

# **Asignatura de Bases teóricas de la ciberdelincuencia**

ONLINE Y SIN HORARIO

# Asignatura Online de Bases teóricas de la ciberdelincuencia

**Inicio**  
11 mar 2026

**100%**  
Online

**Idiomas:** Español, Catalán

**Precio:** 569 €

[Solicita información](#)

[Matricúlate](#)



**Metodología 100% online**



**1.ª universidad online del mundo**



**Acompañamiento personalizado**

## Presentación

¿Qué es un cibercrimen? ¿La cibercriminalidad se parece a la criminalidad tradicional?  
¿Quién es un ciberdelincuente y por qué realiza actos delictivos en el ciberespacio?  
¿Cómo son las víctimas de cibercrímenes y cuántas hay?

Para responder a estas preguntas, la asignatura ofrece al estudiante una introducción a la fenomenología de las distintas formas delictivas relacionadas con las TIC y cometidas en un entorno cibernético. Asimismo, analiza las aplicaciones de las teorías criminológicas tradicionales a la ciberdelincuencia y los resultados de la investigación empírica en el ámbito de la cibercriminalidad.

## La UOC, la mejor universidad online

Somos la universidad online del Estado mejor posicionada en los principales rankings de calidad universitaria.



# Contenidos

## Contenidos

### UNIDAD-NIU 1:

¿Qué es el cibercrimen y cómo se compara con la criminalidad tradicional?

Para trabajar esta unidad, el estudiante contará con los siguientes recursos:

- Capítulo II, apartados 1 y 2 de libro: Miró Llinares, F. (2012). El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons.
- La Vanguardia. "Ciberestafadores engañaron a 552 víctimas y lograron más de 2 millones euros". Disponible en: <https://www.lavanguardia.com/local/madrid/20190319/461130395659/ciberestafadores-enganaron-a-552-victimas-y-obtuvieron-mas-de-dos-millones.html>.
- El País. "El ciberataque: pulsar un botón y desenchufar el mundo". Disponible en: [https://elpais.com/internacional/2017/05/20/actualidad/1495291083\\_920693.html](https://elpais.com/internacional/2017/05/20/actualidad/1495291083_920693.html).
- Huffington Post. "Más de 1.000 jóvenes demandados en Dinamarca por difundir videos sexuales en Facebook". Disponible en: [https://www.huffingtonpost.es/2018/01/16/mas-de-1-000-jovenes-demandados-en-dinamarca-por-difundir-videos-sexuales-en-facebook\\_a\\_23334401/](https://www.huffingtonpost.es/2018/01/16/mas-de-1-000-jovenes-demandados-en-dinamarca-por-difundir-videos-sexuales-en-facebook_a_23334401/).
- Capítulo 2 ("Tipos de cibercrimen y clasificación de los mismos"), apartado 3 (p. 116-139), del libro Miró Llinares, F. (2012). El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons.
- Capítulo 1 ("Cybercrime and the Internet: an introduction") del libro Yar, M. & Steinmetz, K. F. (2019). Cybercrime and society, 3.ª edición. Londres: Sage Publishing.
- Capítulo 1 ("La criminalidad en el ciberespacio") del libro Miró Llinares, F. (2012). El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons.
- Videos de David Wall titulados Cybercrime: a changing cyber-threat landscape i Cybercrime: technology and crime. Disponibles en: <https://study.sagepub.com/cybercrimeandsociety3e/student-resources/podcasts-and-videos>.

### UNIDAD-NIU 2:

¿El cibercrimen es vino viejo en una botella nueva?

Para trabajar esta unidad, el estudiante contará con los siguientes recursos:

- Capítulo 3 del libro Miró Llinares, F. (2012). El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons.
- Incibe, OSI, y AEPD. Privacidad y seguridad en internet. Disponible en: <https://www.osi.es/sites/default/files/docs/guiaprivacidadseguridadinternet.pdf>.
- Incibe, OSI, Policía Nacional, y Ministerio de Sanidad, Servicios Sociales e Igualdad. Compra segura en internet. Disponible en: [https://www.osi.es/sites/default/files/docs/guia\\_compra\\_segura\\_internet\\_web\\_vfinal.pdf](https://www.osi.es/sites/default/files/docs/guia_compra_segura_internet_web_vfinal.pdf).
- Guía práctica para la ciberseguridad en las pymes.
- Miró Llinares, F. (2013). "Victimització per internet: fenomenologia, ofensors i víctimes", ponencia en la III Jornada de Criminología UOC-CEJFE. Disponible en: [https://www.youtube.com/watch?v=atxt5f1sqxw&list=plznazgtuyvtbzywtxbq1u4\\_aqah8qbkl&index=6](https://www.youtube.com/watch?v=atxt5f1sqxw&list=plznazgtuyvtbzywtxbq1u4_aqah8qbkl&index=6).
- Agustina, J. R. (2013). "¿Cómo prevenir conductas abusivas y delitos tecnológicos en la empresa?". IDP. Revista d'Internet, Dret i Política, 16, p. 7-26.
- Agustina, J. R. (2014). "Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización". Cuadernos de Política Criminal (segunda época), 14.

### UNIDAD-NIU 3:

¿Quién es un ciberdelincuente?

Para trabajar esta unidad, el estudiante contará con los siguientes recursos:

- Capítulo 4 del libro Miró Llinares, F. (2012). El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons.
- Capítulo 2 ("Researching and theorizing cybercrime"), apartados 2.1 i 2.2, del libro Yar, M. & Steinmetz, K. F. (2019). Cybercrime and society, 3.ª edición. Londres: Sage Publishing.
- Incibe. Así trabaja el ciberdelincuente ¿se lo vas a permitir? Disponible en: <https://www.youtube.com/watch?v=HJKkkaL6Trc>.
- "Ciberdelincuencia organizada, caso práctico: inteligencia económica... (UCO, Guardia Civil)". XI Jornadas STIC CCN-CERT. Disponible en: <https://www.youtube.com/watch?v=NThbCnhG8AA>.
- Capítulo 11 ("Cybercrime and criminological theories"), p. 439-461, 470-489, del libro Holt, T. J., Bossler, A. M. & Seigfried-Spellar, K. C. (2017). Cybercrime and digital forensics: an introduction. Nueva York: Routledge.

- "Perfil del responsable", p. 45-50. En: Ministerio del Interior. (2018). Estudio sobre la cibercriminalidad en España 2017. Disponible en: <http://www.interior.gob.es/documents/10180/7146983/Estudio+Cibercriminalidad+28af5-4baa-86fa-7f085f7cac07>.
- Apartado 5 ("Agentes de las amenazas"), p. 16-25. En: CNN-CERT. (2018). Ciberamenazas y tendencias. Disponible en: <https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2835-ccn-cert-ia-09-18-ciberamenazas-y-tendencias-edicion-2018-1/file.html>.
- Capítulos 4 y 5 ("Individual cybercrime offenders" y "Cybercriminal networks"). En: Leukfeldt, R. (ed.). (2017). Research agenda: the human factor in cybercrime and cybersecurity. The Hague: Eleven.

### UNIDAD-NIU 4:

Si sufres un cibercrimen, ¿es culpa tuya?

Para trabajar esta unidad, el estudiante contará con los siguientes recursos:

- Capítulo 5 del libro Miró Llinares, F. (2012). El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons.
- Capítulo 11 ("Cybercrime and criminological theories"), p. 462-470, del libro Holt, T. J., Bossler, A. M. & Seigfried-Spellar, K. C. (2017). Cybercrime and digital forensics: an introduction. Nova York: Routledge.
- Capítulo 2 ("Researching and theorizing cybercrime"), apartados 2.3 i 2.4, del libro Yar, M. & Steinmetz, K. F. (2019). Cybercrime and society, 3.ª edición. Londres: Sage Publishing.
- Reep-van den Bergh, C. M. & Junger, M. (2018). "Victims of cybercrime in Europe: a review of victim surveys". Crime Science, 7(1), p. 1-15.
- "Perfil de la víctima", p. 40-44. En: Ministerio del Interior. (2018). Estudio sobre la cibercriminalidad en España 2017. Disponible en: <http://www.interior.gob.es/documents/10180/7146983/Estudio+Cibercriminalidad+28af5-4baa-86fa-7f085f7cac07>.
- Capítulo 5 ("Blaming the victim"). En: Button, M. & Cross, C. (2017). Cyber frauds, scams and their victims. Oxon: Routledge.
- Apartado 2.1, p. 51-111. En: Comisión Europea. (2017). Special Eurobarometer 464a: Europeans' attitudes towards cyber security. Disponible en: <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download>.
- Comisión Europea. Special Eurobarometer 480: Europeans' attitudes towards internet security. Disponible en: <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download>.

## Objetivos y competencias

### Conocimientos, habilidades y competencias

- Conocer las principales clasificaciones de la cibercriminalidad
- Analizar la prevalencia de la cibercriminalidad
- Analizar la cibercriminalidad según el papel de las TIC en el comportamiento criminal o en función del móvil del infractor
- Comprender las amenazas de la cibercriminalidad en función de la posible víctima
- Comprender la multiplicidad de víctimas de cibercrímenes
- Comprender los distintos factores que pueden estar relacionados con la victimización en el ciberespacio
- Relacionar distintos factores con la probabilidad de victimización en casos reales
- Establecer las actividades rutinarias relacionadas con la victimización en el ciberespacio
- Utilizar resultados de estudios cuantitativos y cualitativos para comprender los factores de riesgo de victimización
- Comprender las medidas prácticas de prevención proporcionadas por fuentes oficiales y fuentes académicas
- Analizar los factores de riesgo de varios tipos de ciberdelincuencia en entornos reales
- Aplicar los conocimientos sobre medidas de prevención en entornos reales
- Conocer las características del ciberespacio que condicionan la delincuencia
- Comprender las oportunidades delictivas encontradas en el ciberespacio
- Relacionar varias fuentes de información para explicar la realidad delictiva y las tendencias en la cibercriminalidad
- Utilizar varias fuentes para construir perfiles de delincuentes
- Analizar las distintas teorías criminológicas para comprender la ciberdelincuencia
- Conocer la aplicación de las teorías criminológicas tradicionales a la cibercriminalidad
- Analizar los factores micro y macro que explican la comisión de cibercrímenes
- Identificar las diferentes técnicas empleadas por los ciberdelincuentes
- Conocer las limitaciones de los datos oficiales para entender las tendencias en la cibercriminalidad
- Analizar, sintetizar y relacionar las fuentes de conocimiento sobre la ciberdelincuencia
- Comprender y utilizar el vocabulario criminológico relacionado con el ámbito de la ciberdelincuencia
- Conocer y comprender fuentes de conocimiento en la lengua inglesa
- Aplicar conocimientos académicos a casos prácticos

## Recursos para el aprendizaje

Los recursos para el aprendizaje que ofrece la UOC son digitales y han sido editados por la universidad en multiformato (HTML5, web, EPUB, PDF, etc.). Los recursos con los que cuenta la asignatura son los siguientes:

- Módulos propios sobre teoría de la cultura desde diferentes perspectivas (filosofía, sociología, política cultural, economía y tecnología).
- Selección de lecturas y materiales audiovisuales de cada uno de los temas.

# Profesorado

## Dirección de los Estudios

Ignasi Beltran de Heredia Ruiz

Catedrático de Derecho del Trabajo y de la Seguridad Social. Actualmente es Director de los Estudios de Derecho y Ciencia Política de la Universitat Oberta de Catalunya (UOC). Doctor en Derecho por la Universitat Ramon Llull/ESADE, es licenciado en Derecho y Máster en Derecho por la misma universidad. Ha publicado extensamente en temas de la flexibilidad interna y externa del contrato de trabajo; los fenómenos de pluralidad empresarial; el riesgo de la tecnología sobre los derechos fundamentales y el impacto de la robotización y la inteligencia artificial en las relaciones de trabajo; las instituciones de protección social; las relaciones laborales del personal de la Administración Pública; y también sobre la psicología de la conducta y el análisis económico del derecho del trabajo.

## Profesorado propio

Antonia Linde Garcia

# Requisitos de acceso

## Requisitos previos

Para matricularse de esta asignatura y seguirla no se necesita ninguna titulación académica ni hay que tener conocimientos previos sobre la materia.

## Requisitos técnicos

Para el seguimiento de esta asignatura es necesario disponer de un ordenador de sobremesa o portátil con conexión a internet (por banda ancha, ADSL o cable) y un monitor con una resolución mínima de 1.024 x 768 píxeles. Para poder consultar algunos materiales también puede ser necesario un lector de DVD.

Es recomendable que la CPU (ya sea de un ordenador de sobremesa o de un portátil) tenga como mínimo 2 GB de memoria RAM y 2 GHz de velocidad de procesador.

Es necesario un sistema operativo Windows XP (o superior), Mac OS o Linux\*. También se requiere tener instalado uno de los siguientes navegadores: Internet Explorer 9.0 (o superior), [Mozilla Firefox](#) o [Chrome](#).

\* Debido a la gran variedad de distribuciones que existen, no especificamos todas las versiones posibles.

**La UOC, la mejor universidad online**

# Matrícula y precio

## Proceso de matrícula

### 1 Formularios de matrícula

Rellena el formulario de matrícula del curso concreto que te interesa, que encontrarás a la parte superior de la página.

### 2 Acceso al Campus

Si no recuerdas las claves de acceso al campus virtual, las puedes recuperar desde el [siguiente enlace](#).

### ¿Cuándo te puedes matricular?

En la UOC puedes matricularte en dos momentos diferentes del año. Escoge la opción que mejor se adapte a sus necesidades. Consulta el plazo de matriculación y el inicio de curso en la página de los estudios que te interesen cursar.



#### Matriculación a partir de **abril**

para comenzar el curso en **septiembre u octubre**



#### Matriculación a partir de **octubre**

para comenzar el curso en **febrero o marzo**

Concepto	Precio
Precio del curso	<b>569 €</b>

El precio de este programa será el vigente en el momento de formalizar la matrícula. Sujeto a revisión anual.



**122.750 graduados y graduadas**



**89 % de estudiantes que estudian y trabajan**



**79 % volvería a escoger la UOC**

## Formas de pago

El pago de los cursos se efectúa con tarjeta.

1. TPVV: pago con una tarjeta de crédito o de débito de cualquier entidad financiera, mediante el TPVV (terminal de punto de venta virtual) de «la Caixa».

[Información sobre el desistimiento de matrícula](#)

## Descuentos

La UOC ofrece una serie de descuentos. Si puedes acogerte a alguno, en el momento de hacer la matrícula debes elegirlo en el desplegable del apartado *Descuentos*. En caso de que puedas acogerte a más de uno, tendrás que elegir el más beneficioso.

## Descuentos para a colectivos

### Familia numerosa

Los estudiantes beneficiarios del título de familia numerosa reconocido por el Estado español, o por el organismo competente en el resto de países, tienen derecho a los siguientes descuentos, en función de la categoría:

- Familias numerosas de categoría **especial: descuento del 15%**.
- Familias numerosas de categoría **general: descuento del 7,5%**.

### Personas con discapacidad

Los estudiantes con un grado de discapacidad **igual o superior al 33%** reconocido por el Estado español, o el grado **equivalente** por cualquier otro país, tienen derecho a un **descuento del 15%**.

### Víctimas de actos terroristas

Los estudiantes (o sus hijos o cónyuges) que hayan sido reconocidos como víctimas de actos terroristas por el organismo competente en el Estado español, o de cualquier otro país, tienen derecho a un **descuento del 15%**.

### Víctimas de violencia machista en el ámbito de la pareja

Los estudiantes (y sus hijos o hijas dependientes) que hayan sido reconocidos como víctimas de violencia de género por el organismo competente en el Estado español, o de cualquier otro país, tienen derecho a un **descuento del 15%**.

## Comunidad UOC

- **UOC Alumni: 10% de descuento**

Puedes disfrutar de este descuento si has obtenido un título oficial (de grado, licenciatura, diplomatura, ingeniería o máster universitario) o un máster o posgrado propio en la UOC.

- **Descuentos para empresas**

Si tu empresa u organización tiene un acuerdo con la UOC, podrás beneficiarte de descuentos y ventajas en tu matrícula.

[Consulta las condiciones de los descuentos para empresas](#)

## Programa UOC de acompañamiento al deportista de competición

Los estudiantes considerados deportistas de competición tienen derecho a un descuento sobre el importe de la matrícula.

+ [Consulta la información del programa](#)

# UOC

---

Consulta la oferta formativa de la UOC [uoc.edu/es/estudios](https://uoc.edu/es/estudios)

---

**UOC** Universitat Oberta  
de Catalunya