A quien va dirigido

El máster va dirigido a titulados en carreras técnicas (informática, ingeniería, ciencias, etc.) o bien profesionales con experiencia (*) mínima de tres años en puestos relacionados con la protección y defensa del software que, en el corto plazo, aspiren a desarrollar funciones propias de CISO o CIO en sus organizaciones.

(*) Aquellos participantes en el programa que no posean un título reconocido por la dirección académica del máster recibirán un certificado reconociendo la finalización con éxito del programa, pero no el título oficial.

Horario / Duración

El máster se impartirá los viernes por la tarde en horario de 16:30 a 21:00 y los sábados por la mañana de 9:30 a 14:00.

Será de tres semestres comenzando el 6 de febrero de 2015 y terminando en Junio de 2016 (60 ECTS).

Dos materias se impartirán de forma intensiva, cada una en una semana y a lo largo de todo el día (aproximadamente 40 horas), por profesores del CERT del SEI de CMU.

Inscripciones

Preinscripción: abierta hasta el 16 de enero de 2015. Los interesados en dicho máster tendrán que preinscribirse en: www.upm.es/atenea

La comunicación de las personas seleccionadas se hará del 1 de diciembre de 2014 hasta el 30 de enero de 2015 vía email. En ese momento se detallará como formalizar la inscripción.

Se valorará la formación y la experiencia en el sector.

Lugar de impartición

Escuela Técnica Superior de Ingenieros
de Sistemas Informáticos
Carretera de Valencia Km 7
28031 Madrid

Para cualquier consulta contactar con:
tomas.sanfeliu@upm.es

Para más información:
www.fi.upm.es/mastergapds

Organiza:

Politécnica — Campus de Excelencia Internacional

Colaboran:

everis an NTT DATA Company · incibe_ Instituto Nacional de Ciberseguridad · CERT · CCN Centro Criptológico Nacional · cisco

Con la participación de

ISMS Forum Spain

Máster en Gestión del Aseguramiento, Protección y Defensa del Software, Operaciones y Sistemas

Autorizado por el CERT del SEI de la Carnegie Mellon University

Anticiparse a la seguridad Ese es nuestro objetivo

Hay una escasez de talentos para hacer frente a la guerra cibernética.

La demanda de empresas y gobiernos supera a la oferta de perfiles profesionales cualificados para resolver los desafíos que plantean las amenazas de seguridad en la red.

Este máster está dirigido específicamente a la seguridad y al funcionamiento correcto de los sistemas software.

Consideramos que en el momento actual es fundamental para el gobierno, industrias y servicios de todo tipo el tener una garantía en la utilización de su software, así como establecer mecanismos de prevención y resistencia a los ataques, y de recuperación y actuación rápida ante emergencias mitigando al máximo o incluso anulando los efectos de los incidentes tanto internos como externos.

Contenido

Los contenidos están organizados en las siguientes materias:

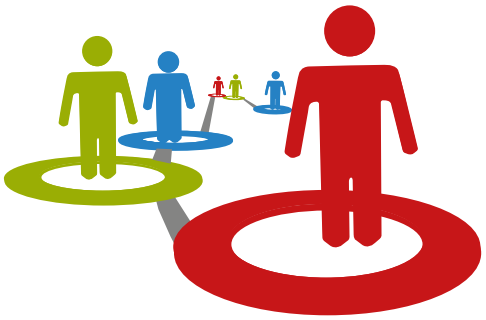
- Evaluación del Aseguramiento (Assurance Assessment, AA).
- Aseguramiento Operativo de Sistemas (System Operational Assurance, SOpA).
- Análisis de Software Seguro (Assured Software Development 1, ASD1).
- Aseguramiento de la Seguridad de Sistemas (System Security Assurance, SSA).
- Diseño de Software Seguro (Assured Software Development 2, ASD2).
- Analíticas de Software Seguro (Assured Software Analytics, ASA).
- Implementación de Software Seguro (Assured Software Development 3, ASD3).
- Gestión del Aseguramiento (Assurance Management, AM).
- Proyecto Fin de Máster (Software Assurance Capstone Experience, SACE).

La materia SACE consistirá en la realización de un proyecto real que recoja todos los conocimientos impartidos.

Resultados esperados

Los graduados tendrán la capacidad de:

- Incorporar tecnologías y métodos de aseguramiento en los procesos del ciclo de vida y en los modelos para el desarrollo de sistemas y para la adquisición de servicios o sistemas.
- Realizar análisis de riesgos y evaluación de alternativas, y priorizar las medidas de seguridad.
- Analizar y validar la eficacia de las operaciones del aseguramiento, y crear evidencias auditables de las medidas de seguridad.
- Realizar casos de negocio para el aseguramiento del software, liderar esfuerzos de aseguramiento, entender estándares, cumplir con regulaciones, planificar la continuidad del negocio, y mantenerse actualizado en las tecnologías de seguridad.
- Incorporar tecnologías y métodos eficaces de seguridad en los sistemas nuevos y existentes.
- Verificar la conformidad de la funcionalidad nueva y existente del sistema de software con los requisitos, y ayudar a revelar contenido malévolo.
- Monitorizar y evaluar la seguridad operacional del sistema, y responder a las nuevas amenazas.



Organizaciones que respaldan este máster

The U.S. Department of Homeland Security (DHS), the National Cyber Security Division (NCSD) encargaron al SEI el diseño del presente máster que se impartirá en la UPM (informática) con la autorización del CERT.

Entidades como INCIBE, CISCO, **everis** e ISMS van a trabajar conjuntamente con la UPM y la Universidad de Carnegie Mellon (CMU) en los contenidos y la definición del máster.

Claustro

El máster será impartido en español (incluidas las materias impartidas por los profesores del CERT/SEI/CMU). Podrán impartirse charlas magistrales; así como desarrollarse actividades complementarias, que en algún caso podrán ser en inglés.

Más de 38 profesores conformará el claustro. Todos ellos miembros de la UPM, Carlos III, UNED, Universidad Rey Juan Carlos, así como especialistas en seguridad del CERT del SEI de la CMU, de INCIBE, de laboratorios acreditados por el CNI/CCN (Applus+ Laboratories, y Epoche and Espri).

También contaremos con profesionales de CISCO, **everis**, Estudio Legal Velázquez, Mapfre e ISMS.

Precios

El precio es de 12.000€ realizándose el pago en cuatro plazos de 3.000€ cada uno.

El primero al realizar la inscripción (tras la aceptación oficial en el máster) y los tres restantes pagos al inicio de cada uno de los tres semestres de duración del máster.