Ciberseguridad de las redes y sistemas ciber-físicos

Curso Académico: (2021 / 2022) **Fecha de revisión: 11-07-2020**

Departamento asignado a la asignatura: Departamento de Ingeniería Telemática

Coordinador/a: LARRABEITI LOPEZ, DAVID

Tipo: Obligatoria Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 1

OBJETIVOS

Competencia 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
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
CG4 Conocimiento y comprensión de los principios de gestión aplicables a entornos productivos y de servicios.
CG5 Capacidad de análisis básicas de los requisitos para el manejo de información y tratamiento de grandes volúmenes de datos.

COMPETENCIAS ESPECIFICAS
CE9 Capacidad para identificar los requisitos de seguridad informática en entornos de industria conectada

RESULTADOS DEL APRENDIZAJE
Como resultados del aprendizaje el alumno será capaz de:
- Configurar los protocolos de transporte seguros,
- Conocer las tecnologías para mitigar amenazas y proteger los datos en sistemas en red.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

- Introducción
- Conceptos de criptografía: cifrado con claves simétricas y pública/privada, autenticación.
- Protocolos de transporte seguros de extremo a extremo: TLS/SSL.
- Amenazas de ciberseguridad en IC4.0: Tipos de Malware. Estructura, Componentes y Vectores de Infección.
- Técnicas y tecnologías para mitigar amenazas: Ataques y contramedidas. Cortafuegos, Sistemas de Detección de Intrusiones y SIEMs.
- Protección de datos en sistemas en red: seguridad en IP. IPsec. VPNs. Seguridad en comunicaciones inalámbricas.

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

ACTIVIDADES FORMATIVAS DEL PLAN DE ESTUDIOS REFERIDAS A MATERIAS
AF1 Clase teórica
AF2 Clases prácticas
AF4 Prácticas de laboratorio
AF5 Tutorías
AF6 Trabajo en grupo

AF7 Trabajo individual del estudiante
AF8 Exámenes parciales y finales

Código actividad	Nº Horas totales	Nº Horas Presenciales	% Presencialidad Estudiante
AF1	36	36	100
AF2	18	18	100
AF4	9	9	100
AF5	6	6	100
AF6	75	0	0
AF7	75	0	0
AF8	6	6	100
TOTAL MATERIA	225	75	33%

METODOLOGÍAS DOCENTES FORMATIVAS DEL PLAN REFERIDAS A MATERIAS

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, 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

SISTEMA DE EVALUACIÓN

SISTEMAS DE EVALUACIÓN DEL PLAN DE ESTUDIOS REFERIDOS A MATERIAS

SE1 Participación en clase
SE2 Trabajos individuales o en grupo realizados durante el curso
SE3 Examen final

Sistemas de evaluación	Ponderación mínima (%)	Ponderación Máxima (%)
SE1	0	20
SE2	20	40
SE3	40	60

Peso porcentual del Examen Final: 60

Peso porcentual del resto de la evaluación: 40

BIBLIOGRAFÍA BÁSICA

- Aditya Gupta The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things, Apress, 2019

- William Stallings Cryptography and Network Security: Principles and Practice. , Prentice Hall, 2013