MASTER UNIVERSITARIO EN CIBERSEGURIDAD M-179

COMPETENCIAS

1. COMPETENCIAS BÁSICAS Y GENERALES

1.1 BÁSICAS

- 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.
- 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.
- 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.
- 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.
- 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.

1.2 GENERALES

- Capacidad para aplicar conocimientos y técnicas de seguridad de la información a la gestión, evaluación, cumplimiento de normativas y diseño de departamentos, programas y proyectos.
- Capacidad para seleccionar y aplicar técnicas, métodos y tecnologías de protección de la información y las comunicaciones en contextos complejos y cambiantes.
- Capacidad para aplicar herramientas a la protección, análisis y evaluación de componentes software, así como para emitir juicios sobre los atributos relacionados con la seguridad de sistemas.
- Capacidad para seleccionar, implantar, desplegar y mantener soluciones de monitorización, defensa e inteligencia en ciberseguridad, combinando diferentes elementos hardware, software y humanos.

2. COMPETENCIAS TRANSVERSALES

- Gestión del tiempo
- Planificación
- Trabajo en equipo
- Resolución de problemas
- Toma de decisiones
- Comunicación verbal
- Comunicación escrita
- Orientación a la calidad

3.COMPETENCIAS ESPECÍFICAS

- Capacidad para aplicar conocimientos a la gestión de equipos, centros y departamentos responsables de la seguridad informática, incluyendo la auditoría de esos sistemas basada en un análisis de riesgos y el establecimiento de políticas.

- Capacidad para razonar y tomar decisiones relativas a la seguridad y la privacidad acordes con el conocimiento de la regulación relevante, nacional e internacional.
- Capacidad para aplicar conocimientos de economía y psicología de la seguridad, incluyendo la ingeniería social y los factores humanos en la ciberseguridad.
- Capacidad para aplicar, escoger y valorar diferentes controles de seguridad, ya sean basados en hardware, software y/o procedimentales.
- Capacidad para aplicar los fundamentos y las técnicas de ingeniería criptográfica a la selección, diseño y evaluación de la seguridad de la información y las comunicaciones.
- Capacidad para diferenciar, seleccionar y desplegar tecnologías y arquitecturas de comunicaciones seguras de acuerdo con los requisitos de usuarios y organizaciones.
- Capacidad para aplicar técnicas avanzadas de ocultación de información sobre diferentes soportes, así como para analizar la presencia de esas informaciones ocultas.
- Capacidad para aplicar técnicas de indagación de vulnerabilidades en el software y en las redes, así como para aplicar contramedidas para esas técnicas.
- Capacidad para analizar software malicioso destinado a la intrusión o exfiltración en sus aspectos estáticos y dinámicos, para componentes individuales o redes complejas.
- Capacidad para aplicar los procesos, métodos y tecnologías del análisis forense digital.
- Capacidad para la selección, configuración y despliegue de componentes y sistemas software de monitorización, agregación de datos, correlación y reacción para la ciberseguridad.
- Capacidad para aplicar técnicas, combinar y analizar datos y seleccionar fuentes de datos para los diferentes aspectos de la ciberinteligencia.
- Capacidad para aplicar técnicas de inteligencia computacional al análisis de datos y al conocimiento situacional en ciberseguridad.
- Capacidad para elaborar un trabajo que aporte una perspectiva nueva sobre una o varias de las diferentes áreas del programa o aplique sus competencias a un problema complejo o innovador, siguiendo estándares profesionales, de planificación y académicos adecuados.
- Capacidad para presentar y defender ante un panel evaluador de perfiles diversos el resultado, conclusiones e implicaciones de un trabajo que pone en práctica las competencias adquiridas en el programa.
- Capacidad para identificar las líneas de actuación que guían la actividad profesional en el sector de la ciberseguridad, y para vincular los contenidos académicos del programa con el ejercicio profesional de la disciplina.
- Capacidad para trabajar de forma efectiva en cooperación con otros profesionales.