Master's degree in Cybersecurity

El **master's degree in Cybersecurity** (**web del máster**) (máster universitario en Ciberseguridad) tiene como misión ofrecer una formación sólida en el ámbito de la seguridad de la información, con una amplia base científica, para aportar a la sociedad profesionales muy especializados en los campos de la protección de los datos, la protección de las infraestructuras y la protección de las aplicaciones.

DATOS GENERALES

Duración e inicio

1 curso académico, 60 créditos ECTS. Inicio septiembre

Horarios y modalidad

Presencial

Precios y becas

Precio aproximado del máster sin gastos adicionales, 1.660 € (2.490 € para no residentes en la UE).
Más información sobre precios y pago de la matrícula
Más información de becas y ayudas

Idiomas

Inglés

Lugar de impartición

- Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona (ETSETB)
- Facultad de Informática de Barcelona (FIB)

Título oficial

Título oficial

ACCESO

Requisitos generales

Requisitos académicos de acceso a un máster

Requisitos específicos

Para acceder al máster se exige el **nivel B2 de inglés**, que se tiene que acreditar en el momento de formalizar la matrícula.

Acceso directo

El perfil recomendado para acceder a este máster es el siguiente:

- Grado en Ciencias y Tecnologías de Telecomunicación.
- Grado que habilite para el ejercicio de la profesión de ingeniero técnico de telecomunicación.
- Grado en Ingeniería de Sistemas Audiovisuales.
- Grado en Ingeniería de Sistemas Electrónicos.
- Grado en Ingeniería de Sistemas de Telecomunicación.
- Grado en Ingeniería Telemática.
- Grado en Ingeniería Electrónica de Telecomunicación.
- Grado en Ingeniería Informática.
- Ingeniería de Telecomunicación.
- Ingeniería Informática

Complementos formativos

Se considera posible pero excepcional la entrada de estudiantes con otras titulaciones de las que se especifican en el perfil de ingreso recomendado.

En estas situaciones excepcionales, la Comisión Académica del máster podrá estudiar el caso y permitir el acceso del estudiantado con algún complemento de formación fuera de los 60 ECTS del máster.

En este caso, los complementos formativos que el estudiante tenga que cursar tendrán que corresponder a los de los grados de los **centros solicitantes** y como máximo podrán equivaler a 10 ECTS.

El número de créditos y las asignaturas que se tengan que cursar variará según la titulación de ingreso, ya sea de grado o de la ordenación de estudios anterior, y de las competencias académicas previas de la estudiante reflejadas en su expediente académico.

Criterios de admisión

El Comité Académico se encarga de las decisiones sobre la admisión de los candidatos. Los criterios son: información académica (50%), currículum y experiencia profesional (40%) y motivación (10%).

Los detalles de los criterios son los siguientes: Información académica:

- Calificación promedio final para el grado que brinda acceso al máster.
- Ranking de la universidad que emite el título anterior, utilizando las clasificaciones más comunes (por ejemplo, ARWU, QS World University, etc.)
- Rendimiento académico en el título anterior.

Curriculum y experiencia profesional:

- Idoneidad del título previo del candidato. Los titulares de títulos de grado en disciplinas en el campo de la informática o la ciencia y la tecnología de las telecomunicaciones tendrán preferencia.
- Experiencia en proyectos de innovación e investigación.

Motivación:

- Currículum y carta de motivación del candidato

Plazas

40

Preinscripción

Preinscripción cerrada (consulta los nuevos periodos de preinscripción en el calendario académico).
¿Cómo se formaliza la preinscripción?

Matrícula

¿Cómo se formaliza la matrícula?

Legalización de documentos

Los documentos expedidos por estados no miembros de la Unión Europea ni firmantes del Acuerdo sobre el espacio económico europeo tienen que estar legalizados por vía diplomática o con correspondiente apostilla.

SALIDAS PROFESIONALES

Salidas profesionales

- Área de tecnologías de la información y comunicación.
- Área de programación informática.
- Administración pública.
- Analista de seguridad.
- Responsable de riesgos de seguridad.
- Consultor de seguridad.
- Analista forense digital.
- Hacker ético.
- Responsable de ZOCO (security operations center).
- CSO en empresas tecnológicas (chief security officer).
- CSO en empresas no tecnológicas pero con departamentos de IT.

Competencias

Competencias transversales

Las competencias transversales describen aquello que un titulado o titulada es capaz de saber o hacer al concluir su proceso de aprendizaje, con independencia de la titulación. **Las competencias transversales establecidas en la**

UPC son la capacidad de espíritu empresarial e innovación, sostenibilidad y compromiso social, conocimiento de una tercera lengua (preferentemente el inglés), trabajo en equipo y uso solvente de los recursos de información.

Competencias específicas

- Diseñar aplicaciones de alto valor añadido basadas en las tecnologías de la información y las comunicaciones (TIC) aplicadas al ámbito de la ciberseguridad.
- Identificar y seleccionar las herramientas más adecuadas para la detección y el análisis de ataques e incidentes de seguridad según su naturaleza y el entorno donde se han producido.
- Identificar y analizar las leyes y regulaciones aplicables en materia de ciberseguridad, y entender las implicaciones éticas que las técnicas de ciberdefensa pueden tener en la privacidad de los usuarios y saber cómo se pueden minimizar.
- Analizar desde un punto de vista matemático protocolos criptográficos de cifrado y gestión de claves según su robustez.
- Diseñar, implementar y operar protocolos de autenticación, autorización y auditoría de sistemas informacionales como por ejemplo las bases de datos.
- Aplicar técnicas de monitorización y análisis del tráfico de la red para la detección de ataques de ciberseguridad y la investigación de incidentes.
- Diseñar, desarrollar, detectar, analizar y eliminar código malicioso que sea capaz de infectar un sistema operativo actual y ocultarse.
- Identificar y aplicar técnicas para mantener en todo momento la seguridad y la privacidad de las aplicaciones distribuidas construidas sobre los protocolos de internet.
- Elaborar individualmente un trabajo original y presentarlo y defenderlo ante un tribunal universitario, consistiendo en un proyecto de ingeniería en el ámbito de la ciberseguridad en el cual se sinteticen las competencias adquiridas en las enseñanzas del máster.

ORGANIZACIÓN ACADÉMICA: NORMATIVAS, CALENDARIOS

Centro docente UPC

Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona (ETSETB)
Facultad de Informática de Barcelona (FIB)

Calendario académico

Calendario académico de los estudios universitarios de la UPC

Normativas académicas

Normativa académica de los estudios de máster de la UPC

PLAN DE ESTUDIOS

Asignaturas	créditos ECTS	Tipo
PRIMER CUATRIMESTRE		
Blockchain	5	Optativa
Gestión de la Seguridad	5	Optativa
Malware	5	Obligatoria
Monitorización y Análisis del Tráfico de Red	5	Obligatoria
Protección de los Datos	5	Obligatoria
Seguridad de Red	5	Obligatoria
Seguridad en Aplicaciones	5	Obligatoria
SEGUNDO CUATRIMESTRE		
Casos de Uso en Ciberseguridad	5	Optativa

Asignaturas	créditos ECTS	Tipo
Computación y Criptografía Cuántica	3	Optativa
Comunicaciones Seguras en Redes de Fibra Óptica	5	Optativa
Curso Breve en las Matemáticas de la Teoría de Códigos y la Criptografía	3	Optativa
Privacidad de Datos	5	Optativa
Seguridad de Red – Autenticación y Autorización	5	Obligatoria
Seguridad en el Hardware de Sistemas Empotrados. Primitivas, Debilidades y Contramedidas	3	Optativa
Seguridad en Redes Fijas 5G	5	Optativa
Trabajo de Fin de Máster	12	Proyecto