



### ANNEX III

#### DESCRIPCIÓ DEL LLOC, FUNCIONS, TEMARI I BIBLIOGRAFIA

<b>CODI</b> 00047530	<b>GRUP</b> I	<b>COMPLEMENT DEL LLOC DE TREBALL</b> 0D	<b>HORARI</b> Continuat de matí
<b>DENOMINACIÓ DEL LLOC DE TREBALL</b> Cap de projecte			
<b>ADSCRIPCIÓ ORGÀNICA</b> Àrea de Tecnologies de la Informació i la Comunicació			
<b>UNITAT</b> Infraestructures TIC		<b>ÀMBIT</b> Infraestructures	
<b>CENTRE DE DESTINACIÓ (UBICACIÓ)</b> Travessera de les Corts, 131-159, 08028 Barcelona			

#### REQUISITS DE TITULACIÓ

Titulació universitària superior, grau universitari o màster universitari oficial o titulació equivalent.

#### MISSIÓ

Planificar i coordinar els processos vinculats als projectes del seu àmbit, d'acord amb les directrius definides pel lloc de comandament, amb la finalitat d'assolir els objectius establerts pel que fa a terminis, costos i qualitat.

#### FUNCIONS GENÈRIQUES

1. Coordinar el personal i els recursos materials assignats, i detectar les necessitats que es puguin produir.
2. Coordinar, gestionar i avaluar les activitats que es duen a terme en el seu àmbit competencial.
3. Aplicar, assessorar i difondre normatives, metodologia i criteris d'actuació del seu àmbit competencial, d'acord amb les directrius establertes.
4. Elaborar informes, criteris d'actuació i documents de seguiment dels projectes del seu àmbit d'actuació.
5. Planificar i definir projectes i serveis informàtics nous, establir-ne els objectius generals, la metodologia i els grups de treball, i avaluar-ne els resultats.
6. Elaborar estudis tècnics i organitzatius que permetin definir la idoneïtat d'implementar solucions informàtiques noves.
7. Negociar amb proveïdors externs el nivell de servei tècnic requerit per a la gestió informàtica del seu àmbit.
8. Dur a terme altres funcions de contingut assimilable a les anteriors, quan escaigui.

#### FUNCIONS ESPECÍFIQUES

1. Desenvolupar i gestionar el Programa de seguretat de la informació de la Universitat de Barcelona.
2. Participar en la contractació pública de subministraments i serveis, i gestionar serveis externalitzats.
3. Vetllar pel compliment normatiu en l'àmbit de la ciberseguretat, i definir polítiques de seguretat corporatives, gestionar incidències i coordinar accions proactives i reactives respecte de les incidències, i coordinar-se amb altres rols de la universitat vinculats amb la seguretat, especialment en l'àmbit de la protecció de dades personals.
4. Treballar conjuntament i col·laborativament amb altres institucions en l'àmbit de la ciberseguretat, especialment amb altres universitats, el CSUC i l'Agència de Ciberseguretat.
5. Donar suport als desenvolupadors de programari de la UB per aplicar seguretat en el disseny i desenvolupament de programari.



### TIPOLOGIA DE LA PROVA

La prova consisteix en un o més exercicis de la tipologia següent:

- Preguntes de tipus test, curtes o obertes.
- Cas pràctic (escrit a mà o amb ordinador).
- Exercici pràctic relacionat amb les funcions del lloc de treball.

### TEMARI I MATERIAL BIBLIOGRÀFIC

#### Temari

Àmbit general:

1. Gestió d'operacions informàtiques
  - Gestió d'equips de treball i del temps propi
  - Recepció, delegació i gestió de l'execució de les operacions
  - Gestió de la base de coneixement d'operacions
  - Gestió de projectes informàtics
  - ITIL com a marc de referència per a l'entrega de serveis TIC
2. L'esquema nacional de seguretat i la seva instrucció tècnica de seguretat
  - El govern de la ciberseguretat
  - Arquitectures de seguretat
  - Organització, rols i responsabilitats
  - Auditoria i control
3. Protecció de dades i protecció de dades personals
  - Principis de la protecció de dades
  - Dades especialment protegides
  - El dret d'accés als fitxers
  - Avaluació d'impacte

Àmbit de la UB:

1. Operativa de ciberseguretat. Desenvolupament segur. Criptografia. Monitorització de la seguretat. Noves tecnologies: la seva aplicació a la ciberseguretat. Anàlisi de vulnerabilitats. Piratge (*hacking*) ètic. Seguretat en l'accés remot i el teletreball
2. Anàlisi i gestió de riscos: principals estàndards nacionals i internacionals. Identificació i gestió de riscos i amenaces. Adequació de l'organització. Ús d'eines de gestió de riscos i compliment
3. Gestió de ciberincidents: fonaments, organització, procés i normativa
4. Qualitat i seguretat de programari. Cicle de vida de desenvolupament segur de programari (SDLC). Tècniques de desenvolupament segur d'aplicacions. Auditoria de codi: eines. Mètriques de qualitat. Estratègies de proves. Bones pràctiques de seguretat
5. Seguretat en sistemes operatius. Vulnerabilitats i pedaços del sistema operatiu. Atacs per mala configuració. Política de contrasenyes. Seguretat física
6. Codi maliciós. Virus i cucs. Troians. Rootkits. Detecció del codi maliciós
7. Seguretat en dispositius mòbils: vulnerabilitats, privacitat, seguretat, recomanacions de seguretat
8. Amenaces a internet. Les xarxes socials. Les xarxes P2P. Els cercadors. Serveis al núvol. La responsabilitat dels usuaris



9. Seguretat en entorns al núvol. Riscos específics del núvol. Seguretat en xarxes, instàncies, dades i desplegament d'infraestructures. Monitoratge i auditoria. Seguretat SAAS
10. Xifratge de dades. Tipus de xifratge. Xifratge de discos i fitxers. Xifratge de comunicacions. Signatura digital. Atacs al xifratge

Normativa en matèria d'igualtat:

1. Pla d'igualtat de la Universitat de Barcelona: punt 3.1 (Context legal) i punt 5.1 (Estructura del Pla i principis generals)
2. Llei orgànica 2/2023, de 22 de març, del sistema universitari: articles 43, 44 i 46

### Material bibliogràfic

- Esquema nacional de seguretat: [ens.ccn.cni.es/ca](https://ens.ccn.cni.es/ca), [Reial decret 311/2022, de 3 de maig, pel qual es regula l'esquema nacional de seguretat](#), [Portal d'administració electrònica: esquema nacional de seguretat](#)
- Protecció de dades i protecció de dades personals: Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals ([BOE-A-2018-16673-C.pdf](#)), [Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD](#)
- Programa de seguretat de la informació: [isaca.org](#), [ISO/IEC 27002](#), [ISO/IEC 27001](#), [ISO/IEC 27000-series](#), [incibe.es](#)
- Seguretat UB: [Seguretat de les dades](#) i [Polítiques i normativa UB](#)
- Resposta a incidents i importància del compliment normatiu: [incibe.es/sites/default/files/contenidos/politicas/documentos/respuesta-incidentes.pdf](#)  
[Compliance y protección de datos: la importancia del cumplimiento normativo \(captio.net\)](#)
- [Pla d'igualtat de la Universitat de Barcelona](#)
- <https://www.boe.es/eli/es/lo/2023/03/22/2/con>