temas y trabajos.

Son aquellas en que se pide al estudiante que defienda sus conocimientos mediante una exposición oral.

3) Prácticas de laboratorio.

Pruebas e informes, especialmente adecuado para laboratorios experimentales. Se le plantea al estudiante unos objetivos que debe ser capaz de conseguir mediante la ejecución de determinadas actividades (manejo de un instrumental,…).

4) Prácticas de informática.

Pruebas e informes, especialmente adecuado para laboratorios experimentales. Se le plantea al estudiante unos objetivos que debe ser capaz de conseguir mediante la ejecución de determinadas actividades (programación de un software, …).

5) Participación y trabajo realizado en actividades formativas.

Constituyen un instrumento que nos permite ir evaluando el proceso de aprendizaje a través de la observación sistemática de las intervenciones de los alumnos/as en el aula, teniendo en cuenta su forma de organizar el trabajo, las estrategias que utiliza, como resuelve las dificultades que se encuentra en la realización de las tareas. Valorar las actitudes y progresos de los alumnos, su interés, participación y trabajo en grupo, esfuerzo diario, comportamiento, motivación, etc.

6) Pruebas escritas u orales

Consiste en la realización de pruebas específicas tanto orales como por escrito que permita una valoración sobre el dominio de la terminología, el conocimiento de los principios básicos expuestos y la comprensión y aplicación de los contenidos. Para comprobar el nivel de conocimiento se hará mediante un sistema de evaluación que permita valorar el dominio de los mismos al inicio, durante o al final del proceso.

7) Memoria, exposición y defensa del TFM

El Trabajo Fin de Máster queda regulado por Reglamento marco UCA/CG07/2012, de 13 de julio de 2012, de Trabajos Fin de Grado y Fin de Máster de la Universidad de Cádiz, aprobado por acuerdo de Consejo de Gobierno de la Universidad de

Cádiz en sesión ordinaria celebrada el día 13 de julio de 2012, publicado en el BOUCA núm. 148.

Estos sistemas irán recogidos en las fichas de las distintas materias con su respectiva ponderación. Sin perjuicio de lo anterior, la ponderación en la calificación final de los exámenes y otras actividades del alumno (prácticas, trabajos, etc.) se establece, con carácter orientativo y a modo de objetivo a alcanzar, en los siguientes intervalos:

- Asignaturas fundamentalmente expositivas: Los exámenes, bien finales o parciales, bien en evaluación continua, tendrán una ponderación comprendida entre el 70% y el 100% del total de actividades evaluables.
- Asignaturas fundamentalmente prácticas: Los exámenes, bien finales o parciales, bien en evaluación continua, tendrán una ponderación comprendida entre el 0% y el 30% del total de actividades evaluables.

Según recoge el Reglamento marco UCA/CG07/2012, de 13 de julio de 2012, de Trabajos Fin de Grado y Fin de Máster de la Universidad de Cádiz , el TFM será evaluado por una comisión evaluadora tras la presentación del mismo por el estudiante mediante la exposición oral de su contenido en sesión pública convocada al efecto. En este sentido, serán objeto de evaluación las competencias, conocimientos y capacidades adquiridas por el estudiante mediante la realización del TFM.

5.3. Planificación y gestión de la movilidad de estudiantes propios y de acogida.

La orientación de los estudiantes sobre los programas de movilidad a los que pueden tener acceso durante el desarrollo de sus estudios consta de varios pasos, en los que intervienen, tanto personal específico de la Oficina de Relaciones Internacionales de la Universidad, como del centro, especialmente a través del "Responsable del programa de movilidad del Centro", persona que asume la coordinación y gestión directa de los programas de movilidad nacional e internacional en el Centro, con el necesario apoyo administrativo. En este marco, la función de la Oficina de Relaciones Internacionales conlleva la promoción y gestión de los programas de movilidad y de proyectos de cooperación e investigación a nivel europeo e internacional. Los principales programas de intercambio de los estudios de Máster de la Universidad de Cádiz pueden ser consultados en español e inglés en su página web (http://www.uca.es/es/internacional), donde se encuentran actualizados de manera permanente.

En dicha página se suministra información detallada sobre todas las convocatorias de ayuda vigentes en cada momento para financiar la movilidad (tanto de Programas Reglados como de Programas Propios de la UCA), con indicación del proceso de solicitud: financiación, impresos, plazos, condiciones, coordinadores académicos, etc. Además, en la página web del centro, se expone de forma permanente información sobre las diferentes convocatorias de movilidad, así como de las personas de contacto y coordinadores, requisitos y recomendaciones, etc., sobre los centros con los que se mantiene acuerdo de movilidad, especialmente dentro del programa ERASMUS. El título, dentro del sistema de garantía de calidad, dispone de un procedimiento para el análisis de los programas de movilidad. El procedimiento de gestión de la movilidad (P06) permite normalizar la definición de los objetivos de movilidad del título, la planificación de los programas en relación con estos objetivos, sistematizar los procedimientos de seguimiento y evaluación, al igual que regularizar los mecanismos de apoyo y orientación a los estudiantes una vez matriculados en lo que respecta a la movilidad.

Debe destacarse la existencia de un Coordinador de Movilidad en la Escuela Superior de Ingeniería de Cádiz, realizando ambos funciones de información, gestión, apoyo y asesoramiento en la movilidad de los estudiantes. Cada convenio bilateral se adecua al contenido curricular de la titulación, y se establecen con instituciones contraparte en las cuales existe similitud desde el punto de vista formativo, lo que asegura el éxito del proceso de intercambio. Durante los últimos cursos académicos, la Escuela ha ampliado de forma significativa el número de Centros extranjeros con los que ha firmado acuerdos de intercambio de estudiantes, PDI y PAS.

5.4. Mecanismos de coordinación.

Los mecanismos de coordinación docente del Máster están recogidos en el Sistema de Garantía Interno de la Calidad de la UCA. La Comisión de Garantía de Calidad del Máster actúa como vehículo de comunicación interna de la política, objetivos, planes, programas, responsabilidades y logros de los sistemas de coordinación. Es el órgano de evaluación y control de la calidad del máster y, en tal sentido, su labor sirve como apoyo para la gestión de los títulos. Asesorará a la Dirección del Centro en todas aquellas medidas que afectan al aseguramiento de la calidad del Máster.

Los Coordinadores de Título, entre los que cabe entender el Coordinador de Máster, se configuran, de acuerdo con lo previsto en el artículo 40.4 de los Estatutos de la Universidad

de Cádiz, como un órgano unipersonal de gobierno de existencia obligatoria y que, de acuerdo con lo previsto en el artículo 67.2 c) tienen la consideración de invitados permanentes, con voz y sin voto, de la Junta de Escuela. Las funciones, competencias y responsabilidades del Coordinador de Título se recogen, con carácter general, en el Manual del Sistema de Garantía de Calidad (SGC) de la Universidad de Cádiz, aprobado por Acuerdo del Consejo de Gobierno 21 de noviembre de 2012.

La figura del Coordinador/a de Título, es de vital importancia para ayudar en las tareas correspondientes a la implantación, revisión y propuestas de mejora del SGC del título de su competencia. El Coordinador de Título asumirá las competencias de la coordinación académica del título, por lo que cuenta entre sus funciones velar por la revisión de los programas, coordina a los responsables de las diferentes asignaturas (Coordinadores/as de asignaturas) y recaba los informes sobre satisfacción y evaluación de las enseñanzas. Otras funciones que desempeñarán son:

- Asegurarse de que se establecen, implantan y mantienen los procesos necesarios para el desarrollo del SGC en el título que coordina.
- Informar a la Comisión de Garantía de Calidad sobre el desempeño del SGC y de cualquier necesidad de mejora.
- Asegurarse de que se promueve el cumplimiento de los requisitos de los grupos de interés a todos los niveles relacionados con el título.

En el procedimiento P02-03 (Informe de análisis del perfil de ingreso), el Coordinador del Máster, en coordinación con la Comisión de Garantía de Calidad, analizará el perfil de ingreso; deberá, previo análisis de los marcos de referencia relativos a dichos procesos y al estudio de la situación actual del sistema universitario más próximo, del entorno social y del entorno profesional, proponer para debate y aprobación el nuevo perfil de ingreso en el título a la Junta de Escuela; se realizará un informe de resultados que se presenta a la Junta de Escuela conjuntamente con las propuestas de modificación del perfil de ingreso si procede.

En el P14-01 (Autoinforme para el seguimiento del Título) se solicita información y propuestas de todos los Departamentos implicados en el título, se recopila, revisa y comprueba la validez de toda la información. A partir de la información disponible se hará el análisis correspondiente realizando las propuestas que considere necesarias para la mejora de los propios procesos del SGC. En el proceso PE04 (Procedimiento para la Planificación, Desarrollo y Mediación de los resultados de la enseñanza), se prepara la documentación e información relacionada con el Máster para el análisis del título con especial atención a los resultados de

carácter académico y la revisión las actuaciones y resultados obtenidos en el título, y se reunirá la CGC que elaborará una propuesta para la revisión de la calidad del programa formativo del título. Para la P04-02 (Informe global del título: síntesis de los informes de asignaturas) se mantendrán reuniones periódicas con los equipos docentes por curso, así como con los coordinadores de módulo/materia/asignatura al objeto de coordinar y revisar el plan docente, y se consideran las propuestas de mejora que puedan derivarse de los resultados.

La Comisión de Garantía de Calidad, a través del coordinador del Máster, convocará al menos una vez cada semestre a los profesores responsables de asignaturas para llevar a cabo reuniones de coordinación docente. Por otro parte, el coordinador del Máster en cada centro convocará, al menos una vez en el curso académico, a los profesores responsables de asignaturas para informar del seguimiento del programa formativo, los resultados de las encuestas entre el alumnado, actualizar las guías docentes, recoger las sugerencias que se propongan y potenciar la comunicación entre los equipos docentes. Los Equipos Docentes de las distintas asignaturas propondrán la actualización anual de la Guía Docente, atendiendo a los objetivos establecidos en esta memoria y a los procedimientos contemplados en el Sistema de Garantía de Calidad. Las Guías Docentes deberán contener, como mínimo, información acerca de los siguientes aspectos:

- Denominación de la asignatura y localización en el Plan de Estudios
- Objetivos
- Metodología de Enseñanza/Aprendizaje
- Requisitos previos de matriculación
- Contenidos
- Programación temporal de la asignatura
- Sistema y criterios de evaluación
- Bibliografía y recursos

5.5. Descripción de los módulos. Fichas de las asignaturas.

FICHA DE MÓDULO	
DENOMINACIÓN DEL MÓDULO:	**REGULACIÓN**

MATERIA 1 DEL MÓDULO	
MATERIA 1:	**REGULACIÓN**

CARÁCTER:	**OBLIGATORIO**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS MATERIA:	**8**	**DESPLIEGUE TEMPORAL:**	**1S**

ASIGNATURAS DE LA MATERIA 1			
Asignatura 1:	**Auditoría y análisis de riesgos**		
CARÁCTER:	**Obligatorio**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS ASIGNATURA:	**4**	**DESPLIEGUE TEMPORAL:**	**1S**
Asignatura 2:	**Legislación y normativa aplicada a la seguridad informática**		
CARÁCTER:	**Obligatorio**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS ASIGNATURA:	**4**	**DESPLIEGUE TEMPORAL:**	**1S**

AUDITORÍA Y ANÁLISIS DE RIESGOS 4 ECTS			
COMPETENCIAS QUE SE ADQUIEREN: ***(indicar código)***			
Com. Básicas	**Com. Generales**	**Com. Específicas**	**Com. Transversales**
CB6 CB9 CB10	**CG3**	**CE1 CE2**	**CT1**
REQUISITOS PREVIOS:			
BREVE DESCRIPCIÓN DE LOS CONTENIDOS:			
Tema 1: Auditoría Tema 2: Análisis y gestión de riesgos de los sistemas de información			
RESULTADOS DE APRENDIZAJE:			
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.			
OBSERVACIONES:			

ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:			
Actividad	**Créditos ECTS**	**Nº de horas**	**Presencialidad (%)**
Clases teórico-prácticas	**1**	**10 horas**	**80%**
Clases prácticas	**2**	**20 horas**	**100%**
Seminarios y conferencias	**1**	**10 horas**	**80%**
Actividades académicas no presenciales		**56 horas**	**0%**
Evaluación		**4 horas**	**100%**
METODOLOGÍAS DOCENTES:			
Lección magistral expositiva Prácticas de ordenador Realización de trabajos			
SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:			
Sistema	**Ponderación Mínima**	**Ponderación Máxima**	
Trabajos escritos realizados por el alumno	**0%**	**50%**	
Exposiciones de ejercicios, temas y trabajos	**0%**	**30%**	
Participación y trabajo realizado en actividades formativas	**10%**	**30%**	
Pruebas escritas u orales	**30%**	**70%**	

LEGISLACIÓN, NORMATIVA Y SU APLICACIÓN EN SEGURIDAD Y PROTECCIÓN DE DATOS 4 ECTS			
COMPETENCIAS QUE SE ADQUIEREN: ***(indicar código)***			
Com. Básicas	**Com. Generales**	**Com. Específicas**	**Com. Transversales**
CB8, CB9, CB10	**CG3, CG4**	**CE3, CE4, CE5**	
REQUISITOS PREVIOS:			
BREVE DESCRIPCIÓN DE LOS CONTENIDOS:			
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.

RESULTADOS DE APRENDIZAJE:

Conocer las consideraciones legales que deben aplicarse en 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

OBSERVACIONES:

ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:

Actividad	Créditos ECTS	Nº de horas	Presencialidad (%)
Clases teórico-prácticas	**3,5**	**35 horas**	**80%**
Seminarios y conferencias	**0,5**	**5 horas**	**80%**
Actividades académicas no presenciales		**56 horas**	**0%**
Evaluación		**4 horas**	**100%**

METODOLOGÍAS DOCENTES:

Lección magistral expositiva
Resolución de problemas y casos prácticos
Realización de trabajos

SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:

Sistema	Ponderación Mínima	Ponderación Máxima

Trabajos escritos realizados por el alumno	**0%**	**50%**
Exposiciones de ejercicios, temas y trabajos	**0%**	**30%**
Participación y trabajo realizado en actividades formativas	**10%**	**30%**
Pruebas escritas u orales	**30%**	**90%**

FICHA DE MÓDULO	
DENOMINACIÓN DEL MÓDULO:	**TECNOLOGÍAS DE SEGURIDAD**

MATERIA 1 DEL MÓDULO			
MATERIA 1:	**TECNOLOGÍAS DE SEGURIDAD**		
CARÁCTER:	**OBLIGATORIO**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS MATERIA:	**24**	**DESPLIEGUE TEMPORAL:**	**1S-2S**

ASIGNATURAS DE LA MATERIA 1			
Asignatura 1:	**Análisis forense**		
CARÁCTER:	**Obligatorio**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS ASIGNATURA:	**5**	**DESPLIEGUE TEMPORAL:**	**1S**
Asignatura 2:	**Criptografía aplicada a la protección de datos**		
CARÁCTER:	**Obligatorio**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS ASIGNATURA:	**2**	**DESPLIEGUE TEMPORAL:**	**1S**
Asignatura 3:	**Desarrollo de aplicaciones seguras**		
CARÁCTER:	**Obligatorio**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS ASIGNATURA:	**4**	**DESPLIEGUE TEMPORAL:**	**1S**
Asignatura 4:	**Ingeniería inversa y arquitecturas seguras**		
CARÁCTER:	**Obligatorio**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS ASIGNATURA:	**4**	**DESPLIEGUE TEMPORAL:**	**1S**
Asignatura 5:	**Hacking ético**		
CARÁCTER:	**Obligatorio**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS ASIGNATURA:	**5**	**DESPLIEGUE TEMPORAL:**	**2S**
Asignatura 6:	**Inteligencia artificial aplicada a la seguridad**		
CARÁCTER:	**Obligatorio**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS ASIGNATURA:	**4**	**DESPLIEGUE TEMPORAL:**	**2S**

ANÁLISIS FORENSE (5 ECTS)			
COMPETENCIAS QUE SE ADQUIEREN: ***(indicar código)***			
Com. Básicas	**Com. Generales**	**Com. Específicas**	**Com. Transversales**
CB6,CB7,CB8,CB9,CB10	CG1,CG2,CG3,CG4	CE6	
REQUISITOS PREVIOS:			
BREVE DESCRIPCIÓN DE LOS CONTENIDOS:			
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			
RESULTADOS DE APRENDIZAJE:			
Conocer el mecanismo para obtener evidencias digitales válidas en procedimientos legales Desarrollar técnicas y herramientas necesarias para la investigación forense.			

OBSERVACIONES:
La superación de la asignatura 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.

ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:

Actividad	Créditos ECTS	Nº de horas	Presencialidad (%)
Teorico-prácticas	5	50	50%
Evaluación		5	0%
Actividades académicas no presenciales		70	0%

METODOLOGÍAS DOCENTES:

Lección magistral expositiva

Resolución de problemas y casos prácticos

Prácticas de laboratorio

SISTEMAS DE EVALUACIÓN DE ADQUISICIÓN DE COMPETENCIAS:

Sistema	Ponderación Mínima	Ponderación Máxima
Prácticas de laboratorio	0%	100%
Pruebas escritas u orales	30%	100%

CRIPTOGRAFÍA APLICADA A LA PROTECCIÓN DE DATOS (2 ECTS)			
COMPETENCIAS QUE SE ADQUIEREN: ***(indicar código)***			
Com. Básicas	**Com. Generales**	**Com. Específicas**	**Com. Transversales**
CB7,CB8,CB10	**CG1,CG2**	**CE7,CE8**	**CT1**
REQUISITOS PREVIOS:			
BREVE DESCRIPCIÓN DE LOS CONTENIDOS:			
Tema 1: Tipologías de Cifrado y ocultación de información Tema 2: Autentificación basada en claves Tema 3: Firma digital			
RESULTADOS DE APRENDIZAJE:			
Dado un sistema con unos requisitos de seguridad establecidos, proponer mecanismos y protocolos necesarios para proporcionar algunos de los servicios básicos de seguridad: autenticación, autorización, privacidad y control de acceso. Dar una medida de su eficacia y limitaciones.			
OBSERVACIONES:			
ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:			
Actividad	**Créditos ECTS**	**Nº de horas**	**Presencialidad (%)**
Clases de teoría	**1**	**10**	**80%**
Clases teórico-prácticas			
Clases de problemas			
Clases de prácticas	**1**	**10**	**100%**
Seminarios y conferencias			
Actividades académicas no presenciales		**26**	**0%**
Evaluación		**4**	**100%**
METODOLOGÍAS DOCENTES:			

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

SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:		
Sistema	**Ponderación Mínima**	**Ponderación Máxima**
Prácticas de informática	**10%**	**30%**
Participación y trabajo realizado en actividades formativas	**0%**	**20%**
Pruebas escritas u orales	**40%**	**70%**

DESARROLLO DE APLICACIONES SEGURAS 4 ECTS			
COMPETENCIAS QUE SE ADQUIEREN: ***(indicar código)***			
Com. Básicas	**Com. Generales**	**Com. Específicas**	**Com. Transversales**
CB6, CB8, CB10	**CG2, CG5**	**CE9, CE10, CE11**	**CT1**

REQUISITOS PREVIOS:

BREVE DESCRIPCIÓN DE LOS CONTENIDOS:
Tema 1: Construcción de aplicaciones seguras Tema 2: Ingeniería del software de sistemas seguros Tema 3: Seguridad en desarrollo web

RESULTADOS DE APRENDIZAJE:
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.

OBSERVACIONES:

ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:			
Actividad	**Créditos ECTS**	**Nº de horas**	**Presencialidad (%)**
Clases teórico-prácticas	**4**	**40**	**100%**
Actividades académicas no presenciales		**64**	**0%**
Tutorías		**2**	**0%**
Evaluación		**4**	**0%**
METODOLOGÍAS DOCENTES:			
Lección magistral expositiva Resolución de problemas y casos prácticos Prácticas de ordenador Realización de trabajos			
SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:			
Sistema	**Ponderación Mínima**	**Ponderación Máxima**	
Exposiciones de ejercicios, temas y trabajos	**10%**	**25%**	
Prácticas de informática	**25%**	**50%**	
Pruebas escritas u orales	**10%**	**25%**	
Participación y trabajo realizado en actividades formativas	**25%**	**50%**	

INGENIERÍA INVERSA Y ARQUITECTURAS SEGURAS (4 ECTS)			
COMPETENCIAS QUE SE ADQUIEREN: ***(indicar código)***			
Com. Básicas	**Com. Generales**	**Com. Específicas**	**Com. Transversales**
CB6, CB7, CB8, CB9, CB10	**CG1, CG2, CG3, CG5**	**CE12, CE13, CE14,CE15, CE16**	**CT1**
REQUISITOS PREVIOS:			

BREVE DESCRIPCIÓN DE LOS CONTENIDOS:
TEMA 1. Introducción a la arquitectura del conjunto de instrucciones x86-32 y x86-64 TEMA 2. Análisis de ficheros binarios TEMA 3. Reconstrucción de código TEMA 4. Ofuscación TEMA 5. Vulnerabilidades de bajo nivel TEMA 6. Trusted Platform Module (TPM)
RESULTADOS DE APRENDIZAJE:
R1. Reconstruir el código de las aplicaciones a partir de los ficheros ejecutables. R2. Conocer y detectar las vulnerabilidades de bajo nivel. R3. Realizar análisis exhaustivos de ataques stack overflow. R4. Conocer los diferentes mecanismos de protección contra ataques stack overflow. R5. Realizar análisis de ficheros binarios. R6. Conocer las aplicaciones y el funcionamiento de los dispositivos de seguridad TPM.
OBSERVACIONES:

ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:			
Actividad	**Créditos ECTS**	**Nº de horas**	**Presencialidad (%)**
Clases teórico-prácticas	3,6	36	100%
Evaluación	0,4	4	100%
Actividades académicas no presenciales		60	0%

METODOLOGÍAS DOCENTES:
Lección magistral expositiva Resolución de problemas y casos prácticos Prácticas de laboratorio Realización de trabajos

SISTEMAS DE EVALUACIÓN DE ADQUISICIÓN DE COMPETENCIAS:		
Sistema	**Ponderación Mínima**	**Ponderación Máxima**
Exposiciones de ejercicios, temas y trabajos	30%	70%
Pruebas escritas u orales	30%	70%

HACKING ÉTICO (5 ECTS)			
COMPETENCIAS QUE SE ADQUIEREN: ***(indicar código)***			
Com. Básicas	**Com. Generales**	**Com. Específicas**	**Com. Transversales**

CB7,CB8,CB10	CG1,CG2,CG5	CE17,CE18	

REQUISITOS PREVIOS:

BREVE DESCRIPCIÓN DE LOS CONTENIDOS:

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

RESULTADOS DE APRENDIZAJE:

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
Desarrollo de técnicas y uso de herramientas para las pruebas de penetración en sistemas informáticos

OBSERVACIONES:

La superación de la asignatura 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.

ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:			
Actividad	**Créditos ECTS**	**Nº de horas**	**Presencialidad (%)**
Teorico-prácticas	5	50	50%
Evaluación		5	0%
Actividades académicas no presenciales		70	0%

METODOLOGÍAS DOCENTES:
Lección magistral expositiva Resolución de problemas y casos prácticos Prácticas de laboratorio

SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:		
Sistema	**Ponderación Mínima**	**Ponderación Máxima**
Prácticas de laboratorio	0%	100%
Pruebas escritas u orales	30%	100%

INTELIGENCIA ARTIFICIAL APLICADA A LA SEGURIDAD 4 ECTS			
COMPETENCIAS QUE SE ADQUIEREN: ***(indicar código)***			
Com. Básicas	**Com. Generales**	**Com. Específicas**	**Com. Transversales**
CB6, CB7, CB10	**CG1, CG2**	**CE19, CE20, CE21, CE22**	**CT1**
REQUISITOS PREVIOS:			
Conocimiento avanzado de programación Conocimiento general de técnicas de IA			
BREVE DESCRIPCIÓN DE LOS CONTENIDOS:			
Tema 1: La inteligencia artificial y sus aplicaciones en seguridad Tema 2: Identificación basada en parámetros biomédicos Tema 3: Detección inteligente de intrusos Tema 4: Mejora automática en la seguridad del software Tema 5: Prevención de la denegación de servicio			
RESULTADOS DE APRENDIZAJE:			
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
OBSERVACIONES:

ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:

Actividad	Créditos ECTS	Nº de horas	Presencialidad (%)
Clases de teoría	**0,5**	**5**	**100%**
Clases teórico-prácticas	**3,5**	**35**	**100%**
Actividades académicas no presenciales		**60**	**0%**

METODOLOGÍAS DOCENTES:

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

SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:

Sistema	Ponderación Mínima	Ponderación Máxima
Exposiciones de ejercicios, temas y trabajos	**0%**	**30%**
Prácticas de informática	**50%**	**100%**
Participación y trabajo realizado en actividades formativas	**0%**	**10%**

FICHA DE MÓDULO	
DENOMINACIÓN DEL MÓDULO:	**SEGURIDAD EN SISTEMAS**

MATERIA 1 DEL MÓDULO			
MATERIA 1:	**SEGURIDAD EN SISTEMAS**		
CARÁCTER:	**OBLIGATORIO**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS MATERIA:	**21**	**DESPLIEGUE TEMPORAL:**	**1S-2S**

ASIGNATURAS DE LA MATERIA 1			
Asignatura 1:	**Seguridad en sistemas abiertos**		
CARÁCTER:	**Obligatorio**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS ASIGNATURA:	**4**	**DESPLIEGUE TEMPORAL:**	**1S**
Asignatura 2:	**Seguridad en redes**		
CARÁCTER:	**Obligatorio**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS ASIGNATURA:	**5**	**DESPLIEGUE TEMPORAL:**	**1S**
Asignatura 3:	**Monitorización de la seguridad de redes**		
CARÁCTER:	**Obligatorio**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS ASIGNATURA:	**2**	**DESPLIEGUE TEMPORAL:**	**2S**
Asignatura 4:	**Seguridad en sistemas e infraestructuras críticas**		
CARÁCTER:	**Obligatorio**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**

ECTS ASIGNATURA:	**4**	**DESPLIEGUE TEMPORAL:**	**2S**
Asignatura 5:	**Seguridad en sistemas distribuidos**		
CARÁCTER:	**Obligatorio**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS ASIGNATURA:	**4**	**DESPLIEGUE TEMPORAL:**	**2S**
Asignatura 6:	**Seguridad inalámbrica**		
CARÁCTER:	**Obligatorio**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS ASIGNATURA:	**2**	**DESPLIEGUE TEMPORAL:**	**2S**

SEGURIDAD EN SISTEMAS ABIERTOS 4 ECTS			
COMPETENCIAS QUE SE ADQUIEREN: ***(indicar código)***			
Com. Básicas	**Com. Generales**	**Com. Específicas**	**Com. Transversales**
CB7,CB8,CB10	**CG1,CG2,CG4,CG5**	**CE23**	
REQUISITOS PREVIOS:			
BREVE DESCRIPCIÓN DE LOS CONTENIDOS:			
Tema 1: Seguridad en sistemas operativos Tema 2: Seguridad en BD Tema 3: Seguridad en sistemas abiertos			
RESULTADOS DE APRENDIZAJE:			
Conocer los problemas de seguridad planteados con los sistemas abiertos, tanto en sistemas operativos, bases de datos y aplicaciones. Establecer una seguridad en los datos gestionados en los sistemas abiertos			
OBSERVACIONES:			

ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:			
Actividad	**Créditos ECTS**	**Nº de horas**	**Presencialidad (%)**
Clases teórico-prácticas	**4**	**40**	**80%**
Actividades académicas no presenciales		**56**	**0%**
Evaluación		**4**	**100%**
METODOLOGÍAS DOCENTES:			
Lección magistral expositiva Resolución de problemas y casos prácticos Prácticas de ordenador			
SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:			
Sistema	**Ponderación Mínima**	**Ponderación Máxima**	
Exposiciones de ejercicios, temas y trabajos	**0%**	**20%**	
Prácticas de informática	**0%**	**70%**	
Pruebas escritas u orales	**30%**	**70%**	

SEGURIDAD EN REDES (5 ECTS)			
COMPETENCIAS QUE SE ADQUIEREN: ***(indicar código)***			
Com. Básicas	**Com. Generales**	**Com. Específicas**	**Com. Transversales**
CB6, CB7 y CB8	**CG1, CG2, CG3 y CG5**	**CE24,CE25,CE26,CE27,CE28,CE29,CE30, CE31,CE32,CE33**	

REQUISITOS PREVIOS:
Conocimientos básicos de redes de computadores.
BREVE DESCRIPCIÓN DE LOS CONTENIDOS:
TEMA 1. AMENAZAS DE SEGURIDAD TEMA 2. SEGURIDAD EN DISPOSITIVOS DE INTERCONEXIÓN TEMA 3. SEGURIDAD EN EL ACCESO A LA RED TEMA 4. SEGURIDAD PERIMETRAL TEMA 5. IMPLEMENTACIÓN DE LA PREVENCIÓN TEMA 6. LAN SEGURA TEMA 7. REDES PRIVADAS VIRTUALES TEMA 8. DISPOSITIVOS TODO EN UNO TEMA 9. GESTIÓN DE REDES SEGURAS
RESULTADOS DE APRENDIZAJE:
1. Adquirir conocimientos básicos de seguridad. 2. Configurar los dispositivos de interconexión de redes de manera segura. 3. Implementar AAA (autenticación, autorización y contabilización) con dispositivos de interconexión de redes (routers y switchs). 4. Implantar y configurar cortafuegos. 5. Implantar y configurar IDS/IPS. 6. Asegurar los nodos finales. 7. Implementar redes privadas virtuales entre sitios. 8. Configurar correctamente dispositivos de redes todo en uno. 9. Gestionar la seguridad de las redes.
OBSERVACIONES:
En la medida que sea posible se ofrecerá al alumnado, en paralelo a la asignatura, la realización del curso CCNA Security.

ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:			
Actividad	**Créditos ECTS**	**Nº de horas**	**Presencialidad (%)**
Clases teórico-prácticas	4,8	48	100%
Evaluación	0.2	2	100%
Actividades académicas no presenciales		73	0%
METODOLOGÍAS DOCENTES:			
Lección magistral expositiva Prácticas de laboratorio			
SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:			
Sistema	**Ponderación Mínima**	**Ponderación Máxima**	
Prácticas de laboratorio	0%	50%	
Pruebas escritas u orales	50%	100%	

MONITORIZACIÓN DE LA SEGURIDAD DE REDES (2 ECTS)
COMPETENCIAS QUE SE ADQUIEREN: ***(indicar código)***

Com. Básicas	Com. Generales	Com. Específicas	Com. Transversales
CB6, CB7, CB8, CB9, CB10	**CG2, CG3, CG4, CG5**	**CE34,CE35,CE36,CE37**	**CT1**

REQUISITOS PREVIOS:

Poseer conocimientos básicos de redes de ordenadores.

BREVE DESCRIPCIÓN DE LOS CONTENIDOS:

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

RESULTADOS DE APRENDIZAJE:

R1. Compresión de los aspectos básicos de la monitorización de la seguridad de redes. Ser capaz de diseñar una estrategia adecuada de monitorización.
R2. Identificar los datos adquiridos en el proceso de monitorización.
R3. Conocimiento de los sistemas de detección y prevención de intrusiones.
R4. Ser capaz de usar aplicaciones de monitorización de seguridad.

OBSERVACIONES:

ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:

Actividad	Créditos ECTS	Nº de horas	Presencialidad (%)
Clases teórico-prácticas	1.8	18	100

Evaluación	0.2	2	100
Actividades académicas no presenciales		30	0

METODOLOGÍAS DOCENTES:

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

SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:

Sistema	Ponderación Mínima	Ponderación Máxima
Exposiciones de ejercicios, temas y trabajos	15%	25%
Prácticas de laboratorio	15%	25%
Pruebas escritas u orales	50%	70%

SEGURIDAD EN SISTEMAS E INFRAESTRUCTURAS CRÍTICAS
4 ECTS

COMPETENCIAS QUE SE ADQUIEREN: ***(indicar código)***

Com. Básicas	Com. Generales	Com. Específicas	Com. Transversales
CB7 CB9 CB10	**CG2 CG4 CG5**	**CE38 CE39 CE40 CE41**	**CT1 CT2**

REQUISITOS PREVIOS:

Haber cursado las asignaturas:

- Análisis forense
- Criptografía aplicada a la protección de datos
- Seguridad en sistemas abiertos

- Seguridad en red

BREVE DESCRIPCIÓN DE LOS CONTENIDOS:

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

RESULTADOS DE APRENDIZAJE:

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

OBSERVACIONES:

ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:

Actividad	Créditos ECTS	Nº de horas	Presencialidad (%)
Clases teórico-prácticas	**3**	**30 horas**	**100%**
Seminarios y conferencias	**1**	**10 horas**	**100%**
Actividades académicas no presenciales		**56 horas**	**0%**
Evaluación		**4 horas**	**100%**

METODOLOGÍAS DOCENTES:

Lección magistral expositiva
Resolución de problemas y casos prácticos
Realización y exposición de trabajos

SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:

Sistema	Ponderación Mínima	Ponderación Máxima

Trabajos escritos realizados por el alumno	**0%**	**50%**
Exposiciones de ejercicios, temas y trabajos	**10%**	**50%**
Participación y trabajo realizado en actividades formativas	**0%**	**25%**
Pruebas escritas u orales	**25%**	**75%**

SEGURIDAD EN SISTEMAS DISTRIBUIDOS 4 ECTS			
COMPETENCIAS QUE SE ADQUIEREN: ***(indicar código)***			
Com. Básicas	**Com. Generales**	**Com. Específicas**	**Com. Transversales**
CB6, CB7, CB9, CB10	**CG2, CG3**	**CE42 CE43 CE44 CE45**	**CT1**
REQUISITOS PREVIOS:			
Se recomienda tener conocimientos de programación orientada a objetos. Se recomienda tener conocimientos de programación en Java.			
BREVE DESCRIPCIÓN DE LOS CONTENIDOS:			
Tema 1: Seguridad en Arquitecturas Orientadas a Servicios y Dirigidas por Eventos Tema 2: Seguridad en Internet de las Cosas Tema 3: Seguridad en Cloud			
RESULTADOS DE APRENDIZAJE:			
Ser capaz de implementar sistemas de seguridad en arquitecturas orientadas a servicios y dirigidas por eventos, en particular arquitecturas con servicios web REST, SOAP y buses de servicios empresariales. Ser capaz de elegir el mecanismo de seguridad más adecuado para una arquitectura orientada a servicios y dirigidas por eventos particular, valorando sus características particulares y la finalidad de uso. Ser capaz de integrar diversos dispositivos/plataformas IoT seguros con buses de servicios empresariales, así como gestionar en tiempo real la información obtenida en distintos formatos.			
OBSERVACIONES:			

ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:			
Actividad	**Créditos ECTS**	**Nº de horas**	**Presencialidad (%)**
Clases de prácticas	**4**	**40 horas**	**100 %**
Actividades académicas no presenciales		**60 horas**	**0 %**
METODOLOGÍAS DOCENTES:			
Lección magistral expositiva Prácticas de ordenador Realización de trabajos			
SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:			
Sistema	**Ponderación Mínima**	**Ponderación Máxima**	
Exposiciones de ejercicios, temas y trabajos	**20**	**80**	
Prácticas de informática	**0**	**80**	
Participación y trabajo realizado en actividades formativas	**40**	**100**	

SEGURIDAD INALÁMBRICA (2 ECTS)			
COMPETENCIAS QUE SE ADQUIEREN: ***(indicar código)***			
Com. Básicas	**Com. Generales**	**Com. Específicas**	**Com. Transversales**
CB6, CB7, CB8, CB9, CB10	**CG1, CG2, CG3, CG5**	**CE46, CE47**	**CT1**
REQUISITOS PREVIOS:			
Haber adquirido las competencias de la asignatura *criptografía aplicada a la protección de datos* del Máster Universitario en Seguridad Informática (Ciberseguridad).			

BREVE DESCRIPCIÓN DE LOS CONTENIDOS:
TEMA 1. Topologías de redes inalámbricas TEMA 2. Amenazas y riesgos de seguridad TEMA 3. Métodos de cifrado utilizados en las comunicaciones inalámbricas TEMA 4. Métodos de autenticación TEMA 5. Infraestructuras de seguridad TEMA 6. Seguridad en redes Ad-Hoc
RESULTADOS DE APRENDIZAJE:
R1. Ser capaz de identificar las amenazas y riesgos de seguridad que afectan a las redes inalámbricas. R2. Conocer los mecanismos de autenticación y cifrado de las redes inalámbricas. R3. Diseñar e implementar servicios de acceso inalámbricos seguros. R4. Conocer los principales métodos utilizados para proteger el anonimato en redes ad-hoc.
OBSERVACIONES:
ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:

Actividad	Créditos ECTS	Nº de horas	Presencialidad (%)
Clases teórico-prácticas	**1,6**	**16**	**100%**
Evaluación	**0,4**	**4**	**100%**
Actividades académicas no presenciales		**30**	**0%**

METODOLOGÍAS DOCENTES:

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

SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:

Sistema	Ponderación Mínima	Ponderación Máxima
Exposiciones de ejercicios, temas y trabajos	30%	70%
Pruebas escritas u orales	30%	70%

FICHA DE MÓDULO	
DENOMINACIÓN DEL MÓDULO:	**TRABAJO FIN DE MÁSTER**

MATERIA 1 DEL MÓDULO			
MATERIA 1:	**TRABAJO FIN DE MÁSTER**		
CARÁCTER:	**OBLIGATORIO**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS MATERIA:	**7**	**DESPLIEGUE TEMPORAL:**	**2S**

ASIGNATURAS DE LA MATERIA 1			
Asignatura 1:	**Trabajo fin de máster**		
CARÁCTER:	**Obligatorio**	**IDIOMA DE IMPARTICIÓN:**	**Español (algunas actividades pueden ser en inglés)**
ECTS ASIGNATURA:	**7**	**DESPLIEGUE TEMPORAL:**	**2S**

INFORMACIÓN DE CADA MATERIA O ASIGNATURA			
COMPETENCIAS QUE SE ADQUIEREN: ***(indicar código)***			
Com. Básicas	**Com. Generales**	**Com. Específicas**	**Com. Transversales**
CB6,CB7,CB8,CB9,CB10	**CG1,CG2,CG3,CG4,CG5**	**CTFM**	

REQUISITOS PREVIOS:
Para poder ser evaluado de este módulo el alumno debe haber cursado y superado el resto de módulos del título.
BREVE DESCRIPCIÓN DE LOS 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.

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.**
OBSERVACIONES:

ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:			
Actividad	**Créditos ECTS**	**Nº de horas**	**Presencialidad (%)**
Clase de teoría	**0,1**	**1**	**100%**
Tutorías	**0,9**	**9**	**0%**
Actividad académica no presencial	**6**	**60**	**0%**
METODOLOGÍAS DOCENTES:			
Seguimiento de TFM			
SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:			
Sistema	**Ponderación Mínima**	**Ponderación Máxima**	
Memoria, exposición y defensa del TFM	**100**	**100**	

7. Personal Académico.

a. Personal académico disponible.

Se especifican en esta memoria los datos correspondientes a los profesores que constituyen el personal académico disponible, aportándose información sobre su vinculación a la universidad y su experiencia docente e investigadora.

La impartición de este máster se realizará en un formato de colaboración dual con la empresa Deloitte, y su CyberSOC-CERT Academy, que aportarán su conocimiento, experiencia y especialización en áreas de elevada cualificación técnica en el ámbito de la ciberseguridad. Esta participación activa proporcionará que 10 ECTS sean impartidos íntegramente por dicha empresa, y 50 ECTS serán impartidos por profesores de la Universidad de Cádiz.

El personal académico permite que la UCA pueda impartir este Máster con un profesorado de alta cualificación, con amplia experiencia investigadora y docente y con un perfil idóneo para las materias que imparten. Este importante equipo humano permitirá transmitir al alumnado los conocimientos teóricos y las técnicas asociadas y posibilitará el que los alumnos alcancen las competencias que requiere el título. Los departamentos y áreas de conocimiento implicados en la docencia del Máster son los siguientes:

- Departamento de Ingeniería en Automática, Electrónica, Arquitectura y Redes de Computadores, área de conocimiento de Arquitectura y Tecnología de Computadores
- Departamento de Ingeniería Informática, áreas de conocimiento Lenguajes y Sistemas Informáticos y Ciencias de la Computación e Inteligencia Artificial
- Departamento de Derecho Internacional Público, Penal y Procesal, área de conocimiento Derecho Penal.

Estos departamentos cuentan con el personal académico que se muestra en la siguiente tabla:

PERSONAL ACADÉMICO						
				DEDICACIÓN		
CATEGORÍA	NÚM.	TOTAL (%)	DOCTORES (%)	TOTAL	PARCIAL	HORAS (%)

Catedrático de Universidad						
Catedrático de Escuela Universitaria						
Profesor Titular de Universidad						
Profesor Titular de Escuela Universitaria						
Profesor Contratado Doctor						
Profesor Colaborador						
Profesor Ayudante Doctor						
Profesor Asociado						
Profesor Ayudante						
Profesor Visitante						
Otros:						

Junto al personal propio de la Universidad de Cádiz, se prevé la colaboración de otros profesionales de reconocido prestigio y acreditada experiencia profesional que, indudablemente, complementarán y enriquecerán la formación teórico-práctica requerida en este nivel de capacitación profesional.

b. Adecuación del profesorado y personal de apoyo al plan de estudios.

En virtud de los datos presentados en la tabla anterior, se puede extraer que la mayoría del profesorado implicado actualmente en las áreas relacionadas con el Máster mantiene una relación contractual estable con la Universidad de Cádiz, que permite que la UCA pueda impartir el Título con suficientes garantías.
El profesorado y personal de apoyo disponible es el idóneo para impartir el Máster en Seguridad Informática, como lo demuestra la experiencia impartiendo el Máster en Ingeniería Informática desde el curso 2014-15. Su preparación y experiencia docente e investigadora permitirá una adecuada formación de los estudiantes y la consecución de los objetivos establecidos. Los profesores-as implicados en el Máster tienen experiencia adecuada al título y conocen el funcionamiento y aplicación de la plataforma de enseñanza virtual a distancia de la UCA (Campus Virtual), con más de diez años de funcionamiento.

El profesorado y personal de apoyo que se proponga tiene que tener una dimensión docente avalada por la experiencia profesional acumulada en el desarrollo de materias similares a las

del Máster, o bien su dimensión investigadora o líneas de trabajo enmarcado en los contenidos de la Seguridad Informática.

El I Plan de Igualdad entre Mujeres y Hombres de la UCA (aprobado por Consejo de Gobierno de 22 de junio de 2011, BOUCA Nº. 122 de 7 de julio) prevé el establecimiento de estrategias para garantizar la igualdad de oportunidades y de trato en el acceso al trabajo y el desarrollo profesional de todos los miembros de la Comunidad universitaria (Eje 4). Específicamente prevé como objetivo "Garantizar la igualdad de oportunidades en la selección y promoción profesional de las mujeres y los hombres en la UCA" (Objetivo 4.1.) y, entre otras medidas para lograr su consecución, establece que "Se vigilará que los criterios y/o procedimientos de selección y promoción establecidos no supongan elementos de discriminación indirecta" (Medida 4.1.2.). En este sentido puede consultarse el documento en:

http://www.uca.es/igualdad/portal.do?TR=A&IDR=1&identificador=7895

El Servicio de Atención a la Discapacidad tiene como objetivo 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.

http://www.uca.es/discapacidad/

c. Otros recursos humanos disponibles.

La oferta docente no sería posible sin el concurso de personal de apoyo que atendiera las labores administrativas y de gestión imprescindibles para el correcto desarrollo de las actividades docentes e investigadoras.

La Escuela Superior de Ingeniería cuenta con el PAS adscrito y con dedicación exclusiva cuyas funciones son las tareas administrativas y de gestión que se derivan de la actividad académica, imprescindibles para el correcto desarrollo de la labor docente. La siguiente tabla recoge la composición del personal de administración y servicios adscrito:

PERSONAL DE APOYO AL TÍTULO EN LA ESI	
Unidad administrativa	**Nº**
Secretaría	1
Conserjería	5
Biblioteca	4

PERSONAL DE APOYO AL TÍTULO EN LA ESI	
Unidad administrativa	**Nº**
Gestores de Departamento	4
Secretaria de Dirección	1

Adicionalmente, se contará con los recursos humanos que componen las distintas unidades administrativas de la Universidad de Cádiz que dan apoyo directo a la gestión como pueden ser las Administraciones de Campus en los que el título se imparta, el personal de apoyo a la plataforma de enseñanza virtual (Campus Virtual de la UCA), la Oficina de Relaciones Internacionales, el área de atención al alumno, la Dirección General de Empleo, Becas, etc.

El personal de apoyo no está implicado directamente en la impartición de la docencia de las materias, sino que se ocupa de la gestión de los procesos de matrícula, tramitación de expedientes, servicio de biblioteca, etc. Se trata de personal propio de la Universidad de Cádiz, con vinculación estable, funcionarial o laboral, y con una amplia experiencia en la gestión de los procesos citados.

8. Recursos Materiales y Servicios.

a. Justificación de la adecuación de los medios materiales y servicios disponibles.

El edificio que ocupa la Escuela Superior de Ingeniería (ESI), dispone de unos 25.000 m2 construidos en una parcela de 60.000 m2, en el Campus Universitario de Puerto Real, que da cabida a una comunidad universitaria formada por más de 3.000 personas entre docentes, investigadores, estudiantes y personal de administración y servicios. Entre sus instalaciones, la ESI dispone de un aparcamiento con capacidad para 490 turismos y 64 motocicletas, y se han habilitado 100 plazas para bicicletas con la idea de reforzar el transporte sostenible.
El edificio está distribuido en tres plantas que cuenta entre otras dependencias con 24 aulas de docencia, 10 aulas de informática, 7 talleres para prácticas, 44 laboratorios, Sala de Juntas, Sala de Reuniones, 4 Salas de Videoconferencia, 18 Salas de Seminarios, Salón de Grados, Salón de Actos, Cafetería, Copistería, Biblioteca, etc.
Se cuenta con un aula exclusiva para el Máster con capacidad para cuarenta alumnos, equipada con proyector, mesa y ordenador de profesor. Las mesas de los alumnos son

configurables para el trabajo en grupo o individual y cuentan con conexión eléctrica y a internet.
Toda la información de las aulas, laboratorios y demás infraestructuras está disponible en la web de la ESI. (http://esingenieria.uca.es/centro/datos-del-centro/aulas/).

Cabe resaltar que en abril de 2016, los servicios de la Universidad de Cádiz fueron reconocidos con el Sello de Excelencia Europea 400+, siendo éste el máximo reconocimiento a la Excelencia en Gestión que se concede en Europa según el Modelo EFQM de Excelencia. Acredita la excelencia, la eficacia en la gestión, la eficiencia operativa y la diferenciación en su entorno competitivo de cualquier tipo de organización.
En esta misma línea, el Área de Deportes de la UCA alcanzó el Sello de Excelencia Europea 500+ en la gestión, siendo el único servicio en el ámbito deportivo de las universidades españolas que cuenta con este reconocimiento.

Biblioteca.
La Escuela Superior de Ingeniería dispone de una Biblioteca propia del Centro integrada en la red de Bibliotecas de la Universidad de Cádiz y del Campus de Puerto Real.
La Biblioteca de la ESI dispone de 5 espacios bien diferenciados:
Zona de estudio que cuenta con fondos bibliográficos específicos de ingeniería con mesas de estudio individual para 244 puestos + 4 puestos para discapacitados, disponen de conexión a internet a través de wifi y red de cable.
Zona de préstamo/circulación que dispone de banco de autopréstamo y con personal de biblioteca para ayuda al usuario. También está disponible el préstamo de portátiles.
Zona administrativa que cuenta con personal de biblioteca.
Espacio de aprendizaje que dispone de portátiles, con capacidad para 40 personas.
Salas de trabajo en grupo. Se dispone de 3 salas de trabajo en grupo con capacidad para 8 personas cada una.
Toda la información sobre la Biblioteca de la ESI y la Biblioteca del Campus de Puerto Real está disponible en los siguientes enlaces: (http://biblioptoreal.uca.es/) y en (http://biblioteca.uca.es/)
Cabe resaltar que el Servicio de Biblioteca y Archivo de la UCA cuenta con un Sello de Excelencia EFQM 500+, siendo un referente a nivel nacional, de lo que se benefician los alumnos del grado.
Campus virtual.
Debe señalarse que la Universidad de Cádiz, y especialmente la ESI, han sido pioneras en el uso de herramientas de Campus Virtual. En la actualidad, el Vicerrectorado de Recursos

Docentes y de la Comunicación mantiene el Campus Virtual de la UCA, en una plataforma informática que utiliza la aplicación de software libre Moodle. El Campus Virtual es una herramienta fundamental para el desarrollo de la docencia universitaria, por ello ha de ser modelado de acuerdo con las necesidades de los títulos y de los Centros con agilidad y flexibilidad. La dirección o vicerrectorado responsable del Campus Virtual tiene la misión de desarrollar el Campus Virtual integrando los servicios que le sean demandados por los títulos y Centros que conforman la Universidad. Para dar servicio seguro y robusto al campus virtual, se integra un conjunto de servidores y servicios que incorporan múltiples tecnologías. Dicha plataforma es utilizada por un porcentaje mayoritario de las asignaturas de las titulaciones que se imparten en los Centros de la Universidad de Cádiz. Además de permitir la disponibilidad de información en la red (apuntes, enlaces a la normativa de prevención de riesgos laborales, etc.), proporciona funcionalidades específicas para la enseñanza a distancia (multimedia, propuesta y resolución de cuestionarios en red, videoconferencia, mecanismos de accesibilidad mediante ficheros de audio, trabajo colaborativo en red, etc.). El acceso a la plataforma se encuentra protegido por una contraseña asociada a cada usuario de la comunidad universitaria (profesorado, alumnado o PAS).

Esta herramienta virtual es fácilmente accesible, al no requerir de la instalación de un software especial por parte del usuario. Sólo precisa de una conexión a internet y de un navegador, disponiendo en la red de una variada oferta de navegadores gratuitos (explorer, mozilla, safari, etc.).

Igualmente, las incidencias que pudieran producirse durante el desarrollo de la actividad académica son resueltas por la dirección o vicerrectorado responsable del Campus Virtual la Universidad de Cádiz a través de un Centro de Atención al Usuario específico y con un enlace disponible en la web del Campus Virtual para el acceso tanto *online* como telefónico. El mantenimiento depende del Área de Informática y el Centro Integrado de Tecnologías de la Información (CITI) de la Universidad de Cádiz.

Dicha plataforma es utilizada por las asignaturas del Master en Seguridad Informática (Ciberseguridad).

Acceso a internet.

Existen tres sub-redes wifi diferenciadas que dan servicio a todos los grupos de interés. La red ucAirPublica da servicio general a todos los estudiantes, la red ucAir está disponible para el PDI y PAS y la red Eduroam ofrece servicio para el uso de profesores visitantes. La cobertura de la red permite cubrir todas las zonas comunes (pasillos, cafetería, Departamentos, Dirección, Secretaría y Administración), así como los espacios docentes tales como aulas, laboratorios, salas de estudio y de trabajo.

Buzón de Atención al Usuario (BAU).

Las consultas, quejas y reclamaciones, comunicaciones de incidencias docentes, sugerencias y felicitaciones de los usuarios se canalizan a través del Buzón de atención al usuario BAU (http://bau.uca.es) quien las dirige, según su naturaleza, a los responsables que correspondan (centros y departamentos). Esta herramienta, en diciembre de 2009, fue galardonada con el Premio a las Mejores Prácticas del Banco de Experiencia de Telescopi Cátedra UNESCO de Dirección Universitaria.

El funcionamiento del BAU se encuentra regulado por la normativa aprobada por acuerdo del Consejo de Gobierno de 28 se septiembre de 2006 (https://buzon.uca.es/docs/NormativaReguladoraBAU.pdf).

Centro de Atención al Usuario (CAU).

Para garantizar la totalidad de servicios y recursos materiales necesarios para el normal funcionamiento de los títulos, la Universidad de Cádiz dispone del Centro de Atención al Usuario (CAU), disponible en https://cau.uca.es/cau/indiceGlobal.do. El CAU es el instrumento electrónico disponible para realizar las solicitudes de servicios y recursos de manera estructurada y sistemática y dispone de una relación detallada de los servicios ofertados organizados en función de las áreas responsables.

El CAU constituye así la ventanilla principal de los servicios de la UCA mediante la que se agiliza la tramitación de peticiones administrativas y de servicios, facilitando con ello al usuario (cualquier miembro de la comunidad universitaria) un sistema único para su resolución y seguimiento.

Los servicios y recursos relacionados con el funcionamiento del título que prestan sus servicios a través del CAU son: Administraciones y Secretarías de Campus, Atención al Alumnado, Servicio de Atención Psicológica y Psicopedagógica, Atención a Centros, Biblioteca y Archivo, Informática, Infraestructuras y Personal.

En el año 2014, la Cátedra Unesco de Dirección Universitaria en su segunda edición de los premios TELESCOPI otorgó el PREMIO A LA MEJOR BUENA PRÁCTICA DEL CRITERIO CLIENTES, al “Centro de Atención al Usuario de la UCA" (CAU).

Sistema Informático de Reserva de Recursos (SIRE).

La reserva de recursos docentes se gestiona a través de la plataforma informática SIRE (https://sire.uca.es). En ella constan todos los espacios disponibles, con indicación de su ocupación y con la posibilidad de solicitar la reserva de espacios que luego, es confirmada por el responsable de la plataforma SIRE en el Centro. Igualmente la reserva de espacios de trabajo puede realizarse a través de la web de Biblioteca, en la dirección anteriormente mencionada.

Otros.

Finalmente, se cuenta además con otros recursos y servicios como son: Delegación de alumnos, Servicio de copistería y Servicio de cafetería/comedor.

9. Resultados previstos.

a. Estimación de valores cuantitativos.

INDICADORES OBLIGATORIOS	VALOR
Tasa de graduación:	65%
Tasa de abandono:	10%
Tasa de eficiencia:	80%

OTROS POSIBLES INDICADORES		
Denominación	Definición	Valor
Tasa de rendimiento	Según P04 del SGC	75%
Tasa de éxito	Según P04 del SGC	80%
Tasa de evaluación	Según P04 del SGC	90%

b. Justificación de las tasas de graduación, eficiencia y abandono, así como el resto de los indicadores definidos.

Para el cálculo de las tasas de resultados propuestas, se han considerado los datos de las actuales titulaciones del área de Ingeniería de la Universidad de Cádiz que se imparten en la Escuela Superior de Ingeniería, así como las tasas de estudios nacionales de carácter similar al que aquí se presenta.

El modelo de docencia planteado, así como el tamaño de grupo reducido en clase, los mecanismos de evaluación continua permitirán conseguir los objetivos planteados. El plan de estudio ajusta su contenido al tiempo de trabajo real de los estudiantes, se han introducido sistemas de evaluación continua en todas las materias y en el último curso o semestre los planes limitan considerablemente la carga lectiva incluyendo el trabajo fin de máster.

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

La evaluación de competencias implica la coordinación de todos los profesores en metodología y criterios de evaluación. Por ello, la Universidad de Cádiz ha optado por un procedimiento general para todas sus titulaciones, integrado en su Sistema de Garantía de Calidad. Con ello se intenta facilitar la coordinación y la evaluación de los aprendizajes y, especialmente, el nivel que alcanzan los alumnos en las competencias generales. En cuanto a los sistemas de evaluación, se realizarán ejercicios escritos y u orales. La adquisición de destrezas y habilidades podría ser objeto de evaluación continua a través de diversas pruebas y actividades realizadas a lo largo del curso.

10. Sistema de Garantía de Calidad del Título.

http://sgc.uca.es

11. Calendario de implantación.

a. Cronograma de implantación del título.

CURSO DE INICIO:	2017-2018

b. Justificación del cronograma de implantación.

El Consejo de Gobierno de la Universidad de Cádiz, ha aprobado, por Acuerdo de 1 de Octubre de 2012, en relación con el Mapa de Másteres de la Universidad de Cádiz para el curso 2013/2014, la autorización para el inicio del proceso de elaboración de las Memorias de Máster o, en su caso, de modificación de las memorias previamente verificadas (publicado en BOUCA nº 150 de 24 de Octubre de 2 012, página 104).

c. Procedimiento de adaptación de los estudiantes de los estudios existentes al nuevo plan de estudios, en su caso.

No procede

d. Enseñanzas que se extinguen por la implantación del título propuesto.

Ninguna