Master's degree in Cybersecurity

El **master's degree in Cybersecurity** (**web del màster**) (màster universitari en Ciberseguretat) té com a missió oferir una formació sòlida en l'àmbit de la seguretat de la informació, amb una àmplia base científica, per aportar a la societat professionals molt especialitzats en els camps de la protecció de les dades, la protecció de les infraestructures i la protecció de les aplicacions.

DADES GENERALS

Durada i inici

1 curs acadèmic, 60 crèdits ECTS. Inici: setembre

Horaris i modalitat

Presencial

Preus i beques

Preu aproximat del màster sense despeses addicionals, 1.660 € (4.150 € per a no residents a la UE).
Més informació sobre preus i pagament de la matrícula
Més informació de beques i ajuts

Idiomes

Anglès

Informació sobre l'ús de llengües a l'aula i els drets lingüístics de l'estudiantat.

Lloc d'impartició

- Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona (ETSETB)
- Facultat d'Informàtica de Barcelona (FIB)

Títol oficial

Títol oficial

ACCÉS

Requisits generals

Requisits acadèmics d'accés a un màster

Requisits específics

Per accedir al màster s'exigeix el **nivell B2 d'anglès**, que s'ha d'acreditar en el moment de formalitzar la matrícula.

Accés directe

El perfil recomanat per accedir a aquest màster és el següent:

- Grau en Ciències i Tecnologies de Telecomunicació.
- Grau que habiliti per a l'exercici de la professió d'enginyer tècnic de telecomunicació:
- Grau en Enginyeria de Sistemes Audiovisuals.
- Grau en Enginyeria de Sistemes Electrònics.
- Grau en Enginyeria de Sistemes de Telecomunicació.
- Grau en Enginyeria Telemàtica.
- Grau en Enginyeria Electrònica de Telecomunicació.
- Grau en Enginyeria Informàtica.
- Enginyeria de Telecomunicació.
- Enginyeria Informàtica

Complements formatius

Es considera possible però excepcional l'entrada d'estudiants amb altres titulacions de les que s'especifiquen en el perfil d'ingrés recomanat.

En aquestes situacions excepcionals, la Comissió Acadèmica del màster podrà estudiar el cas i permetre l'accés de l'estudiantat amb algun complement de formació fora dels 60 ECTS del màster.

En aquest cas, els complements formatius que l'estudiant hagi de cursar hauran de correspondre als dels graus dels **centres sol·licitants** i com a màxim podran equivaler a 10 ECTS.

El nombre de crèdits i les assignatures que s'hagin de cursar variarà segons la titulació d'ingrés, ja sigui de grau o de l'ordenació d'estudis anterior, i de les competències acadèmiques prèvies de l'estudiant reflectides en el seu expedient acadèmic.

Criteris d'admissió

El Comitè Acadèmic s'encarrega de les decisions sobre l'admissió dels candidats. Els criteris són: informació acadèmica (50%), currículum i experiència professional (40%) i motivació (10%).

Els detalls dels criteris són els següents: Informació acadèmica:

- Qualificació mitjana final per al grau que brinda accés al màster.
- Rànquing de la universitat que emet el títol anterior, usant les classificacions més comuns (per exemple, ARWU, QS World University, etc.)
- Rendiment acadèmic en el títol anterior.

Currículum i experiència professional:

- Idoneïtat del títol previ del candidat. Els títols de títols de grau en disciplines en el camp de la informàtica o la ciència i la tecnologia de les telecomunicacions preferències preferencials.
- Experiència en projectes d'innovació i recerca.

Motivació

- Currículum i carta de motivació del candidat.

Places

44

Preinscripció

Període de preinscripció obert.
Termini previst: fins al 03/07/2023.
Com es formalitza la preinscripció?

Admissió i matrícula

Com es formalitza la matrícula?

Legalització de documents

Els documents expedits per estats no membres de la Unió Europea ni signataris de l'Acord sobre l'espai econòmic europeu han d'estar legalitzats per via diplomàtica o amb la postil·la corresponent.

SORTIDES PROFESSIONALS

Sortides professionals

- Àrea de tecnologies de la informació i comunicació.
- Àrea de programació informàtica.
- Administració pública.
- Analista de seguretat.
- Responsable de riscos de seguretat.
- Consultor de seguretat.
- Analista forense digital.
- *Hacker* ètic.
- Responsable de SOC (*security operations center*).
- CSO en empreses tecnològiques (*chief security officer*).
- CSO en empreses no tecnològiques però amb departaments d'IT.

Competències

Competències transversals

Les competències transversals descriuen allò que un titulat o titulada ha de saber o ha de ser capaç de fer en acabar el procés d'aprenentatge, amb independència de la titulació. **Les competències transversals establertes a la UPC** són emprenedoria i innovació, sostenibilitat i compromís social, coneixement d'una tercera llengua (preferentment l'anglès), treball en equip i ús solvent dels recursos d'informació.

Competències específiques:

- Dissenyar aplicacions d'alt valor afegit basades en les tecnologies de la informació i les comunicacions (TIC) aplicades a l'àmbit de la ciberseguretat.
- Identificar i seleccionar les eines més adequades per a la detecció i l'anàlisi d'atacs i incidents de seguretat segons la seva naturalesa i l'entorn on s'han produït.
- Identificar i analitzar les lleis i regulacions aplicables en matèria de ciberseguretat, i entendre les implicacions ètiques que les tècniques de ciberdefensa poden tenir en la privacitat dels usuaris i saber com es poden minimitzar.
- Analitzar des d'un punt de vista matemàtic protocols criptogràfics de xifratge i gestió de claus segons la seva robustesa.
- Dissenyar, implementar i operar protocols d'autenticació, autorització i auditoria de sistemes informacionals com ara les bases de dades.
- Aplicar tècniques de monitoratge i anàlisi del trànsit de la xarxa per a la detecció d'atacs de ciberseguretat i la investigació d'incidents.
- Dissenyar, desenvolupar, detectar, analitzar i eliminar codi maliciós que sigui capaç d'infectar un sistema operatiu actual i ocultar-s'hi.
- Identificar i aplicar tècniques per mantenir en tot moment la seguretat i la privacitat de les aplicacions distribuïdes construïdes sobre els protocols d'internet.
- Elaborar individualment un treball original i presentar-lo i defensar-lo davant un tribunal universitari, consistent en un projecte d'enginyeria en l'àmbit de la ciberseguretat en el qual se sintetitzin les competències adquirides en els ensenyaments del màster.

ORGANITZACIÓ ACADÈMICA: NORMATIVES, CALENDARIS

Centre docent UPC

Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona (ETSETB)
Facultat d'Informàtica de Barcelona (FIB)

Calendari acadèmic

Calendari acadèmic dels estudis universitaris de la UPC

Normatives acadèmiques

Normativa acadèmica dels estudis de màster de la UPC

PLA D'ESTUDIS

Assignatures	crèdits ECTS	Tipus
PRIMER QUADRIMESTRE		
Àlgebra Matricial, Curs Intensiu	3	Optativa
Blockchain	5	Optativa
Criptografia Quàntica	5	Optativa
Gestió de la Seguretat	5	Optativa
Malware	5	Obligatòria
Monitoratge i Anàlisi del Trànsit de Xarxa	5	Obligatòria
Protecció de les Dades	5	Obligatòria
Seguretat de Xarxa	5	Obligatòria

Assignatures	crèdits ECTS	Tipus
Seguretat en Aplicacions	5	Obligatòria
SEGON QUADRIMESTRE		
Casos d'Ús en Ciberseguretat	5	Optativa
Computació i Criptografia Quàntica	3	Optativa
Comunicacions Segures en Xarxes de Fibra Òptica	5	Optativa
Curs Breu en les Matemàtiques De la Teoria de Codis i la Criptografia	3	Optativa
Pràctiques en Computació Quàntica i Intel·ligència Artificial	3	Optativa
Privadesa de Dades	5	Optativa
Seguretat de Xarxa – Autenticació i Autorització	5	Obligatòria
Seguretat Definida per Programari (Sds)	5	Optativa
Seguretat en el Hardware de Sistemes Encastats. Primitives, Debilitats i Contramesures	3	Optativa
Xarxes Òptiques Segures	3	Optativa
Treball de Fi de Màster	12	Projecte