



## Guía docente

### 230152 - CSI - Codificación y Seguridad de la Información

Última modificación: 08/06/2023

**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:** 2023      **Créditos ECTS:** 6.0      **Idiomas:** Castellano

#### 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-assigant-idioma>

#### 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

---

La asignatura se divide en dos partes que se imparten en paralelo, pero de forma coordinada, puesto que los conocimientos ofrecidos en cada parte se reutilizan en la otra.

La primera parte está centrada en la criptografía como herramienta de codificación de la información, y tiene los siguientes objetivos de aprendizaje:

- Aprendizaje de fundamentos matemáticos que se utilizan en criptografía moderna
- Aprendizaje de los sistemas criptográficos de clave pública más utilizados
- Descripción de otros mecanismos utilizados en criptografía
- Descripción del uso de la criptografía más allá del cifrado y la firma digital

La segunda parte de la asignatura se centra en diferentes aspectos de seguridad y privacidad de la información, con los siguientes objetivos de aprendizaje:

- 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 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

### PARTE I. CRIPTOGRAFÍA

#### Descripción:

1. Teoría de números en criptografía (Teoría 8 h, Aprendizaje autónomo 13 h). Conocimientos de teoría de números necesarios para entender los sistemas criptográficos modernos.
2. Sistemas criptográficos de clave pública (Teoría 12 h, Aprendizaje autónomo 21 h). Se estudian los sistemas criptográficos de clave pública más utilizados: RSA, Rabin, Goldwasser-Micali, Diffie-Hellman y El Gamal
3. Otros tipos de criptografía (Teoría 2 h, Aprendizaje autónomo 6 h). Se presentan la Criptografía de Curva Elíptica y la Criptografía Cuántica
4. Otras aplicaciones de la Criptografía (Teoría 4 h, Aprendizaje autónomo 9 h). Se presentan otros usos de la criptografía como jugar cara o cruz por teléfono, reparto de secretos, test de primalidad, etc.

**Dedicación:** 75h

Grupo grande/Teoría: 26h

Aprendizaje autónomo: 49h

### PARTE II. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

#### Descripción:

1. Conceptos de Seguridad en Redes
2. Autenticación y Gestión de Claves
3. Protocolos de Seguridad en Internet
4. Introducción a privacidad de los datos
5. Anonimización de bases de datos
6. Privacidad en sistemas de información personalizados
7. Privacidad diferencial
8. Sistemas de comunicaciones anónimas

**Dedicación:** 75h

Grupo grande/Teoría: 26h

Aprendizaje autónomo: 49h

## 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. En caso de no superar la evaluación continua, el alumno podrá presentarse a un examen final.



## BIBLIOGRAFÍA

---

### Básica:

- Menezes, A. J; Vanstone, Scott A; Van Oorschot, Paul C. Handbook of applied cryptography. Boca Ratón [etc.]: CRC Press, cop. 1997. ISBN 0849385237.
- Templ, Matthias. Statistical disclosure control for microdata: methods and applications in R [en línea]. Cham, Switzerland: Springer International Publishing AG, 2017 [Consulta: 28/06/2022]. Disponible a: <https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pg-origsite=primo&docID=4855639>. ISBN 9783319502724.
- Stallings, W. Cryptography and network security: principles and practice. 8th ed. Boston: Pearson Education Limited, 2023. ISBN 9781292437484.

### Complementaria:

- Navarro-Arribas, Guillermo; Torra i Reventós, Vicenç. Advanced research in data privacy [en línea]. Cham: Springer, cop. 2015 [Consulta: 04/08/2023]. Disponible a: <https://link-springer-com.recursos.biblioteca.upc.edu/book/10.1007/978-3-319-09885-2>. ISBN 9783319098852.
- Hundepool, Anco; Domingo-Ferrer, Josep. Statistical disclosure control [en línea]. Chichester, West Sussex, United Kingdom: John Wiley & Sons Inc, [2012] [Consulta: 28/06/2022]. Disponible a: <https://onlinelibrary-wiley-com.recursos.biblioteca.upc.edu/doi/book/10.1002/9781118348239>. ISBN 9781118348239.

## RECURSOS

---

### Otros recursos:

Información adicional disponible en ATENEA