MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

PERFIL DEL TITULADO

El Máster Universitario en Ciberseguridad brinda dos perfiles de egresados distintos que se ofrecen mediante dos itinerarios de asignaturas optativas, aunque los alumnos también pueden optar por configurar su propia trayectoria de optatividad:

- Ingeniero de Sistemas Seguros, orientado al diseño y desarrollo de componentes y sistemas donde la seguridad juega un importante papel. Su principal nicho de mercado se halla en los departamentos de creación de software (software factory) y de diseño de arquitecturas.
- Analista de Ciberseguridad, orientado a las organizaciones que necesitan protegerse de las ciberamenazas, y requieren de personal que identifique ataques y debilidades en sus sistemas y redes.

COMPETENCIAS

* 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**

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**

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: Conocer de manera somera los requisitos y el procedimiento de certificación de sistemas seguros.