

Guia docent

230157 - SPI - Seguretat i Privadesa de la Informació

Última modificació: 20/06/2024

Unitat responsable: Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona

Unitat que imparteix: 744 - ENTEL - Departament d'Enginyeria Telemàtica.

Titulació: GRAU EN ENGINYERIA DE TECNOLOGIES I SERVEIS DE TELECOMUNICACIÓ (Pla 2015). (Assignatura optativa).

GRAU EN ENGINYERIA ELECTRÒNICA DE TELECOMUNICACIÓ (Pla 2018). (Assignatura optativa).

Curs: 2024

Crèdits ECTS: 6.0

Idiomes: Anglès

PROFESSORAT

Professorat responsable: Consultar aquí / See here:

Altres: Consultar aquí / See here:

METODOLOGIES DOCENTS

- Classes expositives
- Classes d'aplicació
- Treball en grup (no presencial)
- Treball individual (no presencial)
- Presentacions orals
- Proves de resposta llarga

OBJECTIUS D'APRENTATGE DE L'ASSIGNATURA

- Aprenentatge de conceptes generals de seguretat i privacitat de la informació.
- Conèixer els principals mecanismes d'autenticació i gestió de claus.
- Aprofundir en el coneixement dels principals protocols de seguretat usats a Internet.
- Introduir els principals algorismes d'anonimat de dades i les garanties de privadesa associades
- Introduir les principals garanties de privadesa definides per diferents escenaris d'aplicació.
- Comprendre els reptes i mecanismes de privadesa en sistemes d'informació personalitzada
- Introduir els sistemes de comunicacions anònimes

HORES TOTALES DE DEDICACIÓ DE L'ESTUDIANTAT

Tipus	Hores	Percentatge
Hores grup gran	52,0	34.67
Hores aprenentatge autònom	98,0	65.33

Dedicació total: 150 h

CONTINGUTS

1. Conceptes de Seguretat en xarxes

Descripció:

Mecanismes i Serveis de Seguretat; Criptografia simètrica i de clau pública; signatura digital; Seguretat perimetral.

Dedicació: 30h

Grup gran/Teoria: 10h

Aprenentatge autònom: 20h

2. Autenticació i Gestió Claus

Descripció:

Protocols i mecanismes d'autenticació; Protocols de gestió de claus; Infraestructura de clau pública (PKI); Models de confiança.

Dedicació: 16h

Grup gran/Teoria: 6h

Aprenentatge autònom: 10h

3. Protocols de Seguretat a Internet

Descripció:

Seguretat IP i xarxes privades virtuals; Seguretat en correu electrònic, Seguretat en web.

Dedicació: 24h

Grup gran/Teoria: 8h

Aprenentatge autònom: 16h

4. Introducció a la privadesa de les dades

Descripció:

Motivació. Definició de conceptes bàsics. Atacants i parts de confiança. Mètriques de privadesa.

Dedicació: 12h

Grup gran/Teoria: 4h

Aprenentatge autònom: 8h

5. Algorismes d'anonimització de dades

Descripció:

Control de revelació estadística. Algorismes de microagregació de dades. Mesura del compromís privadesa-utilitat.

Dedicació: 26h

Grup gran/Teoria: 10h

Aprenentatge autònom: 16h



6. Privadesa a sistemes d'informació personalitzats

Descripció:

Perfils d'usuari: mesura del risc de privacitat. Mecanismes de privadesa.

Dedicació: 12h

Grup gran/Teoria: 4h

Aprenentatge autònom: 8h

7. Sistemes de comunicació anònims.

Descripció:

Anàlisis de tràfic. Sistemes de comunicacions anònimes: TOR, Crowds, Mix Networks.

Dedicació: 12h

Grup gran/Teoria: 4h

Aprenentatge autònom: 8h

8. Privadesa diferencial

Descripció:

Privadesa sintàctica vs semàntica. Privadesa diferencial en bases de dades interactives.

Dedicació: 18h

Grup gran/Teoria: 6h

Aprenentatge autònom: 12h

SISTEMA DE QUALIFICACIÓ

La nota final de l'assignatura s'obindrà a partir de la qualificació d'avaluació continuada, que contemplarà la participació activa a classe, així com controls, presentacions i treballs proposats pel professor al llarg del curs. La ponderació serà la següent:

- Controls (50%)
- Participació activa a classe (10%)
- Treballs i presentacions (40%)

Cas de no superar l'avaluació continuada, l'alumne podrà presentar-se a un examen final, que en aquest cas suposa un 100% de la nota.

BIBLIOGRAFIA

Bàsica:

- 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.