Guía docente
300049 - SX - Seguridad en Redes

Última modificación: 19/05/2025

Unidad responsable: Escuela de Ingeniería de Telecomunicación y Aeroespacial de Castelldefels
Unidad que imparte: 744 - ENTEL - Departamento de Ingeniería Telemática.

Titulación: GRADO EN INGENIERÍA TELEMÁTICA (Plan 2009). (Asignatura obligatoria).

Curso: 2025 **Créditos ECTS:** 4.0 **Idiomas:** Catalán, Castellano, Inglés

PROFESORADO

Profesorado responsable: Definit a la infoweb de l'assignatura.

Otros:

COMPETENCIAS DE LA TITULACIÓN A LAS QUE CONTRIBUYE LA ASIGNATURA

Específicas:
1. CE 22 TEL. Capacidad para aplicar las técnicas en que se basan las redes, servicios y aplicaciones de telemáticas, tales como sistemas de gestión, señalización y conmutación, encaminamiento y enrutamiento, seguridad (protocolos criptográficos, tunelado, cortafuegos, mecanismos de cobro, de autenticación y de protección de contenidos), ingeniería de tráfico (teoría de grafos, teoría de colas y telegráfico) tarificación y fiabilidad y calidad de servicio, tanto en entornos fijos, móviles, personales, locales o a gran distancia, con diferentes anchos de banda, incluyendo telefonía y datos.(CIN/352/2009, BOE 20.2.2009)

Genéricas:
7. GESTIÓN DE PROYECTOS - Nivel 2: Definir los objetivos de un proyecto bien definido, de alcance reducido, y planificar su desarrollo, determinando los recursos necesarios, tareas a realizar, reparto de responsabilidades e integración. Utilizar adecuadamente herramientas de soporte a la gestión de proyectos.

Transversales:
2. COMUNICACIÓN EFICAZ ORAL Y ESCRITA - Nivel 1: Planificar la comunicación oral, responder de manera adecuada a las cuestiones formuladas y redactar textos de nivel básico con corrección ortográfica y gramatical.
3. COMUNICACIÓN EFICAZ ORAL Y ESCRITA - Nivel 2: Utilizar estrategias para preparar y llevar a cabo las presentaciones orales y redactar textos y documentos con un contenido coherente, una estructura y un estilo adecuados y un buen nivel ortográfico y gramatical.
4. COMUNICACIÓN EFICAZ ORAL Y ESCRITA - Nivel 3: Comunicarse de manera clara y eficiente en presentaciones orales y escritas adaptadas al tipo de público y a los objetivos de la comunicación utilizando las estrategias y los medios adecuados.
5. COMUNICACIÓN EFICAZ ORAL Y ESCRITA: Comunicarse de forma oral y escrita con otras personas sobre los resultados del aprendizaje, de la elaboración del pensamiento y de la toma de decisiones; participar en debates sobre temas de la propia especialidad.
6. EMPRENDEDURÍA E INNOVACIÓN - Nivel 3: Utilizar conocimientos y habilidades estratégicas para la creación y gestión de proyectos, aplicar soluciones sistémicas a problemas complejos y diseñar y gestionar la innovación en la organización.

METODOLOGÍAS DOCENTES

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

Una vez acabada la asignatura de Seguridad en Redes, el estudiante tiene que ser capaz de:
- Entender qué aspectos engloba la seguridad en red y saber identificar los potenciales ataques y los posibles sistemas para evitarlos.
- Identificar y comprender los algoritmos criptográficos más utilizados para dotar de seguridad a las redes.
- Definir los diferentes métodos de confidencialidad, integridad, autenticación, actualidad y gestión del material criptográfico.
- Conocer diferentes sistemas de seguridad perimétrica, como por ejemplo cortafuegos y sistemas de detección de intrusos
- Utilizar los diferentes protocolos de seguridad para los intercambios de datos a Internet: seguridad IP, redes privadas virtuales, mecanismos de seguridad para el correo electrónico, seguridad a la www o sistemas seguros de pago.

HORAS TOTALES DE DEDICACIÓN DEL ESTUDIANTADO

Tipo	Horas	Porcentaje
Horas aprendizaje autónomo	56,0	56.00
Horas grupo pequeño	13,0	13.00
Horas grupo grande	31,0	31.00

Dedicación total: 100 h

CONTENIDOS

1. INTRODUCCIÓN A LA SEGURIDAD EN REDES

Descripción:
Conceptos fundamentales. La seguridad en red engloba: ataques de seguridad, mecanismos de seguridad y servicios de seguridad. A partir del conocimiento de estos tres bloques, se plantea un modelo de seguridad en red que debe estar presente durante toda la asignatura.
Los mecanismos y servicios de seguridad se basan en gran medida en herramientas que garanticen confidencialidad, integridad, autenticación, autorización, AAA, no repudio y anonimato.

Actividades vinculadas:
Examen parcial, examen final

Dedicación: 4h 15m
Grupo grande/Teoría: 2h
Grupo mediano/Prácticas: 0h 15m
Aprendizaje autónomo: 2h

(CAST) 2. EINES DE SEGURETAT DE LA INFORMACIÓ

Descripción:
Aritmética modular y criptografía clásica
Criptografía simétrica moderna
- Cifrado de flujo/bloque
- Modos de funcionamiento cifradores de bloque (ECB, OFB, CBC, CTR, CBC-MAC, CCM, etc.)
Criptografía asimétrica y PKI
- Intro: funciones asimétricas/unidireccionales y criptografía asimétrica
- RSA
Necesidad de autenticar:
- PKI: certificados digitales, firma electrónica
- Secreto compartido: Message Authentication Codes (MAC)
Gestión y acuerdo de claves

Actividades vinculadas:
Examen parcial, examen final

Dedicación: 33h 45m
Grupo grande/Teoría: 10h 30m
Grupo mediano/Prácticas: 1h 15m
Aprendizaje autónomo: 22h

3. RESUMEN AMENAZAS Y CONTRAMEDIDAS

Descripción:
Análisis de las principales amenazas a la seguridad en redes así como resumen de las contramedidas en el estado del arte.

Actividades vinculadas:
Examen parcial, examen final, AD3

Dedicación: 11h 15m
Grupo grande/Teoría: 2h
Grupo mediano/Prácticas: 0h 15m
Actividades dirigidas: 2h
Aprendizaje autónomo: 7h

4. PROTOCOLOS DE SEGURIDAD EN INTERNET

Descripción:
Seguridad aplicada a redes, protocolos de seguridad a nivel de enlace (p.ej. WEP, WPA), a nivel de red (IPSec) y transporte (SSL/TLS, SSH).

Actividades vinculadas:
Examen parcial, examen final, AD1, AD2

Dedicación: 50h 45m
Grupo grande/Teoría: 9h 30m
Grupo mediano/Prácticas: 2h 15m
Actividades dirigidas: 14h
Aprendizaje autónomo: 25h

ACTIVIDADES

AD1. Virtualización de redes, ataques MITM a nivel de enlace y redes privadas virtuales con IPSec

Descripción:
Implementación de escenarios de red virtualizados así como del encaminamiento para garantizar las conectividades necesarias.
Implementación de ataques de man-in-the-middle (MITM) a nivel de enlace.
Implementación de una red privadas virtual (VPN) basada en IPSec.

Dedicación: 16h
Grupo grande/Teoría: 2h
Actividades dirigidas: 7h
Aprendizaje autónomo: 7h

AD2. Autoridades de certificación, SSL/TLS y SSH

Descripción:
Implementación de una autoridad de certificación y para su uso en el escenario IPSec desarrollado en la AD1.
Implementación de ataques a SSL/TLS basados en el ataque MITM de AD1
Implementación de los tres tipos de forwarding SSH

Dedicación: 17h
Grupo grande/Teoría: 2h
Actividades dirigidas: 7h
Aprendizaje autónomo: 8h

AD3. ACTIVIDAD ABIERTA

Descripción:
En función del desarrollo del curso y de las inquietudes de los alumnos, se propondrá una actividad dirigida

Dedicación: 8h
Actividades dirigidas: 2h
Aprendizaje autónomo: 6h

(CAST) PLANIFICACIÓ D'EXÀMENS (RESOLUCIÓ DE PROBLEMES)

Dedicación: 8h
Grupo grande/Teoría: 4h
Aprendizaje autónomo: 4h

Examen parcial

Dedicación: 4h 30m
Grupo grande/Teoría: 1h 30m
Aprendizaje autónomo: 3h

Examen final

Dedicación: 4h 30m
Grupo grande/Teoría: 1h 30m
Aprendizaje autónomo: 3h

SISTEMA DE CALIFICACIÓN