Ciberseguridad de las redes y sistemas ciber-físicos

Curso Académico: (2024 / 2025) **Fecha de revisión: 17-09-2024**

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

- Aprendizaje de conocimientos básicos sobre ciber-seguridad de sistemas digitales conectados
- Aprendizaje de fundamentos de criptografía simétrica y asimétrica
- Conocimiento de las principales amenazas y herramientas de protección
- Conocimiento de arquitecturas de protección en entornos de industria conectada
- Conocimiento práctico de configuración de seguridad en TLS, WiFi y cortafuegos.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

- Introducción
- Conceptos de criptografía: cifrado con claves simétricas y pública/privada, autenticación. Hashing.
- 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

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

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

SISTEMAS DE EVALUACIÓN DEL PLAN DE ESTUDIOS REFERIDOS A LA MATERIA

SE1 Participación en clase (con peso 0 a 20%)
SE2 Trabajos individuales o en grupo realizados durante el curso
SE3 Examen final

La distribución concreta en esta asignatura es: SE1 0%, SE2 40%, SE3 60%.

Es obligatorio obtener un mínimo de 3 sobre 10 puntos en el examen para aprobar la asignatura.

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

BIBLIOGRAFÍA COMPLEMENTARIA

- Ian Neil CompTIA Security+ SY0-701 Certification Guide - Third Edition, Packt Publishing, O'Reilly, 2024