Sistemas de Ciberseguridad

Curso Académico: (2020 / 2021) **Fecha de revisión: 23-11-2020**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: PASTRANA PORTILLO, SERGIO

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 1 Cuatrimestre : 1

OBJETIVOS

COMPETENCIAS BÁSICAS

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.

COMPETENCIAS GENERALES

Capacidad para la dirección de obras e instalaciones de sistemas Informáticos, cumpliendo la normativa vigente, asegurando la calidad del servicio.

Capacidad para la elaboración, planificación estratégica, dirección, coordinación y gestión técnica y económica de proyectos en todos los ámbitos de la Ingeniería Informática siguiendo criterios de calidad y medioambientales.

Capacidad para la dirección general, dirección técnica y dirección de proyectos de investigación, desarrollo e innovación, en empresas y centros tecnológicos, en el ámbito de la Ingeniería Informática.

Capacidad para la puesta en marcha, dirección y gestión de procesos de fabricación de equipos informáticos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.

Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, con la capacidad de integrar conocimientos.

Capacidad para comprender la responsabilidad ética y la deontología profesional de la actividad de la profesión de Ingeniero en Informática.

Capacidad para aplicar los principios de economía y de gestión de recursos humanos y proyectos, así como la legislación, regulación y normalización de la Informática.

Capacidad para el aprendizaje continuado, autodirigido y autónomo.

COMPETENCIAS ESPECIFICAS

Capacidad para asegurar, gestionar, auditar y certificar la calidad de los desarrollos, procesos, sistemas, servicios, aplicaciones y productos informáticos.

Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido.

Capacidad para analizar las necesidades de información que se plantean en un entorno y llevar a cabo en todas sus etapas el proceso de construcción de un sistema de información.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1.- Introducción a la ciberseguridad
1.1.- Conceptos básicos

2.- Análisis de redes y sistemas
2.1.- Introducción a las ciberamenazas
2.2.- Vectores de explotación
2.3.- Técnicas de ciberataque

2.4.- Autenticación e identificación

2.- Ciberseguridad en redes
2.1.- Introducción a los sistemas de ciberdefensa
2.2.- Monitorización de eventos
2.3.- Cortafuegos y segmentación de redes
2.4.- Sistemas de detección y prevención de ataques
2.5.- Sistemas de Gestión de Eventos e Información de Seguridad (SIEM)

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

ACTIVIDADES FORMATIVAS
Clase teórica
Clases prácticas
Clases teórico prácticas
Prácticas de laboratorio
Tutorías
Trabajo en grupo
Trabajo individual del estudiante
Exámenes parciales y finales

METODOLOGÍAS DOCENTES
Exposiciones en clase del profesor con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporciona la bibliografía para complementar el aprendizaje de los alumnos.
Lectura crítica de textos recomendados por el profesor de la asignatura:
Artículos de prensa, informes, manuales y/o artículos académicos, bien para su posterior discusión en clase, bien para ampliar y consolidar los conocimientos de la asignatura.
Resolución de casos prácticos, problemas, etc.¿ planteados por el profesor de manera individual o en grupo
Exposición y discusión en clase, bajo la moderación del profesor de temas relacionados con el contenido de la materia, así como de casos prácticos
Elaboración de trabajos e informes de manera individual o en grupo

SISTEMA DE EVALUACIÓN

Evaluación continua:
Prácticas de laboratorios (60%)
Examen final (40%)

Para superar la asignatura será necesario obtener en el examen final al menos un 40% de su peso y que la suma entre la parte de prácticas y examen final supere el 50% del peso total.

Evaluación no continua:
El examen final contendrá al menos un 50% de contenidos relacionados con las prácticas de laboratorio

Para la evaluación extraordinaria, el proceso será el mismo que el descrito anteriormente.

Peso porcentual del Examen Final:	40
Peso porcentual del resto de la evaluación:	60

BIBLIOGRAFÍA BÁSICA

- David Miller Security information and event management (SIEM), McGraw-Hill, 2011

RECURSOS ELECTRÓNICOS BÁSICOS

- Ross Anderson . Security Engineering: https://www.cl.cam.ac.uk/~rja14/book.html