CYBERSECURITY (2018-19)

Código:	Fecha de aprobación:	Precio:
D104	16/02/2019	39,27 1st registration credits
Créditos:	**Título:**	
60	Master (ECTS)	

RAMA
Engineering and Architecture

PLAN
UNIVERSITY MASTER'S DEGREE IN CYBERSECURITY

TIPO DE ENSEÑANZA
Combined Face-to-face and On line

CENTROS DONDE SE IMPARTE
Polytechnic School

ESTUDIO IMPARTIDO CONJUNTAMENTE CON
Solo se imparte en esta universidad

FECHAS DE EXAMEN
Acceda al listado de fechas de examen para esta titulación.

PLAN DE ESTUDIOS OFERTADO EN EL CURSO 2018-19

Leyenda: No ofertada | Sin docencia

UNIVERSITY MASTER'S DEGREE IN CYBERSECURITY

COMPULSORY SUBJECTS — 48 créditos

Curso	Título	Créditos	Subject
1	COMPULSORY	6	49500 - SECURITY MANAGEMENT SYSTEMS
1	COMPULSORY	6	49501 - INFORMATION PROTECTION
1	COMPULSORY	6	49502 - SECURITY IN OPERATING SYSTEMS
1	COMPULSORY	6	49503 - COMMUNICATIONS SECURITY
1	COMPULSORY	6	49504 - SECURITY IN APPLICATIONS AND DATABASES
1	COMPULSORY	6	49505 - DEVELOPMENT OF SECURE APPLICATIONS
1	COMPULSORY	6	49506 - ETHICAL HACKING AND COUNTERMEASURES
1	COMPULSORY	6	49507 - FORENSIC ANALYSIS

MASTER FINAL WORK — 12 créditos

Curso	Título	Créditos	Subject
1	END OF MASTER WORK	12	49508 - FINAL PROJECT

Superado este bloque se obtiene
UNIVERSITY MASTER'S DEGREE IN CYBERSECURITY

COMPETENCIAS

COMPETENCIAS GENERALES

- CG1:Saber aplicar los conocimientos adquiridos a problemas reales relacionados con la ciberseguridad.
- CG2:Ser capaz de trabajar y aprender de forma autodirigida o autónoma.
- CG3:Adaptarse a nuevas situaciones, en entornos nuevos o poco conocidos, fomentando la creatividad, la capacidad crítica y el espíritu emprendedor.
- CG4:Desenvolverse en contextos multidisciplinares y/o internacionales aportando soluciones desde el punto de vista de la ciberseguridad.
- CG5:Conocer y aplicar en cada situación las responsabilidades sociales, éticas y legales vinculadas a la aplicación de los conocimientos.
- CG6:Gestionar la información y los recursos disponibles.
- CG7:Ser capaz de trabajar en equipo con iniciativa y espíritu colaborador.
- CG8:Ser capaz de adaptarse al ambiente cambiante propio de la disciplina y de comprender y aplicar los nuevos avances técnicocientíficos relacionados con la ciberseguridad.
- CG9:Saber proyectar, diseñar, desarrollar, implantar y mantener productos, aplicaciones y servicios relacionados con la ciberseguridad, teniendo en cuenta aspectos técnicos, económicos y de eficiencia.
- CG10:Saber dirigir proyectos relacionados con la ciberseguridad, cumpliendo la normativa vigente y asegurando la calidad del servicio.

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 ESPECÍFICAS

- CE1:Ser capaz de combinar tecnologías de seguridad activa y pasiva para diseñar soluciones integrales.
- CE2:Ser capaz de fortalecer los sistemas operativos implantando medidas de seguridad.
- CE3:Ser capaz de administrar y configurar de manera segura los servicios de Internet.
- CE4:Ser capaz de diseñar arquitecturas de seguridad de sistemas de comunicaciones.
- CE5:Ser capaz de identificar, analizar y evaluar las vulnerabilidades y riesgos de seguridad de las redes, los sistemas informáticos y las aplicaciones.
- CE6:Ser capaz de diseñar y planificar estrategias de protección y defensa de entornos informáticos corporativos, basándose en las tecnologías y herramientas de seguridad informática existentes.
- CE7:Ser capaz de utilizar las herramientas y técnicas de manipulación de dispositivos electrónicos e informáticos para extraer de ellos cualquier evidencia digital, de adoptar las medidas adecuadas para su preservación como prueba legal.
- CE8:Ser capaz de aplicar el método científico en el desarrollo del caso forense digital, conocer los procedimientos y las herramientas de análisis de las pruebas digitales y ser capaz de documentar adecuadamente los hallazgos de la investigación en un informe forense con validez judicial.
- CE9:Ser capaz de integrar distintas primitivas criptográficas para diseñar protocolos de seguridad.
- CE10:Ser capaz de seleccionar y utilizar las diferentes técnicas criptográficas de protección de la información más adecuadas.
- CE11:Ser capaz diseñar y desarrollar aplicaciones que garanticen la privacidad y la seguridad de la información.

- CE12:Ser capaz de diseñar y desarrollar aplicaciones seguras atendiendo a criterios de usabilidad, robustez y eficiencia.
- CE13:Ser capaz de conocer y aplicar los diferentes enfoques y metodologías del desarrollo y auditoría de software seguro.
- CE14:Ser capaz de diseñar el plan de continuidad de negocio y el plan de concienciación y formación en seguridad informática de una organización.
- CE15:Ser capaz de construir un sistema de clasificación de la información de una organización.
- CE16:Ser capaz de diseñar un plan de seguridad de la información.
- CE17:Ser capaz de diseñar, desarrollar, presentar y defender, individualmente ante un tribunal universitario, un trabajo integral de ciberseguridad en el que se sinteticen los conocimientos adquiridos en las enseñanzas.

TRANSVERSAL COMPETENCES

- CT1:Desarrollar competencias en un idioma extranjero a nivel técnico en el ámbito de la ciberseguridad
- CT2:Mostrar competencias informáticas e informacionales en el ámbito de la ciberseguridad.
- CT3:Reunir competencias en comunicación oral y escrita.