CENTRO DE FORMACIÓN CONTINUA
UNIVERSIDAD AUTÓNOMA DE MADRID

PROPUESTAS DE CREACION
DE
ESTUDIO PROPIO

NOMBRE DEL ESTUDIO

Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen

No EDICIÓN: 1º

Fecha de inicio edición (mes y año):	Marzo-2015
Fecha de finalización (mes y año):	Febrero-2016

Madrid,…… de …….. de 201

Firma del Director/es

Nota Importante:

Para su entrega y registro en el Centro de Formación Continua, el documento de Solicitud deberá presentarse en soporte papel y electrónico incluyendo:
Información General
Información Académica
Información Económica

1. DESCRIPCIÓN DEL TÍTULO

1.1. Denominación: Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen

1.2. Universidades participantes:

Centro, Departamento o Instituto responsable del Programa:

Instituto de Ciencias Forenses y de la Seguridad (ICFS-UAM)

Director (Doctor en caso de máster):

Álvaro Ortigosa (Escuela Politécnica Superior-UAM)

Subdirector:

Dña. Laura Requena Espada (Instituto de Ciencias Forenses y de la Seguridad-ICFS)

Secretario:

Instituto de Ciencias Forenses y de la Seguridad (ICFS)
Escuela Politécnica Superior (EPS)
C/ Francisco Tomás y Valiente, 11. 28049
Ext. 2620

Comisión responsable:

Álvaro Ortigosa (ICFS-UAM)
Juan de Dios Toledo Martínez (Guardia Civil)
Fernando Fernández Lázaro (CNP)

Datos de contacto e información:

Contacto:
master.analisisevidenciasdigitales@uam.es
91 497 26 20

Dirección:
Ciudad Universitaria de Cantoblanco
C/ Francisco Tomás y Valiente, Escuela Politécnica Superior
28049 MADRID

1.3. Tipo de enseñanza:

Máster Propio de la Universidad Autónoma de Madrid

1.4. Número de plazas ofertadas:

24 plazas

1.5 Número de becas ofrecidas:

Un mínimo de 20% de las matriculas registradas

1.6. Número mínimo de créditos europeos de matrícula por estudiante y Periodo lectivo y, en su caso, normas de permanencia

Número de créditos del título: 60 ECTS

Número mínimo de créditos de matrícula por estudiante y periodo lectivo: 60 ECTS

1.7 Entidades colaboradoras:

Escuela Politécnica Superior
Guardia Civil
Cuerpo Nacional de Policía

1.8 Lugar de Impartición:

Escuela Politécnica Superior

1.9 Precios y plazos

Titulación	Precio por crédito	Precio total	Nº de créditos
Máster	108 €	6.500 €	60

Plazos	Pago

Pago fraccionado	**Si X** **No** ☐
Nº Plazos/ indicar cantidades a pagar	**2**
1er plazo	(50%) 3.250**€**
2do plazo	(50%) 3.250**€**

Fechas de preinscripción	15 de diciembre de 2014 a 13 de febrero 2015
Fechas de matrícula	12 de enero a 27 de febrero de 2015

2. JUSTIFICACIÓN

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

La evolución y desarrollo de las nuevas tecnologías es una constante que obliga a los estados y a las organizaciones a adoptar las medidas e iniciativas necesarias -tanto a nivel funcional y de formación, como a nivel legislativo-para minimizar los riesgos de seguridad derivados de su uso. Desde la perspectiva del delito, el Cibercrimen representa un reto para las Fuerzas y Cuerpos de Seguridad de los Estados que deben adaptar sus conocimientos a un tipo de investigación que requiere de conocimientos técnicos específicos y avanzados. En este contexto, la disciplina de la Informática-forense, permite obtener las pruebas relacionadas con unos hechos investigados en los que existen dispositivos electrónicos involucrados o fueron cometidos a través de Internet.

El Máster propuesto, responde a la necesidad de formación específica que requieren las Fuerzas y Cuerpos de Seguridad del Estado así como cualquier otro profesional que desarrolle su labor en el ámbito de la seguridad y la defensa. En esta dirección, el abordaje del contenido se realizará desde un punto de vista teórico y práctico, para mejorar sus conocimientos en materia de Cibercrimen - con carácter general- prueba electrónica, herramientas forenses disponibles y respecto al correcto tratamiento de la información y los datos de contenido electrónico para asegurar su correcta manipulación durante toda la investigación –de manera específica-.

En este sentido, cabe resaltar que el contexto en el que se desarrolla este máster es el del Centro Nacional de Excelencia (CNEC) de la UAM, habiendo recorrido dos años de formación, certificaciones y proyectos de investigación, para Fuerzas y Cuerpos de Seguridad del Estado, bajo la financiación de la Comisión Europea.

3. OBJETIVOS

3.1 Objetivos

El Máster en Análisis de Evidencias Digitales y lucha contra el cibercrimen tiene como objetivo preparar a las profesionales de la seguridad y la defensa para formarse en materia de análisis de evidencias digitales, evaluación de amenazas, gestión de redes de seguridad y otras funciones de protección IT.

El programa propuesto introduce conceptos, principios y enseña las destrezas y capacidades para aplicar en la práctica profesional en el área de la ciberseguridad.

3.2. Principales Competencias

Competencias básicas:

CG1. Capacidad para analizar y prever los riesgos a los que se enfrentan los dispositivos informáticos.

CG2. Capacidad para analizar y diseñar sistemas de protección ante amenazas digitales.

CG3. Capacidad para adquirir conocimientos y procesar información técnica y científica, utilizando los conocimientos adquiridos como base para poder ser innovadores en el desarrollo y aplicación de ideas.

CG4. Capacidad de reunir e interpretar datos relevantes para emitir juicios, incluso resolviendo problemas en entornos distintos.

CG5. Tener la formación, aptitudes, destrezas y métodos necesarios para la realización de informes en el ámbito de la Ciberseguridad.

Competencias específicas:

- CE01: Adquisición de conocimiento y comprensión de los conceptos básicos relacionados con la Informática Forense y la ciberseguridad.
- CE02: Capacidad para cuestionar planteamientos previos, que pueden ser erróneos o inducidos.
- CE03: Saber cómo detectar y prevenir los principales sesgos en el análisis de información.
- CE04: Conocer y evaluar los diferentes tipos de fuentes de información.
- CE5: Conocer el catálogo de técnicas que pueden ser combinadas para el estudio de casos concretos de evidencias digitales.

- CE6: Conocer y detectar los riesgos ligados a las nuevas tecnologías y la necesidad de establecer estrategias de seguridad al respecto.
- CE7: Dominio de las herramientas que permitan la gestión adecuada de las situaciones de crisis, su control y comunicación.
- CE8: Desarrollar conocimientos sólidos sobre aplicaciones para la gestión de fuentes abiertas, así como la capacidad para valorar las posibilidades, ventajas e inconvenientes de las tecnologías propias.
- CE9: Manejo y dominio de los métodos y técnicas aplicados a la investigación de las ciberamenazas.

4. ACCESO Y ADMISIÓN DE ESTUDIANTES

4.1 Sistemas de información previa a la matriculación y procedimientos accesibles de acogida y orientación de los estudiantes de nuevo ingreso para facilitar su incorporación a la Universidad y la titulación

El Centro Nacional de Excelencia de Ciberseguridad (CNEC) dispone de personal de gestión que ofrece información previa a la matriculación a través de distintos medios a los alumnos que están interesados en cursar el Máster en Análisis de Evidencias Digitales y lucha contra el cibercrimen. Esta labor de información se realiza a partir de los siguientes medios:

1. A través de ***correo electrónico*** ofreciendo una pronta información a los alumnos que solicitan información a través de dicho medio.
2. El ICFS dispondrá de una ***página web*** con toda la información referente a los siguientes aspectos:
   - Relación de la oferta académica del Máster en Análisis de Evidencias Forenses y lucha contra el cibercrimen.
   - Procedimiento y plazos de solicitud de admisión.
   - Procedimiento y plazos de matriculación.
   - Tasas académicas.
   - Relación completa de la documentación que deben presentar los alumnos.
   - Relación de becas de posgrado accesibles desde la UAM y otros organismos nacionales y extranjeros.
   - Normativa y procedimiento para la obtención de la homologación de títulos extranjeros.
   - Información relevante para los alumnos extranjeros que quieren estudiar el máster y no saben a qué lugares dirigirse para encontrar información sobre cualquier cuestión relevante para su estancia en España: alojamiento, procedimientos de renovación de permisos de estudiante y residencia, gastos medios de su estancia en España, residencias o lugares de alojamiento, etc.

3. A través del ***teléfono*** para aquellas personas que quieran ponerse en contacto a través de este medio. El personal de gestión del máster está disponible todas las mañanas de lunes a viernes.

La solicitud de admisión de los alumnos puede realizarse a través del correo electrónico. Una vez comprobado desde la dirección del máster que la documentación presentada es adecuada, se realiza la valoración de las solicitudes que también es revisada por el Centro de Estudios de Posgrado. La comisión directiva responsable del máster es quien valora los méritos y propone la admisión en función de los criterios de admisión y requisitos generales expuestos a continuación.

4.2.1 Requisitos de acceso y condiciones o pruebas de acceso especiales

De acuerdo con el artículo 28 de la Normativa de Enseñanzas Propias y Formación Continua, los requisitos de acceso para el Máster universitario en Análisis de Evidencias Digitales y lucha contra el cibercrimen son los siguientes:

a) Para acceder a los estudios propios de posgrado será necesario estar en posesión de una titulación superior universitaria en ciencias relacionadas con la informática forense: Informática, Telecomunicaciones, principalmente. Asimismo podrán acceder los titulados universitarios conforme a sistemas educativos extranjeros sin necesidad de la homologación de sus títulos, siempre que acrediten un nivel de formación equivalente a los correspondientes títulos universitarios oficiales españoles y que faculten en el país expedidor del título para el acceso a enseñanzas de posgrado.

b) La Comisión de Estudios de Posgrado y Formación Continua examinará el procedimiento de equivalencias de títulos de formación universitaria provenientes de países no integrados en el Espacio Europeo de Educación Superior.

c) La Comisión de Estudios de Posgrado y Formación Continua podrá eximir a candidatos a estudios propios de posgrado del requisito del título correspondiente mediante el análisis de la documentación que acredite una notable experiencia profesional que garantice el logro de las competencias del perfil de acceso en el campo de actividades propias del curso. La Comisión de Estudios de Posgrado y Formación Continua establecerá los criterios que se deberán tener presentes para evaluar la experiencia profesional.

d) La Comisión de Estudios Posgrado y Formación Continua podrá autorizar la admisión a aquellos estudiantes a quienes les falte alguna asignatura para obtener los correspondientes requisitos de acceso con las condiciones que se determinen.

A su vez, el carácter del propio Máster propuesto se dirige especialmente a los miembros de Fuerzas y Cuerpos de Seguridad del Estado español o cualquier otro país, siempre que acredite su posición en el mismo. A su vez está dirigido a cualquier otro profesional que desarrolle su labor en el ámbito de la seguridad y la defensa.

4.2.2 Criterios de Selección:

a. Admisión de estudiantes:

El Máster en el Análisis de Evidencias Digitales y lucha contra el cibercrimen por cuestiones de seguridad se encuentra dirigido a los siguientes colectivos: Guardia Civil, Cuerpo Nacional de Policía, Ertzaintza, Mossos d'squadra, Policías locales, cuerpos militares, Instituciones Penitenciarias, personal de los juzgados, etc. También serán evaluadas las solicitudes de estudiantes extranjeros pertenecientes a organizaciones equivalentes en sus respectivos países. Los alumnos del Máster serán seleccionados por los directores atendiendo a los siguientes criterios:

- Titulación
- Experiencia profesional
- Méritos académicos
- Nivel de inglés

Cabe especificar con respecto a la selección de estudiantes:

i) La preferencia la tendrán los miembros de FCSE y otras organizaciones del área de seguridad del estado, u otros estados.

ii) Además del punto i) podrán realizar el máster personas de organizaciones/empresas que colaboren con FCSE.

iii) En todo caso, el ingreso de personas no pertenecientes a FCSE será sometido a su aprobación.

Admisión de Becarios:

Los alumnos que solicitan becas serán seleccionados en base a los siguientes criterios:

- Curriculum académico y/ o profesional.
- Declaración de la Renta o documento similar.
- Entrevista personal

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

Después del periodo de matrícula se realiza una reunión informativa con los estudiantes para darles la bienvenida y se les presenta a los directores y coordinadores del Máster. En dicho acto también se les informa de los servicios disponibles en la Universidad así como su forma de disfrutarlos.

El personal coordinador del máster desarrolla los mecanismos necesarios para que exista un sistema de apoyo permanente a los estudiantes durante sus estudios a través de los siguientes métodos:

- Atención y tutorías personales ante cuestiones planteadas directamente por parte de los alumnos.

- Responsables de comunicación entre los alumnos y la dirección del máster para asegurar que la comunicación e interacción entre alumnos y el máster es fluida y satisfactoria para los alumnos.
- Reuniones periódicas con los alumnos para informar sobre el desarrollo del curso a los alumnos y recoger las inquietudes o cuestiones relevantes que inquietan o sugieren los alumnos del máster.

Otras oficinas relevantes para los estudiantes una vez matriculados son:
- Oficina de Información y Atención al Estudiante
- Oficina de Relaciones Internacionales
- Oficina de Prácticas

5. PLANIFICACIÓN DE LAS ENSEÑANZAS

5.1. Estructura de las enseñanzas. Explicación general de la planificación del plan de estudios.

El Máster propuesto tiene una duración de un año y se estructura en 60 créditos ECTS de obligado cumplimiento para la obtención del título. La totalidad de los créditos serán cursados *presencialmente* en la Escuela Politécnica Superior de la Universidad Autónoma de Madrid (incluyendo 6 créditos de trabajo fin de Máster).

El horario de impartición del Máster será jueves y viernes en horario de 15.00 a 20.30 horas y los sábados de 9.00 a 14.30 horas, es decir, un total de 15 horas de docencia presencial semanales.

La matriculación se realizará en la UAM y el título será emitido por dicha universidad.

El programa se divide en tres bloques:

Bloque 1. Fundamentos en ciberseguridad
Bloque 2. Métodos y herramientas contra el cibercrimen
Bloque 3. Investigación de ciberamenazas

Cada uno de estos bloques será evaluado por una prueba de conocimientos y de análisis de casos prácticos al finalizar las horas de docencia asignadas.

Bloque 1. Fundamentos en ciberseguridad (10,5 ECTS)

- Módulo 1.1. Fundamentos en ciberseguridad
- Módulo 1.2. Fundamentos en cibercrimen y ciberterrorismo
- Módulo 1.3. Fundamentos de Informática forense

Bloque 2. Métodos y herramientas contra el cibercrimen (26,5 ECTS)

- Módulo 2.1. Análisis de evidencias forenses y sistemas biométricos
- Módulo 2.2. Linux para investigadores
- Módulo 2.3. Scripting

- Módulo 2.4. Investigación forense de datos volátiles - Módulo 2.5. Técnicas computacionales avanzadas para el análisis de datos - Módulo 2.6. Fuentes abiertas - Módulo 2.7. Investigación forense de móviles
Bloque 3. Investigación de ciberamenazas (17 ECTS)
- Módulo 3.1. Redes de comunicaciones - Módulo 3.2. Investigación de VOIP y redes inalámbricas - Módulo 3.3. Hacking y Malware - Módulo 3.4. Crímenes contra menores - Módulo 3.5. Delitos financieros en Internet y lavado de dinero

- **Distribución del plan de estudios en créditos ECTS, por tipo de materia para los títulos propios**

TIPO DE MATERIA	CRÉDITOS
Obligatorias	54 (540 horas)
Optativas ofertadas en el título	**----**
Optativas a cursar por el estudiante	**----**
Prácticas externas	----
Trabajo fin del título	6 (150 horas)
Total Horas de docencia	**540**
Total horas de trabajo del estudiante	**960**
CRÉDITOS TOTALES	**60**

Tabla 1. Resumen de las materias y distribución en créditos ECTS

5.3 Descripción detallada de los módulos o materias de enseñanza-aprendizaje de que consta el plan de estudios

BLOQUE 01: FUNDAMENTOS EN CIBERSEGURIDAD

Denominación: Fundamentos en ciberseguridad
Número de créditos europeos (ECTS): 3 presencial
Carácter (obligatorio/optativo): obligatorio
Unidad Temporal: 1er trimestre
Competencias:

- Capacidad para analizar y prever los riesgos a los que se enfrentan los dispositivos informáticos.

- Adquisición de conocimiento y comprensión de los conceptos básicos relacionados con la Informática Forense y la ciberseguridad.
- Capacidad para cuestionar planteamientos previos, que pueden ser erróneos o inducidos.

Requisitos previos (en su caso):
Actividades formativas y su relación con las competencias:

Docencia presencial	30 horas
Trabajo personal	43 horas
Actividades de evaluación	2 horas
Total	75horas/ 3 créditos

Acciones de coordinación (en su caso):
Sistemas de evaluación y calificación:

La evaluación de esta asignatura se realizará de forma conjunta a todas las asignaturas del bloque I mediante un *examen común tipo test* que tendrá en cuenta los siguientes criterios:

- Asistencia a las sesiones presenciales 20%
- Evaluación teórica a partir de un examen 80%

Breve descripción de los contenidos:
- Fundamentos Jurídicos en Ciberseguridad.
- Seguridad en Tecnologías de la Información y la Comunicación.
- Gestión de la Ciberseguridad.

Profesor/es:

Álvaro Ortigosa (Profesor contratado doctor Escuela Politécnica Superior UAM)
Profesor UAM a determinar
Rafael Pedrera (Centro Nacional para la Protección de Infraestructuras Críticas- CNPIC)
Santiago González (Centro Nacional para la Protección de Infraestructuras Críticas- CNPIC)

Denominación: Fundamentos de cibercrimen y ciberterrorismo
Número de créditos europeos (ECTS): 4,5 presenciales
Carácter (obligatorio/optativo): obligatorio
Unidad Temporal: 1er trimestre
Competencias:
- Capacidad para analizar y prever los riesgos a los que se enfrentan los dispositivos informáticos.
- Adquisición de conocimiento y comprensión de los conceptos básicos relacionados con la Informática Forense y la ciberseguridad.
- Capacidad para cuestionar planteamientos previos, que pueden ser erróneos o inducidos.

Requisitos previos (en su caso):
Actividades formativas y su relación con las competencias:

Docencia presencial	45 horas

Trabajo personal	65,5 horas
Actividades de evaluación	2 horas
Total	112,5horas/ 4,5créditos

Acciones de coordinación (en su caso):
Sistemas de evaluación y calificación:

La evaluación de esta asignatura se realizará de forma conjunta a todas las asignaturas del bloque I mediante un *examen común tipo test* que tendrá en cuenta los siguientes criterios:

- Asistencia a las sesiones presenciales 20%
- Evaluación teórica a partir de un examen 80%

Breve descripción de los contenidos:

- Historia y clasificación.
- Delitos en red: metodologías de Hacking y su historia.
- Introducción al malware: virus, denegación de servicios, Troyanos.
- Robos de identidad: phising, spoofing, pharming y spear phishing.
- Contramedidas: criptografía, honeyspots. Autenticación mutual y parches de seguridad.
- Navegadores seguros.
- Autenticación biométrica.
- El futuro: la expansión de Internet, ingeniería social.

Profesor/es:

Miguel Manzanas (Cuerpo Nacional de Policía)
Arturo Espejo (Guardia Civil)
Tomás Vicente (Cuerpo Nacional de Policía)
David Arroyo (EPS-UAM)

Denominación: Fundamentos de informática forense
Número de créditos europeos (ECTS): 3 presenciales
Carácter (obligatorio/optativo): obligatorio
Unidad Temporal: 1er trimestre
Competencias:

- Capacidad para analizar y prever los riesgos a los que se enfrentan los dispositivos informáticos.
- Adquisición de conocimiento y comprensión de los conceptos básicos relacionados con la Informática Forense y la ciberseguridad.
- Capacidad para cuestionar planteamientos previos, que pueden ser erróneos o inducidos.

Requisitos previos (en su caso):
Actividades formativas y su relación con las competencias:

Docencia presencial	30 horas
Trabajo personal	43 horas
Actividades de evaluación	2 horas
Total	75horas/ 3 créditos

Acciones de coordinación (en su caso):
Sistemas de evaluación y calificación:

La evaluación de esta asignatura se realizará de forma conjunta a todas las asignaturas del bloque I mediante un *examen común tipo test* que tendrá en cuenta los siguientes criterios:

- Asistencia a las sesiones presenciales 20%
- Evaluación teórica a partir de un examen 80%

Breve descripción de los contenidos:

- Aspectos técnicos y legales.
- Herramientas para la estación forense.

Profesor/es:

Javier Pagès (Informática Forense, S.L.)
Alberto Orduna (Guardia Civil)
Francisco Benítez (Cuerpo Nacional de Policía)

BLOQUE 02: MÉTODOS Y HERRAMIENTAS CONTRA EL CIBERCRIMEN

Denominación: Análisis de evidencias forenses y sistemas biométricos
Número de créditos europeos (ECTS): 4,5 presenciales
Carácter (obligatorio/optativo): obligatorio
Unidad Temporal: 1er trimestre
Competencias:

- Capacidad de reunir e interpretar datos relevantes para emitir juicios, incluso resolviendo problemas en entornos distintos.
- Tener la formación, aptitudes, destrezas y métodos necesarios para la realización de informes en el ámbito de la Ciberseguridad

Requisitos previos (en su caso):
Actividades formativas y su relación con las competencias:

Docencia presencial	45 horas
Trabajo personal	65,5 horas
Actividades de evaluación	2 horas
Total	112,5horas/ 4,5créditos

Acciones de coordinación (en su caso):
Sistemas de evaluación y calificación:
La evaluación de esta asignatura se realizará de forma conjunta a todas las asignaturas del bloque II mediante un *examen común tipo test* que tendrá en cuenta los siguientes criterios:

- Asistencia a las sesiones presenciales 20%
- Evaluación teórica a partir de un examen 50%

A su vez el carácter más práctico de esta asignatura supone que se incluya como criterio de evaluación la *resolución de casos prácticos* propuestos por los docentes de

la materia, debiendo entregar una memoria con los resultados obtenidos para su corrección. Esta evaluación supone el 30% de la nota.

Breve descripción de los contenidos:

- Estadística básica y análisis de datos.
- Valoración de evidencias forenses.
- Errores de razonamiento y sesgos cognitivos en la valoración de la evidencia.
- Validación de métodos de valoración de evidencias.
- Informes evaluativos periciales en ciencia forense.
- Sistemas biométricos utilizando diferentes rasgos (huella dactilar, firma manuscrita y escritura, voz, iris, cara, etc.).
- Seguridad en sistemas biométricos.
- Uso de los sistemas biométricos en ciencia forense

Profesor/es:
Javier Ortega (Catedrático UAM)
Joaquín González (Catedrático UAM)
Julían Fiérrez (Profesor titular UAM)
Daniel Ramos (Profesor titular UAM)

Denominación: Linux para el análisis del cibercrimen
Número de créditos europeos (ECTS): 5 presenciales
Carácter (obligatorio/optativo): obligatorio
Unidad Temporal: 1er trimestre
Competencias:

- Capacidad para analizar y diseñar sistemas de protección ante amenazas digitales.
- Conocer el catálogo de técnicas que pueden ser combinadas para el estudio de casos concretos de evidencias digitales.
- Conocer y detectar los riesgos ligados a las nuevas tecnologías y la necesidad de establecer estrategias de seguridad al respecto.

Requisitos previos (en su caso):
Actividades formativas y su relación con las competencias:

Docencia presencial	50 horas
Actividades y casos prácticos a realizar en clase	10 horas
Trabajo personal	63 horas
Actividades de evaluación	2 horas
Total	125 horas/ 5 créditos

Acciones de coordinación (en su caso):
Sistemas de evaluación y calificación:

La evaluación de esta asignatura se realizará de forma conjunta a todas las asignaturas del bloque II mediante un *examen común tipo test* que tendrá en cuenta los siguientes criterios:

- Asistencia a las sesiones presenciales 20%
- Evaluación teórica a partir de un examen 50%

A su vez el carácter más práctico de esta asignatura supone que se incluya como criterio de evaluación la *resolución de casos prácticos* propuestos por los docentes de la materia, debiendo entregar una memoria con los resultados obtenidos para su corrección. Esta evaluación supone el 30% de la nota.

Breve descripción de los contenidos:

- El objetivo es mostrar la utilidad del sistema operativo Linux en la realización de análisis forenses. La mayor parte del curso se dedica a demostrar las técnicas de análisis forense en Linux a través de la investigación de casos reales.
- Linux como plataforma de análisis.

Profesor/es:
David Pérez Martín Esperanza (Cuerpo Nacional de Policía)
Francisco Benítez (Cuerpo Nacional de Policía)

Denominación: Scripting
Número de créditos europeos (ECTS): 5 presenciales
Carácter (obligatorio/optativo): obligatorio
Unidad Temporal: 1er trimestre
Competencias:

- Capacidad para analizar y diseñar sistemas de protección ante amenazas digitales.
- Conocer el catálogo de técnicas que pueden ser combinadas para el estudio de casos concretos de evidencias digitales.
- Conocer y detectar los riesgos ligados a las nuevas tecnologías y la necesidad de establecer estrategias de seguridad al respecto.

Requisitos previos (en su caso):
Actividades formativas y su relación con las competencias:

Docencia presencial	50 horas
Actividades y casos prácticos a realizar en clase	10 horas
Trabajo personal	63 horas
Actividades de evaluación	2 horas
Total	125 horas/ 5 créditos

Acciones de coordinación (en su caso):
Sistemas de evaluación y calificación:
La evaluación de esta asignatura se realizará de forma conjunta a todas las asignaturas del bloque II mediante un *examen común tipo test* que tendrá en cuenta los siguientes criterios:

- Asistencia a las sesiones presenciales 20%
- Evaluación teórica a partir de un examen 50%

A su vez el carácter más práctico de esta asignatura supone que se incluya como criterio de evaluación la *resolución de casos prácticos* propuestos por los docentes de

la materia, debiendo entregar una memoria con los resultados obtenidos para su corrección. Esta evaluación supone el 30% de la nota.

Breve descripción de los contenidos:
- Introducción a programación Python
- Introducción a SQL a través de Python
- Aplicaciones a:
  Test de penetración (PenTesting) con Python
  Investigación forense con Python, incluyendo "data carving"
  Análisis de tráfico de redes con Python.

Profesor/es:
Luis Javier Martín Vallejos (Guardia Civil)

Denominación: Investigación forense de datos volátiles
Número de créditos europeos (ECTS): 3 presenciales
Carácter (obligatorio/optativo): Obligatorio
Unidad Temporal: 1er trimestre
Competencias:
- Capacidad para analizar y diseñar sistemas de protección ante amenazas digitales.
- Conocer el catálogo de técnicas que pueden ser combinadas para el estudio de casos concretos de evidencias digitales.
- Conocer y detectar los riesgos ligados a las nuevas tecnologías y la necesidad de establecer estrategias de seguridad al respecto.
- Dominio de las herramientas que permitan la gestión adecuada de las situaciones de crisis, su control y comunicación.

Requisitos previos (en su caso):
Actividades formativas y su relación con las competencias:

Docencia presencial	30 horas
Actividades y casos prácticos a realizar en clase	5 horas
Trabajo personal	38 horas
Actividades de evaluación	2 horas
Total	75 horas/3 créditos

Acciones de coordinación (en su caso):
Sistemas de evaluación y calificación:
La evaluación de esta asignatura se realizará de forma conjunta a todas las asignaturas del bloque II mediante un *examen común tipo test* que tendrá en cuenta los siguientes criterios:

- Asistencia a las sesiones presenciales 20%
- Evaluación teórica a partir de un examen 50%

A su vez el carácter más práctico de esta asignatura supone que se incluya como criterio de evaluación la *resolución de casos prácticos* propuestos por los docentes de la materia, debiendo entregar una memoria con los resultados obtenidos para su corrección. Esta evaluación supone el 30% de la nota.

Breve descripción de los contenidos:

- Se estudian las herramientas, técnicas y procedimientos para la preservación y análisis de evidencia volátil contenida en la memoria principal (RAM) de un ordenador. El temario incluye:
    - Introducción a la Investigación Forense de Datos Volátiles.
    - El proceso completo de Investigación Forense de Datos Volátiles.
    - Preparación de la búsqueda.
    - Herramientas de adquisición de RAM (hardware y software).
    - Herramientas de análisis de RAM.
    - Herramientas de recogida de información del sistema.
    - Detección de volúmenes encriptados, preservación de la información.
    - Análisis e informe de la información recogida.

Profesor/es:
Alberto Orduna (GC)

Denominación: Técnicas computacionales avanzadas para el análisis de datos
Número de créditos europeos (ECTS): 3 presenciales
Carácter (obligatorio/optativo): Obligatoria
Unidad Temporal: 2º trimestre
Competencias:

- Capacidad para analizar y diseñar sistemas de protección ante amenazas digitales.
- Conocer el catálogo de técnicas que pueden ser combinadas para el estudio de casos concretos de evidencias digitales.
- Conocer y detectar los riesgos ligados a las nuevas tecnologías y la necesidad de establecer estrategias de seguridad al respecto.
- Dominio de las herramientas que permitan la gestión adecuada de las situaciones de crisis, su control y comunicación.

Requisitos previos (en su caso):
Actividades formativas y su relación con las competencias:

Docencia presencial	30 horas
Actividades y casos prácticos a realizar en clase	5 horas
Trabajo personal	38 horas
Actividades de evaluación	2 horas
Total	75 horas/3 créditos

Acciones de coordinación (en su caso):
Sistemas de evaluación y calificación:
La evaluación de esta asignatura se realizará de forma conjunta a todas las asignaturas del bloque II mediante un *examen común tipo test* que tendrá en cuenta los siguientes criterios:

- Asistencia a las sesiones presenciales 20%
- Evaluación teórica a partir de un examen 50%

A su vez el carácter más práctico de esta asignatura supone que se incluya como criterio de evaluación la *resolución de casos prácticos* propuestos por los docentes de la materia, debiendo entregar una memoria con los resultados obtenidos para su corrección. Esta evaluación supone el 30% de la nota.

Breve descripción de los contenidos:

- Data mining for criminal fighting.
- Pattern discovery.
- Data integrity.
- Data exchange and data base interoperability.

Profesor/es:
David Camacho (profesor asociado Escuela Politécnica Superior UAM)

Denominación: Fuentes abiertas
Número de créditos europeos (ECTS): 3 presenciales
Carácter (obligatorio/optativo): obligatorio
Unidad Temporal: 2º trimestre
Competencias:

- Capacidad de reunir e interpretar datos relevantes para emitir juicios, incluso resolviendo problemas en entornos distintos.
- Tener la formación, aptitudes, destrezas y métodos necesarios para la realización de informes en el ámbito de la Ciberseguridad
- Conocer y evaluar los diferentes tipos de fuentes de información.
- Desarrollar conocimientos sólidos sobre aplicaciones para la gestión de fuentes abiertas, así como la capacidad para valorar las posibilidades, ventajas e inconvenientes de las tecnologías propias.

Requisitos previos (en su caso):
Actividades formativas y su relación con las competencias:

Docencia presencial	30 horas
Actividades y casos prácticos a realizar en clase	5 horas
Trabajo personal	38 horas
Actividades de evaluación	2 horas
Total	75 horas/3 créditos

Acciones de coordinación (en su caso):
Sistemas de evaluación y calificación:
La evaluación de esta asignatura se realizará de forma conjunta a todas las asignaturas del bloque II mediante un *examen común tipo test* que tendrá en cuenta los siguientes criterios:

- Asistencia a las sesiones presenciales 20%
- Evaluación teórica a partir de un examen 50%

A su vez el carácter más práctico de esta asignatura supone que se incluya como criterio de evaluación la *resolución de casos prácticos* propuestos por los docentes de la materia, debiendo entregar una memoria con los resultados obtenidos para su corrección. Esta evaluación supone el 30% de la nota.

Breve descripción de los contenidos:

- Introducción a la recogida de fuentes abiertas para el uso en Inteligencia
- Bases de la búsqueda de información
- Realizar búsquedas de información efectivas
- Fiabilidad de los resultados obtenidos
- Temáticas de búsqueda
- Bases de datos on-line y herramientas para la recogida de información de Internet
- Procesamiento de los resultados, análisis y presentación.
- Investigación en Redes sociales

Profesor/es:
Personal Centro Nacional de Inteligencia a determinar
José María Blanco (Guardia Civil)

Denominación: Investigación forense de móviles
Número de créditos europeos (ECTS): 3 presenciales
Carácter (obligato rio/optativo): obligatorio
Unidad Temporal: 2º trimestre
Competencias:

- Capacidad para analizar y diseñar sistemas de protección ante amenazas digitales.
- Conocer el catálogo de técnicas que pueden ser combinadas para el estudio de casos concretos de evidencias digitales.
- Conocer y detectar los riesgos ligados a las nuevas tecnologías y la necesidad de establecer estrategias de seguridad al respecto.
- Dominio de las herramientas que permitan la gestión adecuada de las situaciones de crisis, su control y comunicación.

Requisitos previos (en su caso):
Actividades formativas y su relación con las competencias:

Docencia presencial	30 horas
Actividades y casos prácticos a realizar en clase	5 horas
Trabajo personal	38 horas
Actividades de evaluación	2 horas
Total	75 horas/3 créditos

Acciones de coordinación (en su caso):
Sistemas de evaluación y calificación:
La evaluación de esta asignatura se realizará de forma conjunta a todas las asignaturas del bloque II mediante un *examen común tipo test* que tendrá en cuenta los siguientes criterios:

- Asistencia a las sesiones presenciales 20%
- Evaluación teórica a partir de un examen 50%

A su vez el carácter más práctico de esta asignatura supone que se incluya como criterio de evaluación la *resolución de casos prácticos* propuestos por los docentes de la materia, debiendo entregar una memoria con los resultados obtenidos para su corrección. Esta evaluación supone el 30% de la nota.

Breve descripción de los contenidos:

- Introducción a las redes móviles.
- Análisis de herramientas
- SIM UICC
- El teléfono móvil como evidencia forense
- Desafíos forenses en móviles: iOS, Android, WindowsMobile, Blackberry
- Whatsupp, joyn, line,…
- Desarrollo de aplicaciones para móviles.

Profesor/es:

Daniel Martínez (Guardia Civil)
David Martín (Cuerpo Nacional de Policía)
Manuel Jurado (Cuerpo Nacional de Policía)

BLOQUE 03: INVESTIGACIÓN DE CIBERAMENAZAS

Denominación: Redes de comunicaciones
Número de créditos europeos (ECTS): 3 presenciales
Carácter (obligatorio/optativo): obligatorio
Unidad Temporal: 2º trimestre
Competencias:

- Capacidad para analizar y diseñar sistemas de protección ante amenazas digitales.
- Conocer el catálogo de técnicas que pueden ser combinadas para el estudio de casos concretos de evidencias digitales.
- Conocer y detectar los riesgos ligados a las nuevas tecnologías y la necesidad de establecer estrategias de seguridad al respecto.
- Dominio de las herramientas que permitan la gestión adecuada de las situaciones de crisis, su control y comunicación.

Requisitos previos (en su caso):
Actividades formativas y su relación con las competencias:

Docencia presencial	30 horas
Actividades y casos prácticos a realizar en clase	5 horas
Trabajo personal	38 horas
Actividades de evaluación	2 horas
Total	75 horas/3 créditos

Acciones de coordinación (en su caso):
Sistemas de evaluación y calificación:
La evaluación de esta asignatura se realizará de forma conjunta a todas las asignaturas del bloque III mediante un *examen común tipo test* que tendrá en cuenta los siguientes criterios:

- Asistencia a las sesiones presenciales 20%
- Evaluación teórica a partir de un examen 50%

A su vez el carácter más práctico de esta asignatura supone que se incluya como criterio de evaluación la *resolución de casos prácticos* propuestos por los docentes de la materia, debiendo entregar una memoria con los resultados obtenidos para su corrección. Esta evaluación supone el 30% de la nota.

Breve descripción de los contenidos:

- Tipos de redes, estructura de una red, protocolos de seguridad, certificaciones de seguridad, cómo funciona una red, wireshark,…
- Criptografía
- Análisis de redes
- Análisis forense en el entorno Web.
- Análisis forense de correos electrónicos.

Profesor/es:

Jorge López de Vergara (profesor titular Escuela Politécnica Superior UAM)

Denominación: Hacking y malware
Número de créditos europeos (ECTS): 5 presenciales
Carácter (obligatorio/optativo): obligatorio
Unidad Temporal: 2º trimestre
Competencias:

- Capacidad para analizar y diseñar sistemas de protección ante amenazas digitales.
- Conocer el catálogo de técnicas que pueden ser combinadas para el estudio de casos concretos de evidencias digitales.
- Conocer y detectar los riesgos ligados a las nuevas tecnologías y la necesidad de establecer estrategias de seguridad al respecto.
- Dominio de las herramientas que permitan la gestión adecuada de las situaciones de crisis, su control y comunicación.

Requisitos previos (en su caso):
Actividades formativas y su relación con las competencias:

Docencia presencial	50 horas
Actividades y casos prácticos a realizar en clase	10 horas
Trabajo personal	63 horas
Actividades de evaluación	2 horas
Total	125 horas/ 5 créditos

Acciones de coordinación (en su caso):
Sistemas de evaluación y calificación:
La evaluación de esta asignatura se realizará de forma conjunta a todas las asignaturas del bloque III mediante un *examen común tipo test* que tendrá en cuenta los siguientes criterios:

- Asistencia a las sesiones presenciales 20%
- Evaluación teórica a partir de un examen 50%

A su vez el carácter más práctico de esta asignatura supone que se incluya como criterio de evaluación la *resolución de casos prácticos* propuestos por los docentes de la materia, debiendo entregar una memoria con los resultados obtenidos para su corrección. Esta evaluación supone el 30% de la nota.

Breve descripción de los contenidos:

- Delitos relacionados al *hacking*, tal como los define El Convenio para el Cibercrimen del Consejo de Europa
- Pasos y técnicas para la intrusión informática
- Técnicas de investigación sobre intrusión informática
- Introducción al *malware*
- Modelo de negocio del *malware*
- Introducción al análisis de malware
- Determinación del objetivo de un programa ejecutable desconocido.
- Prevención de intrusiones: amenazas, soluciones, políticas de seguridad, análisis de riesgo, herramientas, control de acceso.

Profesor/es:

Juan de Dios Toledo (Guardia Civil)

Denominación: Investigación de VOIP y redes inalámbricas
Número de créditos europeos (ECTS): 3 presenciales
Carácter (obligatorio/optativo): obligatorio
Unidad Temporal: 2º trimestre
Competencias:

- Capacidad para analizar y diseñar sistemas de protección ante amenazas digitales.
- Conocer el catálogo de técnicas que pueden ser combinadas para el estudio de casos concretos de evidencias digitales.
- Conocer y detectar los riesgos ligados a las nuevas tecnologías y la necesidad de establecer estrategias de seguridad al respecto.
- Dominio de las herramientas que permitan la gestión adecuada de las situaciones de crisis, su control y comunicación.

Requisitos previos (en su caso):
Actividades formativas y su relación con las competencias:

Docencia presencial	30 horas
Actividades y casos prácticos a realizar en clase	5 horas
Trabajo personal	38 horas
Actividades de evaluación	2 horas
Total	75 horas/3 créditos

Acciones de coordinación (en su caso):
Sistemas de evaluación y calificación:
La evaluación de esta asignatura se realizará de forma conjunta a todas las asignaturas del bloque III mediante un *examen común tipo test* que tendrá en cuenta los siguientes criterios:

- Asistencia a las sesiones presenciales 20%
- Evaluación teórica a partir de un examen 50%

A su vez el carácter más práctico de esta asignatura supone que se incluya como criterio de evaluación la *resolución de casos prácticos* propuestos por los docentes de la materia, debiendo entregar una memoria con los resultados obtenidos para su corrección. Esta evaluación supone el 30% de la nota.

Breve descripción de los contenidos:
Las tecnologías de Voz sobre IP (VoIP) y redes inalámbricas, de uso muy frecuente hoy en día, presentan nuevos retos para los investigadores, como por ejemplo la dificultad de identificar y localizar a los usuarios móviles, así como el extendido uso de la tecnología de encriptación. Este módulo cubre el estado del arte de las técnicas de investigación orientadas a superar estos desafíos.
Temario:

- Introducción a la tecnología inalámbrica
- Introducción a la seguridad inalámbrica
- Recogida pasiva de información.
- Recogida activa de información.
- Introducción a VoIP.
- Investigaciones en Skype.

Profesor/es:
Jorge López de Vergara (profesor titular Escuela Politécnica Superior UAM)

Denominación: Crímenes contra menores
Número de créditos europeos (ECTS): 3 presenciales
Carácter (obligatorio/optativo): obligatorio
Unidad Temporal: 2º trimestre
Competencias:

- Resolviendo problemas en entornos distintos.
- Capacidad para cuestionar planteamientos previos, que pueden ser erróneos o inducidos.
- Conocer y detectar los riesgos ligados a las nuevas tecnologías y la necesidad de establecer estrategias de seguridad al respecto.
- Desarrollar conocimientos sólidos sobre aplicaciones para la gestión de fuentes abiertas, así como la capacidad para valorar las posibilidades, ventajas e inconvenientes de las tecnologías propias.

Requisitos previos (en su caso):
Actividades formativas y su relación con las competencias:

Docencia presencial	30 horas
Actividades y casos prácticos a realizar en clase	5 horas
Trabajo personal	38 horas
Actividades de evaluación	2 horas
Total	75 horas/3 créditos

Acciones de coordinación (en su caso):
Sistemas de evaluación y calificación:
La evaluación de esta asignatura se realizará de forma conjunta a todas las asignaturas del bloque III mediante un *examen común tipo test* que tendrá en cuenta los siguientes criterios:

- Asistencia a las sesiones presenciales 20%
- Evaluación teórica a partir de un examen 50%

A su vez el carácter más práctico de esta asignatura supone que se incluya como criterio de evaluación la *resolución de casos prácticos* propuestos por los docentes de la materia, debiendo entregar una memoria con los resultados obtenidos para su corrección. Esta evaluación supone el 30% de la nota.

Breve descripción de los contenidos:

- Explotación Sexual Infantil y cómo es facilitada por Internet.
- Por qué y cómo estos delincuentes usan Internet para obtener, distribuir y crear material sobre Abuso Infantil, cómo los procesos de grooming; recolección de inteligencia, y servicios online de tecnologías usadas para cometer este tipo de crímenes.
- Técnicas para el reconocimiento de víctimas, análisis de fotos y películas.

Profesor/es:

Carlos Igual Garrido (Guardia Civil)
Celia Carreira (Cuerpo Nacional de Policía)

Denominación: Delitos financieros en Internet y de lavado de dinero
Número de créditos europeos (ECTS): 3 presenciales
Carácter (obligatorio/optativo): obligatorio
Unidad Temporal: 2º trimestre
Competencias:

- Resolviendo problemas en entornos distintos.
- Capacidad para cuestionar planteamientos previos, que pueden ser erróneos o inducidos.
- Conocer y detectar los riesgos ligados a las nuevas tecnologías y la necesidad de establecer estrategias de seguridad al respecto.
- Desarrollar conocimientos sólidos sobre aplicaciones para la gestión de fuentes abiertas, así como la capacidad para valorar las posibilidades, ventajas e inconvenientes de las tecnologías propias.

Requisitos previos (en su caso):
Actividades formativas y su relación con las competencias:

Docencia presencial	30 horas
Actividades y casos prácticos a realizar en clase	5 horas
Trabajo personal	38 horas
Actividades de evaluación	2 horas
Total	75 horas/3 créditos

Acciones de coordinación (en su caso):
Sistemas de evaluación y calificación:
La evaluación de esta asignatura se realizará de forma conjunta a todas las asignaturas del bloque III mediante un *examen común tipo test* que tendrá en cuenta los siguientes criterios:

- Asistencia a las sesiones presenciales 20%
- Evaluación teórica a partir de un examen 50%

A su vez el carácter más práctico de esta asignatura supone que se incluya como criterio de evaluación la *resolución de casos prácticos* propuestos por los docentes de la materia, debiendo entregar una memoria con los resultados obtenidos para su corrección. Esta evaluación supone el 30% de la nota.

Breve descripción de los contenidos:

- Métodos y mecanismos para lavar dinero, respuestas legales internacionales a este delito y un análisis detallado sobre las técnicas de investigación y rastreo de fondos ilícitos.
- También se incluye un análisis de inteligencia estructurado, en el contexto del crimen financiero.
- Fraude financiero.

Profesor/es:

David Sanz (Unidad Técnica de Policía Judicial-Guardia Civil)

BLOQUE 4. TRABAJO FINAL DE MÁSTER

En el Trabajo Fin de Máster (6 ECTS/ 150 horas) el estudiante desarrollará un trabajo original realizado individualmente por él, bajo la dirección y supervisión de un tutor. Se trata de un proyecto integral de Análisis de Evidencia Digital de naturaleza profesional. Su desarrollo debe involucrar la articulación de los conocimientos, habilidades y destrezas adquiridos a lo largo de la formación en el máster.
Se fomentará y facilitará la realización del proyecto correspondiente al trabajo de fin de máster en el entorno profesional del estudiante, que requiera la aplicación de los conocimientos y competencias asociados al título y que permita comprobar que el estudiante ha logrado obtener las capacidades necesarias para analizar problemas complejos, diseñar soluciones tecnológicas para dichos problemas, e implementarlas dentro del ámbito de la Ingeniería Informática en el ámbito de las materias propuestas.
El TFM será tutorizado por un profesor del máster. En el caso que el estudiante desarrolle el TFM en su entorno profesional, el trabajo podrá ser tutorizado por una persona externa al máster, en cuyo caso deberá contar con un profesor del máster en el papel de ponente.
La defensa del Trabajo Fin de Máster se realizará una vez aprobadas el resto de asignaturas necesarias para finalizar los estudios de Máster. El Trabajo Fin de Máster será evaluado mediante la elaboración de un informe sobre los resultados del proyecto realizado por el estudiante y su defensa por parte del estudiante ante un tribunal universitario.

6. PERSONAL ACADÉMICO

6.1. Profesorado y otros recursos humanos necesarios y disponibles para llevar a cabo el plan de estudios propuesto. Incluir información sobre su adecuación.

Apellidos	Nombre	Horas presenciales docencia	Centro de procedencia	Créditos de cada profesor	Asignatura a que corresponden los créditos
Pedrera	Rafael	2	CNPIC	0,2	Fundamentos de Ciberseguridad
González	Santiago	2	CNPIC	0,2	Fundamentos de Ciberseguridad
Ortigosa	Álvaro	13	UAM	1,3	Fundamentos de Ciberseguridad
Ariza	María Jesús	13	Derecho UAM	1,3	Fundamentos de Ciberseguridad
Manzanas	Miguel	15	Cuerpo Nacional de Policía	1,5	Fundamentos de cibercrimen y ciberterrorismo
Espejo	Arturo	10	Guardia Civil	1	Fundamentos de cibercrimen y ciberterrorismo
Vicente	Tomás	10	Cuerpo Nacional de Policía	1	Fundamentos de cibercrimen y ciberterrorismo
Arroyo	David	10	Universidad Autónoma de Madrid	1	Fundamentos de cibercrimen y ciberterrorismo
Pàges	Javier	10	Informática Forense S.L.	1	Fundamentos de Informática Forense
Orduna	Alberto	40	Guardia Civil	4	Fundamentos de Informática Forense Investigación forense de datos volátiles
Benítez	Francisco	30	Cuerpo Nacional de Policía	3	Fundamentos de Informática Forense

					Linux para el análisis del cibercrimen
Pérez Martín Esperanza	David	30	Cuerpo Nacional de Policía	3	Linux para el análisis del cibercrimen
López de Vergara	Jorge	60	UAM	6	Redes de comunicaciones
					Investigación de VOIP y redes inalámbricas
Toledo	Juan de Dios	50	Guardia Civil	5	Hacking y Malware
Martín Vallejos	Luis Javier	50	Guardia Civil	5	Scripting
Igual	Carlos	15	Guardia Civil	1,5	Crímenes contra menores
Carreira	Celia	15	Cuerpo Nacional de Policía	1,5	Crímenes contra menores
Pérez	David	20	Cuerpo Nacional de Policía	2	Linux para el análisis del cibercrimen
Camacho	David	30	UAM	3	Técnicas computacionales avanzadas para el análisis de datos
Blanco	José María	15	Guardia Civil	1,5	Fuentes abiertas
Candau	Javier	15	Centro Criptológico Nacional	1,5	Fuentes abiertas
Martínez	Daniel	10	Guardia Civil	1	Investigación forense de móviles
Martín	David	10	Cuerpo Nacional de Policía	1	Investigación forense de móviles
Jurado	Manuel	10	Cuerpo Nacional de Policía	1	Investigación forense de móviles

Ortega	Javier	15	UAM	1,5	Análisis de evidencias forenses y sistemas biométricos
González	Joaquín	10	UAM	1	Análisis de evidencias forenses y sistemas biométricos
Fiérrez	Julián	10	UAM	1	Análisis de evidencias forenses y sistemas biométricos
Ramos	Daniel	10	UAM	1	Análisis de evidencias forenses y sistemas biométricos
Sanz	David	30	UTPJ-GC	3	Delitos financieros en Internet y de lavado de dinero

*Currículum Vitae de los profesores externos

6.2 Recursos Humanos: apoyo administrativo o técnico

7. RECURSOS MATERIALES Y SERVICIOS

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

El máster cuenta con aula en la Escuela Politécnica Superior. La Secretaría administrativa se encuentra en un espacio compartido del Instituto de Ciencias Forenses y de la Seguridad en el edificio C de la Escuela Politécnica Superior de la UAM.

Teléfonos:
Dirección: Ciudad Universitaria de Cantoblanco
C/ Francisco Tomás y Valiente, Escuela Politécnica Superior
28049 MADRID

Secretaría Administrativa: 91 497 26 20

Correo electrónico: master.informaticaforense@uam.es
Página web: www.cnec.es

7.2 Previsión de adquisición de los recursos materiales y servicios necesarios.

8. RESULTADOS PREVISTOS

Valores cuantitativos estimados para los indicadores y su justificación.

TASA DE GRADUACIÓN	**96%**
TASA DE ABANDONO	**4%**
TASA DE EFICIENCIA	**96%**

Introducción de nuevos indicadores (en su caso)

Denominación:
Definición:
Valor:

Justificación de las estimaciones realizadas.

9. SISTEMA DE GARANTÍA DE CALIDAD DEL TÍTULO

POSGRADO

9.1 Responsables del sistema de garantía de calidad del plan de estudios.

9.2 Procedimientos de evaluación y mejora de la calidad de la enseñanza y el profesorado.

9.3 Procedimiento para garantizar la calidad de las prácticas externas y los programas de movilidad.

9.4 Procedimientos de análisis de la inserción laboral de los graduados y de la satisfacción con la formación recibida.

9.5 Procedimiento para el análisis de la satisfacción de los distintos colectivos implicados (estudiantes, personal académico y de administración y servicios, etc.) y de atención a la sugerencias y reclamaciones. Criterios específicos en el caso de extinción del título

10. CALENDARIO DE IMPLANTACIÓN

10.1 Cronograma de implantación de la titulación

El primer curso del Máster en Análisis de Evidencias Digitales y lucha contra las ciberamenazas tiene previsto comenzar en el mes de marzo de 2015 y finalizar en febrero de 2015.

En caso de extinción de un título interior, detallar el procedimiento.

INFORME ECONÓMICO(CREACIÓN, RENOVACIÓN Y FINAL) EDICIÓN : I

Nombre del Estudio

Máster en Análisis de evidencias digitales y lucha contra el cibercrimen

Período de impartición **Inicio:** **01/03/2015** **Finalización:** **26/02/2016**

GASTOS

1. Gestión institucional UAM (15% del total de Ingresos presupuestados. Apartado 4 d **18.525 €**

2. Dirección y coordinación (incluido art. 83 LOU e IRPF)

APELLIDOS	NOMBRE	CARGO/PROCEDENCIA	PRESUPUESTADO	EJECUTADO
Ortigosa	Álvaro	Director del Máster	7.000 €	0 €
Requena Espada	Laura	Sudirectora del Máster	7.000 €	0 €
				0 €
				0 €
TOTAL Euros.....			**14.000 €**	**0 €**

3. Profesorado UAM (incluido art. 83 LOU e IRPF)

APELLIDOS		NOMBRE	HORAS	PRESUPUESTADO	EJECUTADO
Teoría					
López de Vergara		Jorge	60,00	5.400 €	
Arroyo		David	10,00	900 €	
Ortega		Javier	15,00	1.350 €	
Camacho		David	30,00	2.700 €	
González		Joaquín	10,00	900 €	
Ramos		Daniel	10,00	900 €	
Fiérrez		Julián	10,00	900 €	
Ortigosa		Álvaro	13,00	1.170 €	
Ariza		María Jesús	13,00	1.170 €	
Total Profesorado UAM Teoría.			**171,00**	**15390**	**0 €**

4. Profesorado externo (incluido IRPF)

APELLIDOS		NOMBRE	HORAS	PRESUPUESTADO	EJECUTADO
Pedrera		Rafael	2,00	180 €	
González		Santiago	2,00	180 €	
Manzanas		Miguel	15,00	1.350 €	
Espejo		Arturo	10,00	900 €	
Vicente		Tomás	10,00	900 €	
Pàges		Javier	10,00	900 €	
Orduna		Alberto	40,00	3.600 €	
Benítez		Francisco	30,00	2.700 €	
Pérez Martín Esperanza		David	30,00	2.700 €	
Toledo		Juan de Dios	50,00	4.500 €	
Martín Vallejos		Luis Javier	50,00	4.500 €	
Igual		Carlos	15,00	1.350 €	
Carreira		Celia	15,00	1.350 €	
Blanco		José María	15,00	1.350 €	
Candau		Javier	15,00	1.350 €	
Martínez		Daniel	10,00	900 €	
Martín		David	10,00	900 €	
Jurado		Manuel	10,00	900 €	
Sanz		David	30,00	2.700 €	

Total Profesores EXTERNOS	**369,00**	**33.210 €**

5. Personal administrativo UAM (incluido IRPF)

APELLIDOS	NOMBRE	.....	PRESUPUESTADO	EJECUTADO
		.....		0 €
		.....		0 €
				0 €
		.....		0 €
TOTAL Euros.....		.....	**0 €**	**0 €**

6. Personal administrativo externo (incluido IRPF)

APELLIDOS	NOMBRE	PRESUPUESTADO	EJECUTADO
Personal de gestión y administración ICFS (UAM)		18.000 €	0 €
		0 €	0 €
		0 €	0 €
TOTAL Euros.....		**18.000 €**	**0 €**

7. Material Inventariable.

DESCRIPCIÓN	PRESUPUESTADO	EJECUTADO
Equipos y software de tecnologías de la información y comunicación	10.000 €	0 €
	0 €	0 €
	0 €	0 €
TOTAL Euros.....	**10.000 €**	**0 €**

8. Gestión Económica. FGUAM (6%)

	6.299 €	**0 €**

9. Gastos varios

DESCRIPCIÓN	PRESUPUESTADO	EJECUTADO
9.1 Tasa por Expedición de Título	2.700 €	0 €
9.2 Seguro de Accidente	380 €	0 €
9.3 Gastos de Representación, Viajes y Dietas (Inicio / Cierre de Cursos)	2.016 €	0 €
9.4 Reprografía, Publicidad y Difusión (mantenimiento WEB)	3.500 €	0 €
9.5 Material Fungible	2.642 €	0 €
9.6 Otros Gastos (Imprevistos)	470 €	0 €
LOU	2275	
TOTAL Euros.....	**13983**	**0 €**

10. TOTAL GASTOS.

DESCRIPCIÓN	PRESUPUESTADO	EJECUTADO
TOTAL Euros (=total 1+...+total 9)	**123.108 €**	0 €

INGRESOS

1. Tasas.

Número de Alumnos Previstos con sus correspondientes gastos (seguro, títulos, prácticas...): 24

Número de becas a otorgar (20%): 5

Ingresos previstos: Los asociados a 19 Alumnos.

P.V.P. MATRÍCULA	PLAZAS PREVISTAS	BECAS	PRESUPUESTADO	EJECUTADO
6.500 €	24	32.500,00 €	**123.500 €**	0 €

2. Subvenciones, donaciones y otros ingresos.

NOMBRE ENTIDAD	PRESUPUESTADO	EJECUTADO
	0 €	0 €
	0 €	0 €
	0 €	0 €
TOTAL Euros.....	**0 €**	**0 €**

3. REMANENTE EDICIONES ANTERIORES

DESCRIPCIÓN	PRESUPUESTADO	EJECUTADO
	0 €	0 €
	0 €	0 €
TOTAL Euros.....	**0 €**	0 €

4. TOTAL INGRESOS. **0 €**

DESCRIPCIÓN	PRESUPUESTADO	EJECUTADO
TOTAL Euros (=total 1+...+total 3)	**123.500 €**	0 €

BALANCE FINAL

GASTOS		INGRESOS	
PRESUPUESTADO	**EJECUTADO (A)**	**PRESUPUESTADO**	**EJECUTADO (B)**
123.108 €	0 €	**123.500 €**	0 €

Balance INGRESOS - GASTOS (B-A)	**392 €**

OBSERVACIONES

'€ consideran a efectos de que se inscriban un número menor de alumnos a los considerados y se re