Universidad
Carlos III de Madrid
www.uc3m.es

MEMORIA DE VERIFICACIÓN DEL MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD POR LA UNIVERSIDAD CARLOS III DE MADRID

Universidad Carlos III de Madrid
www.uc3m.es

1. DESCRIPCIÓN DEL TÍTULO

1.1 DATOS BÁSICOS

Denominación del Título

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD POR LA UNIVERSIDAD CARLOS III DE MADRID

- **Especialidad**: No hay especialidades

Rama de conocimiento Ingeniería y Arquitectura

Clasificación ISCED 2011

- ISCED 1: Ingeniería y profesiones afines
- ISCED 2: Ciencias de la computación

Habilita para profesión regulada: No

Títulos conjuntos con otras Universidades: No

1.2 DISTRIBUCIÓN DE CRÉDITOS EN EL TÍTULO

Número de créditos del Título

TIPO DE MATERIA	CRÉDITOS
Obligatorias	36
Optativas	12
Prácticas Externas*	0
Trabajo Fin de Máster	12
Créditos Totales	60

1.3 DATOS ASOCIADOS AL CENTRO

Centro en que se imparte

Centro de Postgrado

Tipo de Enseñanza

Presencial

Número de plazas de nuevo ingreso ofertadas

Primer año de implantación: 60 | Segundo año de implantación: 60

Número de créditos de matrícula por estudiante y período lectivo

Matrícula a tiempo completo

	Nº mínimo	Nº máximo
Primer curso	60	60
Resto de cursos	31	60

Matrícula a tiempo parcial

	Nº mínimo	Nº máximo
Primer curso	30	30
Resto de cursos	18	30

Normativa de permanencia

http://www.uc3m.es/portal/page/portal/postgrado_mast_doct/normativa/normativa_permanencia.pdf

Lenguas utilizadas a lo largo del proceso formativo

El programa es bilingüe español e inglés.

2. JUSTIFICACIÓN

2.1 Justificación del Título propuesto, argumentando el interés académico, científico o profesional del mismo

El mercado de la ciberseguridad va a ser un sector en auge. Según los datos de mercado mundial de Visiongain, se prevén unos ingresos 68.340 millones de dólares en 2013 [1].

Anteriormente, 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: "*Despite continued economic pressures, organizations are spending more to address information security challenges, including those related to delivering security in a borderless environment. 46% of respondents indicated that their annual investment in information security is increasing, with only 6% planning to reduce their information security investment. Further investigation found that 55% of respondents are increasing the level of information security investment related to their top five areas of IT risk*." [3]

En nuestro país, la preocupación creciente por la privacidad, la reciente 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 demanda creciente de profesionales en ciberseguridad.

Por si ello fuera poco, el incremento de los ciberataques se reflejó ya en la Estrategia Española de Seguridad de 2011, que considera a los mismos: "una amenaza actual, real y en crecimiento para los intereses nacionales", haciendo hincapié en la necesidad de garantizar el uso seguro del ciberespacio. En este sentido, el Ministerio de Defensa acaba de crear el Mando Conjunto de Ciberdefensa de las FF AA [5].

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.

Respecto a los grados de referencia en los perfiles de acceso previsto, barajamos los proporcionados por la Comunidad de Madrid en sus últimos informes de egresados universitarios y su inserción laboral en 2006-2007 y 2008-2011. Los datos son:

Titulación	Egresados 2006/07	Egresados 2008/11
I. T de telecomunicación, especialización sistemas de telecomunicación.	245	86
I. T de telecomunicación, especialización en sistemas electrónicos	149	68
I. T de telecomunicación, especialización en sonido e imagen	131	68
I. T de telecomunicación, especialización en telemática	183	108
I.T. en informática de gestión	810	274
I.T. en informática de sistemas	534	297
Ingeniería de telecomunicación	685	619
Ingeniería en informática	1.021	722
Total	3.758	2.242

Por supuesto, esta previsión es muy conservadora, esperando atraer alumnos de fuera de la Comunidad de Madrid, dado que este título propone un enfoque de estudios muy novedoso en cuanto a la seguridad. Además, esperamos poder ofrecer becas de estudio mediante el patrocinio de empresas, y 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: http://www.visiongain.com/Report/951/Global-Cyber-Security-Market-2013-2023. 13 Diciembre 2012.

[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 crítica.

[5]. Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas

[6]. http://www.idg.es/cio/estructura/imprimir.asp?id=193751&cat=art

[7]. http://www.comptia.org/home.aspx

2.1.1. Orientación del Título

Académica	X	Investigación		Profesional	

Justificar la orientación del título

El objetivo del máster es formar profesionales integrales en el ámbito de la seguridad. Para ello se aplicará una metodología didáctica basada en clases presenciales, seminarios especializados, estudio de casos prácticos, sesiones prácticas en laboratorio, tutorías, estudio y auto-aprendizaje, etc. El programa propuesto intenta cubrir los principales aspectos de la ciberseguridad, haciendo especial hincapié en aspectos técnicos.

- **Enseñanzas que se imparten en varias modalidades (presencial, semipresencial o a distancia).**
  Presencial

- ***Títulos que habilitan para el ejercicio de una actividad profesional regulada**
  No procede

- ***Especialidades**
  No procede

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

Dado el interés de la seguridad en las tecnologías de la información y las comunicaciones, en la Comunidad de Madrid ya se imparten varios títulos de posgrado relacionados con la seguridad de la información, aunque la mayoría de ellos 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 mucho más técnica y centrada en los retos actuales, contemplando de manera especial los ataques provenientes de la red: la ciberseguridad. En la Comunidad de Madrid, solo se imparten dos másteres reconocidos por la ANECA y ambos en universidades privadas: la Universidad Alfonso X El Sabio y la Universidad Europea de Madrid. El plan de estudios de ambos másteres no ofrece optatividad y tiene una carga de gestión de la seguridad igual o superior al 50%. El resto de la oferta son títulos propios.

Títulos oficiales:

- Universidad Europea de Madrid (UEM) - Máster Universitario en Seguridad de Tecnologías de la Información y Comunicaciones [http://madrid.universidadeuropea.es/estudios-

universitarios/master-universitario-en-seguridad-de-tecnologias-de-la-informacion-y-de-las-comunicaciones] (60 ECTS). Ofrece dos itinerarios, uno de investigación y otro de práctica profesional.

- Universidad Alfonso X El Sabio (UAX) - Máster Universitario en Seguridad de Tecnologías de la Información y Comunicaciones [http://www.uax.es/que-estudiar/postgrado/masteres/ingenieria/master-universitario-en-ingenieria-de-seguridad-de-la-informacion-y-las-comunicaciones/plan-de-estudios.html]

Otros títulos:

- Universidad Politécnica de Madrid (UPM) - Máster en Dirección y Gestión de Seguridad de la Información [http://www.master.etsit.upm.es/masterDGSI] (60 ECTS)
- Universidad Autónoma de Madrid (UAM) - Máster en Auditoría, Seguridad, Gobierno y Derecho de las TIC [http://www.uam.es/ss/Satellite/EscuelaPolitecnica/es/estudios/ensenanzas-propias-de-la-uam/programa-de-titulos-propios/Page/subhome/master-en-auditoria,-seguridad,--gobierno-y-derecho-de-las-tic.htm] (60 ECTS)
- Asociación de Ingenieros e Ingenieros Técnicos en Informática (ALI):
  - Máster en Auditoría Informática [http://masters.ali.es/?p=177]
  - Máster en Seguridad Informática [http://masters.ali.es/?p=181]

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. Los centros y programas son:

- Dakota StateUniversity, South Dakota [http://www.dsu.edu/majors-programs/computer-network-security.aspx];
- Naval PostgraduateSchool, California [http://www.cisr.us/sfscourses.STEM.html];
- Northeastern University, Massachusetts [http://www.ccs.neu.edu/graduate/degree-programs/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 el M.Sc. in ComputerScience and Forensics de la Universidad de Bedfordshire [http://www.beds.ac.uk/howtoapply/courses/postgraduate/current-year/computer-security-and-

forensics] o el M.Sc. in Security and Forensic Computing de la Ciudad de Dublín [http://www.dcu.ie/prospective/deginfo.php?classname=MSSF].

2.2 Descripción de los procedimientos de consulta internos y externos utilizados para la elaboración del plan de estudios

El procedimiento de aprobación de másteres oficiales de la Universidad Carlos III de Madrid está aprobado en la sesión de su C. de Gobierno de 26 de febrero de 2009 y es el seguido en el máster propuesto, tal y como se indica en los apartados que siguen

-Procedimientos de consulta internos

1. Los departamentos proponentes elaboraron una propuesta de máster, incluyendo un informe ejecutivo preliminar constituido por los siguientes apartados:

JUSTIFICACIÓN DEL TÍTULO
- Justificación de la existencia de una demanda potencial de estudiantes no cubierta adecuadamente por otras Universidades de nuestro entorno educativo
- Interés académico, científico o profesional del título
- Referentes nacionales e internacionales
- Complementariedad de los estudios propuestos con la oferta actual, evitando la competencia con estudios ya implantados
- Contribución a la internacionalización de la Universidad

OBJETIVOS
- Objetivos generales
- Competencias: Generales, específicas, profesionales, transversales y nucleares

CONTRIBUCIÓN A LA MEJORA O EL REFUERZO DE LAS CAPACIDADES INVESTIGADORAS O ARTÍSTICAS DE LAS ÁREAS DE LA UNIVERSIDAD

2. La propuesta fue elevada al Vicerrector de Posgrado para su traslado al Rector. Éste, asistido por el Comité de dirección y con asesoramiento externo aprobó dicha propuesta e informe incorporando todo ello al Orden del Día de la sesión del C de Gobierno celebrado el 4 de julio de 2013.

3. El Consejo de Gobierno en la sesión indicada estudió la propuesta, e informe ejecutivo así como la propuesta de composición de la Comisión de elaboración del plan de estudios y su calendario de trabajo (ambos detallados en el apartado siguiente).

4. Una vez concluido el plan de estudios y la memoria de verificación del mismo por la Comisión arriba citada, el Vicerrector de Postgrado lo sometió a información pública de la comunidad universitaria por un plazo de un mes.

5. Finalizado el periodo de información pública, el plan de estudios fue aprobado por el Consejo de Gobierno de la Universidad a propuesta del Rector.

-Procedimientos de consulta externos

Como ya se ha indicado la elaboración del Plan de estudios correspondió a una Comisión nombrada por el C de Gobierno y constituida por tres representantes de cada uno de los Departamentos proponentes y seis representantes de empresas y organismos relacionadas con la seguridad de las TIC. Estas empresas fueron: el Banco de Santander (como empresa “consumidora” de seguridad), Indra (como empresa “fabricante” de seguridad), Deloitte (como consultora de seguridad), la Dirección General de Modernización Administrativa del Ministerio de Hacienda y Administraciones Públicas (como representante de las AA PP), el Centro de Estudios Superiores de la Defensa (por la relevancia creciente de la ciberdefensa) y el Cuerpo de la Guardia Civil (dada la importancia creciente de los delitos informáticos).

Concretamente, la composición nominal de la Comisión fue la siguiente:

Coordinador

D. Arturo Ribagorda Garnacho

Catedrático de Universidad. Departamento de Informática

Secretario.

D. Andrés Marín López

Profesor Titular de Universidad. Departamento de Ingeniería Telemática

Vocales.

D. Raúl Sánchez Reillo

Profesor Titular de Universidad. Departamento de Tecnología Electrónica

D. Óscar de la Cruz

Comandante. Jefe de la Unidad de Delitos Telemáticos. Cuerpo de la Guardia Civil

D. Juan Salom

Tte. Coronel. Servicio de Innovación Tecnológica y Seguridad Informática. Cuerpo de la Guardia Civil

D. Miguel Ángel Amutio

Cuerpo Superior de Sistemas y Tecnologías de la Información. Secretaría de Estado de AA PP. Ministerio de Hacienda y Administraciones Públicas.

Dr. Jorge López Hernández-Ardieta

Doctor en Informática. Full-Time Senior Engineer in the Cybersecurity Unit. INDRA.

Rubén Frieiro Barro.

Senior Manager del departamento de IT ERS. DELOITTE

Ángel Redondo Fernández-Rebollos

Responsable de Arquitectura Técnica de Seguridad. Grupo Banco Santander

José Tomás Hidalgo Tarrera

Coronel. Profesor de la Escuela de Altos Estudios de la Defensa. Centro Superior de Estudios de la Defensa Nacional (CESEDEN)

2.3 Diferenciación de títulos dentro de la misma Universidad

El Máster ofrece unos estudios muy diferentes a los actualmente ofertados en la Universidad. Aunque los departamentos que impartirán el Máster: Ingeniería Informática, Ingeniería Telemática y

Tecnología Electrónica participan en la impartición de diversos másteres académicos (Máster de Ingeniería Informática, Máster de Ingeniería de Telecomunicación, Máster de Ingeniería Industrial), ninguno de ellos versa sobre las materias del presente Título, ni ofrece unas competencias como las que requiere la ciberseguridad. Tampoco se oferta nada similar en los títulos de carácter de investigación, profesionales, ni títulos propios de la Universidad Carlos III de Madrid.

- **Diferencias en el perfil de los distintos egresados y divergencias en los contenidos y en su profundización y tratamiento entre uno y otro.**

La dependencia de nuestra sociedad de las redes, especialmente Internet, y sistemas de información ha derivado en la aparición de nuevas amenazas de creciente impacto potencial. El presente Máster académico en Ciberseguridad es una propuesta nueva de estudios académicos al objeto de proporcionar a la sociedad egresados con los conocimientos y habilidades requeridos para ayudar a nuestras instituciones y empresas a contrarrestar tales amenazas. El Máster tiene un marcado carácter técnico y práctico, a diferencia de otros títulos existentes muy orientados a la gestión de la seguridad.
Durante la elaboración del plan de estudios, el Comité creado al efecto (apartado 2.2 de la presente memoria) propuso ofrecer dos perfiles de egresados distintos: **ingeniero de sistemas seguros**, y **analista de ciberseguridad**.
El primer perfil, ingeniero de sistemas seguros, se orienta al diseño y desarrollo de componentes y sistemas donde la seguridad es un elemento crucial. Su principal nicho de mercado se encuentra en empresas productoras de seguridad, fundamentalmente en los departamentos de creación de software (*software factory*) y de diseño de arquitecturas. Este perfil tiene que conocer de manera profusa las consideraciones de seguridad de las amenazas en red y sus implicaciones en el ciclo de vida de la Ingeniería de Sistemas (incluyendo la Ingeniería del Software) en todas sus vertientes, para trasladarlas a nuevos productos, así como las interioridades de los mecanismos de defensa para poder colaborar en el desarrollo de otros nuevos y su evolución constante en la carrera por la seguridad.
El segundo perfil, analista de ciberseguridad, se orienta a las organizaciones que necesitan protegerse de las ciberamenazas, y requieren de personal que sepa identificar ataques y potenciales debilidades en sus sistemas y redes, y sea capaz de proponer el uso y despliegue de medidas y contramedidas para asegurarlos. Se podría informalmente decir que este segundo perfil es más "probador", al apoyarse en productos de ataque y defensa que, a través de pruebas y auditorías, le ayudan a mantener los riesgos de seguridad controlados y a actuar frente a ataques. Este segundo perfil encuentra cabida en un número creciente de empresas, cada vez más dependientes de sus sistemas de información e Internet y de forma específica en sectores críticos, empresariales (como la banca, la energía o el transporte) o públicos (ciertos organismos, las FF AA o las fuerzas y Cuerpos de la Seguridad del Estado).

Ambos perfiles tienen en común asignaturas en ciberdefensa y ciberataque, que representan un porcentaje significativo de créditos obligatorios, la diferenciación se establece en base a la optatividad, que se orienta más al "hecho" creativo en el caso del primer perfil, o a la aplicación de herramientas y estudio analítico de resultados y de casos prácticos, más propio del segundo perfil.
También ambos requieren la soltura en el manejo de un conjunto común de herramientas y conocimientos, que se desarrollan en la parte obligatoria del Máster y que son comunes para el ciberataque y la ciberdefensa. La diferencia radica en el cuándo, y con qué propósito, más que en el cómo se usan estas herramientas y conocimientos comunes.

Desde el punto de vista operativo, los perfiles se ofrecen a través de dos configuraciones concretas de las asignaturas optativas que se ofertan en las materias del Máster. De esta forma los alumnos pueden optar por seguir cualquiera de los dos itinerarios, o por la configuración que elijan.

3. COMPETENCIAS

3.1 Competencias

Competencias Básicas

Competencias Básicas	
CB6	Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7	Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8	Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9	Que los estudiantes sepan comunicar sus conclusiones –y los conocimientos y razones últimas que las sustentan– a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10	Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo

Competencias Generales

Competencias Generales	
CG1	Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica.
CG2	Concebir, diseñar, poner en práctica y mantener un sistema global de Ciberdefensa 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	Desarrollar, implantar y mantener un Sistema de Gestión de la Seguridad de la Información (ISMS).

Competencias Específicas

Competencias Específicas	
CE1	Analizar y detectar anomalías y firmas de ataques en los sistemas y redes.
CE2	Analizar y detectar técnicas de ocultación de ataques a sistemas y redes.
CE3	Conocer las tendencias actuales en técnicas de ciberataque y las experiencias aprendidas en casos reales.
CE4	Analizar sistemas para encontrar evidencias de ataques en los mismos y adoptar las medidas precisas para mantener la cadena de custodia de dichas evidencias.
CE5	Aplicar los servicios, mecanismos y protocolos de seguridad oportunos en un caso concreto.
CE6	Diseñar y evaluar arquitecturas de seguridad de sistemas y redes.
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	Analizar los riesgos de la introducción de dispositivos personales en un entorno profesional. Conocer y aplicar las medidas para controlar dichos riesgos.
CE9	Capacidad para aplicar las metodologías existentes al análisis de riesgos, transmitir los resultados y proponer las medidas para disminuir los riesgos de acuerdo con el caso concreto de la organización, partiendo del inventario de activos de una organización

4. ACCESO Y ADMISIÓN DE ESTUDIANTES

4.1 Sistemas de información previa a la Matriculación.

Cada máster dispone de un espacio web con información específica sobre el programa: el perfil de ingreso, los requisitos de admisión, el plan de estudios, los objetivos, y otras informaciones especialmente orientadas a las necesidades de los futuros estudiantes, incluidos los procesos de admisión y matriculación. Las páginas web de la Universidad Carlos III funcionan bajo el gestor de contenidos "oracle portal", lo que permite una fácil modificación, evita enlaces perdidos y ofrece un entorno uniforme en todas las páginas al nivel doble A de acuerdo con las Pautas de Accesibilidad de Contenidos Web, publicadas en mayo de 1999 por el grupo de trabajo WAI, perteneciente al W3C (World Wide Web Consortium). Esta información se puede encontrar en la siguiente dirección:

http://www.uc3m.es/portal/page/portal/postgrado_mast_doct/Estudios_Oficiales_de_Postgrado/Programas_de_Master_Oficial

La Universidad participa en diversas ferias educativas dentro y fuera de España, de acuerdo con las directrices del Vicerrectorado de Estudiantes y Vida Universitaria y del Vicerrectorado de Relaciones Internacionales y realiza diferentes campañas de difusión de sus estudios en los medios de comunicación y redes sociales. En estas acciones colaboran los servicios universitarios Espacio Estudiantes, Relaciones Internacionales, Servicio de Comunicación y del Servicio de Postgrado.

Existe un servicio general de información y atención a futuros estudiantes de grado y postgrado por teléfono y a través de vía correo electrónico.

http://www.uc3m.es/portal/page/portal/inicio/Informate

Además los estudiantes pueden dirigirse a las oficinas de información y atención a estudiantes de postgrado en todos los campus con horario continuado de 9:00 a 18:00 horas.

Todos estos servicios facilitan una información de primer nivel, canalizando las demandas de información especializada, orientación y asesoramiento a la unidad correspondiente: dirección del programa o unidades administrativas de apoyo.

Sistemas de información específicos para los estudiantes con discapacidad que acceden a la universidad.

Los estudiantes con discapacidad reciben atención específica a sus necesidades especiales a través del Programa de Integración de Estudiantes con Discapacidad (PIED) que gestiona el Espacio Estudiantes bajo el impulso del Vicerrectorado de Estudiantes y Vida Universitaria.

Asimismo, estos pueden recibir la atención personal bien de manera presencial, bien por teléfono o correo electrónico. La dirección de este último es: integracion@uc3m.es

La Universidad dispone de información detallada sobre sus recursos y servicios para estudiantes con discapacidad, así como otra de interés para este alumnado (noticias, enlaces, etc.) en las siguientes direcciones de su página web:

http://www.uc3m.es/portal/page/portal/orientacion_personal_participacion/PIED1

o http://www.uc3m.es/portal/page/portal/cultura_y_deporte

4.2 Requisitos de acceso y criterios de admisión

Este Máster está orientado a Ingenieros, Ingenieros Técnicos y Graduados relacionados con las Tecnologías de la Información y las Comunicaciones (TIC), además de profesionales que ya estén trabajando en el ámbito de las TIC y que deseen especializarse en temas de seguridad. En ese caso se ofrecerán asignaturas de nivelación para proporcionar los conocimientos tecnológicos básicos necesarios.

Requisitos de acceso

El establecido por el Real Decreto 1393/2007, modificado por el Real Decreto 861/2010

Estar en posesión de un título de Ingeniero o Graduado en Ingeniería en Informática, Telecomunicación, en cualquiera de sus especialidades, o de título similar relacionado con las TIC. En caso de un título de Ingeniero o Licenciado ajeno, se deberá acreditar experiencia profesional en el campo de las TIC.

Los solicitantes con titulaciones cuyas competencias sean diferentes a las anteriores serán evaluados por el Comité del Máster basándose en las materias cursadas y las evidencias de capacidades y aprovechamiento.

Perfil de Ingreso

El alumno que quiera cursar este Máster debe tener una buena base de informática y telemática. El carácter práctico del Máster requiere experiencia en programación y redes para poder seguir las clases prácticas y ejercicios. El interés por la seguridad en sistemas informáticos en red es igualmente interesante, así como la creatividad, la capacidad de innovación, el pensamiento crítico y el interés por el aprendizaje continuo.

Criterios de admisión

Los criterios de admisión serán aplicados por el Comité de dirección que se describe en el punto de este documento.

- Expediente académico de los estudios de acceso 5 puntos
- Nivel de conocimiento de inglés 1 punto
- Motivación, interés, cartas de recomendación 0.5 puntos
- Otros 3.5 puntos
    - Experiencia profesional 1-2.5
    - Calificaciones obtenidas en materias esenciales para cursar el máster 1-2.5

El proceso de admisión comenzará con el envío de la solicitud de admisión por parte del alumno a través de la plataforma on line de la Universidad Carlos III de Madrid, en las fechas y periodos aprobados y publicados para cada curso académico.

Recibida la solicitud, el personal administrativo revisará la misma a los efectos de verificar el correcto envío de la documentación necesaria, que estará publicada en la página web de la titulación, contactando con el alumno en caso de necesidad de subsanación de algún documento, o validando la candidatura en caso de estar completa.

La solicitud de admisión validada, pasará a la dirección del Máster que valorará la candidatura en base a los criterios y ponderaciones descritos, comunicando al alumno su admisión al Máster, la denegación de admisión motivada o la inclusión en una lista de espera provisional.

Toda la información sobre el proceso de admisión, guías de apoyo y accesos a las aplicaciones on line, se encuentran publicadas en la siguiente url:

http://www.uc3m.es/portal/page/portal/postgrado_mast_doct/Admision/Masteres_Universitarios

4.3 Apoyo y orientación a estudiantes una vez matriculados

La Universidad Carlos III realiza un acto de bienvenida dirigido a los estudiantes de nuevo ingreso en los másteres universitarios en el que se lleva a cabo una presentación de la Universidad y de los estudios de postgrado, así como guiadas por los campus universitarios.

Los Directores Académicos de los másteres con el apoyo del personal del Centro de Postgrado, realizan diversas acciones informativas específicas para cada programa sobre las características de los mismos por una parte, y por otro lado sobre los servicios de apoyo directo a la docencia (bibliotecas, aulas informáticas, etc.) y el resto de servicios que la universidad pone a disposición de los estudiantes: deporte, cultura, alojamientos, etc. Estas acciones informativas permiten a los nuevos estudiantes conocer los servicios generales del campus y del Campus Virtual (Campus Global), así como dar una guía práctica y específica del Máster Académico. En el caso del Máster de Ciberseguridad se utiliza para explicar la dinámica del Máster y orientar sobre los perfiles y la oferta de asignaturas optativas.

La universidad cuenta además con los siguientes servicios específicos de apoyo y orientación a los estudiantes:

Orientación psicopedagógica - asesoría de técnicas de estudio: existe un servicio de atención personalizada al estudiante con el objetivo de optimizar sus hábitos y técnicas de estudio y por tanto su rendimiento académico.

Programa de mejora personal: cursos de formación y talleres en grupo sobre diferentes temáticas psicosociales. Su objetivo es el de contribuir a la mejora y al desarrollo personal del individuo, incrementando sus potencialidades y en última instancia, su grado de bienestar. El abanico de cursos incluye los siguientes: “Psicología y desarrollo personal”, “ Argumentar, debatir y convencer”, “Educación, aprendizaje y modificación de conducta”, “Creatividad y solución de problemas”, “Técnicas de autoayuda”, “Taller de autoestima”, “Habilidades sociales”, “Entrenamiento en relajación”, “Trabajo en equipo”, “Gestión del tiempo”, “Comunicación eficaz”, “Hablar en público” y “Técnicas para superar el miedo y la ansiedad”.

Orientación psicológica - terapia individual: tratamiento clínico de los diferentes problemas y trastornos psicológicos (principalmente trastornos del estado de ánimo, ansiedad, pequeñas obsesiones, afrontamiento de pérdidas, falta de habilidades sociales, problemas de relación, etc.).

Prevención psico-educativa: este programa tiene por objetivo el desarrollo y difusión de materiales informativos (folletos y Web) con carácter preventivo y educativo (por ejemplo: ansiedad al hablar

en público, consejos para el estudio, gestión del tiempo, depresión, estrés, relación de pareja, superación de las rupturas, trastornos de la alimentación, consumo y abuso de sustancias, mejora de la autoestima, sexualidad, etc.). Se pretende así facilitar la detección precoz de los trastornos, prevenirlos, acercar la psicología a la comunidad universitaria y motivar la petición de ayuda.

Una vez matriculados, los estudiantes obtienen su cuenta de correo electrónico y pueden acceder a la Secretaría virtual de estudiantes de postgrado con información académica específica sobre diferentes trámites y procesos académicos, así como información personalizada sobre horarios, calificaciones, situación de la beca, etc.

Oficinas de Postgrado: a través de los servicios del Centro de Postgrado, se atienden las necesidades de los estudiantes, de modo telefónico, por correo electrónico info.postgrado@uc3m.es o presencialmente en las Oficinas de Postgrado de los Campus. Además resuelven los trámites administrativos relacionados con su vida académica (matrícula, becas, certificados, se informa y orienta sobre todos los procesos relacionados con los estudios del Máster (como horarios, becas, calendario de exámenes, etc.)

Los estudiantes tienen acceso al portal virtual de apoyo a la docencia para las asignaturas matriculadas: programas, materiales docentes, contacto con los profesores, entre otros.
De igual manera, estos tienen acceso a un servicio de tutoría proporcionado por los profesores que imparten cada una de las asignaturas. A este respecto cabe subrayar que los profesores deben publicar en la herramienta virtual de soporte a la docencia los horarios semanales de atención a los estudiantes.

Finalmente, es preciso mencionar que a través de la Fundación UC3M (Servicio de Orientación y Planificación Profesional) se ofrecen diferentes servicios de orientación y se realizan acciones encaminadas a la inserción laboral y profesional de los estudiantes.

Apoyo y orientación específicos para los estudiantes con discapacidad que acceden a la universidad.

Sistemas de acogida

Comunicación mediante correo electrónico con todos los estudiantes matriculados con exención de tasas por discapacidad: información y oferta de los servicios PIED. Envío periódico (correo electrónico) de informaciones específicas de interés: convocatorias, becas, actividades, etc.

Reunión informativa en cada Campus.

Entrevista personal: información de recursos y servicios y valoración de necesidades (elaboración de plan personalizado de apoyo)

Sistemas de apoyo y orientación

Existe un plan personalizado de apoyo para la atención a las necesidades especiales del estudiante, cuya coordinación implica a los responsables académicos, los docentes y los servicios universitarios. Los apoyos específicos y adaptaciones más comunes que se realizan son:

Asesoramiento para la realización de matrícula: lo que incluye un cupo de reserva, prioridad en asignaturas optativas, orientación para la selección y organización de asignaturas, entre otros.

Adaptaciones curriculares: necesidades específicas en el proceso de aprendizaje (relación y comunicación profesor-alumno, acceso a apuntes o materiales didácticos, participación en las

clases, etc.), necesidades específicas en trabajos y pruebas de conocimiento, adaptaciones en el programa y actividades de las asignaturas, son algunos de ellos.

Apoyo al estudio: éste incluye proveer al alumno con un profesor-tutor, proporcionarle apoyo humano (toma de apuntes, desplazamientos...), adaptación de materiales de estudio, préstamo de ayudas técnicas, recursos informáticos específicos, servicios especiales en Bibliotecas (atención personalizada, ampliación plazos de préstamo...), ayudas económicas, etc.

Accesibilidad-adaptaciones en aulas y Campus: adaptaciones de mobiliario, reserva de sitio en aulas de características especiales, reserva de taquillas, plazas de aparcamiento, o habitaciones adaptadas en Residencias de Estudiantes.

Por último, cabe destacar las adaptaciones para la participación en actividades socioculturales y deportivas.

4.4 Sistemas de Transferencia y reconocimiento de créditos

La Universidad Carlos III de Madrid ha implantado los procedimientos de transferencia y reconocimiento de créditos adaptados a lo dispuesto en el Real Decreto 1393/2007. Nótese que este puede ser consultado en la siguiente dirección:

http://www.uc3m.es/portal/page/portal/organizacion/secret_general/normativa/estudiantes/estudios_grado/reconocimientoyconvalidacion.pdf

PROCEDIMIENTO DE RECONOCIMIENTO DE CRÉDITOS

El alumno deberá cumplir el siguiente procedimiento para que recibir el reconocimiento de créditos:

a. El estudiante debe solicitar el reconocimiento de créditos acompañando la documentación acreditativa de las asignaturas superadas y los programas oficiales de las mismas. En el supuesto de que solicitara el reconocimiento de determinada experiencia profesional en los términos previstos en la normativa aplicable, deberá presentar un certificado de las entidades en las que hubiera realizado su actividad profesional en el que se especifiquen de las actividades laborales desarrolladas con indicación de la fecha de inicio y finalización de las mismas.

b. Una resolución motivada del Director del Máster que evaluará la adecuación entre las competencias y conocimientos asociados a las materias superadas en estudios oficiales de postgrado, los adquiridos en las actividades laborales o profesionales desarrolladas por el solicitante o en asignaturas superadas en estudios no oficiales, y los previstos en el plan de estudios El Director del Máster podrá recabar el asesoramiento de la Comisión Académica del Máster o del Departamento que tenga asignada la docencia de la asignatura cuyo reconocimiento se solicita.

c. La incorporación de la asignatura reconocida al expediente del estudiante con la calificación obtenida en el Centro de procedencia salvo que se trate de asignaturas superadas en másteres no oficiales o de experiencia profesional, para las que no se incorporará calificación alguna figurando en el expediente como reconocidas.

No se permite la incorporación de reconocimientos de créditos superiores a 9 créditos ECTS por actividades profesionales y por asignaturas superadas en másteres no oficiales.

PROCEDIMIENTO DE TRANSFERENCIA DE CRÉDITOS

Los créditos cursados en enseñanzas que no hayan conducido a la obtención de un título oficial se trasferirán al expediente académico del alumno, que deberá solicitarlo adjuntando el correspondiente certificado académico y documento en el que se acredite que no ha finalizado los estudios cuya transferencia solicita.

Dichos créditos se transfieren al expediente académico previa resolución de la Dirección del programa.

Sistema de transferencia y reconocimiento de créditos		
Concepto	**Mínimo**	**Máximo**
Reconocimiento de créditos cursados en enseñanzas superiores oficiales no universitarias	0	0
Reconocimiento de créditos cursados en títulos propios	0	15%
Reconocimiento de créditos cursados por acreditación de experiencia laboral y profesional	0	15%

4.5 Complementos formativos para el máster

5. PLANIFICACIÓN DE LAS ENSEÑANZAS

5.1 Descripción general del plan de estudios.

a) Descripción general del plan de estudios

El programa de estudios de este Máster pretende que los alumnos adquieran conocimientos científicos y tecnológicos avanzados sobre la Ciberseguridad. Para ello, se les formará en un conjunto de principios teóricos, métodos formales e instrumentos tecnológicos que les capaciten para llevar a cabo trabajos de investigación, desarrollo e innovación en esta área. Por tanto, el principal objetivo de este Máster es proporcionar habilidades, aptitudes y conocimientos en aspectos avanzados de la Ciberseguridad, de manera sólida pero flexible para facilitar su adaptación a un entorno tan rápidamente cambiante como este.

El programa de estudios se estructura alrededor de tres grandes **bloques**:

- **Técnicas de Ciberataque:** Las asignaturas comprendidas en esta área cubren en detalle las amenazas a las que los sistemas de ciberdefensa deben hacer frente, incluyendo las técnicas actuales de penetración de redes y explotación maliciosa de sistemas el análisis e ingeniería de malware, las técnicas que permiten la fuga de información y las perspectivas actuales en ciberdelitos, ciberterrorismo y ciberguerra.

- **Técnicas de Ciberdefensa y Comunicaciones Seguras:** Esta área agrupa los conocimientos y tecnologías relacionados con los sistemas de ciberdefensa, la criptografía aplicada y su uso en protocolos y esquemas que garanticen la seguridad de las comunicaciones. Las distintas materias abarcan la protección de datos y comunicaciones, las técnicas de identificación y autenticación de usuarios y sistemas, los sistemas de ciberdefensa, el análisis forense de equipos informáticos, la seguridad en sistemas y comunicaciones móviles, y la ingeniería y desarrollo de sistemas seguros.

- **Gestión de la Ciberseguridad:** Las asignaturas en esta área comprenden los aspectos de gestión y administración de la Ciberseguridad, incluyendo el ciclo de vida y los procedimientos operativos de los centros de ciberdefensa, la creación de planes de seguridad de continuidad y de formación y concienciación del personal, las metodologías de análisis y gestión de riesgos, los procesos de normalización y certificación de productos y sistemas, y el marco legal y regulador de la ciberseguridad.

Respecto de la organización temporal, el máster se imparte en un curso académico, teniendo el primer cuatrimestre una carga asociada de 30 créditos ECTS, mientras que en el segundo es de 18 créditos ECTS. El Trabajo Fin de Máster, de 12 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 cuatrimestre, de ahí la asimetría en ambos cuatrimestres.

En términos del carácter de las asignaturas, la distribución de asignaturas por cuatrimestre es también asimétrica:

El primer cuatrimestre está compuesto mayoritariamente por materias obligatorias (24 créditos ECTS de asignaturas obligatorias más otros 3 ECTS de seminarios). Adicionalmente, el alumno dispone de 3 créditos ECTS optativos para elegir una asignatura entre las dos siguientes:

- “Ciberdelitos, Ciberterrorismo y Ciberguerra”
- “Análisis de Riesgos en Ciberseguridad”

Por su parte, el segundo cuatrimestre contiene 6 créditos ECTS de asignaturas obligatorias y otros 3 ECTS de seminarios. Los restantes 9 créditos se distribuyen entre tres asignaturas optativas que el alumno debe elegir entre las seis ofertadas para este cuatrimestre. Estas asignaturas se han agrupado en dos perfiles o itinerarios formativos con objeto de proporcionar al alumno, si así lo desea, un nivel adicional de especialización de acuerdo con sus preferencias. Los itinerarios contemplados son:

Itinerario "Ingeniería de Sistemas Seguros" (I1): Este itinerario está destinado a alumnos que quieran mejorar su formación en aspectos relacionados con la especificación, diseño y desarrollo, implantación y mantenimiento de sistemas seguros. Las asignaturas optativas asociadas son:

- "Ingeniería de Sistemas Seguros"
- "Arquitecturas Seguras"
- "Seguridad en Sistemas y Comunicaciones Móviles"

Itinerario "Analista de Ciberseguridad" (I2): Este itinerario está destinado a alumnos que deseen una formación adicional como analista de seguridad de sistemas. Las asignaturas optativas asociadas son:

- "Análisis e Ingeniería de Malware"
- "Amenazas persistentes y Fugas de Información"
- "Análisis Forense de Sistemas Informáticos"

CUADRO 1

ORGANIZACIÓN TEMPORAL POR ASIGNATURAS DEL MÁSTER UNIVERSITARIO EN										
Curso	Ctr	ASIGNATURA (1)	Tipo	ECTS		Curso	Ctr	ASIGNATURA	Tipo	ECTS
1	1	Comunicaciones Seguras	OB	6		1	2	Identificación y Autenticación	OB	3
1	1	Explotación de Sistemas Software	OB	3		1	2	Gestión y Administración de la Ciberseguridad	OB	3
1	1	Protección de Datos	OB	3		1	2	SEMINARIO	OB	3
1	1	Sistemas de Ciberdefensa	OB	6		1	2	OPTATIVAS		9
1	1	Técnicas de Ciberataque	OB	6		1	2	Ingeniería de Sistemas Seguros (I1)	OP	3
1	1	Seminario	OB	3		1	2	Arquitecturas Seguras (I1)	OP	3
		OPTATIVAS	OP	3		1	2	Seguridad en Sistemas y Comunicaciones Móviles (I1)	OP	3
1	1	Ciberdelitos, Ciberterrorismo y Ciberguerra	OP	3		1	2	Análisis e Ingeniería de Malware (I2)	OP	3
1	1	Análisis de Riesgos en Ciberseguridad	OP	3		1	2	Amenazas persistentes y Fugas de Información (I2)	OP	3
						1	2	Análisis Forense de Sistemas Informáticos (I2)	OP	3
						1	2	Trabajo Fin de Máster	TFM	12

Universidad Carlos III de Madrid
www.uc3m.es

ESTRUCTURA DEL PLAN DE ESTUDIOS POR MATERIAS

CUADRO 2

ESTRUCTURA DEL PLAN DE ESTUDIOS POR MATERIAS MÁSTER UNIVERSITARIO EN					
MATERIA	**ASIGNATURA**	**ECTS**	**Tipo**	**Cur-so**	**Ctr.**
TÉCNICAS DE CIBERATAQUE (M1)	Explotación de Sistemas Software	3	OB	1	1
	Técnicas de Ciberataque	6	OB	1	1
	Amenazas persistentes y Fugas de Información (I2)	3	OP	1	2
	Análisis e Ingeniería de Malware (I2)	3	OP	1	2
	Ciberdelitos, Ciberterrorismo y Ciberguerra	3	OP	1	1
	TOTAL ECTS MATERIA	**18**			
TÉCNICAS DE CIBERDEFENSA Y COMUNICACIO-NES SEGURAS (M2)	Comunicaciones Seguras	6	OB	1	1
	Identificación y Autenticación	3	OB	1	2
	Protección de Datos	3	OB	1	1
	Sistemas de Ciberdefensa	6	OB	1	1
	Análisis Forense de Sistemas Informáticos (I2)	3	OP	1	2
	Arquitecturas Seguras (I1)	3	OP	1	2
	Ingeniería de Sistemas Seguros (I1)	3	OP	1	2
	Seguridad en Sistemas y Comunicaciones Móviles (I1)	3	OP	1	2
	TOTAL ECTS MATERIA	**30**			
GESTIÓN DE LA CIBERSEGURI-DAD (M3)	Gestión y Administración de la Ciberseguridad	3	OB	1	2
	Análisis de Riesgos en Ciberseguridad	3	OP	1	1
	TOTAL ECTS MATERIA	**6**			
TRABAJO FIN DE MÁSTER (M4)	**Trabajo fin de máster**	**12**	TFM	1	2
SEMINARIOS (M5)	Seminario 1	3	OB	1	1
	Seminario 2	3	OB	1	2
	TOTAL ECTS MATERIA	**18**			

b) Planificación y gestión de la movilidad de estudiantes propios y de acogida

En este momento no existen acuerdos específicos de movilidad para este Máster, sin perjuicio de que en el futuro puedan establecerse algunos acuerdos concretos, que se irán incorporando a la memoria en la medida en que se vayan firmando, que ayuden incluso al desarrollo futuro de acuerdos de dobles titulaciones que se adjuntarán igualmente a la presente memoria. La acreditada presencia internacional de nuestra Universidad contribuirá a la consecución de este objetivo. Conviene recordar que la Universidad Carlos III de Madrid mantiene Convenios de Intercambio de estudiantes con más de 200 Universidades en 30 países. A su vez, nuestra Universidad es miembro de prestigiosas Organizaciones Internacionales como la Asociación Universitaria Iberoamericana de Postgrado (AUIP), CINDA (Centro Interuniversitario de Desarrollo) y la Red Iberoamericana de Estudios de Postgrado (REDIBEP). Una parte importante de los estudiantes matriculados en los másteres universitarios de la Universidad Carlos III son estudiantes internacionales.

La dirección del programa junto con la Comisión Académica del Máster serán los encargados de asegurar la adecuación de los convenios de movilidad con los objetivos del título. Bajo la supervisión de la Dirección del Máster existirá un coordinador y tutor de los estudios en programas de movilidad que orientará los contratos de estudios y realizará el seguimiento de los cambios y del cumplimiento de los mismos. Asimismo, las asignaturas incluidas en los contratos de estudios autorizadas por el tutor serán objeto de reconocimiento académico incluyéndose en el expediente del alumno. De igual manera, los estudiantes de másteres universitarios pueden participar en el programa *Erasmus placement* reconociéndose la estancia de prácticas en su expediente académico con el carácter previsto en el plan de estudios o como formación complementaria.

En la actualidad, la Universidad Carlos III de Madrid participa en un programa financiado por la Comisión Europea: Erasmus Mundus “GreenIT” (http://www.emundusgreenit.uvigo.es/), en el que se ofrecen becas para estudiantes del norte de África en distintos programas de postgrado, y en concreto algunos programas de Máster Académicos de la Universidad Carlos III de Madrid. Este Máster tiene la posibilidad de adherirse a la oferta de dicho programa, y estamos estudiando la posibilidad de participar en la elaboración de propuestas similares, más específicas en el ámbito de la seguridad, para atraer alumnos e intercambiar docentes.

ESAT - COSIC, Computer Security and Industrial Cryptography. Katholieke Universiteit Leuven, Belgica. http://www.esat.kuleuven.be/cosic/

Information Security Group, Universitat Politècnica de Catalunya, http://isg.upc.edu

SPRINGER - Security and Privacy Innovation Group.Università di Roma Tre, Italia
http://ricerca.mat.uniroma3.it/users/dipietro/gruppoRicerca/index.html

Security Group. University of York, Reino Unido
http://www.cs.york.ac.uk/security/

Security Research Group. Hacettepe University, Turkey
http://seclab.cs.hacettepe.edu.tr/

Embedded, Networked and Distributed Systems Group. University of Glasgow, Reino Unido

http://www.gla.ac.uk/schools/computing/research/researchgroups/embeddednetworkedanddistributedsystems/

NICS. Universidad de Málaga, España.
http://www.nics.uma.es

NESG - Network Engineering & Security Group.Universidad de Granada, España.
http://nesg.ugr.es/

Information Security & Privacy Lab. Delft University of Technology, The Netherlands.
http://isplab.tudelft.nl/

Erasmus Medical Center, Neuroscience Department, The Netherlands.
http://www.neuro.nl/

Department of Computer Science & Engineering, Chalmers University of Technology, Switzerland.
http://www.chalmers.se/cse/EN/organization/divisions/networks-systems

Department of Electrical Engineering, Shahid Rajaee Teacher Training University, Tehran, Iran.
http://www.srttu.edu/Electrical/EnIndex.aspx#

Fraunhofer Research Institution for Applied and Integrated Security FhI-AISEC (antes, Fraunhofer Institute for Secure Information Technologies FhI-SIT), Munich, Alemania
http://www.aisec.fraunhofer.de/en.html

c) Procedimientos de coordinación docente horizontal y vertical del plan de estudios

MECANISMOS DE COORDINACIÓN DOCENTE

La coordinación docente del **Máster Universitario en Ciberseguridad** es responsabilidad del Director del Máster. Corresponde al Director las siguientes actividades:

- Presidir la Comisión Académica de la titulación.
- Presidir el Comité de Dirección.
- Vigilar la calidad docente de la titulación.
- Procurar la actualización del plan de estudios para garantizar su adecuación a las necesidades sociales.
- Promover la orientación profesional de los estudiantes.
- Coordinar la elaboración de la Memoria Académica de Titulación.

El Comité de Dirección asiste al Director del Máster en algunas de sus tareas. El Comité de Dirección estará formado por miembros internos de la Universidad y por miembros externos, previsiblemente de las empresas que han formado parte del Comité Externo de elaboración del Plan de Estudios. La pertenencia al Comité de Dirección no conlleva ningún tipo de remuneración monetaria en ningún caso. El Comité de Dirección tendrá las siguientes responsabilidades:

- Seleccionar los estudiantes que serán admitidos en el Máster.
- Gestionar todos los aspectos de transferencia y reconocimiento de créditos de acuerdo con la normativa de la Universidad.

- Resolver las propuestas de Matrículas de Honor de los Trabajos Fin de Máster, conforme a la normativa de la Universidad.
- Planificar los seminarios.

La Universidad Carlos III de Madrid dispone de un Sistema de Garantía Interna de la Calidad (SGIC). Dicho sistema ha sido diseñado por la Universidad conforme a los criterios y directrices recogidas en los documentos "Directrices, definición y documentación de Sistemas de Garantía Interna de Calidad de la formación universitaria" y "Guía de Evaluación del diseño del Sistema de Garantía Interna de Calidad de la formación universitaria" proporcionados por la ANECA (Programa AUDIT convocatoria 2007/08. Este diseño está formalmente establecido y es públicamente disponible. La ANECA emitió en febrero de 2009 una valoración POSITIVA del diseño del SGIC-UC3M. Este diseño se ha implantado por primera vez en el curso 2008/09.

Dentro del SGIC de la Universidad Carlos III de Madrid, la Comisión Académica de la Titulación, está definida como el órgano que realiza el seguimiento, analiza, revisa, evalúa la calidad de la titulación y las necesidades de mejora y aprueba la Memoria Académica de Titulación.

La Comisión Académica del **Máster Universitario en Ciberseguridad** estará formada por el Director del Máster, que preside sus reuniones y por representantes de los Departamentos que imparten docencia en la titulación, así como por los alumnos, siendo preferente la participación del delegado de la titulación electo en cada momento, y en su defecto o por ausencia, cualquier otro alumno de la titulación, así como por algún representante del personal de administración y servicios vinculado con la titulación siempre que sea posible.

La Comisión Académica del Máster tendrá las siguientes responsabilidades:

- Supervisar los criterios aplicados en el proceso de selección de los estudiantes que serán admitidos en el Máster.
- Supervisar el correcto cumplimiento de los objetivos académicos.
- Gestionar todos los aspectos de transferencia y reconocimiento de créditos de acuerdo con la normativa de la Universidad.
- Y en general, gestionar y resolver todos los aspectos asociados con el correcto funcionamiento del Máster.
- Recoger, evaluar y gestionar las necesidades y propuestas de los alumnos, docentes y resto de miembros implicados en el proceso de enseñanza-aprendizaje en relación con la titulación.

Además, la Comisión Académica del Máster velará por la integración de las enseñanzas, intentando identificar y promover sinergias entre asignaturas, así como haciendo los propio con sistemas de coordinación que garanticen evitar el solapamiento entre asignaturas y las lagunas en las mismas.

5.2 Estructura del plan de estudios

ACTIVIDADES FORMATIVAS DEL PLAN DE ESTUDIOS REFERIDAS A MATERIAS	
AF1	Clase teórica
AF2	Clases prácticas
AF3	Clases teórico prácticas
AF4	Prácticas de laboratorio
AF5	Tutorías
AF6	Trabajo en grupo
AF7	Trabajo individual del estudiante
AF8	Exámenes parciales y finales

METODOLOGÍAS DOCENTES FORMATIVAS DEL PLAN REFERIDAS A MATERIAS	
MD1	*Exposiciones en clase del profesor* con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporciona la bibliografía para complementar el aprendizaje de los alumnos.
MD2	*Lectura crítica de textos* recomendados por el profesor de la asignatura: Artículos de prensa, informes, manuales y/o artículos académicos, bien para su posterior discusión en clase, bien para ampliar y consolidar los conocimientos de la asignatura.
MD3	*Resolución de casos prácticos, problemas, etc.… planteados por el profesor de manera individual o en grupo*
MD4	*Exposición y discusión en clase*, bajo la moderación del profesor *de temas* relacionados con el contenido de la materia, así como de casos prácticos
MD5	Elaboración de trabajos e informes de manera individual o en grupo

SISTEMAS DE EVALUACIÓN DEL PLAN DE ESTUDIOS REFERIDOS A MATERIAS	
SE1	Participación en clase
SE2	Trabajos individuales o en grupo realizados durante el curso
SE3	Examen final

TABLA DE COMPETENCIAS POR MATERIAS					
COMPETENCIAS	**MATERIAS**				
	M1	**M2**	**M3**	**M4**	**M5**
CB6	X	X		X	X
CB7	X	X		X	X
CB8	X	X	X	X	X
CB9	X	X	X	X	
CB10	X	X	X	X	X
CG1	X			X	X
CG2		X		X	X
CG3	X	X		X	
CG4	X	X	X	X	X
CG5			X	X	
CE1	X				
CE2	X				
CE3	X				X
CE4		X		X	
CE5		X		X	X
CE6		X		X	
CE7	X	X		X	
CE8		X			X
CE9			X		

M1: Técnicas de Ciberataque

M2: Técnicas de Ciberdefensa y Comunicaciones Seguras

M3: Gestión de la Ciberseguridad

M4: TFM

M5: SEMINARIOS

TABLA DE METODOLOGIAS DOCENTES					
METODOLOGIAS DOCENTES	MATERIAS				
	M1	M2	M3	M4	M5
MD1	X	X	X		X
MD2	X	X	X	X	X
MD3	X	X			
MD4	X	X	X		X
MD5	X	X	X	X	X

TABLA DE SISTEMAS DE EVALUACIÓN POR MATERIAS					
	MATERIAS				
	M1	M2	M3	M4	M5
SE1	X	X	X		X
SE 2	X	X	X		X
SE 3	X	X		X	X

MATERIA 1	
Denominación: Técnicas de Ciberataque	
Número de créditos ECTS	**Carácter de la materia (obligatoria/optativa/mixto/trabajo fin de máster/etc.)**
18	Mixto

Duración y ubicación temporal dentro del plan de estudios

Esta materia está compuesta por dos asignaturas obligatorias y una optativa que se imparten en el primer cuatrimestre, y de dos optativas que se imparten en el segundo cuatrimestre del curso.

Competencias que el estudiante adquiere con esta materia

CB6, CB7, CB8, CB9, CB10. CG1, CG3, CG4, CE1, CE2, CE3, CE7

Resultados de aprendizaje que adquiere el estudiante

A la superación de esta materia los estudiantes deberán ser capaces de:

- Adquirir remotamente inteligencia de carácter técnico sobre los componentes de un sistema objetivo, usando para ello tanto fuentes abiertas como técnicas de enumeración y reconocimiento
- Detectar, en un tiempo fijado, un elevado porcentaje de las vulnerabilidades de un sistema en red dado.
- Explicar al menos una manera de introducirse en un sistema cuyas vulnerabilidades han sido detectadas.
- Justificar mediante informes razonados las vulnerabilidades encontradas y el procedimiento detallado que se seguiría para la intrusión.
- Explicar otras técnicas de ataque a un sistema que no sea susceptible de intrusión directa.
- Conocidas las dependencias entre los distintos servicios en red de un sistema, explicar cómo evolucionarían distintos ataques propuestos y cómo se verían afectadas las distintas partes y el total para cada uno de dichos ataques.
- Conocido el tipo de información y los mecanismos de defensa desplegados en un sistema, explicar el impacto de distintas amenazas e intrusiones y en especial de las fugas de información.
- Proponer distintos ataques que se puedan realizar desde dentro de un sistema en un entorno controlado y explicar sus consecuencias.
- Elegir con criterio la mejor herramienta de análisis en el proceso de investigación iniciado por las sospechas de presencia de malware.
- Explicar los mecanismos que pueden utilizarse para ocultar la intrusión en un sistema.

Actividades formativas de la materia indicando su contenido en horas y % de presencialidad

Código actividad	Horas totales	Horas Presenciales (2)	% presencialidad Estudiante (3)
AF1	90	90	100%
AF2	30	30	100%
AF3	30	30	100%
AF4	30	30	100%
AF5	20	0	0%
AF6	30	0	0%
AF7	220	0	0%
AF8	10	10	100%
TOTAL MATERIA	460	190	40%

Metodologías docentes que se utilizarán en esta materia

MD1, MD2, MD3, MD4, MD5

Sistemas de evaluación y calificación. Indicar su ponderación máxima y mínima

Sistemas de evaluación	Ponderación mínima	Ponderación máxima
SE1	0%	5%
SE2	40%	60%
SE3	40%	60%

Asignaturas de la materia

Asignatura	Créditos	Cuatrim	Carácter	Idioma
Explotación de Sistemas Software	3	1	OB	Bilingüe
Técnicas de Ciberataque	6	1	OB	Bilingüe
Amenazas persistentes y Fugas de Información	3	2	OP	Bilingüe
Análisis e Ingeniería de Malware	3	2	OP	Bilingüe
Ciberdelitos, Ciberterrorismo y Ciberguerra	3	1	OP	Bilingüe

Breve descripción de contenidos

Explotación de Sistemas Software:

1. Introducción
   1.1. Vulnerabilidades en Componentes Software
   1.2. Mecanismos de Explotación
   1.3. Herramientas y Laboratorio de Análisis y Síntesis

2. Explotación de Vulnerabilidades en el Software
   2.1. Violaciones de Memoria
   2.2. Validación de Entrada de Datos e Inyección de Código
   2.3. Condiciones de Carrera
   2.4. Confusión de Privilegios
   2.5. Explotación de la Interfaz de Usuario
   2.6. Abuso de Funcionalidad y Configuraciones
   2.7. Explotación de Cachés

3. Explotación de Sistemas Web
   3.1. Vulnerabilidades en el Canal
   3.2. Vulnerabilidades en el Servidor
   3.3. Vulnerabilidades en el Navegador

4. Información sobre Vulnerabilidades y Formas de Explotación
   4.1. Repositorios
   4.2. Lenguajes y Estándares de Representación e Intercambio

Técnicas de Ciberataque:

1. Introducción a las técnicas de ciberataque
   1.1. Conceptos y definiciones
   1.2. Tipos de ciberataques
   1.3. Fases típicas de una intrusión

2. Adquisición de información del objetivo y análisis de vulnerabilidades
   2.1. Técnicas de reconocimiento. Fuentes abiertas.
   2.2. Enumeración de redes y escaneo de servicios.
   2.3. Identificación y análisis de vulnerabilidades

3. Explotación
   3.1. Explotación de sistemas de autenticación
   3.2. Explotación de software
   3.3. Consumo de recursos y DoS
   3.4. Malware
   3.5. Ingeniería social
   3.6. Técnicas de evasión

4. Persistencia
   4.1. Eliminación de evidencias
   4.2. Escalado de privilegios
   4.3. Establecimiento de canales de acceso alternativos
   4.4. Ocultación de presencia

5. Casos de estudio

Amenazas Persistentes y Fugas de Información:

1. Amenazas Persistentes
   - 1.1. Técnicas de persistencia en sistemas comprometidos
     - 1.1.1. Escalada de privilegios y movimientos laterales
     - 1.1.2. Establecimiento de vectores de acceso alternativos
     - 1.1.3. Ocultación de evidencias
     - 1.1.4. Técnicas de evasión avanzadas (AET)
   - 1.2. APTs
     - 1.2.1. Definiciones
     - 1.2.2. Casos prácticos
     - 1.2.3. Contramedidas
       - 1.2.3.1. Protección de los datos
       - 1.2.3.2. Prevención y detección
       - 1.2.3.3. Respuesta a incidentes
     - 1.2.4. Tendencias

2. Canales encubiertos. Esteganografía y estegoanálisis
   - 2.1. Definición de la ciencia de la esteganografía. Historia
   - 2.2. Clasificación de sistemas esteganográficos. Evaluación de su seguridad
   - 2.3. Esteganografía moderna
     - 2.3.1. Ocultación de información en dispositivos hardware
     - 2.3.2. Ocultación de información en protocolos de comunicación
     - 2.3.3. Ocultación en sistemas de ficheros y formatos digitales
     - 2.3.4. Esteganografía lingüística
     - 2.3.5. Esteganografía multimedia: imagen, audio y video.
   - 2.4. Estegoanálisis moderno
     - 2.4.1. Detección de patrones. Ataques visuales y estadísticos
     - 2.4.2. Estegoanálisis a ciegas
   - 2.5. Recomendaciones de diseño seguro.

Análisis e Ingeniería de Malware:

1. Introducción al Análisis e Ingeniería de Malware
   - 1.1. Conceptos y Evolución Histórica
   - 1.2. Tipos de Malware. Estructura, Componentes y Vectores de Infección
   - 1.3. Ingeniería e Ingeniería Inversa de Malware

2. Herramientas de Análisis y Síntesis de Malware
   - 2.1. Análisis Estático de Código
   - 2.2. Análisis Dinámico. Entornos de Depuración y Ejecución Controlada
   - 2.3. Ingeniería Inversa y Re-ingeniería de Código
   - 2.4. Laboratorios de Análisis y Síntesis de Malware

3. Análisis e Ingeniería de Malware
   - 3.1. Análisis de Firmas
   - 3.2. Detección y Análisis de Capacidades y Comportamientos
   - 3.3. Técnicas de Ofuscación
   - 3.4. Técnicas de Persistencia y Propagación

3.5. Técnicas Anti-ingeniería Inversa

Ciberdelitos, Ciberterrorismo y Ciberguerra:

1. Introducción, Definiciones y Conceptos Básicos

2. Ciberataques y ciberactivismo
   2.1. Tipos de Ciberataques
   2.2. Ciberdelitos
   2.3. Ciberespionaje
   2.4. Análisis de Casos Prácticos
   2.5. Aspectos Legales

3. Ciberterrorismo y Ciberoperaciones contra Infraestructuras Críticas
   3.1. Infraestructuras Críticas: Interconexión y Vulnerabilidades
   3.2. Sistemas de Control Industrial
   3.3. Otras Infraestructuras Críticas
   3.4. Análisis de Casos Prácticos

4. Ciberguerra
   4.1. Ciberarmamento: Instrumentos Lógicos, Físicos y Psicológicos
   4.2. Ciberdoctrina
   4.3. Análisis de Casos Prácticos

Lenguas en que se impartirá la materia

Bilingüe: Español e inglés según se explica en el apartado 1.3

Observaciones

Dentro del máster se impartirán dos seminarios que son asignaturas obligatorias de 3 créditos ECTS (10 horas presenciales) cada uno. El objetivo es acercar los problemas y soluciones más acuciantes de la industria, administración, defensa e investigación a los alumnos. A través de los distintos seminarios que se propongan los alumnos podrán tener acceso a la experiencia de profesionales de reconocido prestigio cuya labor profesional está relacionada con la ciberseguridad: auditorías, prevención y detección de amenazas, contramedidas, etc. Por otra parte los seminarios más académicos pondrán a los alumnos en contacto con el estado de la técnica en conceptos, protocolos, desarrollos y herramientas en temas concretos relacionados con la ciberseguridad. Por tanto los seminarios podrán encuadrarse dentro de cualquiera de las materias del máster.

Respecto a la consecución de competencias, esta materia es fundamental para alcanzar la competencia CG1 “Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica”, y se alcanza a través de las asignaturas obligatorias. También contribuye a alcanzar las competencias CG3 y CG4 junto con otras materias. Respecto a las competencias específicas, las asignatura optativas se han planteado para desarrollar las competencias específicas de la materia: “Análisis e Ingeniería de Malware” (CE1), “Amenazas persistentes y Fugas de Información” (CE2, CE7), “Ciberdelitos, Ciberterrorismo y Ciberguerra” (CE3).

MATERIA 2	
Denominación: Técnicas de Ciberdefensa y Comunicaciones Seguras	
Número de créditos ECTS	**Carácter de la materia (obligatoria/optativa/mixto/trabajo fin de máster/etc.)**
30	Mixto

Duración y ubicación temporal dentro del plan de estudios

Esta materia está compuesta por tres asignaturas obligatorias que se imparten en el primer cuatrimestre, y de otra obligatoria y cuatro optativas que se imparten en el segundo cuatrimestre del curso.

Competencias que el estudiante adquiere con esta materia

CB6, CB7, CB8, CB9, CB10, CG2, CG3, CG4, CE4, CE5, CE6, CE7, CE8

Resultados de aprendizaje que adquiere el estudiante

A la superación de esta materia los estudiantes deberán ser capaces de:

- Diseñar estrategias de sensorización para distintos elementos de un sistema en red y analizar los eventos observados en un ataque concreto para distinguir cuáles son de interés.
- Dado un sistema bajo distintos tipos de ataques, ser capaz de detectar las características de la mayoría de dichos ataques y señalar las fuentes más probables.
- Identificado un ataque y su fuente, proponer las contramedidas para contrarrestarlo explicando la medida de su eficacia. Evaluar estrategias de zonificación de redes y diseñar políticas de filtrado de tráfico.
- 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.
- Explicar la problemática de seguridad asociada a los dispositivos móviles personales en un entorno profesional dado y aplicar las técnicas estudiadas a la ingeniería de sistemas seguros.
- Dado un sistema atacado, encontrar algunas de las evidencias del ataque y explicar las medidas necesarias para mantener la cadena de custodia de dichas evidencias.
- Evaluar la arquitectura de seguridad de un sistema vulnerable dado y proponer mejoras.
- Diseñar y evaluar medidas apropiadas para la identificación y autenticación de usuarios, así como la gestión de las identidades y las autorizaciones asociadas.
- Conocer los principios de desarrollo y mantenimiento de sistemas seguros, incluyendo el desarrollo y adquisición de componentes software, durante todo su ciclo de vida
- Conocer la normativa legal y técnica de aplicación en el marco de la ciberseguridad.

Actividades formativas de la materia indicando su contenido en horas y % de presencialidad

Código actividad	Horas totales	Horas Presenciales (2)	% presencialidad Estudiante (3)
AF1	150	150	100%
AF2	50	50	100%
AF3	50	50	100%

AF4	50	50	100%
AF5	20	0	0%
AF6	30	0	0%
AF7	400	0	0%
AF8	16	16	100%
TOTAL MATERIA	766	316	40%

Metodologías docentes que se utilizarán en esta materia

MD1, MD2, MD3, MD4, MD5

Sistemas de evaluación y calificación. Indicar su ponderación máxima y mínima

Sistemas de evaluación	Ponderación mínima	Ponderación máxima
SE1	0%	5%
SE2	40%	60%
SE3	40%	60%

Asignaturas de la materia

Asignatura	Créditos	Cuatrim	Carácter	Idioma
Comunicaciones Seguras	6	1	OB	Bilingüe
Identificación y Autenticación	3	2	OB	Bilingüe
Protección de Datos	3	1	OB	Bilingüe
Sistemas de Ciberdefensa	6	1	OB	Bilingüe
Análisis Forense de Sistemas Informáticos	3	2	OP	Bilingüe
Arquitecturas Seguras	3	2	OP	Bilingüe
Ingeniería de Sistemas Seguros	3	2	OP	Bilingüe
Seguridad en Sistemas y Comunicaciones Móviles	3	2	OP	Bilingüe

Breve descripción de contenidos

Comunicaciones Seguras:

1. Principios de seguridad de redes de comunicaciones
   1.1. Definiciones y conceptos. Servicios de seguridad vs Mecanismos de seguridad
   1.2. Ataques más comunes a las redes de comunicaciones
   1.3. Contramedidas. Costes de la seguridad.

2. Seguridad en el nivel físico y de enlace. Ataques y defensas.

3. Seguridad en el nivel de red.
   3.1. Protocolos auxiliares (ICMP, DHCP). Ataques y defensas
   3.2. Protocolos de encaminamiento. Ataques y defensas.
   3.3. Seguridad en IPv4 e IPv6. IPSec

4. Seguridad en el nivel de transporte.
   4.1. TLS/SSL.
   4.2. Redes privadas virtuales

5. Seguridad en el nivel de aplicación.
   5.1. Seguridad en DNS
   5.2. Seguridad en HTTP
   5.3. Seguridad en correo electrónico
   5.4. Seguridad en otras aplicaciones: ejecución remota, transferencia de ficheros, ficheros en red.

6. Seguridad en comunicaciones inalámbricas
   6.1. Seguridad en familia IEEE 802.11

Identificación y Autenticación:

1. Autenticación de usuarios
   1.1. Conceptos y definiciones
   1.2. Esquemas de autenticación. Autenticación de varios factores
   1.3. Autenticación robusta. Autenticación mediante la firma digital
   1.4. Análisis de seguridad
   1.5. Arquitecturas de autenticación. Kerberos

2. Identificación biométrica
   2.1. Definiciones y principios de funcionamiento
   2.2. Sistemas biométricos
   2.3. Seguridad, privacidad y aspectos prácticos

3. Gestión de identidades
   3.1. Ciclo de vida de la identidad digital
   3.2. Gestión de la identidad en sistemas distribuidos
   3.3. Estándares y sistemas federados

4. Aspectos éticos y legislación asociada a la privacidad.
   4.1. Normativa sobre identificación

4.2. LOPD y Reglamento de desarrollo

Protección de Datos:

1. Introducción a la protección de la información
   1.1. Definiciones
   1.2. Dimensiones de la seguridad de la información

2. Criptografía moderna
   2.1. Clasificación de los sistemas de cifra
   2.2. Gestión de claves criptográficas

3. Cifrado con clave secreta o simétrica.
   3.1. Cifradores de flujo
   3.2. Cifradores de bloque

4. Autenticación y funciones unidireccionales
   4.1. Funciones hash criptográficas
   4.2. Códigos de Autenticación de Mensajes (MAC)

5. Cifrado con clave pública o asimétrica
   5.1. Clasificación y seguridad
   5.2. Criptosistema de clave pública. Ejemplos
   5.3. Firma digital. Estándares

6. Certificados digitales e infraestructuras de clave pública (PKI)
   6.1. Certificados digitales. ITU-T X.509v3
   6.2. Autoridades de confianza (CA) e infraestructuras de clave pública (PKI)
   6.3. Legislación de firma electrónica

7. Aplicaciones
   7.1. Cifrado de ficheros y discos
   7.2. Integridad de datos

Sistemas de Ciberdefensa:

1. Introducción a los Sistemas de Ciberdefensa

2. Sensores Locales: Auditoría y Análisis de Eventos
   2.1. Gestión de Usuarios y Accesos
   2.2. Análisis de logs de seguridad

3. Cortafuegos y Zonificación de Redes
   3.1. Fundamentos de Filtrado de Tráfico
   3.2. Tipos de Cortafuegos
   3.3. Zonificación de Redes

4. Sistemas de Detección y Prevención de Ataques
   4.1. Detección de Firmas de Ataque
   4.2. Detección de Anomalías
   4.3. Arquitecturas Distribuidas de Sensores de Detección
   4.4. Respuesta Automática a Intentos de Intrusión

5. Sistemas de Gestión de Eventos e Información de Seguridad (SIEM)
   5.1. Conceptos y Arquitecturas de SIEMs
   5.2. Reglas de Agregación y Correlación
   5.3. Estrategias de Sensorización de Redes

Análisis Forense de Sistemas Informáticos:

1. Introducción al Análisis Forense
   1.1. ¿Qué es la informática forense?
   1.2. Casos de ejemplo
   1.3. Conceptos técnicos clave
   1.4. Legislación asociada

2. Laboratorio de Análisis Forense
   2.1. Laboratorio
   2.2. Políticas y procedimientos
   2.3. Garantía de la calidad
   2.4. Herramientas
   2.5. Evidencias: obtención, análisis y custodia
   2.6. Informes forenses

3. Herramientas de Análisis Forense
   3.1. Análisis forense de sistemas de ficheros
   3.2. Análisis forense de memoria
   3.3. Análisis forense en redes de ordenadores
   3.4. Internet y correo electrónico
   3.5. Análisis forense en dispositivos móviles
   3.6. Herramientas y técnicas anti-forense

Arquitecturas Seguras:

1. Arquitecturas Seguras
   1.1. Motivación y Casos Prácticos
   1.2. Principios generales de seguridad en el diseño
   1.3. Virtualización y Computación en la Nube

2. Tolerancia Frente a Ataques
   2.1. Protección DDoS. Balanceo de Carga
   2.2. Sistemas de Respaldo

3. Autorización
   3.1. Modelos de Control de Accesos Discrecional (DAC)
   3.2. Modelos de Control de Accesos basados en Roles (RBAC)
   3.3. Arquitecturas de control de acceso. XACML/SAML.

4. Sistemas de Seguridad Multinivel y Multilateral
   4.1. Clasificación de la Información y Habilitaciones de Seguridad
   4.2. Principios y Procedimientos de Manejo de Información Clasificada
   4.3. Sistemas MLS. Ejemplos y Consideraciones Prácticas

5. Seguridad Física
   5.1. Seguridad frente a las emanaciones. TEMPEST
   5.2. Sistemas Hardware Resistentes a Intrusiones

Ingeniería de Sistemas Seguros:

1. Conceptos de Ingeniería de Sistemas Seguros
   1.1. Propiedades de Seguridad
   1.2. Principios de Diseño para la Seguridad
   1.3. Gestión de Riesgos
   1.4. Regulaciones y Aspectos de Privacidad
   1.5. Arquitecturas Software

2. Requisitos de Software Seguro
   2.1. Descomposición de Políticas
   2.2. Identificación y Elicitación

3. Diseño de Software Seguro
   3.1. Procesos de Diseño
   3.2. Consideraciones de Diseño
   3.3. Seguridad de la Arquitectura
   3.4. Tecnologías

4. Implementaciones Seguras
   4.1. Seguridad de los Lenguajes de Programación
   4.2. Bases de Datos de Vulnerabilidades
   4.3. Prácticas y Controles Defensivos
   4.4. Código Fuente. Versiones
   4.5. Entornos de Desarrollo
   4.6. Revisión y Análisis de Código
   4.7. Técnicas Anti-manipulación de Código

5. Pruebas
   5.1. Estrategias, Planes y Casos de prueba
   5.2. Tipos de pruebas
   5.3. Evaluación de Impacto y Acciones Correctivas
   5.4. Gestión del Ciclo de Vida de los Datos de Prueba

6. Otros aspectos.

Seguridad en Sistemas y Comunicaciones Móviles:

1. Introducción a los estándares de telefonía móvil activos

2. Seguridad en comunicaciones inalámbricas y terminales

2.1. Protección de datos (A5/1, Kasumi, túneles en IMS)
2.2. Esquema interno del operador
2.3. Seguridad en redes de datos móviles y posicionamiento
2.4. Seguridad en comunicaciones de bajo alcance
2.5. Distribución de claves en telefonía móvil

3. Ataques conocidos a redes de telefonía/datos móviles
   3.1. Ataques a tarjetas y replicación de tarjetas
   3.2. Ataques al canal radio

4. Sistemas operativos móviles
   4.1. Protección de los recursos radio
   4.2. Protección de los recursos software
   4.3. Protección contra ingeniería social

5. Seguridad en smartphones
   5.1. Handover vertical y horizontal (entre redes seguras e inseguras)
   5.2. Aplicaciones maliciosas
   5.3. Localización

Lenguas en que se impartirá la materia

Bilingüe: Español e inglés según se explica en el apartado 1.3

Observaciones

Dentro del máster se impartirán dos seminarios que son asignaturas obligatorias de 3 créditos ECTS (10 horas presenciales) cada uno. El objetivo es acercar los problemas y soluciones más acuciantes de la industria, administración, defensa e investigación a los alumnos. A través de los distintos seminarios que se propongan los alumnos podrán tener acceso a la experiencia de profesionales de reconocido prestigio cuya labor profesional está relacionada con la ciberseguridad: auditorías, prevención y detección de amenazas, contramedidas, etc. Por otra parte los seminarios más académicos pondrán a los alumnos en contacto con el estado de la técnica en conceptos, protocolos, desarrollos y herramientas en temas concretos relacionados con la ciberseguridad. Por tanto los seminarios podrán encuadrarse dentro de cualquiera de las materias del máster.

Respecto a la consecución de competencias, esta materia es fundamental para alcanzar la competencia CG2 “Concebir, diseñar, poner en práctica y mantener un sistema global de Ciberdefensa en un contexto definido” y las competencias específicas CE5 y CE7, que se alcanzan a través de las asignaturas obligatorias y una de las asignaturas optativas: “Ingeniería de Sistemas Seguros”. También contribuye a alcanzar las competencias CG3 y CG4 junto con otras materias. Respecto a las competencias específicas, las asignatura optativas se han planteado para desarrollar las competencias específicas de la materia: “Análisis Forense de Sistemas Informáticos” (CE4), “Arquitecturas Seguras” (CE6), “Seguridad en Sistemas y Comunicaciones Móviles” (CE8).

MATERIA 3	
Denominación: Gestión de la Ciberseguridad	
Número de créditos ECTS	**Carácter de la materia (obligatoria/optativa/mixto/trabajo fin de máster/etc.)**
6	Mixto

Duración y ubicación temporal dentro del plan de estudios

Esta materia está compuesta por una asignatura obligatoria que se imparte en el segundo cuatrimestre, y de una optativa que se imparte en el primer cuatrimestre del curso.

Competencias que el estudiante adquiere con esta materia

CB8, CB9, CB10, CG4, CG5, CE9

Resultados de aprendizaje que adquiere el estudiante

- Partiendo del plan director de tecnologías de la información de una organización, de su plan general de seguridad (contra riesgos naturales, tecnológicos, etc.) y conociendo sus recursos humanos, tecnológicos, etc., elaborar un plan de seguridad de la información.
- Desarrollar un análisis de riesgos para una organización y a partir de él, y conociendo el umbral de riesgo y el riesgo asumible, gestionar los riesgos resultantes.
- Construir un plan de continuidad conocido el tiempo máximo de recuperación admisible
- Elaborar un plan de concienciación y formación en seguridad adaptado a la estructura organizativa de una empresa
- Conocer los principales criterios (singularmente los Commons Criteria) y las correspondientes metodologías de evaluación y certificación de la seguridad y sus implicaciones en el desarrollo de arquitecturas seguras.
- Conocer el Esquema Nacional de Evaluación y Certificación de las Tecnologías de la Información, los requisitos y las funciones de los laboratorios de evaluación y del Organismo de Certificación, así como el alcance del acuerdo de reconocimiento mutuo de certificados.
- Conocer el funcionamiento de los Centros de Operaciones de Seguridad, sus relaciones mutuas y las normas de intercambio de informaciones acerca de incidentes de seguridad

Actividades formativas de la materia indicando su contenido en horas y % de presencialidad

Código actividad	Horas totales	Horas Presenciales (2)	% presencialidad Estudiante (3)
AF1	40	40	100%
AF2	0	0	0%
AF3	20	20	100%
AF4	0	0	0%
AF5	20	0	0%
AF6	30	0	0%

AF7	40	0	0%
AF8	4	4	100%
TOTAL MATERIA	154	64	40%

Metodologías docentes que se utilizarán en esta materia

MD1, MD2, MD4, MD5

Sistemas de evaluación y calificación. Indicar su ponderación máxima y mínima

Sistemas de evaluación	Ponderación mínima	Ponderación máxima
SE1	0%	5%
SE2	50%	70%
SE3	30%	50%

Asignaturas de la materia

Asignatura	Créditos	Cuatrim	Carácter	Idioma
Gestión y Administración de la Ciberseguridad	3	2	OB	Español
Análisis de Riesgos en Ciberseguridad	3	1	OP	Español

Breve descripción de contenidos

Gestión y Administración de la Ciberseguridad:

1. Introducción y Conceptos Básicos

2. Gestión de la Seguridad
   2.1. Normas ISO/IEC. Serie 27XXX
   2.2. Modelos Organizativos
   2.3. Planes de seguridad
   2.4. Formación y Concienciación
   2.5. Planes de Continuidad. ISO/IEC 22301 y 71599

3. Centros de operaciones de ciberseguridad
   3.1. Estructura y organización
   3.2. Personal, procesos y procedimientos
   3.3. Metodologías de Respuesta a Incidentes. CSIRTs

4. Estrategias y Marco Legal de la Ciberseguridad

Análisis de Riesgos en Ciberseguridad:

1. Introducción y Conceptos Generales de Análisis de Riesgos
   1.1. Conceptos: Activos, Amenazas, Vulnerabilidades, Salvaguardas
   1.2. Análisis Cualitativo y Cuantitativo
   1.3. Análisis Estático y Dinámico

2. Metodologías de Análisis de Riesgos
   2.1. ISACA(COSO), CRAMM, EBIOS, PCI-DSS
   2.2. ISO-27005. MAGERIT.

3. Retos Actuales y Futuros de Aplicación
   3.1. Cloud Computing
   3.2. Big Data & IA
   3.3. Internet of Things (IoT)
   3.4. Entornos móviles

Lenguas en que se impartirá la materia

Español

Observaciones

Dentro del máster se impartirán dos seminarios que son asignaturas obligatorias de 3 créditos ECTS (10 horas presenciales) cada uno. El objetivo es acercar los problemas y soluciones más acuciantes de la industria, administración, defensa e investigación a los alumnos. A través de los distintos seminarios que se propongan los alumnos podrán tener acceso a la experiencia de profesionales de reconocido prestigio cuya labor profesional está relacionada con la ciberseguridad: auditorías, prevención y detección de amenazas, contramedidas, etc. Por otra parte los seminarios más académicos pondrán a los alumnos en contacto con el estado de la técnica en conceptos, protocolos, desarrollos y herramientas en temas concretos relacionados con la ciberseguridad. Por tanto los seminarios podrán encuadrarse dentro de cualquiera de las materias del máster.

Respecto a la consecución de competencias, esta materia es fundamental para alcanzar la competencia CG5 “Desarrollar, implantar y mantener un Sistema de Gestión de la Seguridad de la Información (ISMS)” que se alcanza a través de la asignatura obligatoria. También contribuye a alcanzar la competencia CG4 junto con otras materias. Respecto a las competencias específicas, se ha planteado una única asignatura específica para desarrollar la competencia específica de la materia: “Análisis de Riesgos y Certificación de Sistemas” (CE9).

MATERIA 4

Denominación: Trabajo Fin de Máster

Número de créditos ECTS	Carácter de la materia (obligatoria/optativa/mixto/trabajo fin de máster/etc.)
12	Obligatoria

Duración y ubicación temporal dentro del plan de estudios

Segundo cuatrimestre del curso.

Competencias que el estudiante adquiere con esta materia

CB6, CB7, CB8, CB9, CB10, CG1, CG2, CG3, CG4, CG5

Resultados de aprendizaje que adquiere el estudiante

El Trabajo Fin de Máster (TFM) consistirá en la realización, presentación y defensa de un ejercicio original realizado individualmente ante un tribunal universitario, consistente en un proyecto integral en el ámbito del Ciberataque o la Ciberdefensa. En el TFM se acabarán de sintetizar las competencias adquiridas.

Tras la superación del TFM el alumno habrá:

- Adquirido los conocimientos generales en cuanto a la elaboración de un proyecto profesional completo relacionado con algún aspecto de la titulación de Máster en Ciberseguridad.
- Elaborado la parte técnica de un proyecto completo usando los medios técnicos necesarios y desarrollando prototipos, simulaciones, realizando informes, etc.
- Realizado una presentación escrita y oral de su trabajo.
- Adquirido conciencia de los aspectos sociales y éticos de la Ciberseguridad para su incorporación al mercado laboral.

Actividades formativas de la materia indicando su contenido en horas y % de presencialidad

Código actividad	Horas totales	Horas Presenciales (2)	% presencialidad Estudiante (3)
AF1	4	4	100%
AF2	0	0	0%
AF3	0	0	0%
AF4	0	0	0%
AF5	46	0	0%
AF6	0	0	0%
AF7	250	0	0%
TOTAL MATERIA	300	0	0%

Metodologías docentes que se utilizarán en esta materia

MD2, MD5

Sistemas de evaluación y calificación. Indicar su ponderación máxima y mínima

Sistemas de evaluación	Ponderación mínima	Ponderación máxima
SE1	0%	0%
SE2	0%	0%
SE3	100%	100%

Asignaturas de la materia

Asignatura	Créditos	Cuatrim	Carácter	Idioma
Trabajo Fin de Máster	12	2	OB	Bilingüe

Breve descripción de contenidos

Temas comunes a las asignaturas

- Presentación de temas de trabajo
- Normativa y guía práctica para la realización del TFM

Temas específicos de cada asignatura

Cada TFM debe ser original y puede enfocarse de forma distinta y sobre distintos aspectos de la Ciberseguridad, por lo que cada uno ahondará en una temática distinta, contenida o ampliando lo estudiado en las asignaturas impartidas.

Lenguas en que se impartirá la materia

No se aplica

Observaciones

El acto de presentación y defensa del TFM será público y anunciado para general conocimiento con suficiente antelación.

Es requisito para la lectura del Trabajo de Fin de Máster haber superado los 36 créditos ECTS de asignaturas obligatorias (incluyendo los seminarios) y 12 créditos de optativas.

Esta materia culmina el máster y contribuye a desarrollar todas las competencias generales fijadas.

MATERIA 5	
Denominación: Seminarios	
Número de créditos ECTS	**Carácter de la materia (obligatoria/optativa/mixto/trabajo fin de máster/etc.)**
6	Obligatoria

Duración y ubicación temporal dentro del plan de estudios

Primer y Segundo cuatrimestre del curso.

Competencias que el estudiante adquiere con esta materia

CB6, CB7, CB8, CB10, CG1, CG2, CG4, CE3, CE5, CE8

Resultados de aprendizaje que adquiere el estudiante

A la superación de esta materia los estudiantes los estudiantes deberán ser capaces de:

Comprender las nuevas tendencias de las TIC, sus riesgos asociados, así como juzgar la idoneidad para contrarrestarlos de los servicios y mecanismos de seguridad actuales y en desarrollo.

Conocer el marco legal, español, comunitario e internacional en el que desenvuelve la Ciberseguridad, Ciberdefensa y Ciberataque.

Diseñar un modelo integral (legal, físico, administrativo-organizativo y técnico) de protección un (o varios) sistema de información real, operando en un cierto entorno.

Conocer en las actuaciones del Poder Judicial, los Cuerpos de Seguridad y las Fuerzas Armadas en la prevención y persecución de ciberdelincuentes, ciberterroristas y ciberespías y la protección de las infraestructuras críticas.

Actividades formativas de la materia indicando su contenido en horas y % de presencialidad

Código actividad	Horas totales	Horas Presenciales (2)	% presencialidad Estudiante (3)
AF1	30	30	100%
AF2	0	0	0%
AF3	10	10	100%
AF4	0	0	0%
AF5	5	0	0%
AF6	30	5	16,7%
AF7	70	0	0%
AF8	4	4	100%
TOTAL MATERIA	154	49	30%

Metodologías docentes que se utilizarán en esta materia

MD1, MD2, MD4, MD5.

Sistemas de evaluación y calificación. Indicar su ponderación máxima y mínima

Sistemas de evaluación	Ponderación mínima	Ponderación máxima
SE1	0%	10%
SE2	40%	50%
SE3	40%	60%

Asignaturas de la materia

Asignatura	Créditos	Cuatrim	Carácter	Idioma
Seminario 1	3	1	OB	Bilingüe
Seminario 2	3	2	OB	Bilingüe

Breve descripción de contenidos

Dentro del máster se impartirán dos seminarios que tienen la consideración de asignaturas obligatorias de 3 créditos ECTS cada uno, aunque podrán cambiar de año en año, según lo aconseje un campo tan variable como es el de la ciberseguridad. El objetivo es acercar los problemas y soluciones más acuciantes en cada momento de la industria, administración, defensa e investigación a los alumnos. A través de los distintos seminarios que se propongan los alumnos podrán tener acceso a la experiencia de profesionales de reconocido prestigio cuya labor profesional está relacionada con la Ciberseguridad en sus facetas legales, administrativas y de gestión y legales. Por otra parte, los seminarios más académicos pondrán a los alumnos en contacto con el estado de la técnica en conceptos, protocolos, desarrollos y herramientas en temas concretos relacionados con la ciberseguridad. Por tanto los seminarios podrán encuadrarse dentro de cualquiera de las materias del máster.

Lenguas en que se impartirá la materia

Bilingüe: Español e inglés según se explica en el apartado 1.3

Observaciones

6. PERSONAL ACADÉMICO

6.1 Personal académico disponible

A continuación se indica la estructura del profesorado de la Universidad Carlos III de Madrid por categorías, con un mayor detalle del profesorado adscrito a los departamentos universitarios de las áreas implicadas en el desarrollo del Plan de Estudios.

La incorporación de 20 nuevos estudiantes, aumentando así el número de plazas ofertadas de 40 a 60, implicará la creación de un grupo reducido adicional para los laboratorios. Los departamentos implicados cuentan con el personal suficiente para abordar este incremento de plazas.

ESTRUCTURA PROFESORADO DE LA UNIVERSIDAD CARLOS III DE MADRID

CATEGORÍA	NÚMERO
Catedrático de Universidad	149
Profesor titular de universidad	463
Profesor Visitante	164
Contratado doctor	16
Profesor Ayudante doctor	117
Profesor Ayudante	105
Personal investigador en formación	265
Profesor asociado	607
TOTAL	**1.886**

DEPARTAMENTOS PARTICIPANTES EN EL PLAN DE ESTUDIOS

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD	
Departamento de Ingeniería Informática	45%
Departamento de Ingeniería Telemática	45%
Departamento de Tecnología Electrónica	10%
Total de la participación	100,00%

ESTRUCTURA PROFESORADO DE LOS DEPARTAMENTOS PARTICIPANTES EN EL PLAN DE ESTUDIOS

Departamento de Ingeniería Informática:

CATEGORÍA	NÚMERO
Catedrático de Universidad	10
Profesor titular de universidad	41
Profesor Visitante	16
Contratado doctor	1
Profesor Ayudante doctor	7
Profesor Ayudante	4
Personal investigador en formación	10
Profesor asociado	32
TOTAL	**121**

Departamento de Ingeniería Telemática:

CATEGORÍA	NÚMERO
Catedrático de Universidad	4
Profesor titular de universidad	17
Profesor titular de universidad interino	12
Profesor Visitante	9
Contratado doctor	
Profesor Ayudante doctor	1
Profesor Ayudante	2
Personal investigador en formación	6
Profesor asociado	5
TOTAL	**56**

Departamento de Tecnología Electrónica:

CATEGORÍA	NÚMERO
Catedrático de Universidad	5
Profesor titular de universidad	22
Profesor Visitante	
Contratado doctor	
Profesor Ayudante doctor	12
Profesor Ayudante	4
Personal investigador en formación	18
Profesor asociado	29
TOTAL	

PROFESORADO DEDICADO AL TÍTULO			
CATEGORIAS	Total %	Doctores %	Horas dedicación al Título
Catedrático de Universidad	6%	100	20 horas (3,6%)
Profesor titular de universidad	53%	100	300 (54,6%)
Profesor Visitante	18%	100	85 horas (15,5%)
Profesor Ayudante doctor	0%	100	
Profesor Ayudante	18%	30	84 horas (15,3%)
Profesor asociado	6%	100	60 horas (10,9%)

La experiencia docente e investigadora de los profesores es la siguiente:

PROFESORADO POR CATEGORÍAS	VINCULACIÓN*	Nº PROFESORES	TRIENIOS	QUINQUENIOS	SEXENIOS
Catedrático de Universidad	Permanente	2	16	10	5
Profesor titular de universidad	Permanente	12	57	24	18
P T U (Interino)	No permanente	6	21	-	-
Profesor Visitante	No permanente	6	5	-	-
Contratado doctor		0			
Profesor Ayudante doctor	No permanente	0			
Profesor Ayudante	No permanente	6	-	-	-
Personal investigador en formación		0			
Profesor asociado	No permanente	2			
TOTAL		34	100	34	23

***permanente / no permanente**

Departamento de Informática

El Departamento de Informática es uno de los más numerosos de la Universidad Carlos III de Madrid, con más de 80 doctores, 51 de ellos pertenecientes a los cuerpos docentes universitarios. Todos los doctores están comprendidos en 11 grupos de investigación reconocidos como tales por la Universidad. Por consiguiente, el total de líneas de investigación es considerable, habiéndose reseñado sólo unas pocas de cuatro de tales grupos, el último de los cuales es el proponente del título objeto de esta memoria. Una reseña completa de los grupos, sus líneas, proyectos de investigación, etc. se puede consultar en: http://www.inf.uc3m.es/es/investigacion

Departamento de Ingeniería Telemática

El Departamento de Ingeniería Telemática está formado por un equipo consolidado de Doctores e Ingenieros de Telecomunicación e Informática de más de 50 personas, de los que más de 40 son doctores, que se reparten en dos grupos de investigación reconocidos por la Universidad. Este equipo cuenta con un amplio historial de actividad, reconocimiento y experiencia contrastada a nivel nacional e internacional en proyectos de investigación y desarrollo, formación y consultoría. Estas

actividades se realizan para, o en colaboración con, empresas de servicios, fabricantes y administraciones públicas.
Con la filosofía de ofrecer soluciones novedosas basadas en tecnologías punteras en el ámbito de la Telemática hemos desarrollado desde soluciones a problemas concretos de gran complejidad hasta soluciones completas e integrales. Una de las fortalezas de nuestro grupo es que su elevado número de expertos nos permite combinar conocimientos muy especializados, abordar propuestas desde múltiples perspectivas e integrar las tecnologías más eficientes y avanzadas.
En esta línea, venimos manteniendo numerosas colaboraciones y prestando servicios de consultoría técnica y estratégica, coordinación y gestión de grandes proyectos, desarrollo de pilotos de servicios basados en nuevas tecnologías, proyectos de investigación aplicados a productos y servicios innovadores, proyectos de integración de sistemas y desarrollos a medida de software, servicios y aplicaciones, e impartiendo cursos de formación especializada a medida.
Para más información se puede consultar la memoria de investigación desde la página del departamento http://www.it.uc3m.es/investigacion/investigacion.htm.

Departamento de Tecnología Electrónica
El Departamento de Tecnología Electrónica (DTE) de la Universidad Carlos III de Madrid, es muy activo en la investigación básica y aplicada, tal como lo demuestran el número de proyectos de investigación (tanto de tipo europeo como nacional) y publicaciones. El DTE es un departamento que está en continua evolución para lograr la excelencia dentro de una institución joven (apenas 25 años) que contribuye a la mejora de la sociedad ofreciendo una educación de calidad y desarrollando una actividad de investigación avanzada conforme a los exigentes criterios internacionales. Dentro de la plantilla del DTE formada por unas 100 personas, un conjunto de 30 profesores y 20 doctores se dedican a las actividades de investigación. Uno de los objetivos más importante dentro del DTE es crear un ambiente estimulante y de apoyo para la investigación innovadora.

Los profesores y los investigadores del DTE persiguen una amplia gama de temas de investigación organizados en diferentes áreas de colaboración claves (microelectrónica, optoelectrónica, fotónica, electrónica de potencia y tecnologías de identificación) que permiten afrontar proyectos de investigación complejos y aplicaciones para la industria. Una reseña completa de los grupos, sus líneas de investigación, proyectos de investigación, etc. está disponible en: http://www.uc3m.es/portal/page/portal/dpto_tecnologia_electronica/investigacion.

Principales líneas de investigación

Nombre del grupo de investigación	Responsable	Líneas de investigación
DPTO. INFORMÁTICA Computer Security Lab (COSEC)	Arturo Ribagorda	Ciberdefense Data leakage protection Smartphone security Computer Forensic
DPTO. INGENIERÍA TELEMÁTICA GAST: Grupo de Aplicaciones y servicios telemáticos	Carlos Delgado Kloos, Carlos García Rubio, Marisol García Valls, Andrés Marín López, Luis Sánchez Fernández	Computación ubicua: seguridad y movilidad E-Learning Tecnologías Web Tiempo Real

DPTO. INGENIERÍA TELEMÁTICA RYSC: Redes y Servicios de Comunicaciones	Francisco Valera Pintor, Arturo Azcorra Saloña, David Larrabeiti López, María Calderón Pastor	Arquitectura de redes Protocolos de comunicación Servicios distribuidos y diseño de redes IPv6 y protocolos relacionados Servicios y redes móviles Redes programables Conmutación de alto rendimiento Tecnologías Internet Redes MPLS/IP multi-servicio Redes vehiculares Tecnología de Redes Ópticas de Acceso, Metropolitanas y Troncales Seguridad en Redes de Comunicaciones Eficiencia Energética en Sistemas y Redes de Telecomunicación Análisis de Tráfico
DPTO TECNOLOGÍA ELECTRÓNICA Grupo Universitario de Tecnologías de Identificación (GUTI)	Raúl Sánchez Reillo	- Identificación biométrica Mono-modal (iris, huella, geometría de la mano, vascular, firma manuscrita) - Identificación biométrica multimodal - Tarjetas inteligentes y otros dispositivos de identificación - Dispositivos de identificación con tecnología Match-on-Card / Match-on-Token - Seguridad en sistemas de identificación - Evaluación de la seguridad y el rendimiento de sistemas de identificación

El profesorado que impartirá el Máster tiene una intensa actividad de investigación en el área de la seguridad. Sus resultados se publican en los congresos internacionales especializados en el área de la seguridad y en muchas de las revistas indexadas más referenciadas en el ámbito de las TIC, como por ejemplo: Computers and Security, Computer Networks, Computer Communications, Computer Standards & Interfaces, Ad-hoc Networks, IEEE Transactions on Consumer Electronics, Multimedia Tools and Applications, IEEE Transactions on Information Forensics and Security, etc. También en prensa española como la Revista Española de Protección de Datos o Administración Electrónica y Ciudadanos, y también algunas aportaciones técnicas en revistas jurídicas.
A continuación se da una lista de las publicaciones en seguridad en revistas indexadas de los últimos tres años:

1. Publicaciones aceptadas, en prensa
    - G. Suarez-Tangil, E. Palomar, A. Ribagorda, I. Sanz. Providing SIEM Systems with Self-Adaptation. Information Fussion. In press.
    - A. I. González-Tablas Ferreres, A. Alcaide, J. M. de Fuentes, J. Montero. Privacy-preserving and Accountable On-the-road Prosecution of Invalid Vehicular Mandatory Authorizations. In press.
    - A. Alcaide, E. Palomar, J. Montero, A. Ribagorda. Anonymous Authentication for Privacy-preserving IoT Target-driven Applications. Computers and Security Journal. In press.
    - J.E. Tapiador, A Orfila, A. Ribagorda, B. Ramos. Key-Recovery Attacks on KIDS, A Keyed Anomaly Detection System. IEEE Transactions on Dependable and Secure Computing. In press.
    - M. Gil, J.E. Tapiador, J.A. Clark, G. Martinez, A.F. Skarmeta. Trustworthy Placements: Improving Quality and Resilience in Collaborative Attack Detection. Computer Networks. In press.

- G. Suarez, J.E. Tapiador, P. Peris, J. Blasco. Dendroid: A Text Mining Approach to Analyzing and Classifying Code Structures in Android Malware Families. Expert Systems With Applications. In press.
- J.E. Tapiador, J.A. Clark. The Placement-Configuration Problem for Intrusion Detection Nodes in Wireless Sensor Networks. Computers & Electrical Engineering. In press.
- N. Bagheri, M. Safkhani, P. Peris, J.E. Tapiador. Weaknesses in New Ultralightweight RFID Authentication Protocol with Permutation - RAPP. Security and Communication Networks. In press.

2. Publicaciones del 2013

- Florina Almenárez Mendoza, Patricia Arias Cabarcos, Andrés Marín López, Daniel Díaz-Sánchez, Rosa Sánchez-Guerrero. "Overhead of using Secure Wireless Communications in Mobile Computing" . IEEE Transactions on Consumer Electronics, vol.59, no.2, pp.335-342.
- Patricia Arias Cabarcos, Florina Almenárez, Félix Gómez Mármol and Andrés Marín, "To Federate or not To Federate: a reputation-based mechanism to dynamize cooperation in identity management infrastructures", Springer Wireless Personal Communications, "Special Issue on Advances in Trust, Security and Privacy for Wireless Communication Networks".
- N. Bagheri, M. Safkhani, P. Peris, J.E. Tapiador. Comments on "Security Improvement of an RFID Security Protocol of ISO/IEC WD 29167-6". IEEE Communications Letters, 17(4):805-807.
- Daniel Díaz-Sánchez, Florina Almenárez, Andrés Marín, Rosa Sánchez-Guerrero and Patricia Arias, Media Gateway: bringing privacy to Private Multimedia Clouds connections. Telecommunication Systems.
- H. Martin, E. San Millan, P. Peris, J.E. Tapiador. Efficient ASIC Implementation and Analysis of Two EPC-C1G2 RFID Authentication Protocols. IEEE Sensors Journal, 13(10):3537-3547.
- P. Picazo, N. Bagheri, P. Peris, J.E. Tapiador. Two RFID Standard-based Security Protocols for Healthcare Environments. Journal of Medical Systems, 37(5):9962.
- Pablo Picazo-Sanchez, Lara Ortiz-Martin, Pedro Peris-Lopez, Julio César Hernández Castro: Cryptanalysis of the RNTS system. The Journal of Supercomputing 65(2): 949-960.
- Nikolai Stoianov, Manuel Urueña, Marcin Niemiec, Petr Machnik, Gema Maestro "Integrated Security Infrastructures for Law Enforcement Agencies". Multimedia Tools and Applications. June 2013.
- Manuel Urueña, Rubén Cuevas, Ángel Cuevas, Albert Banchs "A Model to Quantify the Success of a Sybil Attack Targeting RELOAD/Chord Resources". IEEE Communication Letters, vol. 17, no. 2, pp. 428-431. Feb. 2013.

3. Publicaciones del 2012

- Patricia Arias Cabarcos, Florina Almenárez Mendoza, Rosa Sánchez-Guerrero, Andres Marín López , Daniel Díaz-Sánchez. "SuSSo: Seamless and Ubiquitous Single Sign-on for Cloud Service Continuity across devices" . IEEE Transactions on Consumer Electronics, vol.58, no.4, pp.1425-1433.
- Patricia Arias, Florina Almenárez Mendoza, Andrés Marín López, Daniel Díaz Sánchez and Rosa Sánchez Guerrero. A metric-based approach to assess risk for "On Cloud" Federated Identity Management. Springer's Journal of Network and Systems

Management, Special Issue on Cloud Computing, Networking, and Service (CCNS) Management. Vol. 20, no.4, pp.513-533.

- D. F. Barrero, J.C. Hernandez, P. Peris, D. Camacho, M.D. Rodriguez. A genetic tango attack against the David-Prasad RFID ultra-lightweight authentication protocol. Expert Systems.
- J. Blasco, J.C. Hernandez-Castro, J.E. Tapiador, A. Ribagorda. Bypassing information leakage protection with trusted applications. Computers & Security. 31(4):557-568.
- J. Blasco, J. C. Hernandez-Castro, J. M. de Fuentes, B. Ramos. A framework for avoiding steganography usage over HTTP. Journal of Network and Computer Applications 35(1):491-501.
- Corujo, D.; Aguiar, Rui L.; Vidal, I.; Garcia-Reinoso, J., "A named data networking flexible framework for management communications," Communications Magazine, IEEE, vol.50, no.12, pp.36,43, December 2012.
- J. M. Estevez, J.C. Hernandez, P. Peris. Online Randomization Strategies to Obfuscate User Behavioral Patterns. Journal of Network and Systems Management 20(4):561-578.
- F. Le Fessant, A. Papadimitriou, A. Carneiro Viana, C. Sengul, E. Palomar. A Sinkhole Resilient Protocol for Wireless Sensor Networks: Performance and Security Analysis. Computer Communications 35(2):234-248.
- J. M De Fuentes, A.I Gonzalez-Tablas, J.Lopez, A. Ribagorda. Towards an automatic enforcement for speeding: enhanced model and intelligent transportation systems realisation. IET intelligent transport systems 6:270-281.
- J. C. Hernandez-Castro, J.E. Tapiador, P. Peris, J.A. Clark, E.-G Talbi. Metaheuristic Traceability Attack against SLMAP, an RFID Lightweight Authentication Protocol. Int. J. Foundations of Computer Science. 23(2):543-553.
- Liu-Jimenez, J.; Sanchez-Reillo, R.; Mengibar-Pozo, L.; Miguel-Hurtado, O.; , "Optimisation of biometric ID tokens by using hardware/software co-design," Biometrics, IET , vol.1, no.3, pp.168-177, Sept. 2012.
- J. Lopez, A.I Gonzalez-Tablas, J.M De Fuentes, B. Ramos. A taxonomy and survey of attacks on digital signatures . Computers and security 67-112.
- E. Palomar, A. Alcaide, A. Ribagorda, Y. zhang. The Peer's Dilemma: A general framework to examine cooperation in pure peer-to-peer systems. Computer networks 56(17):3756-3766.
- E. Palomar, J. de Fuentes, A.I. Gonzalez-Tablas, A. Alcaide. Hindering False Event Dissemination in VANETs with Proof-of-Work Mechanisms. Transportation Research Part C, 23:85-97.
- S. Pastrana, A. Mitrokotsa, A. Orfila, P. Peris. Evaluation of Classification Algorithms for Intrusion Detection in MANETs. Knowledge Based Systems. 36:217-225.
- P. Peris-Lopez, A. Orfila, E. Palomar, J. C. Hernandez-Castro. A Secure Distance-based RFID Identification Protocol with an Off-line Back-end Database. Personal and Ubiquitous Computing 16(3):351-365. Springer London.
- Rosa Sánchez, Florina Almenares, Patricia Arias, Daniel Díaz-Sánchez and Andres Marín. "Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing". IEEE Transactions on Consumer Electronics, vol.58, no.1, pp.95-103.

- Rosa Sánchez-Guerrero, Florina Almenárez, Daniel Díaz-Sánchez, Andres Marín, Patricia Arias and Fabio Sanvido. An Event Driven Hybrid Identity Management Approach to Privacy Enhanced e-Health". Sensors. vol.12, no.5, pp.6129-6154, May 2012.
- Sanchez-Reillo, R., Alonso-Moreno, R., Fernandez-Saavedra, B., Kwon, Y.-B., “Standardised system for automatic remote evaluation of biometric algorithms”, Computer Standards and Interfaces, 34 (5), pp. 413-425, Sept. 2012.
- Manuel Urueña, Alfonso Muñoz, David Larrabeiti. "Analysis of privacy vulnerabilities in Single Sign-On mechanisms for multimedia websites". Multimedia Tools and Applications. DOI: 10.1007/s11042-012-1155-4. July 2012.

4. Publicaciones del 2011

- Florina Almenárez Mendoza, Andrés Marín, Daniel Díaz Sánchez, Alberto Cortés, Celeste Campo, Carlos García-Rubio: Trust management for multimedia P2P applications in autonomic networking. Ad Hoc Networks 9 (4): 687-697.
- Florina Almenárez Mendoza, Patricia Arias, Daniel Díaz Sánchez, Andrés Marín, Rosa Sanchez Guerrero: fedTV: personal networks federation for IdM in mobile DTV. IEEE Trans. Consumer Electronics 57(2): 499-506
- Javier Díez, Marcelo Bagnulo, Francisco Valera and Iván Vidal. “Security for multipath TCP: a constructive approach “. International Journal of Internet Protocol Technology, vol 6, num 3, 146-155, 2011. ISSN 1743-8209
- H. Gascon, A. Orfila, J. Blasco. Analysis of Update Delays in Signature-based Network Intrusion Detection Systems. Computers & Security, 30(8): 613-624.
- M. Naser, P. Peris-Lopez, R. Budiarto, B. Ramos Alvarez. A Note on the Security of PAP. Computer Communications 34(18):2248-2249.
- P. Peris-Lopez, A. Orfila, J. C. Hernandez-Castro, J. C. A. van der Lubbe. Flaws on RFID Grouping-Proofs. Guidelines for Future Sound Protocols. Journal of Network and Computer Applications 34:833-845.
- P. Peris-Lopez, A. Orfila, A. Mitrokotsa, J.C.A. van der Lubbe. A Comprehensive RFID Solution to Enhance Inpatient Medication Safety. International Journal of Medical Informatics 80(1):13-24.
- P. Peris, J.C. Hernandez-Castro, J.E. Tapiador, J.C.A. van der Lubbe. Cryptanalysis of an EPC Class-1 Generation-2 Standard Compliant Authentication Protocol. Engineering Applications of Artificial Intelligence 24(6):1061-1069.
- Davide Proserpio, Daniel Díaz Sánchez, Florina Almenárez Mendoza, Andrés Marín, Rosa Sanchez Guerrero: Achieving IPTV service portability through delegation. IEEE Trans. Consumer Electronics 57(2): 492-498
- A. Ribagorda. Aspectos técnicos de seguridad en la Ley 11/2007 y su Reglamento de desarrollo parcial. Administración electrónica y ciudadanos. Cívitas. Thomson Reuters. España. 2011, pp. 718-742.
- J.E. Tapiador, J.A. Clark. Masquerade Mimicry Attack Detection: A Randomized Approach. Computers & Security 30:297-310.
- J.E. Tapiador, J.A. Clark. Masquerade Mimicry Attack Detection: A Randomized Approach. Computers & Security 30:297-310.

6.2 Otros recursos humanos disponibles

En relación con la cuantificación del porcentaje de dedicación del personal de apoyo a la titulación, existen una serie de servicios centrales de la Universidad de apoyo directo a las titulaciones y a los estudiantes. Cabe sumar el personal de apoyo directo a la gestión académica del Centro, integrado en la Unidad denominada Centro de Postgrado. Se ha efectuado una aproximación de su dedicación a la titulación sobre la base de las siguientes consideraciones:

-Dedicación de los servicios centrales al postgrado. Se ha establecido teniendo en cuenta los porcentajes de alumnos matriculados en grado y postgrado, por lo que la dedicación de los servicios centrales se verá modificada en la medida en que estos porcentajes varíen. Estos son los siguientes: 100 % del Centro de Postgrado, 5% del Servicio Espacio Estudiantes, 5% del Servicio de Relaciones Internacionales, 5% de

-La dedicación del personal de laboratorios a la docencia se estima también en el 80% para el grado y el 20% para el postgrado.

Sobre la base de las anteriores consideraciones se puede establecer la siguiente dedicación del personal de apoyo a esta titulación:

MASTER UNIVERSITARIO EN CIBERSEGURIDAD	Nº personas	% dedicación Postgrado	Personas asignadas POSTGRADO
CENTRO DE POSTGRADO	51	100	51
BIBLIOTECA	77	5	4
SERVICIO DE INFORMÁTICA	63	5	3
ESPACIO ESTUDIANTES	32	5	1
SERVICIO REL. INTERNACIONALES	18	5	2
TÉCNICOS DE LABORATORIOS	43	20	1
SERVICIOS GENERALES CAMPUS	112	5	3
	396		65

En el caso de técnicos de laboratorio se hace referencia al área de audiovisuales, docencia en red, multimedia, etc.

A continuación se recoge el perfil y cualificación profesional del personal de las unidades indicadas anteriormente.

Subunidad	Grupo	Nº Empleados
CENTRO DE POSTGRADO	A1	6
	A2	6
	C1	5
	C2	34
		Suma: 51
SERVICIOS GENERALES CAMPUS	A1	15
	C1	50
	C2	47

		Suma:112
BIBLIOTECA	A1	10
	A2	30
	C1	36
	C2	1
		Suma: 77
LABORATORIOS	A1	3
	A2	8
	C1	32
		Suma: 43
ESPACIO ESTUDIANTES	A1	7
	A2	11
	C1	6
	C2	8
		Suma: 32
SERVICIO DE INFORMATICA	A1	11
	A2	29
	C1	22
	C2	1
		Suma: 63
SERVICIO DE RELACIONES INTERNACIONALES	A1	3
	A2	6
	C1	5
	C2	4
		Suma: 18

Mecanismos para asegurar la igualdad entre hombres y mujeres y la no discriminación de personas con discapacidad

La Universidad Carlos III de Madrid cumple rigurosamente el marco normativo europeo y español sobre igualdad y no discriminación en materia de contratación, acceso al empleo público y provisión de puestos de trabajo, y en particular, de lo previsto en:

-La Ley Orgánica de Universidades 6/2001, de 21 de diciembre, en su redacción modificada por la Ley Orgánica 4/2007 de 12 de abril, que contempla específicamente estos aspectos en:

- El artículo 48.3 respecto al régimen de contratación del profesorado, que debe realizarse conforme a los principios de igualdad, mérito y capacidad.

- El artículo 41.4, respecto de la investigación; esto es que los equipos de investigación deben procurar una carrera profesional equilibrada tanto a hombres como a mujeres. En cumplimiento de esta previsión, el Consejo de Gobierno ha aprobado unas Medidas de apoyo a la investigación para

la igualdad efectiva entre mujeres y hombres en la Universidad Carlos III de Madrid, en la sesión del 12 de julio de 2007.

-Disposición Adicional 24ª, en relación con los principios de igualdad y la no discriminación a las personas con discapacidad.

-El Estatuto Básico del Empleado Público.

-La Ley Orgánica 3/2007, de 22 de marzo, para la igualdad de mujeres y hombres

-La Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.

-El Convenio Colectivo de Personal Docente e Investigador contratado de las Universidades Públicas de la Comunidad de Madrid (artículo 16.2)

-Los Estatutos de la Universidad Carlos III de Madrid (artículo 102.2), que recogen finalmente, el principio de igualdad en materia de contratación de profesorado universitario.

7. RECURSOS MATERIALES Y SERVICIOS

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

Desde su creación, la Universidad Carlos III de Madrid ha impulsado la mejora continua de las infraestructuras necesarias para la docencia y la investigación. En particular, en el ámbito de los servicios de apoyo a las actividades de aprendizaje de los estudiantes, cabe destacar el papel desempeñado por Biblioteca e Informática.

A continuación se indican los espacios generales directamente destinados a la docencia: aulas de clase, aulas informáticas, aulas de grados, y aulas magnas. La Universidad ha mejorado las aulas docentes, dotándolas en su totalidad de PC y un sistema de video proyección fija, que incluye la posibilidad de realizar esta proyección desde PC, DVD y VHS; y conexión a la red de datos, así como pizarras electrónicas en varias aulas y proyectores digitales de transparencias.

La Universidad dispone de más de 1100 PCs en sus aulas informáticas, para tareas de docencia y realización de prácticas y trabajos libres de los alumnos en horario de 9:00 a 21:00 horas, ofreciendo unas 70.000 horas-PC por semana. Existen puestos de trabajo con Windows y con Linux, y algunos con arranque dual Windows/Linux a elección. Desde cada puesto se ofrece acceso libre a Internet, el uso de los programas más habituales de ofimática y el *software* específico de docencia. Está prevista también la creación de aulas más polivalentes con un equipamiento diferente y sistemas para conexión de ordenadores portátiles.

ESPACIOS DOCENTES

ESPACIOS DE TRABAJO	COLMENAREJO		GETAFE		LEGANES		TOTALES	
	Nº	M2	Nº	M2	Nº	M2	Nº s	M2
AULA INFORMATICA	7	542	30	2.268	32	2.576	69	5.386
AULA DE DOCENCIA	21	2.309	122	10.789	72	6.964	215	20.062
AULA MAGNA	1	286	1	413	1	1200	3	1.899
AULA MULTIMEDIA	1	99	3	295	2	181	6	575
SALON DE GRADOS	1	113	1	188	1	65	3	366
Totales	31	3.349	157	13.953	108	10.986	296	28.288

La incorporación de 20 nuevos estudiantes, aumentando así el número de plazas ofertadas de 40 a 60, implicará la creación de un grupo reducido adicional para los laboratorios. La universidad cuenta con los medios materiales necesarios (en concreto, aulas de teoría y prácticas en el campus de Puerta de Toledo).

La Universidad ha asignado un aula con capacidad para 75 alumnos para las clases magistrales y seminarios del Máster en horario de tarde. Para las sesiones de laboratorio/prácticas, se han asignado dos aulas equipadas con ordenadores personales, cada una de ellas con una capacidad de 40 puestos de trabajo. Adicionalmente, el Máster dispone de un entorno virtualizado utilizando software de VMWare en el que los alumnos disponen de un escenario base en el que pueden configurar diferentes elementos como Cortafuegos, SIEMs, servidores, clientes y atacantes. Este entorno es accesible remotamente a través del acceso VPN de la Universidad.

La Universidad cuenta con cuatro bibliotecas en sus diferentes campus, que se configuran como Centros de Recursos para el Aprendizaje y la Investigación (CRAIs) con una alta tecnificación de sus procesos de trabajo y de los servicios ofrecidos y un amplio abanico de recursos electrónicos que ofrece a su comunidad de usuarios, y que se integran perfectamente en un Sistema de Gestión de Aprendizaje (LMS).

Acceso a los servicios de las bibliotecas UC3M: http://www.uc3m.es/portal/page/portal/biblioteca

Bibliotecas	Puestos de lectura	Superficie M2	Puntos consulta de catálogo	Puntos consulta de bases de información	Otros Puntos
B. María Moliner de la Ciencias Sociales y Jurídicas (Getafe)	712	6.500	13	4	67
B. Concepción Arenal de Humanidades, Comunicación y Documentación (Getafe)	80	606	7		15

B. Rey Pastor de Ingeniería (Leganés)	620	9.000	14	4	105
B.Menéndez Pidal (Colmenarejo)	586	4200	16	18	92
Total	1.998	22.304	356		
Nº de alumnos por puesto de lectura	7,17				
WIFI	*Existen en todos los edificios conexiones WIFI				

Como centros de recursos para el aprendizaje, las bibliotecas de la universidad disponen de puestos informáticos y salas de trabajo para los estudiantes.

Conviene resaltar que todos sus edificios, al igual que el resto de instalaciones universitarias, tienen conexión inalámbrica (wi-fi) lo que ha favorecido la puesta en marcha desde el año 2005 del préstamo de portátiles a los alumnos que acuden a la biblioteca y desean una mayor movilidad en sus accesos a Internet. Asimismo, las bibliotecas tienen diversos tipos de recursos audiovisuales (lectores de microfichas, microfilms, CD, DVD, etc.), que incluyen la integración de los centros de recursos para el aprendizaje de idiomas de la Universidad (aula de idiomas).

La UC3M tiene previsto la habilitación de nuevos espacios docentes destinados a másteres en los Campus de Getafe, Leganés y en el Campus Madrid-Puerta de Toledo, y cuyos datos generales incluimos a continuación.

En el Campus de Getafe. Edificio 18, cuya construcción concluirá en el 2.013. Tiene una superficie de 1.800 m2 de aulas y 4.000 m2 destinados a una nueva biblioteca de Humanidades.

En el Campus de Leganés. El edificio Juan Benet II ha entrado en funcionamiento en este campus en el curso 2012-2013. Destinado a postgrado, la construcción dispone de cuatro aulas y un espacio de 600 m2.

Se va a iniciar la construcción de una nueva residencia de estudiantes en el Campus de Getafe con 316 habitaciones especialmente orientada a estudiantes de postgrado e investigadores que realizan estancias en la Universidad, que viene a completar las plazas disponibles actualmente en las residencias universitarias (380 en Getafe, 300 en Leganés y 300 en Colmenarejo).

La Universidad Carlos III de Madrid, a través del Vicerrectorado de Infraestructuras y Medio Ambiente, y apoyándose especialmente en los Servicios de Biblioteca e Informática, ha migrado a una nueva plataforma tecnológica educativa (conocida por el nombre de “Aula Global 2”) como mecanismo de apoyo a la docencia presencial, que permite las siguientes funcionalidades:

- Acceder a los listados del grupo.

- Comunicarse con los alumnos tanto personal como colectivamente.

- Colocar todo tipo de recursos docentes para que sean utilizados por los alumnos.

- Organizar foros de discusión.

- Proponer cuestionarios de autoevaluación a los estudiantes.

- Recoger las prácticas planteadas.

El uso de la anterior plataforma de apoyo docente (Aula Global) a lo largo de los últimos 6 años ha sido muy intenso, tanto por profesores como por alumnos, constituyendo un sólido cimiento del desarrollo los en formación a distancia que esta universidad ha comenzado a emprender recientemente. Así, la Universidad Carlos III de Madrid ha seguido apostando en los últimos años por la teleducación y las nuevas tendencias europeas en el ámbito de TEL *(Technology Enhanced Learning)* para la educación superior, participando activamente en el proyecto ADA-MADRID, en el que se integran las universidades públicas madrileñas. En muchas de las asignaturas diseñadas específicamente para este espacio de aprendizaje, se han ensayado y empleado diversas tecnologías de interés, tales como H.320 (RDSI), H.323 (Videoconferencia sobre IP), herramientas colaborativas, telefonía IP, grabación de vídeo, etc.

Finalmente, se debe señalar que la Universidad puso en marcha hace unos años una serie de actuaciones para la mejora de la accesibilidad de sus instalaciones y servicios, así como recursos específicos para la atención a las necesidades especiales de personas con discapacidad:

- Edificios y urbanización de los Campus: la Universidad consta de un plan de eliminación de barreras (incorporación de mejoras como puertas automáticas, ascensores, rampas, servicios adaptados, etc.), de otro plan de accesibilidad de polideportivos (vestuarios, gradas, entre otros) construcción de nuevos edificios con criterios de accesibilidad, plazas de aparcamiento reservadas para personas con movilidad reducida, etc.

- Equipamientos: mobiliario adaptado para aulas (mesas regulables en altura, sillas ergonómicas, etc.), mostradores con tramo bajo en servicios de información y cafeterías; recursos informáticos específicos disponibles en aulas informáticas y bibliotecas (programas de magnificación y lectura de pantalla para discapacidad visual, impresoras braille, programa de reconocimiento de voz, etc.), ayudas técnicas para aulas y bibliotecas (bucle magnético portátil, equipos de FM o Lupas-TV.)

- Residencias de estudiantes: habitaciones adaptadas para personas con movilidad reducida.

- La Web y la Intranet de la UC3M han mejorado considerablemente en relación a la Accesibilidad Web y los criterios Internacionales de diseño web universal, con el objetivo de asegurar una accesibilidad de nivel “AA”, según las WCAG (W3C/WAI).

- El Proyecto de elaboración de “Plan de Accesibilidad Integral”, que contempla todos los aspectos de los recursos y la vida universitaria:

a) Edificios y urbanización de los Campus: mejoras de accesibilidad física, accesibilidad en la comunicación y señalización (señalizaciones táctiles, facilitadores de orientación, sistemas de aviso, facilitadores audición…)

b) Acceso externo a los Campus: actuaciones coordinadas con entidades locales en urbanización (aceras o semáforos...) y transporte público.

c) Equipamientos: renovación y adquisiciones con criterios de diseño para todos, equipamientos adaptados y cláusulas específicas en contratas.

d) Residencias de Estudiantes: accesibilidad de espacios y equipamientos comunes, mejoras en las habitaciones adaptadas.

e) Sistemas y recursos de comunicación, información y gestión de servicios: mejoras en Web e Intranet, procedimientos, formularios, folletos, guías, mostradores, tablones informativos...

f) Recursos para la docencia y el aprendizaje: materiales didácticos accesibles, adaptación de materiales y recursos para el aprendizaje, ayudas técnicas y apoyo humano especializado

g) Planes de emergencia y evacuación.

h) Sensibilización y conocimiento de la discapacidad en la comunidad universitaria.

Mecanismos para realizar o garantizar la revisión y el mantenimiento de los materiales y servicios disponibles en la Universidad y en las instituciones colaboradoras, así como los mecanismos para su actualización.

El Vicerrectorado de Infraestructuras y Medio Ambiente tiene a su cargo las siguientes áreas competenciales:

-Servicios de Biblioteca e Informática.

-Laboratorios.

-Medio Ambiente.

-Infraestructuras Docentes e Investigadoras.

En el ámbito de la Administración universitaria, además de las competencias específicas del Gerente en algunas de estas áreas, la gestión de los recursos corresponde a los cuatro servicios siguientes:

SERVICIO DE OBRAS Y MANTENIMIENTO.

SERVICIO DE INFORMÁTICA.

SERVICIO DE BIBLIOTECA.

SERVICIO DE PREVENCIÓN DE RIESGOS LABORALES, LABORATORIOS, Y MEDIO AMBIENTE.

Nuestro sistema interno de garantía de calidad recoge el proceso de gestión y mejora de los recursos materiales y servicios, que tiene por objeto definir, planificar y ejecutar las actividades de gestión de los recursos así como posibilitar su mejora continua para adaptarlos a las nuevas necesidades y expectativas. Sus objetivos son:

·Definir las necesidades de los servicios que influyen en la calidad del proceso de enseñanza-aprendizaje de las enseñanzas impartidas

·Definir y diseñar la prestación de nuevos servicios universitarios y actualizar las prestaciones habituales en función de sus resultados.

·Realizar un seguimiento y análisis que sirve a la realización de un informe del Centro así como de los índices de satisfacción, reclamaciones y procesos abiertos relacionados con los mismos, elaborando finalmente propuestas para subsanar debilidades detectadas. Estas propuestas se remiten al Comité de Calidad que elaborará un Plan de Mejoras.

·Informar de los resultados de la gestión de los servicios prestados a los órganos que corresponda y a los distintos grupos de interés.

Los documentos que evidencian los mecanismos de control referidos anteriormente son los siguientes:

- El Presupuesto que incluye los objetivos anuales y plurianuales.
- La Memoria Académica.
- La Memoria económica y de gestión.
- Los planes de mejora.

Se han fijado también los procesos, sus responsables y los principales indicadores.

Existen diferentes Comisiones como elementos de mantenimiento y soporte de las infraestructuras académicas:

- La Comisión Informática como soporte al software docente y al equipamiento informático de los profesores. Este Comité dispone también de una partida presupuestaria contemplada en el Plan Plurianual de Inversiones de la Universidad con el objetivo de garantizar la dotación de infraestructuras y mantenerla en perfecto estado de actualización y uso.

- La Comisión Biblioteca como soporte a los manuales docentes de sala y depósito. Esta Comisión dispone también de una partida presupuestaria contemplada en el Plan Plurianual de Inversiones de la Universidad con el objetivo de garantizar la dotación de los recursos bibliográficos necesarios.

En relación con los protocolos de mantenimiento de los materiales y servicios, así como con los mecanismos de actuación establecidos en la Universidad Carlos III, se recogen a continuación los principales protocolos de mantenimiento de los sistemas eléctricos, de climatización, mobiliario, carpintería y cerrajería y equipamiento audiovisual.

-MANTENIMIENTO DEL SISTEMA ELECTRICO EN GENERAL

Mantenimiento semestral de los **Centros de transformación**, donde se comprueba y verifica:

A) Los sistemas de control y protección.

B) Las estructuras, aisladores y embarrados.

C) La red de tierras.

D) Los elementos de seguridad y emergencia.

E) Seccionadores, Disyuntores, Interruptores o ruptofusibles.

H) Transformadores.

I) Sinópticos y correcta señalización de las maniobras y contactos auxiliares.

Cuadros generales de distribución en baja tensión, con una periodicidad semestral. El protocolo de mantenimiento se ajusta más a lo establecido por el Reglamento de Baja Tensión, (RBT) referente a sobreintensidades, cortocircuitos y defectos de tierra o protección diferencial, así como el aspecto general y la efectividad de los enclavamientos.

Podemos incluir con el mismo nivel de verificación las **baterías de condensadores.**

Además cada dos años se revisara la instalación con una OCA (Entidad colaboradora de la Administración), de acuerdo a lo establecido en el RBT.

Cuadros eléctricos en edificios:

1- MENSUALMENTE, donde aseguramos la operación y buen estado de todos elementos que constituyen los cuadros eléctricos.

2-TRIMESTRALMENTE, donde además se cuida el aspecto general, así como la efectividad de los enclavamientos y se realizan mediciones y reaprietes.

3-SEMESTRAL Y ANUALMENTE, donde se realizaran las acciones ya descritas para los cuadros generales de baja tensión.

Motores eléctricos:

Donde MENSUALMENTE, se comprueba su estado general y se registran sus deficiencias con las medidas a tomar.

TRIMESTRALMENTE, donde además de lo establecido mensualmente, se verifica mediante instrumentos y herramientas su estado eléctrico y mecánico.

SEMESTRAL/ANUAL, donde el motor es enviado al taller para una revisión más especifica (aislamiento, holguras, etc.)

Alumbrado interior y exterior:

Se verifica SEMANALMENTE los puntos de luz para su reparación y/o sustitución.

MENSUALMENTE, donde se comprueba los mecanismos de encendido tanto en local como en remoto, así como la propia soportación,

Y TRIMESTRALMENTE, donde se verifican las tomas de tierra, arrancadores/cebadores como las rejillas y difusores limpiándolos si procede.

-MANTENIMENTO DE SISTEMA DE CLIMATIZACIÓN (REFRIGERACION Y CALEFACCION)

1.-PLANTAS ENFRIADORAS: cada día se verifica visualmente su funcionamiento.

Mensualmente, se revisan todos los parámetros eléctricos y frigoríficos, actuando sobre los cuales presenten alguna deficiencia (niveles, fugas, etc.).

1.2.- TORRES DE REFRIGERACIÓN: cada día se visualiza el funcionamiento correcto y análisis del agua para comprobar la eficacia del biocida.

Mensualmente, se comprueban los elementos mecánicos en giro y transmisiones, así como los elementos de regulación y control (termostato, nivel, etc.)

Semestralmente, se procede a un vaciado y limpieza intensiva y/o reparación de sus elementos (balsa, separadores de gotas, turbinas, etc.)

(*) A los motores eléctricos les será ejecutado su mantenimiento específico.

1.3.- MANTENIMIENTO DE BOMBAS: su funcionamiento se verifica diariamente.

Su estado general se comprueba mensualmente, así como la ausencia de ruidos y calentamientos así como sus elementos de maniobra (válvulas, etc.)

Las vibraciones y el estado de los anclajes son verificados semestral y anualmente.

Cada dos años, la bomba se desmonta y envía al taller donde se revisa, se limpia y se repara los defectos que tenga (juntas, cojinetes, eje, cuerpo).

(*) A los motores eléctricos les será ejecutado su mantenimiento específico.

1.4.- MANTENIMIENTO FAN-COILS, UDS. DE TRATAMIENTO DE AIRE y GRUPOS AUTONOMOS PARTIDOS.

Mensualmente, se limpian las baterías, se revisan y cambian los filtros, correas, sistemas de control, fugas, etc.

Trimestralmente, se cambian filtros, se comprueba el funcionamiento y la regulación de válvulas, así como las temperaturas.

Semestral y anualmente se procede a limpieza química de la batería, revisión elementos mecánicos en giro, antivibratorios, etc.

(*) A los motores eléctricos les será ejecutado su mantenimiento específico.

Complementariamente a este sistema se revisarán mecánicamente los difusores y rejillas de distribución de aire para asegurar una uniformidad en el flujo de aire.

2. CALDERAS: la comprobación del funcionamiento se comprueba visualmente a diario.

Mensualmente, se comprueba su combustión (consumo, CO2, tiro, etc.)

Trimestralmente, se verifican los elementos de regulación y control, y los sistemas de ignición y ventilación, procediéndose a la eliminación de residuos y limpieza.

Los circuitos hidráulicos y de gas se revisan semestralmente, con limpieza.

2.1.- MANTENIMIENTO BOMBAS PRIMARIO/SECUNDARIO: se procede de igual forma que en lo descrito para el punto 1.3.

2.2.- CHIMENEAS, cada 5 años se verifica su estanqueidad y a los 10 años se limpia.

3.-VENTILADORES Y EXTRACTORES

Mensualmente, se comprueba la ausencia de ruidos y calentamientos, así como la transmisión y elementos de regulación y mando.

La verificación de los antivibradores, los anclajes y la soportación es anual.

(*) A los motores eléctricos les será ejecutado su mantenimiento específico.

4.- REDES DE DISTRIBUCION DE AGUA FRIA Y CALIENTE

Anualmente, se revisan las fugas en distribución horizontal, aislamientos, corrosiones y limpieza de filtros, prueba de válvulas y comprobación de aparatos de medida.

5.-GRUPO DE PRESIÓN

La comprobación visual del funcionamiento y giro es semanal.

La revisión de las válvulas, los niveles, los cierres mecánicos, los elementos de presión y flujo, el automatismo secuencial y la prueba en manual son semestrales.

Anualmente, se procede al mismo mantenimiento que las bombas (punto 1.3)

A los cinco años se limpia el depósito de acumulación.

(*) A los motores eléctricos les será ejecutado su mantenimiento específico.

6.-AGUA FRIA, CALIENTE Y SANITARIOS

Trimestralmente, se revisan calentadores, grifos, válvulas, fluxómetros, sanitarios, tanto hidráulicamente como mecánicamente (soportación).

La revisión de las válvulas generales lo que incluye su limpieza y reparación si procede tiene lugar una vez al año.

-MANTENIMIENTO MOBILIARIO, CARPINTERIA Y CERRAJERÍA

Respecto del **Mobiliario** para uso por el profesor y el alumno se hace el siguiente protocolo de mantenimiento.

Una vez a la semana, se procede a identificación y retirada del mobiliario con roturas que lo hagan inservible o peligroso para las personas, reponiendo por otro de similares características.

Mensualmente, se procede a su reparación, acopiando los elementos de repuesto cuando es internamente o envío a talleres exteriores.

Respecto **puertas interiores y exteriores y ventanas** de aulas, se revisa semanalmente su estado, procediendo a la sustitución de elementos móviles, y se repara semestralmente mediante su retirada a taller de otros elementos como junquillos, cristales, bisagras, etc. Su alineación se revisa y corrige una vez al año.

Asimismo con el mantenimiento de pizarras, se verifica su apariencia exterior diariamente, revisándose semestralmente sus elementos móviles, como su nivelación y suportación y la bandejas de tizas.

-MANTENIMIENTO DEL EQUIPAMIENTO AUDIOVISUAL

El equipamiento audiovisual es muy variado e incluye, entre otros: cañones de proyección, con ordenador encastrado en la mesa del profesor, con soporte para audio y video, elementos portátiles como proyectores, televisores, reproductores VHS/DVD, megafonía, etc.; Son dos las revisiones periódicas que se hacen coincidiendo con las vacaciones de verano y Navidad., donde se comprueba el correcto funcionamiento de cada uno de los equipos.

Finalmente, se indican otros servicios auxiliares que complementan el apoyo a la docencia y el mantenimiento de las aulas y otros espacios docentes como pueden ser laboratorios, que solo pasamos a enunciar tales como:

LIMPIEZA INTERIOR DE EDIFICIOS (AULAS Y LOCALES DOCENTES).

LIMPIEZA Y CONSERVACION EXTERIOR EDIFICIOS, JARDINES Y MOBILIARIO URBANO.

VIGILANCIA Y SEGURIDAD.

SISTEMAS DE DETECCION Y CONTRAINCENDIOS.

INSTALACIONES ESPECÍFICAS PARA LABORATORIOS COMO REDES DE AIRE COMPRIMIDO, VAPOR, AGUA CALIENTE, VACIO, ETC.

8. RESULTADOS PREVISTOS

8.1 Valores cuantitativos estimados para los indicadores y su justificación.

La Universidad ha fijado unos objetivos de mejora de estas tasas comunes en todas las titulaciones, por considerar que este objetivo común permite incrementar el nivel de compromiso de los profesores, de los responsables académicos de la titulación, de los Departamentos y de los Centros, así como de la comunidad universitaria en su conjunto, ya que además han sido aprobadas por el Consejo de Gobierno de la Universidad Carlos III de Madrid en su sesión de 7 de febrero de 2008 junto con otra serie de medidas de acompañamiento para la implantación de los nuevos planes de estudio.

	Tasa de graduación	Tasa de Abandono	Tasa de eficiencia
PROPUESTA VERIFICA	**60%**	**20%**	**85%**

Aunque, como se ha indicado, las tasas actuales en estos estudios se consideran satisfactorias, los cambios introducidos en los planes de estudio, y en el modelo de docencia, con clases en grupos reducidos y mecanismos de evaluación continua, así como las adaptaciones realizadas en la normativa de permanencia y matrícula de la Universidad van a permitir mejorarlas y conseguir los objetivos planteados.

Los nuevos planes han ajustado los contenidos 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 y las prácticas profesionales.

Las normas de permanencia y matrícula, aunque han mantenido la orientación reflejada en los Estatutos de la Universidad Carlos III, respecto del número de convocatorias, se ha flexibilizado la necesidad de aprobar el primer curso completo en un número de años determinado y la limitación de la libre dispensa con objeto de introducir la modalidad matrícula a tiempo parcial, con el fin de cubrir las necesidades de los diferentes tipos de estudiantes, y también para permitir a los estudiantes la matrícula a tiempo completo, evitando la demora en sus estudios, ya que antes no siempre podían matricularse de un curso completo cuando tenían asignaturas pendientes.

La experiencia demuestra que la incorporación a la educación continua, compatibilizando las acciones orientadas a la formación permanente en las empresas, que permitan la adquisición y actualización constante de las competencias profesionales, proporciona oportunidades únicas para facilitar o consolidar contactos locales y regionales, diversificar la financiación y así contribuir mejor al desarrollo regional.

Las herramientas de Bolonia, en particular el Marco Europeo de Cualificaciones para el EEES, permiten una oferta más diversa de programas educativos y facilitan el desarrollo de sistemas de reconocimiento del aprendizaje informal adquirido en ocupaciones anteriores.

8.2 Progreso y resultados de aprendizaje

El nuevo modelo de aprendizaje que resulta del plan de estudios planteado y adaptado a las exigencias del Espacio Europeo de Educación Superior, es un aprendizaje con una rica base de información, pero también de conocimiento práctico, de habilidades, de estrategias y vías de resolución de nuevos problemas, de intercambio y estímulo interpersonal.

Para valorar el progreso y los resultados del buen aprendizaje de los estudiantes de la titulación, así entendido, se cuenta con varios instrumentos.

Por un lado, se cuenta con unas encuestas que se realizan cuatrimestralmente a todos los estudiantes, donde valoran, entre otros aspectos, su propio nivel de preparación previo para poder seguir la asignatura de forma adecuada. En ellas también valoran la utilidad de la materia y del método empleado para dicho aprendizaje y comprensión.

Junto a éste, otro instrumento para pulsar los resultados del aprendizaje es el informe-cuestionario que realizarán cuatrimestralmente los profesores sobre sus grupos de docencia, donde indicarán su percepción sobre el nivel de los alumnos, y si han participado en las diferentes actividades propuestas en cada materia.

Por otro lado, resultan esenciales las evaluaciones continuadas y directas del profesor de los conocimientos adquiridos por el estudiante durante el periodo docente, y cuyos sistemas se han detallado en el apartado 5º de esta memoria en cada una de las materias que conforman los planes de estudio.

La universidad tiene establecido un sistema de seguimiento de resultados académicos que se analizan anualmente por las Comisiones Académicas de cada título, que proponen medidas de mejora en los casos en que no se alcancen las tasas mínimas establecidas por la Universidad.

Finalmente se debe resaltar la evaluación del Trabajo Fin de Máster, concebido para que el alumno demuestre las habilidades y conocimientos adquiridos en el Máster de Ciberseguridad. Al tratarse de un Máster Académico, permitirá una profundización práctica bien en desarrollo seguro, bien más orientado a ciberdefensa, pero que formalmente contemplará el panorama completo ofrecido por éste Plan de Estudios y se ajustará a un formato establecido. La evaluación por parte de la(s) comisión(es), nombradas por el Comité de Dirección del Máster se realizará tanto de la parte documental como de la presentación pública y oral por parte del alumno, de acuerdo con la normativa vigente de la Universidad Carlos III de Madrid, y la específica del Máster.

9. SISTEMA DE GARANTÍA DE CALIDAD DEL TÍTULO

La Universidad Carlos III de Madrid ha realizado el diseño de su Sistema de Garantía Interna de Calidad (SGIC- UC3M) conforme a los criterios y directrices proporcionados por la ANECA (Programa AUDIT)

La Universidad ha obtenido la certificación positiva de todos sus centros por la ANECA.

http://www.uc3m.es/portal/page/portal/prog_mejora_calidad

10. CALENDARIO DE IMPLANTACIÓN

10.1 Cronograma de implantación de la titulación

CALENDARIO DE IMPLANTACIÓN	
TITULACIÓN	**CURSO 2014/15**
MASTER UNIVERSITARIO EN CIBERSEGURIDAD	1º

10.2 Procedimiento de adaptación, en su caso, al nuevo plan de estudios por parte de los estudiantes procedentes de la anterior ordenación universitaria.

No es aplicable.

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

No es aplicable.