Guía docente
230617 - NS - Seguridad de Red

Última modificación: 26/05/2023

Unidad responsable: Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona
Unidad que imparte: 744 - ENTEL - Departamento de Ingeniería Telemática.

Titulación: MÁSTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIÓN (Plan 2013). (Asignatura optativa).
MÁSTER UNIVERSITARIO EN TECNOLOGÍAS AVANZADAS DE TELECOMUNICACIÓN (Plan 2019). (Asignatura optativa).
MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD (Plan 2020). (Asignatura obligatoria).

Curso: 2023 **Créditos ECTS:** 5.0 **Idiomas:** Inglés

PROFESORADO

Profesorado responsable: Consultar aquí / See here:
https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/responsables-assignatura

Otros: Consultar aquí / See here:
https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/professorat-assignat-idioma

CAPACIDADES PREVIAS

Debe tenerse conocimientos básicos de Redes IP y administración básica de sistema operativo Linux.
Se recomienda nociones previas de criptografía

COMPETENCIAS DE LA TITULACIÓN A LAS QUE CONTRIBUYE LA ASIGNATURA

Específicas:
1. Capacidad para modelar, diseñar, implantar, gestionar, operar, administrar y mantener redes, servicios y contenidos.
2. Capacidad para realizar la planificación, toma de decisiones y empaquetamiento de redes, servicios y aplicaciones considerando la calidad de servicio, los costes directos y de operación, el plan de implantación, supervisión, los procedimientos de seguridad, el escalado y el mantenimiento, así como gestionar y asegurar la calidad en el proceso de desarrollo.
3. Capacidad de comprender y saber aplicar el funcionamiento y organización de Internet, las tecnologías y protocolos de Internet de nueva generación, los modelos de componentes, software intermediario y servicios.

Transversales:
4. TRABAJO EN EQUIPO: Ser capaz de trabajar como miembro de un equipo interdisciplinar, ya sea como un miembro más o realizando tareas de dirección, con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos teniendo en cuenta los recursos disponibles.

5. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información en el ámbito de especialidad, y valorar de forma crítica los resultados de dicha gestión.

6. TERCERA LENGUA: Conocer una tercera lengua, preferentemente el inglés, con un nivel adecuado oral y escrito y en consonancia con las necesidades que tendrán los titulados y tituladas.

METODOLOGÍAS DOCENTES

Clase magistral 1h a la semana
Prácticas en laboratorio (2h/s)

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

HORAS TOTALES DE DEDICACIÓN DEL ESTUDIANTADO

Tipo	Horas	Porcentaje
Horas aprendizaje autónomo	86,0	68.80
Horas grupo grande	19,5	15.60
Horas grupo pequeño	19,5	15.60

Dedicación total: 125 h

CONTENIDOS

(CAST) 1. Introduction

Dedicación: 8h
Grupo grande/Teoría: 2h
Aprendizaje autónomo: 6h

(CAST) 2. Authentication, authorization and accounting (AAA)

Dedicación: 21h
Grupo grande/Teoría: 4h
Grupo pequeño/Laboratorio: 3h
Aprendizaje autónomo: 14h

(CAST) 3. Perimeter Security

Dedicación: 26h
Grupo grande/Teoría: 6h
Grupo pequeño/Laboratorio: 2h
Aprendizaje autónomo: 18h

(CAST) 4. LAN protection

Dedicación: 14h
Grupo grande/Teoría: 2h
Grupo pequeño/Laboratorio: 2h
Aprendizaje autónomo: 10h

(CAST) 5. Virtual Private Networks VPNs

Dedicación: 18h
Grupo grande/Teoría: 4h
Grupo pequeño/Laboratorio: 2h
Aprendizaje autónomo: 12h

(CAST) 6. Manage a secure network

Dedicación: 18h
Grupo grande/Teoría: 4h
Grupo pequeño/Laboratorio: 2h
Aprendizaje autónomo: 12h

(CAST) 7. Network Forensics

Dedicación: 20h
Grupo grande/Teoría: 4h
Grupo pequeño/Laboratorio: 2h
Aprendizaje autónomo: 14h

ACTIVIDADES

(CAST) LABORATORY

(CAST) EXERCISES

(CAST) ORAL PRESENTATION

(CAST) SHORT ANSWER TEST (CONTROL)

(CAST) SHORT ANSWER TEST (TEST)

(CAST) EXTENDED ANSWER TEST (FINAL EXAMINATION)

SISTEMA DE CALIFICACIÓN

Control parcial: 30%
Examen final: 40%
Asistencia y participación en clase: 10%
Trabajos: 20%

NORMAS PARA LA REALIZACIÓN DE LAS PRUEBAS.

Los grupos en el laboratorio son de 4 personas (5 máximo)
Se necesita 2 portátiles por grupo

BIBLIOGRAFÍA

Básica:
- Anderson, R.J. Security engineering : a guide to building dependable distributed systems [en línea]. 3rd ed. Indianapolis, Indiana: John Wiley & Sons, Inc., 2020 [Consulta: 25/01/2021]. Disponible a: https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?docID=6412239. ISBN 9781119642831.

Complementaria:
- Bosworth, S.; Kabay, M.E.; Whyne, E. Computer security handbook [en línea]. 5th ed. New York: John Wiley & Sons, 2012 [Consulta: 08/06/2022]. Disponible a: https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/reader.action?docID=707226. ISBN 9780470413746.