

|              |                                                           |
|--------------|-----------------------------------------------------------|
| Any acadèmic | 2016-17                                                   |
| Assignatura  | 11547 - Tecnologies de Seguretat per al Comerç Electrònic |
| Grup         | Grup 1, 2S                                                |
| Guia docent  | C                                                         |
| Idioma       | Català                                                    |

## Identificació de l'assignatura

|                             |                                                                                          |
|-----------------------------|------------------------------------------------------------------------------------------|
| <b>Assignatura</b>          | 11547 - Tecnologies de Seguretat per al Comerç Electrònic                                |
| <b>Crèdits</b>              | 0,72 de presencials (18 hores) 2,28 de no presencials (57 hores) 3 de totals (75 hores). |
| <b>Grup</b>                 | Grup 1, 2S (Campus Extens)                                                               |
| <b>Període d'impartició</b> | Segon semestre                                                                           |
| <b>Idioma d'impartició</b>  | Català                                                                                   |

## Professors

| Professor/a                                                                                | Horari d'atenció als alumnes |            |          |              |            |         |
|--------------------------------------------------------------------------------------------|------------------------------|------------|----------|--------------|------------|---------|
|                                                                                            | Hora d'inici                 | Hora de fi | Dia      | Data d'inici | Data de fi | Despatx |
| Macià Mut Puigserver<br><a href="mailto:macia.mut@uib.es">macia.mut@uib.es</a>             | 16:20                        | 17:00      | Dimarts  | 12/09/2016   | 13/01/2017 | D-224   |
| Maria Magdalena Payeras<br>Capellà<br><a href="mailto:mpayeras@uib.es">mpayeras@uib.es</a> | 11:00                        | 12:00      | Dimecres | 12/12/2016   | 30/09/2017 | 135     |

## Contextualització

L'assignatura de Tecnologies de Seguretat per al Comerç Electrònic tracta, per una banda, aspectes essencials de la seguretat computacional i de les xarxes de comunicacions, que poden ser d'utilitat en diferents entorns dins l'àmbit de les tecnologies de la informació i de les comunicacions. D'altra banda es tracten continguts específics de determinades aplicacions, fonamentant-se en les necessitats del comerç electrònic.

## Requisits

### Recomanables

Encara que l'assignatura no presenta requisits essencials es recomana que l'alumne tingui coneixements bàsics de criptografia i de programació.

## Competències

### Específiques

- \* Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido..

|              |                                                           |
|--------------|-----------------------------------------------------------|
| Any acadèmic | 2016-17                                                   |
| Assignatura  | 11547 - Tecnologies de Seguretat per al Comerç Electrònic |
| Grup         | Grup 1, 2S                                                |
| Guia docent  | C                                                         |
| Idioma       | Català                                                    |

## Genèriques

- \* Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contexto más amplios y multidisciplinares, siendo capaces de integrar estos conocimientos..
- \* Capacidad para comprender y aplicar la responsabilidad ética, la legislación y la deontología profesional de la actividad de la profesión de Ingeniero en Informática..

## Bàsiques

- \* Podeu consultar les competències bàsiques que l'estudiant ha d'haver assolit en acabar el màster a l'adreça següent: [http://estudis.uib.cat/master/comp\\_basiques/](http://estudis.uib.cat/master/comp_basiques/)

## Continguts

- Criptografia: Confidencialitat i autenticitat en els sistemes d'informació. Sistemes d'autenticació i d'intercanvi de claus.
- Firma Digital i Certificats digitals.
- Aplicacions de la criptografia: Correuelectrònic certificat, Protocols segurs, Comerç electrònic i Firma electrònica.
- Sistemes de pagament electrònic.
- Aplicaciones Avanzadas.

## Continguts temàtics

1. Criptografia: Confidencialitat i autenticitat en els sistemes d'informació. Sistemes d'autenticació i d'intercanvi de claus.
  - o Criptosistemes de clau privada (DES, IDEA, AES).
  - o Criptosistemes de clau pública (RSA, El Gamal)
  - o Sistemes d'autenticació i d'intercanvi de claus.
  - o Ús de criptosistemes.
  - o Criptoanàlisi.
2. Firma Digital i Certificats digitals.
  - o Firma digital amb l'algorisme RSA.
  - o Altres esquemes de firma digital.
  - o Autoritats de certificació.
  - o Certificats X.509.
3. Aplicacions de la criptografia.
  - o Correu electrònic: PGP, S/MIME.
  - o Protocols segurs: SSL, IPSEC.
  - o Comerç electrònic i Signatura electrònica.
4. Sistemes de Pagament Electrònic

- o Conceptes generals.
  - o Seguretat en els sistemes de pagament electrònic.
  - o Diners electrònics.
  - o Micropagaments
  - o Autenticació, cost i anonim.
5. Aplicacions Avançades
- o Contractació Electrònica.
  - o Notificacions Electròniques.
  - o Tiquets Electrònics.
  - o Autenticació, cost i anonim.

## Metodologia docent

### Activitats de treball presencial

| Modalitat           | Nom                   | Tip. agr.      | Descripció                                                                                                              | Hores |
|---------------------|-----------------------|----------------|-------------------------------------------------------------------------------------------------------------------------|-------|
| Classes teòriques   |                       | Grup gran (G)  | De cada tema del curs s'impartiran sessions de tres hores de durada de classes teòriques                                | 12    |
| Seminaris i tallers | Seminari              | Grup mitjà (M) | Durant el curs es podrà realitzar un seminari impartit per un expert sobre un tema afí als continguts del curs.         | 2     |
| Classes pràctiques  | Pràctiques i treballs | Grup gran (G)  | Les classes d'aquesta modalitat es dedicaran a la presentació de les pràctiques i els treballs realitzats pels alumnes. | 3     |
| Tutories ECTS       | Tutories              | Grup petit (P) | Realització de tutories amb els alumnes                                                                                 | 1     |
| Avaluació           | Avaluació             | Grup gran (G)  | Es realitzarà una avaluació sobre els continguts teòrics de l'assignatura.                                              | 0     |

A començament del semestre hi haurà a disposició dels estudiants el cronograma de l'assignatura a través de la plataforma UIBdigital. Aquest cronograma inclourà almenys les dates en què es faran les proves d'avaluació contínua i les dates de lliurament dels treballs. A més, el professor o la professora informará els estudiants si el pla de treball de l'assignatura es durà a terme a través del cronograma o per una altra via, inclosa la plataforma Campus Extens.

### Activitats de treball no presencial

| Modalitat                           | Nom | Descripció                                                                       | Hores |
|-------------------------------------|-----|----------------------------------------------------------------------------------|-------|
| Estudi i treball autònom individual |     | Estudi per a la consolidar els coneixements adquirits en les classes presencials | 30    |

|              |                                                           |
|--------------|-----------------------------------------------------------|
| Any acadèmic | 2016-17                                                   |
| Assignatura  | 11547 - Tecnologies de Seguretat per al Comerç Electrònic |
| Grup         | Grup 1, 2S                                                |
| Guia docent  | C                                                         |
| Idioma       | Català                                                    |

| Modalitat                        | Nom | Descripció                                                            | Hores |
|----------------------------------|-----|-----------------------------------------------------------------------|-------|
| Estudi i treball autònom en grup |     | Realització de treballs i/o pràctiques i preparació de presentacions. | 27    |

### Riscs específics i mesures de protecció

Les activitats d'aprenentatge d'aquesta assignatura no comporten riscos específics per a la seguretat i salut dels alumnes i, per tant, no cal adoptar mesures de protecció especials.

### Avaluació de l'aprenentatge dels estudiants

L'avaluació constarà, per una part, de l'elaboració d'un treball pràctic i un de teòric de recerca. Es realitzarà la presentació a classe dels resultats dels treballs, amb mateix pes sobre la nota final. L'altra part de l'avaluació es realitzarà mitjançant una col·lecció d'exercicis o, alternativament, d'un examen. La nota mínima de cada part és un 4.

#### Pràctiques i treballs

|                      |                                                                                                                      |
|----------------------|----------------------------------------------------------------------------------------------------------------------|
| Modalitat            | Classes pràctiques                                                                                                   |
| Tècnica              | Proves orals ( <b>no recuperable</b> )                                                                               |
| Descripció           | Les classes d'aquesta modalitat dedicaran a la presentació de les pràctiques i els treballs realitzats pels alumnes. |
| Criteris d'avaluació | Correcció dels continguts, adequació al tema proposat, complexitat, qualitat de l'exposició.                         |

Percentatge de la qualificació final: 50% amb qualificació mínima 4

#### Avaluació

|                      |                                                                                                                  |
|----------------------|------------------------------------------------------------------------------------------------------------------|
| Modalitat            | Avaluació                                                                                                        |
| Tècnica              | Proves de resposta llarga, de desenvolupament ( <b>recuperable</b> )                                             |
| Descripció           | Es realitzarà una avaluació sobre els continguts teòrics de l'assignatura.                                       |
| Criteris d'avaluació | Aquesta part de l'avaluació es realitzarà mitjançant una col·lecció d'exercicis o, alternativament, d'un examen. |

Percentatge de la qualificació final: 50% amb qualificació mínima 4

### Recursos, bibliografia i documentació complementària

Els apunts de l'assignatura es proporcionaran en gran part a través de la plataforma Campus Extens.

Els enunciats de les pràctiques i els treballs a realitzar es proporcionaran als alumnes a través de la plataforma Campus Extens.

#### Bibliografia bàsica

Bruce Schneier: "Applied Cryptography: Protocols, Algorithms, and Source Code in C"; Ed. Wiley



**Universitat**  
de les Illes Balears

## Guia docent

|              |                                                           |
|--------------|-----------------------------------------------------------|
| Any acadèmic | 2016-17                                                   |
| Assignatura  | 11547 - Tecnologies de Seguretat per al Comerç Electrònic |
| Grup         | Grup 1, 2S                                                |
| Guia docent  | C                                                         |
| Idioma       | Català                                                    |

William Stallings: "Network Security Essentials: Applications and Standards"; Prentice Hall

