GUIA DOCENT

SEGURETAT D'APLICACIONS I COMUNICACIONS

Coordinació: OJEDA CONTRERAS, JESUS

Any acadèmic 2022-23

SEGURETAT D'APLICACIONS I COMUNICACIONS 2022-23

Informació general de l'assignatura

<table>
<tr><td>Denominació</td><td>SEGURETAT D'APLICACIONS I COMUNICACIONS</td></tr>
<tr><td>Codi</td><td>102380</td></tr>
<tr><td>Semestre d'impartició</td><td>1R Q(SEMESTRE) AVALUACIÓ CONTINUADA</td></tr>
<tr><td>Caràcter</td><td>
<table>
<tr><th>Grau/Màster</th><th>Curs</th><th>Caràcter</th><th>Modalitat</th></tr>
<tr><td>Grau en Tècniques d'Interacció Digital i de Computació</td><td>3</td><td>OBLIGATÒRIA</td><td>Presencial</td></tr>
</table>
</td></tr>
<tr><td>Nombre de crèdits assignatura (ECTS)</td><td>6</td></tr>
<tr><td>Tipus d'activitat, crèdits i grups</td><td>
<table>
<tr><th>Tipus d'activitat</th><th>PRALAB</th><th>TEORIA</th></tr>
<tr><td>Nombre de crèdits</td><td>3</td><td>3</td></tr>
<tr><td>Nombre de grups</td><td>1</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>Coordinació</td><td>OJEDA CONTRERAS, JESUS</td></tr>
<tr><td>Departament/s</td><td>INFORMÀTICA I ENGINYERIA INDUSTRIAL</td></tr>
<tr><td>Distribució càrrega docent entre la classe presencial i el treball autònom de l'estudiant</td><td>6 ECTS = 25x6 = 150 hores de treball
40% -> 60 hores presencials
60% -> 90 hores treball autònom de l'estudiant</td></tr>
<tr><td>Informació important sobre tractament de dades</td><td>Consulteu aquest enllaç per a més informació.</td></tr>
<tr><td>Idioma/es d'impartició</td><td>Castellà / Català</td></tr>
</table>

SEGURETAT D'APLICACIONS I COMUNICACIONS 2022-23

Professor/a (s/es)	Adreça electrònica professor/a (s/es)	Crèdits impartits pel professorat	Horari de tutoria/lloc
OJEDA CONTRERAS, JESUS	jesus.ojedacontreras@udl.cat	6	

Informació complementària de l'assignatura

Per a qualsevol dubte i/o qüestió, podeu enviar un correu electrònic a professor de l'assignatura.

Objectius acadèmics de l'assignatura

- Entendre els conceptes, problemes i procediments de seguretat informàtica
- Entendre els conceptes i mecanismes principals de la criptografia
- Entendre i ser capaços de fer una anàlisi de riscos
- Dissenyar i configurar esquemes de tallafocs

Competències

- CT3. Implementar noves tecnologies i tecnologies de la informació i la comunicació.
- CG2. Capacitat per dissenyar, desenvolupar, avaluar i garantir l'accessibilitat, ergonomia, usabilitat i seguretat dels sistemes informàtics.
- CG3. Capacitat per utilitzar plataformes de maquinari i programari adequades per al desenvolupament i execució d'aplicacions digitals interactives.
- CE7. Conèixer, administrar i mantenir sistemes, serveis i aplicacions informàtiques interactives.
- CE12. Conèixer i saber aplicar les característiques, funcionalitat i estructura de les xarxes d'ordinadors i internet, i dissenyar i implementar aplicacions interactives basades en elles.

Continguts fonamentals de l'assignatura

1. Fonaments de seguretat de la informació
2. Criptografia
    - Funcions Hash (MD5, SHA)
    - Criptografia simètrica (DES, AES)
    - Criptografia asimètrica (RSA, ElGamal)
3. Seguretat de sistema operatiu
    - Sandboxing (chroot)
    - Tallafocs (iptables)
4. Riscos, vulnerabilitats i atacs

Eixos metodològics de l'assignatura

Atenent a l'horari de l'assignatura, cada setmana l'estudiant assisteix a 2 hores de Teoria i a 2 hores presencials de laboratori (PRALAB).

A les sessions de Teoria es presenten els temes que es poden consultar a l'apartat de continguts. Incorporen exemples il·lustratius i propostes de problemes per resoldre en les classes de laboratori.

Les sessions PRALAB s'imparteixen al laboratori i presenten problemes i s'analitzen les solucions proposades. També es poden presentar les pràctiques de l'assignatura i es realitza el treball de laboratori corresponent.

SEGURETAT D'APLICACIONS I COMUNICACIONS 2022-23

El treball autònom de l'estudiant consisteix en la resolució dels exercicis proposats i les tasques de pràctiques quan així s'indiqui.

El llenguatge de programació usat en les pràctiques és Python. També es faran servir màquines virtuals com VirtualBox.

Pla de desenvolupament de l'assignatura

Sem	Descripció	Activitat Teoria	Activitat PRALAB	Treball autònom
1	Fonaments	T1: Fonaments	Repàs Python	Consulta de bibliografia i programa, Repàs Python
2	Funcions Hash	T2: Criptografia	Python, Presentació P1	P1, Problemes T2
3	Funcions Hash	T2: Criptografia	Problemes T2	P1, Problemes T2
4	Cripto simètrica	T2: Criptografia	P1	P1, Problemes T2
5	Cripto simètrica	T2: Criptografia	Problemes T2	P1, Problemes T2
6	Cripto asimètrica	T2: Criptografia	P1	P1, Problemes T2
7	Cripto asimètrica	T2: Criptografia	P1 - Lliurament P1	Problemes T2
8	Sandboxing	T3: Seguretat SO	Dubtes T1	Problemes T3
9		1r Parcial		Estudiar
10	Sandboxing	T3: Seguretat SO	Presentació P2	P2, Problemes T3
11	Tallafocs	T3: Seguretat SO	P2, Problemes T3	P2, Problemes T3
12	Tallafocs	T3: Seguretat SO	P2	P2, Problemes T3
13	Riscos i Atacs	T4: Riscos i Atacs	P2, Problemes T4	P2, Problemes T4
14	Riscos i Atacs	T4: Riscos i Atacs	Lliurament P2	Problemes T4
15	Riscos i Atacs	T4: Riscos i Atacs	Dubtes T3 i T4	Problemes T4
16/17		2n Parcial		Estudiar
18				
19		Recuperació		Estudiar

Sistema d'avaluació

Acr	Activitat d'avaluació	Ponderació	Nota Mínima	En grup	Obligatòria	Recuperable
PE1	Examen 1r Parcial	25%	-	No	No	Sí
PE2	Examen 2n parcial	25%	-	No	No	Sí
P1	Pràctica 1	25%	-	Sí (<= 2)	No	No
P2	Pràctica 2	25%	-	Sí (<= 2)	No	No

Nota Final = 0.25 * PE1 + 0.25 * PE2 + 0.25 * P1 + 0.25 * P2

Recuperació de les proves escrites 1 i 2: Si la nota final obtinguda en l'assignatura és <5, llavors l'estudiant pot optar a millorar/recuperar el 50% que representen les proves escrites (l'estudiant podrà triar quina part vol recuperar, o triar les dues parts).

Excepte nova situació d'excepcionalitat, les proves escrites seran presencials.

Bibliografia i recursos d'informació

- William Stallings. Cryptography and Network Security. Prentice Hall. 2005.
- Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press. 1996.
- Adam Shostack. Threat modeling: designing for security. Wiley. 2014.
- Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, Terron Williams. Gray Hat Hacking: The Ethical Hackers Handbook. McGraw-Hill. 2011.