



Guía docente

230157 - SPI - Seguridad y Privacidad de la Información

Última modificación: 20/06/2024

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

Titulación: GRADO EN INGENIERÍA DE TECNOLOGÍAS Y SERVICIOS DE TELECOMUNICACIÓN (Plan 2015). (Asignatura optativa).
GRADO EN INGENIERÍA ELECTRÓNICA DE TELECOMUNICACIÓN (Plan 2018). (Asignatura optativa).

Curso: 2024 **Créditos ECTS:** 6.0 **Idiomas:** Inglés

PROFESORADO

Profesorado responsable: Consultar aquí / See here:

Otros: Consultar aquí / See here:

METODOLOGÍAS DOCENTES

- Clases expositivas.
- Clases de aplicación.
- Trabajo en grupo (no presencial).
- Trabajo individual (no presencial).
- Presentaciones orales.
- Pruebas de respuesta larga.

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

- Aprendizaje de conceptos generales de seguridad y privacidad de la información.
- Conocer los principales mecanismos de autenticación y gestión de claves.
- Profundizar en el conocimiento de los principales protocolos de seguridad usados en Internet.
- Introducir los principales algoritmos de anonimato de datos y las garantías de privacidad asociadas
- Introducir las principales garantías de privacidad definidas por distintos escenarios de aplicación.
- Comprender los retos y mecanismos de privacidad en sistemas de información personalizada
- Introducir los sistemas de comunicaciones anónimas

HORAS TOTALES DE DEDICACIÓN DEL ESTUDIANTADO

Tipo	Horas	Porcentaje
Horas grupo grande	52,0	34.67
Horas aprendizaje autónomo	98,0	65.33

Dedicación total: 150 h

CONTENIDOS

1. Conceptos de Seguridad en redes

Descripción:

Mecanismos y Servicios de Seguridad; Criptografía simétrica y de clave pública; firma digital; Seguridad perimetral.

Dedicación: 30h

Grupo grande/Teoría: 10h

Aprendizaje autónomo: 20h

2. Autenticación y Gestión Claves

Descripción:

Protocolos y mecanismos de autenticación; Protocolos de gestión de claves; Infraestructura de clave pública (PKI); Modelos de confianza.

Dedicación: 16h

Grupo grande/Teoría: 6h

Aprendizaje autónomo: 10h

3. Protocolos de Seguridad en Internet

Descripción:

Seguridad IP y redes privadas virtuales; Seguridad en correo electrónico; Seguridad en Web.

Dedicación: 24h

Grupo grande/Teoría: 8h

Aprendizaje autónomo: 16h

4. Introducción a la privacidad de los datos

Descripción:

Motivación. Definición de conceptos básicos. Atacantes y partes de confianza. Métricas de privacidad.

Dedicación: 12h

Grupo grande/Teoría: 4h

Aprendizaje autónomo: 8h

5. Algoritmos de anonimización de datos

Descripción:

Control de revelación estadística. Algoritmos de microagregación de datos. Medida del compromiso privacidad-utilidad.

Dedicación: 26h

Grupo grande/Teoría: 10h

Aprendizaje autónomo: 16h

6. Privacidad en sistemas de información personalizados

Descripción:

Perfiles de usuario: medida del riesgo de privacidad. Tecnologías de privacidad.

Dedicación: 12h

Grupo grande/Teoría: 4h

Aprendizaje autónomo: 8h

7. Sistemas de comunicación anónimos.

Descripción:

Análisis de tráfico. Sistemas de comunicaciones anónimas: TOR, Crowds, Mix Networks.

Dedicación: 12h

Grupo grande/Teoría: 4h

Aprendizaje autónomo: 8h

8. Privacidad diferencial

Descripción:

Privacidad sintáctica vs semántica. Privacidad diferencial en bases de datos interactivas.

Dedicación: 18h

Grupo grande/Teoría: 6h

Aprendizaje autónomo: 12h

SISTEMA DE CALIFICACIÓN

La nota final de la asignatura se obtendrá a partir de la calificación de evaluación continua, que contemplará la participación activa en clase, así como controles, presentaciones y trabajos propuestos por el profesor a lo largo del curso. La ponderación será la siguiente:

- Controles (50%)
- Participación activa en clase (10%)
- Trabajos y presentaciones (40%)

En caso de no superar la evaluación continua, el alumno podrá presentarse a un examen final, que en este caso supone un 100% de la nota.

BIBLIOGRAFÍA

Básica:

- Templ, Matthias. Statistical disclosure control for microdata : methods and applications in R . Cham, Switzerland : Springer International Publishing AG, 2017. ISBN 9783319502724.
- Stallings, William. Cryptography and network security : principles and practice . 7th ed., global edition. Boston : Prentice Hall, cop. 2017. ISBN 9781292158587.