

Guia docent

230990 - DP - Privadesa de Dades

Última modificació: 13/06/2025

Unitat responsable: Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona
Unitat que imparteix: 744 - ENTEL - Departament d'Enginyeria Telemàtica.

Titulació: MÀSTER UNIVERSITARI EN ENGINYERIA DE TELECOMUNICACIÓ (Pla 2013). (Assignatura optativa).
MÀSTER UNIVERSITARI EN CIBERSEGURETAT (Pla 2020). (Assignatura optativa).

Curs: 2025 **Crèdits ECTS:** 5.0 **Idiomes:** Anglès

PROFESSORAT

Professorat responsable: JAVIER PARRA ARNAU

Altres:

METODOLOGIES DOCENTS

- Classes expositives
- Pràctiques de laboratori
- Treball individual (no presencial)
- Treball en grup
- Proves de resposta curta (Test)
- Proves de resposta llarga (Examen Final)

OBJECTIUS D'APRENENTATGE DE L'ASSIGNATURA

La privacitat de les dades és l'adaptació a la Societat de la Informació del dret fonamental a la privacitat i la vida privada. Aquest curs es centra en diferents aspectes tecnològics per garantir la privacitat de la informació, que inclouen:

- Presentar les principals mètriques de privacitat proposades en la literatura, tant aquelles qualitatives com, especialment, les quantitatives.
- Avaluar riscos i analitzar tecnologies de privacitat en el camp de control de revelació estadística.
- Avaluar riscos i analitzar tecnologies de privacitat en els sistemes d'informació personalitzats.
- Avaluar riscos i analitzar tecnologies de privacitat en els sistemes de comunicacions anònimes.
- Comprendre el compromís inherent entre privacitat i usabilitat de les dades.

HORES TOTALES DE DEDICACIÓ DE L'ESTUDIANT

Tipus	Hores	Percentatge
Hores aprenentatge autònom	86,0	68.80
Hores grup gran	26,0	20.80
Hores grup petit	13,0	10.40

Dedicació total: 125 h

CONTINGUTS

1. Introducció

Descripció:

En aquest primer tema es pretén donar una visió global de l'assignatura, fent especial èmfasi en la motivació i als requeriments legals (i també ètics) que sustenten les tècniques de protecció de la privacitat.

Objectius específics:

- Oferir una visió general de l'assignatura.
- Motivar la necessitat de protegir la privacitat dels usuaris en els sistemes d'informació i comunicacions.
- Introduir el marc legal i les implicacions ètiques que requereixen la protecció de la privacitat.
- Introduir els camps d'aplicació de les tecnologies de privacitat.
- Definir conceptes bàsics de la terminologia de l'assignatura.
- Presentar els models de confiança sobre els quals es basa l'assignatura, identificant els atacants dels que intentem protegir-nos.

Dedicació: 7h

Grup gran/Teoria: 3h

Aprenentatge autònom: 4h

2. Anonimització de bases de dades

Descripció:

Aquest tema tracta sobre l'anonimització de bases de dades, possiblement un dels camps d'aplicació més rellevants actualment per als estudiants que s'incorporen a el mercat laboral. Es presenten tècniques d'estimació de risc, així com diferents tècniques i algoritmes d'anonimat, tant per dades categòriques com numèrics. Es fa especial èmfasi a el compromís entre privacitat i usabilitat, considerant també mètriques de pèrdua d'usabilitat de les dades anonimitzades.

Objectius específics:

- Presentar els riscos de publicació de bases de dades que incloguin informació personal dels usuaris.
- Formular el compromís entre privacitat i usabilitat inherent a les tècniques perturbatives.
- Presentar les principals tècniques d'estimació de riscos de revelat d'informació privada en bases de dades estadístiques.
- Presentar els algoritmes d'anonimat per dades categòriques.
- Presentar els algoritmes d'anonimat per dades numèriques.
- Presentar tècniques de generació de dades sintètiques.
- Ser capaç de mesurar la pèrdua d'usabilitat de les dades anonimitzades.

Dedicació: 24h

Grup gran/Teoria: 9h

Aprenentatge autònom: 15h

3. Privadesa a sistemes d'informació personalitzada

Descripció:

En aquest tema es contemplen els mecanismes de privacitat basats en la pertorbació de dades que es fan servir en camps diferents a SDC. D'una banda, s'estudia la problemàtica de la privacitat en sistemes d'informació personalitzats i en sistemes de recomanació. D'altra banda, s'aborda el tema de la privacitat en aplicacions que tenen accés a informació geo-localitzada.

Objectius específics:

- Introduir els reptes de privacitat en sistemes de recomanació i personalitzats, incloent sistemes de publicitat en línia.
- Quantificar el risc de privacitat inherent a la creació de perfils d'usuari per terceres parts.
- Presentar diferents estratègies de generació falsa de consultes, incloent TrackMeNot.
- Presentar mecanismes de protecció en sistemes basats en anotacions semàntiques.
- Introduir la problemàtica de privacitat en la localització
- Ressaltar el compromís entre privacitat i usabilitat, inherent a tot sistema basat en pertorbació de dades.

Dedicació: 9h

Grup gran/Teoria: 3h

Aprenentatge autònom: 6h

4. Sistemes de comunicació anònims

Descripció:

Tot i que les comunicacions vagin xifrades, l'atacant pot obtenir sensible analitzant les capçaleres dels protocols i inferint qui i quan s'està comunicant amb qui. Els sistemes de comunicació anònims, que s'estudien en aquest tema, permeten protegir-se davant aquests atacs d'anàlisi de tràfic.

Objectius específics:

- Presentar tècniques d'anàlisi de tràfic i justificar la necessitat de comunicacions anònimes.
- Definir la terminologia bàsica dels sistemes de comunicació anònims.
- Presentar i analitzar els sistemes de comunicacions anònims basats en Mix Networks.
- Presentar i analitzar els sistemes de comunicacions anònims basats en Onion Routing.
- Presentar i analitzar els sistemes de comunicacions anònims basats en la col·laboració d'usuaris en xarxes P2P.

Dedicació: 9h

Grup gran/Teoria: 3h

Aprenentatge autònom: 6h

5. Privadesa diferencial

Descripció:

contingut català

Objectius específics:

En aquest tema s'introdueixen els principals conceptes relacionats amb la privadesa diferencial

Dedicació: 23h

Grup gran/Teoria: 8h

Aprenentatge autònom: 15h

6. Laboratori. Pràctiques d'anonimització de dades

Descripció:

L'objectiu principal de les pràctiques proposades és servir de suport a l'assignatura Data Privacy, perquè l'alumne aprofundeixi a través de l'experimentació en diferents aspectes importants, especialment els relacionats amb l'anonimització de dades.

Objectius específics:

- Introducció al control de la divulgació estadística (SDC)
- Introducció al llenguatge de programació R.
- Avaluació del risc de divulgació
- Mesura de la utilitat d'un conjunt de dades
- Mètodes d'anonimització de variables categòriques
- Mètodes d'anonimització de variables numèriques
- Privacitat diferencial

Dedicació: 49h

Grup petit/Laboratori: 13h

Aprenentatge autònom: 36h

SISTEMA DE QUALIFICACIÓ

- Aquesta assignatura té avaluació de teoria (65%) i de laboratori (35%).
- La nota de teoria s'obté mitjançant dos controls realitzats durant el curs.
- La nota de laboratori s'obté mitjançant la realització del exercicis pràctics i l'entrega de les memòries corresponents.

BIBLIOGRAFIA

Bàsica:

- Torra i Reventós, Vicenç. Data privacy : foundations, new developments and the big data challenge. Skövde: Springer, 2017. ISBN 9783319573564.
- Templ, Matthias. Statistical disclosure control for microdata : methods and applications in R [en línia]. Cham, Switzerland: Springer International Publishing AG, 2017 [Consulta: 05/07/2021]. Disponible a: <https://ebookcentral.proquest.com/lib/upcatalunya-ebooks/detail.action?docID=4855639>. ISBN 9783319502724.
- Hundepool, Anco; Domingo-Ferrer, Josep. Statistical disclosure control [en línia]. Chichester, West Sussex, United Kingdom: John Wiley & Sons Inc, [2012] [Consulta: 05/07/2021]. Disponible a: <https://onlinelibrary.wiley.com/doi/book/10.1002/9781118348239>. ISBN 9781118348239.