

GRAU EN ENGINYERIA INFORMÀTICA DE GESTIÓ I SISTEMES D'INFORMACIÓ

103826 - INTRODUCCIÓ A LA CIBERSEGURETAT

Informació general

- Curs acadèmic 2026/27
- Departament: Tecnologia
- Tipus d'assignatura: Optativa
- Curs: Quart
- Trimestre: Tercer
- Nombre de crèdits: 6
- Professorat:
 - Pere Vidiella Catalan pvidiellaa@tecnocampus.cat

Llengües de docència

- Anglès

La impartició de les classes de teoria i de laboratori, així com la documentació de l'assignatura i les proves d'avaluació, seran exclusivament en anglès. Per tant, els i les alumnes han de poder seguir les explicacions dels docents de l'assignatura en anglès, així com llegir i comprendre textos escrits en anglès tècnic. Pel que fa a les activitats d'avaluació i les entregues dels informes, els i les alumnes podran respondre-les en català, castellà o anglès, segons els hi resulti més convenient, tot i que es recomana fer-ho en anglès. Finalment, durant les activitats d'avaluació, els i les alumnes podran fer preguntes als docents de l'assignatura per tal de facilitar la comprensió dels enunciats i la seva resolució.

Presentació de l'assignatura

En general, aquesta assignatura abasta els següents descriptors especificats per a la matèria a la qual pertany (Arquitectura de Computadors, Sistemes Operatius i Xarxes d'Ordinadors):

1. Xarxes d'àrea local (arquitectura i tipologies, Ethernet, xarxes sense fils).
2. Xarxes IP (protocol, encaminament, ARP, traducció d'adreces, DNS, firewalls, xarxes privades).
3. Conceptes avançats dels protocols TCP/IP, proveïdors de serveis d'Internet (ISP) algorismes d'encaminament i protocols multimèdia.
4. Aplicacions en xarxa (paradigma client-servidor, intercanvi de documents (HTTP, FTP), correu electrònic (SMTP, POP3, IMAP), representació de la informació estructurada (BASE64, XML, JSON)).
5. Seguretat en les xarxes d'ordinadors: protecció, protocols de seguretat, comerç electrònic, gestió de les aplicacions.

Competències/Resultats d'aprenentatge

Bàsica

- B2_ Que els estudiants sàpiguin aplicar els seus coneixements a la seva feina o vocació d'una forma professional i tinguin les competències que demostrin mitjançant l'elaboració i defensa d'arguments i la resolució de problemes dins de la seva àrea d'estudi

Comú

- CIN1_Capacitat per a dissenyar, desenvolupar, seleccionar i avaluar aplicacions i sistemes informàtics, assegurant la seva fiabilitat, segureta i qualitat, segons els principis ètics i la legislació i normativa vigent
- CIN2_Capacitat per a planificar, concebre, desplegar i dirigir projectes, serveis i sistemes informàtics en tots els àmbits, liderant la seva posada en marxa i la seva millora contínua i valorant el seu impacte econòmic i social
-

CIN5_Coneixement, administració i manteniment de sistemes, serveis i aplicacions informàtiques

- CIN8_Capacitat per analitzar, dissenyar, construir i mantenir aplicacions de forma robusta, segura i eficient, escollint el paradigma i els llenguatges de programació més adequats
- CIN10_Coneixement de les característiques, funcionalitats i estructura dels Sistemes Operatius i dissenyar i implementar aplicacions basades en els seus serveis
- CIN11_Coneixement i aplicació de les característiques, funcionalitats i estructura dels Sistemes Distribuïdors, les xarxes de computadores i Internet i dissenyar i implementar aplicacions basades amb elles.
- CIN18_Coneixement de la normativa i la regulació de la informàtica en els àmbits nacional europeus i internacional

Específica

- ESI1_Capacitat per integrar solucions de Tecnologies de la Informació i de les Comunicacions i processos empresarials per a satisfer les necessitats d'informació de les organitzacions, permetent arribar als seus objectius de forma efectiva i eficient, aconseguint així avantatges competitives
- ESI2_Capacitat per determinar els requisits dels sistemes d'informació i comunicació d'una organització, atenent a aspectes de seguretat i compliment de la normativa i legislació vigent
- ESI3_Capacitat per participar activament en l'especificació, disseny, implementació i manteniment dels sistemes d'informació i comunicació
- ESI5_Capacitat per comprendre i aplicar els principis de l'avaluació de riscos i aplicar-los correctament en l'elaboració i execució de plans d'actuació

Transversal

- T1_Que els estudiants coneixin un tercer idioma, que serà preferentment l'anglès, amb un nivell adequat de forma oral i per escrit, d'acord amb les necessitats que tindran les graduades i els graduats a cada titulació

No definides

Continguts

L'assignatura està estructurada tal com s'indica a continuació:

- Tema 1: Introducció a la ciberseguretat
- Tema 2: Vulnerabilitats
- Tema 3: Amenaces
- Tema 4: Gestió del risc
- Tema 5: Compliment (normes)
- Tema 6: Criptografia
- Tema 7: Ciberseguretat forense

Per al correcte seguiment de l'assignatura, els i les estudiants treballaran amb el seu ordinador personal (portàtil), que hauran de portar a totes les classes.

L'aula (física o virtual) és un espai segur, lliure d'actituds masclistes, racistes, homofòbes, transfòbes i discriminatòries, sigui cap a l'alumnat o cap al professorat. Confiam que entre totes i tots puguem crear un espai segur on ens puguem equivocar i aprendre sense haver de patir prejudicis d'altres.

Objectius de Desenvolupament Sostenible

- 08 - Treball digne i creixement econòmic
- 04 - Educació de qualitat
- 09 - Indústria, Innovació i Infraestructures

Activitats i Sistema d'avaluació

L'assignatura s'avalua a través de l'avaluació contínua i una prova de validació de coneixements, tal com s'indica a continuació:

- Avaluació contínua (CONTINUA): 80%
- Prova de validació (VALIDACIÓ): 20%

La nota final de l'assignatura (NFA) es calcula segons:

- $FINAL = CONTINUA \times 0,8 + VALIDACIÓ \times 0,2$
- Si $VALIDACIÓ \geq 5$: $NFA = FINAL$
- Si $VALIDACIÓ < 5$: $NFA = VALIDACIÓ$

Consideracions addicionals:

- Totes les activitats són de caràcter obligatori; les activitats a les quals no s'ha assistit o no s'han realitzat s'avaluen amb un zero (0).
- La nota de la prova de validació és recuperable en data oficial, mentre que les notes de l'avaluació contínua no són recuperables.
- Qualsevol indicatiu de còpia o plagi (de companys, de fonts no citades, o d'eines com ChatGPT, Claude, Gemini...) comportarà que l'activitat s'avalui amb un zero (0).
- El comportament reiterat de còpia o plagi comportarà que l'assignatura s'avalui amb un zero (0) i l'estudiant sigui reportat a la direcció de la Universitat.

Bibliografia i Recursos

- J. Graham, R. Howard, R. Olson. Cybersecurity Essentials. CRC Press.
- The Cyber Security Body of Knowledge (CyBOK). Disponible en línia a: <https://www.cybok.org/>.