Sistemas de Ciberseguridad

Curso Académico: (2023 / 2024) **Fecha de revisión: 16-05-2023**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: PASTRANA PORTILLO, SERGIO

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 1 Cuatrimestre : 1

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

AF1 - Clase teórica. - [30 horas con un 100% de presencialidad, 1 ECTS]
AF2 - Clases prácticas - [3.33 horas con un 100% de presencialidad, 0.11 ECTS]
AF3 - Clases teórico prácticas - [6 horas con un 100% de presencialidad, 0.20 ECTS]
AF4 - Prácticas de laboratorio - [9 horas con un 100% de presencialidad, 0.30 ECTS]
AF5 - Tutorías - [3 horas con un 25% de presencialidad, 0.10 ECTS]
AF6 - Trabajo en grupo - [40 horas con un 0% de presencialidad, 1.33 ECTS]
AF7 - Trabajo individual del estudiante - [84.66 horas con un 0% de presencialidad, 2.82 ECTS]
AF8 - Exámenes parciales y finales - [4 horas con un 100% de presencialidad, 0.13 ECTS]

METODOLOGIA DOCENTE

MD1 - 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.
MD2 - 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.
MD3 - Resolución de casos prácticos, problemas, etc.... planteados por el profesor de manera individual o en grupo
MD4 - Exposición y discusión en clase, bajo la moderación del profesor de temas relacionados con el contenido de la materia, así como de casos prácticos
MD5 - Elaboración de trabajos e informes de manera individual o en grupo

SISTEMA DE EVALUACIÓN

Evaluación continua:
SE2 [60%] Trabajos y examen individuales realizados durante el curso relacionados con los contenidos teóricos y de los laboratorios

SE3 [40%]
Examen final

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

- National Institute of Standards and Technology (NIST) . Guide to Computer Security Log Management: https://csrc.nist.gov/publications/detail/sp/800-92/final
- Ross Anderson . Security Engineering: https://www.cl.cam.ac.uk/~rja14/book.html