

**Garantia de la Informació i Seguretat**

Codi: 102757

Crèdits: 6

| Titulació                      | Tipus | Curs | Semestre |
|--------------------------------|-------|------|----------|
| 2502441 Enginyeria Informàtica | OB    | 3    | 2        |
| 2502441 Enginyeria Informàtica | OT    | 4    | 2        |

La metodologia docent i l'avaluació proposades a la guia poden experimentar alguna modificació en funció de les restriccions a la presencialitat que imposin les autoritats sanitàries.

**Professor/a de contacte**

Nom: Guillermo Navarro Arribas

Correu electrònic: Guillermo.Navarro@uab.cat

**Utilització d'idiomes a l'assignatura**

Llengua vehicular majoritària: català (cat)

Grup íntegre en anglès: No

Grup íntegre en català: No

Grup íntegre en espanyol: No

**Equip docent**

Jordi Casas Roma

**Prerequisits**

No hi ha requisits oficials, però sí es recomana tenir coneixements bàsics sobre criptografia, xarxes i programació. Aquests coneixements són assolibles amb assignatures prèvies del grau: Xarxes, Informació i Seguretat, Fonaments i Tecnologia de la Informació, i Metodologia de la Programació.

**Objectius**

L'objectiu d'aquesta assignatura és que l'alumnat assoleixi uns coneixements bàsics sobre la problemàtica de la seguretat de la informació i els mecanismes existents per a la protecció de sistemes informàtics. D'aquesta manera, l'alumnat pot desenvolupar una visió crítica envers la seguretat informàtica. Per altra banda l'alumnat haurà de ser capaç de posar en pràctica alguns aspectes de l'assignatura. Conèixer com es realitzen certs atacs és un pas important per entendre les necessitats de seguretat dels sistemes, i poder després aplicar tècniques de protecció adequades en cada cas.

**Competències**

- Enginyeria Informàtica
- Adquirir hàbits de pensament.
- Capacitat per a comprendre i aplicar els principis de l'avaluació de riscos i aplicar-los correctament a l'elaboració i execució de plans d'actuació.
- Capacitat per a comprendre, aplicar i gestionar la garantia i seguretat dels sistemes informàtics.
- Capacitat per a determinar els requisits dels sistemes d'informació i comunicació d'una organització atenent a aspectes de seguretat i compliment de la normativa i la legislació vigent.
- Capacitat per dissenyar, desenvolupar, avaluar i assegurar l'accessibilitat, l'ergonomia, la usabilitat i la seguretat dels sistemes, serveis i aplicacions informàtiques, així com de la informació que gestionen.

- Concebre i desenvolupar sistemes o arquitectures informàtiques centralitzades o distribuïdes integrant hardware, software i xarxes.
- Treballar en equip.

## Resultats d'aprenentatge

1. Col·laborar en el disseny i seguiment de les polítiques de seguretat de sistemes informàtics.
2. Comprendre i aplicar els principis de seguretat a l'elaboració i execució de plans d'actuació.
3. Conèixer els principis de la informàtica forense i del tractament dels delictes informàtics.
4. Conèixer i comprendre les possibilitats tècniques d'implantació de polítiques de seguretat en sistemes distribuïts.
5. Desenvolupar un mode de pensament i raonament crítics.
6. Determinar els requisits de seguretat i compliment de la normativa i la legislació vigent en els sistemes d'informació i comunicació d'una organització.
7. Determinar els requisits de seguretat i confidencialitat, així com identificar els principals tipus d'atacs i amenaces.
8. Dissenyar sistemes de protecció de la informació: control d'accés i integritat.
9. Treballar cooperativament.

## Continguts

### Mecanismes de seguretat

- Autenticació
- Autorització i control d'accés
- Infraestructura de clau pública
- Seguretat del software
- Detecció de malware i detecció d'intrusions
- Privacitat de dades

### Gestió de la seguretat i altres aspectes

- Gestió de vulnerabilitats
- Modelat d'amenaces i atacs, pentesting
- Gestió de riscos
- Informàtica forense i pericial
- Enginyeria social

En aquesta assignatura es veuen mecanismes concrets de seguretat pel disseny de sistemes de protecció de la informació, control d'accés i integritat. S'estudia també una visió global de la seguretat, gestió d'amenaces, es veuen també tècniques de modelat d'amenaces, gestió de riscos, i s'introdueixen disciplines com la informàtica forense i pericial. Cal destacar que l'ordre en el que es tractaran els temes pot variar respecte a l'estipulat en aquesta guia per motius de planificació docent.

## Metodologia

L'assignatura es desenvolupa en 50 hores d'activitats dirigides repartides en sessions de teoria, de problemes i de laboratori. En el plantejament de l'assignatura es potenciarà el treball tutoritzat sobre aspectes concrets de l'assignatura. Aquest treball es divideix en una part supervisada que es realitzarà a les sessions (de teoria, problemes i laboratori), i una part no supervisada que l'alumnat realitzarà de manera autònoma.

- Sessions de teoria: classes realitzades a les sessions de teoria on el professorat subministrarà informació sobre els coneixements de l'assignatura i sobre estratègies per adquirir, ampliar i organitzar aquests coneixements. Aquestes sessions poden incloure sessions impartides per professionals de l'àmbit de la seguretat informàtica en forma de seminaris.

- Sessions de problemes: on es plantejen uns problemes o activitats que l'alumnat haurà de desenvolupar en grup o individualment (depenent de l'activitat concreta). Aquest treball pot constar d'una part de treball supervisat i una part de treball autònom.
- Sessions de pràctiques al laboratori: on es tractaran amb profunditat i a nivell pràctic temes relacionats amb els exposats a les sessions de teoria.

Durant el curs es plantejarà un treball a l'alumnat que es realitzarà en grup i/o de forma individual. Aquest treball supervisat varia a cada curs i es planteja a l'inici de curs. Pot consistir en petits exercicis plantejats com a reptes o en un projecte de major entitat.

Durant tot el curs es farà servir l'aula Moodle del Campus Virtual de la UAB com a mitjà principal de comunicació entre el professorat i l'alumnat. Això inclou la publicació de materials, publicació de notes parcials, fòrum de discussió, lliurament de treballs, ...

Competències transversals:

- T01.01 - Desenvolupar un mode de pensament i raonament crítics. Juga un paper important en el treball tutoritzat proposat, així com en altres activitats desenvolupades a les altres parts de l'assignatura.
- T03.01 - Treballar cooperativament. Es treballarà i avaluarà en les sessions de problemes i de laboratori.

Nota: es reservaran 15 minuts d'una classe, dins del calendari establert pel centre/titulació, per a la complementació per part de l'alumnat de les enquestes d'avaluació de l'actuació del professorat i d'avaluació de l'assignatura/mòdul.

## Activitats formatives

| Títol  | Hores | ECTS | Resultats d'aprenentatge  |
|--|-------|------|---------------------------|
| Tipus: Dirigides   |       |      |                           |
| Sessions de laboratori   | 12    | 0,48 | 1, 2, 3, 4, 5, 6, 7, 8, 9 |
| Sessions de problemes  | 12    | 0,48 | 1, 2, 3, 4, 5, 6, 7, 8, 9 |
| Sessions de teoria   | 26    | 1,04 | 1, 2, 3, 4, 5, 6, 7, 8    |
| Tipus: Supervisades  |       |      |                           |
| Treball tutoritzat   | 18    | 0,72 | 1, 2, 3, 4, 5, 6, 7, 8    |
| Tipus: Autònomes   |       |      |                           |
| Preparació i estudi de les proves d'avaluació                  | 30    | 1,2  | 1, 2, 3, 4, 5, 6, 7, 8    |
| Preparació, estudi i treball autònom de pràctiques i problemes | 45    | 1,8  | 1, 2, 3, 4, 5, 6, 7, 8, 9 |

## Avaluació

L'avaluació es farà en base al seguiment de l'alumnat durant l'assignatura. Es divideix principalment en dos blocs:

- Avaluació individual: es divideix en evidències concretes sobre el contingut de l'assignatura i avaluació del treball supervisat de forma individual. Tot i que pot haver una part d'avaluació de caire pràctic, es tracta majoritàriament de treball teòric.
- Avaluació col·lectiva: consta majoritàriament de l'avaluació del treball supervisat tant a nivell teòric com pràctic.

Com es pot veure, les activitats d'avaluació es divideixen en proves individuals i col·lectives tant de caire pràctic com de caire teòric. Les proves individuals es duran a terme al llarg del curs de forma continuada. Tot i així es preveu la realització d'una prova final que permeti recuperar les proves parcials d'avaluació individual.

#### Avaluació final:

Sobre l'avaluació continuada que es durà a terme durant el curs es preveu la realització de:

- 2 proves parcials d'avaluació individual. La nota mínima exigida de cadascuna de les proves és de 4.5 sobre 10.
- Avaluació de pràctiques al laboratori. La nota mínima exigida de cadascuna de les pràctiques és de 4.5 sobre 10.
- Avaluació del treball supervisat (treball realitzat fora de l'aula) i problemes o activitats a les sessions de problemes. Aquesta part no requereix nota mínima.

Per poder aprovar l'assignatura cal que l'avaluació de cadascuna de les parts superi el mínim exigít i que l'avaluació total superi els 5 punts.

En cas de no superar l'assignatura degut a que alguna de les activitats d'avaluació no arriba a la nota mínima requerida, la nota numèrica de l'expedient serà el valor menor entre 4.5 i la mitjana ponderada de les notes.

La qualificació de "no avaluable" s'otorgarà a l'alumnat que no participi en cap de les activitats d'avaluació.

La qualificació de "matricula d'honor" s'otorgarà a l'alumnat amb nota igual o superior a 9 per ordre de millor nota final.

#### Recuperació de notes de l'avaluació continuada:

Es realitzarà un examen final de recuperació que permetrà recuperar els exàmens parcials. Així mateix es permetrà un lliurament final per recuperar aquelles pràctiques suspeses (aquest lliurament addicional comportarà una penalització a la nota final de la pràctica). La part de problemes i o activitats que no requereix nota mínima no es podrà recuperar.

#### Convalidacions parcials a l'alumnat repetidor:

Inicialment no es planteja la possibilitat de convalidar parts de l'assignatura, ni la realització de proves de sistèms especials a l'alumnat repetidor. Tot i així aquest fet es pot reconsiderar a començament de curs en funció dels continguts de cada part.

#### Dates d'activitats d'avaluació:

Les dates d'avaluació continuada i lliurament de treballs i pràctiques es publicaran al campus virtual i poden estar subjectes a canvis de programació per motius d'adaptació a possibles incidències. Sempre s'informarà al campus virtual sobre aquests canvis ja que s'entén és el mecanisme habitual d'intercanvi d'informació entre el professorat i l'alumnat.

Així mateix, es detallaran amb prou temps d'antelació els mecanismes d'avaluació, metodologia o funcionament general de l'assignatura que no s'hagin concretat en aquesta guia.

Per a cada activitat d'avaluació, s'indicarà un lloc, data i hora de revisió en la que l'estudiant podrà revisar l'activitat amb el professor. En aquest context, es podran fer reclamacions sobre la nota de l'activitat, que seran avaluades pel professorat responsable de l'assignatura. Si l'estudiant no es presenta a aquesta revisió, no es revisarà posteriorment aquesta activitat.

#### Compromís ètic:

Sense perjudici d'altres mesures disciplinàries que s'estimin oportunes, i d'acord amb la normativa acadèmica vigent, les irregularitats comeses per l'alumnat que puguin conduir a una variació de la qualificació, es qualificaran amb un zero (0). Les activitats d'avaluació qualificades d'aquesta forma i per aquest procediment no seran recuperables. Si és necessari superar qualsevol d'aquestes activitats d'avaluació per aprovar

l'assignatura, aquesta assignatura quedarà suspesa directament, sense oportunitat de recuperar-la en el mateix curs. Aquestes irregularitats inclouen, entre d'altres:

- la còpia total o parcial d'una pràctica, informe, o qualsevol altra activitat d'avaluació;
- deixar copiar;
- presentar un treball de grup no fet íntegrament pels membres del grup;
- presentar com a propis materials elaborats per un tercer, encara que siguin traduccions o adaptacions, i en general treballs amb elements no originals i exclusius de l'estudiant;
- tenir dispositius de comunicació (com telèfons mòbils, smart watches, etc.) accessibles durant les proves d'avaluació teórico-pràctiques individuals (exàmens).

La nota numèrica de l'expedient serà el valor menor entre 3.0 i la mitjana ponderada de les notes en cas que l'estudiant hagi comès irregularitats en un acte d'avaluació (i per tant no serà possible aprovar l'assignatura per compensació).

## Activitats d'avaluació

| Títol                              | Pes | Hores | ECTS | Resultats d'aprenentatge  |
|------------------------------------|-----|-------|------|---------------------------|
| Problemes, exercicis, i activitats | 15% | 2     | 0,08 | 1, 2, 3, 4, 5, 6, 7, 8, 9 |
| Proves individuals                 | 45% | 3     | 0,12 | 1, 2, 3, 4, 5, 6, 7, 8    |
| Pràctiques laboratori              | 40% | 2     | 0,08 | 1, 2, 3, 4, 5, 6, 7, 8, 9 |

## Bibliografia

De manera orientativa es dóna la següent bibliografia per a l'assignatura:

- Mark Stamp (2011) Information Security: principles and practice, 2n Edition. John Wiley & Sons. Biblioteca UAB: [https://cataleg.uab.cat/iii/encore/record/C\\_\\_Rb1934013](https://cataleg.uab.cat/iii/encore/record/C__Rb1934013)
- Adam Shostack (2014) Threat Modeling. Designing for security. John Wiley & Sons. Biblioteca UAB: [https://cataleg.uab.cat/iii/encore/record/C\\_\\_Rb1956467](https://cataleg.uab.cat/iii/encore/record/C__Rb1956467)
- Xabiel García Pañeda, David Melendi Palacio (2008) La peritación informática, un enfoque práctico, Colegio Oficial de Ingenieros en Informática Principado de Asturias. Biblioteca UAB: [https://cataleg.uab.cat/iii/encore/record/C\\_\\_Rb1999885](https://cataleg.uab.cat/iii/encore/record/C__Rb1999885)
- Vicens Torra (2017) Data Privacy: Foundations, New Developments and the Big Data Challenge. Springer. Biblioteca UAB: [https://cataleg.uab.cat/iii/encore/record/C\\_\\_Rb2038206](https://cataleg.uab.cat/iii/encore/record/C__Rb2038206)
- Peter Szor (2005) The Art of Computer Virus Research and Defense. Addison-Wesley. Biblioteca UAB: [https://cataleg.uab.cat/iii/encore/record/C\\_\\_Rb1876518](https://cataleg.uab.cat/iii/encore/record/C__Rb1876518)
- Wenliang Du (2017) Computer Security. A Hands-on Approach. Biblioteca UAB: [https://cataleg.uab.cat/iii/encore/record/C\\_\\_Rb2060405](https://cataleg.uab.cat/iii/encore/record/C__Rb2060405)
- Matt Bishop (2002) Computer Security: Art and Science, Addison-Wesley. Biblioteca UAB: [https://cataleg.uab.cat/iii/encore/record/C\\_\\_Rb1876515](https://cataleg.uab.cat/iii/encore/record/C__Rb1876515)
- Dieter Gollmann (2011) Computer Security, 3rd Edition. John Wiley & Sons. Biblioteca UAB: [https://cataleg.uab.cat/iii/encore/record/C\\_\\_Rb1909014](https://cataleg.uab.cat/iii/encore/record/C__Rb1909014)
- Michael Sikorski, Andrew Honig (2012) Practical Malware Analysis. The hands-on guide to dissecting malicious software. No Starch Press.

## Programari

Donada la multidisciplinarietat d'aquesta assignatura es faran servir diferents eines i llenguatges de programació depenent de l'activitat concreta a realitzar, tant per les pràctiques com per les activitats i exercicis. Es fan servir llenguatges de programació com Python, R, o C, i diferent programari i eines de sistemes (principalment Linux) com: eines de virtualització (virtualbox), metasploit, openssl, etc.

