Master's degree in Cybersecurity

The aim of the **master's degree in Cybersecurity** (**master's degree website**) is to offer students a solid scientific grounding in the field of information technology security so as to provide society with professionals who are highly specialised in data protection, infrastructure protection and application protection.

GENERAL DETAILS

Duration and start date

1 academic year, 60 ECTS credits. Starting September

Timetable and delivery

Face-to-face

Fees and grants

Approximate fees for the master's degree, excluding other costs, €1,660 (€4,150 for non-EU residents).
More information about fees and payment options
More information about grants and loans

Language of instruction

English

Information on language use in the classroom and students' language rights.

Location

- Barcelona School of Telecommunications Engineering (ETSETB)
- Barcelona School of Informatics (FIB)

Official degree

Official degree

ADMISSION

General requirements

Academic requirements for admission to master's degrees

Specific requirements

English Level B2 is required for admission to the master's degree and must be demonstrated when you enrol.

Direct admission

The following are recommended entrance qualifications for the master's degree:

- Bachelor's degree in Telecommunications Science and Technology.
- A bachelor's degree that qualifies the holder for professional practice as a technical telecommunications engineer.
- Bachelor's degree in Audiovisual Systems Engineering.
- Bachelor's degree in Electronic Systems Engineering.
- Bachelor's degree in Telecommunications Systems Engineering.
- Bachelor's degree in Network Engineering.
- Bachelor's degree in Electronic Engineering and Telecommunications.
- Bachelor's degree in Informatics Engineering.
- Pre-EHEA degree in Telecommunications Engineering.
- Pre-EHEA degree in Informatics Engineering.

Bridging courses

Exceptionally, applicants with other degrees may be admitted.

The academic committee of the master's degree reviews these cases and may admit these applicants on the condition

that they take bridging courses in addition to the 60 credits for the master's degree.

These bridging courses will be subjects on the bachelor's degrees at the schools that teach the master's degree, up to a maximum of 10 ECTS credits.

The number of credits and bridging courses to be taken will depend on the entrance qualification, whether a bachelor's degree or a pre-EHEA degree, and the academic competencies of the applicants, as reflected in their academic records.

Admission criteria

The Academic Committee is in charge of the admission decisions of the candidates.
The criteria are: Academic Information (50%), Background and professional experience (40%) and Motivation (10%).

The criteria details follow:

Academic Information:
- Final average grade for the undergraduate degree that provides access to the master's degree
- Ranking of the university issuing the previous degree, using the most common rankings (e.g. ARWU, QS World University, etc.)
- Academic performance on the previous degree

Background and professional experience:
- Suitability of the candidate's previous degree. Holders of bachelor's degrees in disciplines in the field of Computer Science or Telecommunications Science and Technology will be given preference
- Experience in innovation and research projects

Motivation:
- Candidate's resume and motivation letter

Places

40

Pre-enrolment

Pre-enrolment closed (consult the new pre-enrolment periods in the academic calendar).
How to pre-enrol

Enrolment

How to enrol

Legalisation of foreign documents

All documents issued in non-EU countries must be legalised and bear the corresponding apostille.

PROFESSIONAL OPPORTUNITIES

Professional opportunities

- Information and communication technologies.
- Computer programming.
- Public administration.
- Security analyst.
- Security risk specialist.
- Security consultant.
- Digital forensic analyst.
- Ethical hacker.
- Security operations centre (SOC) specialist.
- Chief security officer (CSO) in technology companies.
- CSO in non-technological companies that have IT departments.

Competencies

Generic competencies

Generic competencies are the skills that graduates acquire regardless of the specific course or field of study. The generic competencies established by the UPC are capacity for innovation and entrepreneurship, sustainability and social commitment, knowledge of a foreign language (preferably English), teamwork and proper use of information resources.

Specific competencies

- To design applications that have a high added value and are based on information and communication technologies (ICTs) applied to cybersecurity.
- To identify and select the most appropriate tools for detecting and analysing attacks and security incidents according to their nature and the setting in which they occurred.
- To identify and analyse the laws and regulations that apply in matters of cybersecurity and understand the ethical implications of cyber-defence techniques for users' privacy and how to minimise them.
- To analyse cryptographic key encryption and management protocols according to their robustness from a mathematical perspective.
- To design, implement and operate authentication, authorisation and auditing protocols for information systems such as databases.
- To apply network traffic monitoring and analysis techniques for detecting cybersecurity attacks and investigating incidents.
- To design, develop, detect, analyse and eliminate malicious code that is able to infect and conceal itself within a current operating system.
- To identify and apply techniques for maintaining the security and privacy of distributed applications built on internet protocols.
- To carry out and present and defend before an examination committee an original, individual piece of work consisting of a cybersecurity engineering project that synthesisesthe competencies acquired on the master's degree.

ORGANISATION: ACADEMIC CALENDAR AND REGULATIONS

UPC school

Barcelona School of Telecommunications Engineering (ETSETB)
Barcelona School of Informatics (FIB)

Academic calendar

General academic calendar for bachelor's, master's and doctoral degrees courses

Academic regulations

Academic regulations for master's degree courses at the UPC

CURRICULUM

Subjects	ECTS credits	Type
FIRST SEMESTER		
Applications Security	5	Compulsory
Blockchain	5	Optional
Cybersecurity Management	5	Optional
Data Protection	5	Compulsory
Malware	5	Compulsory
Matrix Algebra, Accelerated Program	3	Optional
Network Security	5	Compulsory
Network Traffic Monitoring and Analysis	5	Compulsory
SECOND SEMESTER		
Brief Course on The Mathematics Behind Coding Theory and Cryptography	3	Optional
Cybersecurity Usecases	5	Optional
Data Privacy	5	Optional

Subjects	ECTS credits	Type
Hardware Security in Embedded Systems. Primitives, Weaknesses and Countermeasures	3	Optional
Network Security - Authentication and Authorization	5	Compulsory
Quantum Computing and Cryptography	3	Optional
Secure Communications in Fiber-Optic Networks	5	Optional
Software-Defined Security (Sds)	5	Optional
Master's Thesis	12	Project