

Competencias

Competencias básicas y generales

- » 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.
- » Aplicar los conocimientos adquiridos y ser capaces de resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con el área de la seguridad informática.
- » Integrar conocimientos para formular juicios a partir de determinada información. A la vez, incluir reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios en materia de asesoramiento en seguridad informática.
- » Mantener una actitud que les permita estudiar de manera autónoma y promover la formación continua en su futuro desempeño profesional como experto en seguridad informática.
- » Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarrollarlos mediante los métodos y procesos adecuados.
- » Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de las entidades de TI.

- » Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática.
- » Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes.
- » Tener la capacidad analítica y de resolución para atender a los problemas reales de acuerdo con los valores éticos y sociales y con el máximo respeto a la legalidad vigente.
- » Manejar adecuadamente información relativa al sector de la seguridad informática. Atendiendo a la legislación vigente, notas técnicas, revistas especializadas, Internet, documentos internos de la empresa, etc.

Competencias transversales

- » Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line.
- » Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc.
- » Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento.
- » Capacidad para realizar una enseñanza personalizada adaptada al espacio (aula virtual multicultural y multirracial) a los recursos y a las situaciones y necesidades personales de los alumnos.
- » Capacidad de investigar y comunicar los resultados de la investigación.

Competencias específicas

- » Discernir sobre los distintos entornos de seguridad existentes para poder seleccionar el óptimo siguiendo un razonamiento profesional y completo.
- » Analizar el funcionamiento de herramientas de seguridad y su uso conjugado.
- » Comprender el funcionamiento, características y nivel de riesgo de los servicios de las empresas y establecer mecanismos de protección.
- » Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos.
- » Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada implantación en su infraestructura.
- » Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad.

- » Discernir los distintos mecanismos criptográficos para seleccionar el óptimo en cada ámbito de aplicación.
- » Optimizar las políticas de seguridad de la infraestructura de la red de la entidad.
- » Analizar la infraestructura de red para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas.
- » Diseñar las políticas de recuperación de datos más adecuadas para disminuir el impacto ante desastres.
- » Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones.