Instituto de
Ciencias Forenses y de la Seguridad

Universidad Autónoma de Madrid

MÁSTER EN ANÁLISIS DE EVIDENCIAS DIGITALES Y LUCHA CONTRA EL CIBERCRIMEN

CNEC
CENTRO NACIONAL
EXCELENCIA EN CIBERSEGURIDAD

ICFS Instituto de Ciencias Forenses y de la Seguridad ICFS

PRESENTACIÓN

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, Fuerzas Armadas, 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 en Ciberseguridad (CNEC) de la UAM, habiendo recorrido dos años de formación, certificaciones y proyectos de investigación, para Fuerzas y Cuerpos de Seguridad del Estado, con la financiación de la Comisión Europea.

OBJETIVO

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.

DIRIGIDO A

Para consultar el perfil de acceso, contacte con ciber@icfs.es

CARACTERÍSTICAS DEL TÍTULO

GENERALES

- **Número de Créditos**: 60 ECTS
- **Número de Plazas**: 35
- **Modalidad**: Semipresencial. 15 sábados presenciales a lo largo del curso.
- **Lugar de Impartición**: Aulas de la Universidad Autónoma de Madrid
- **Horario**: las clases presenciales se impartirán un sábado al mes de 8:30 a 20:30
- **Duración**:
  - **Fecha de inicio**: septiembre de 2020.
  - **Finalización**: diciembre de 2021.

ESTRUCTURA

MÓDULO 1: INTRODUCCIÓN. CONCEPTOS BÁSICOS (6 ECTS)

- **Asignatura 1.1.** Introducción I
- **Asignatura 1.2.** Introducción II

MÓDULO 2. FUNDAMENTOS EN CIBERSEGURIDAD (9 ECTS)

- **Asignatura 2.1.** Fundamentos en ciberseguridad, ciberterrorismo y cibercrimen. Criptodivisas y blockchain
- **Asignatura 2.2.** Fundamentos de Informática forense.

MÓDULO 3. MÉTODOS Y HERRAMIENTAS CONTRA EL CIBERCRIMEN (31 ECTS)

- **Asignatura 3.1.** Análisis de evidencias forenses y sistemas biométricos.
- **Asignatura 3.2.** Linux para investigadores. Preparación para Certified Information**.** Systems Security Professional (CISSP)
- **Asignatura 3.3.** Ciberseguridad Industrial.
- **Asignatura 3.4.** Investigación forense de datos volátiles.
- **Asignatura 3.5.** Análisis de datos para la seguridad.
- **Asignatura 3.6.** Redes de comunicaciones. Investigación de VOIP y redes inalámbricas
- **Asignatura 3.7.** Investigación Forenses de móviles
- **Asignatura 3.8.** Seguridad de Internet de las Cosas
- **Asignatura 3.9.** Forense de dispositivos embebidos.

MÓDULO 4. INVESTIGACIÓN DE CIBERAMENAZAS PARA FFCCSE (8 ECTS)

- **Asignatura 4.1.** Fuentes abiertas
- **Asignatura 4.2.** Hacking y Malware

MÓDULO 5: TRABAJO FINAL DE MÁSTER (6 ECTS)

En el Trabajo Fin de Máster (300 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.

ORGANIZACIÓN

CNEC (Centro Nacional de Excelencia en Ciberseguridad) – ICFS (Instituto de Ciencias Forenses y de la Seguridad de la Universidad Autónoma de Madrid)

Dirección del título

- **Álvaro Ortigosa.** Codirector del CNEC, Director del Instituto de Ciencias Forenses y de la Seguridad de la Universidad Autónoma de Madrid y Profesor del Departamento de Ingeniería Informática de la Escuela Politécnica Superior de la UAM.

Codirección del título

- **Luis Fernando Hernández García.** Coronel de la Guardia Civil. Unidad de Ciberseguridad de la Jefatura de Información de la Guardia Civil.

Subdirección del título

- **Óscar Maqueda.** Empresa DISRUPTIVE CONSULTING. Sector IT y Telecomunicaciones. Experiencia en Microsoft, Airtel, Telefónica, y un largo etc. además del sector público, Ministerio del Interior, Justicia y Defensa en diversas etapas.

Coordinación: Personal ICFS (ciber@icfs.es

INSCRIPCIÓN Y MATRICULACIÓN

TASAS

Consultar en el correo ciber@icfs.es

REQUISITOS DE ADMISIÓN

Consultar en el correo ciber@icfs.es

INSCRIPCIÓN

Fechas de inscripción y matrícula de marzo a septiembre de 2020.

INFORMACIÓN Y CONTACTO

Ante cualquier consulta, puede ponerse en contacto con nosotros:

- Email: ciber@icfs.es
- Teléfono: 91 497 61 35
- Dirección: C/ Francisco Tomás y Valiente 11. 28049 Madrid (Edificio C- Escuela Politécnica Superior, despacho 302). Universidad Autónoma de Madrid. Carretera de Colmenar km 15.