UAB
Universitat Autònoma de Barcelona

Ciberseguridad

Código: 107929
Créditos ECTS: 6

2025/2026

Titulación	Tipo	Curso
Criminología	OP	4

Contacto

Nombre: Jose Cañabate Perez

Correo electrónico: josep.canabate@uab.cat

Idiomas de los grupos

Puede consultar esta información al final del documento.

Prerrequisitos

No hay prerequisitos.

La docencia de la asignatura se impartirá teniendo en cuenta la perspectiva de los Objetivos de Desarrollo Sostenible.

Objetivos y contextualización

- Comprender los principios esenciales de la ciberseguridad, incluyendo los conceptos de confidencialidad, integridad, disponibilidad, autenticación y trazabilidad de la información.
- Identificar los principales vectores de ataque y amenazas cibernéticas, tales como malware, ransomware, ataques de denegación de servicio (DDoS), phishing, suplantación de identidad o explotación de vulnerabilidades.
- Conocer las medidas de protección técnica y organizativa más comunes, como cortafuegos, sistemas de detección de intrusos (IDS/IPS), antivirus, cifrado, autenticación multifactor, segmentación de redes y gestión de parches.
- Entender el ciclo de gestión del riesgo en ciberseguridad, incluyendo la identificación de activos críticos, análisis de amenazas y vulnerabilidades, evaluación del impacto y definición de controles.
- Explorar el marco normativo y regulatorio aplicable a la ciberseguridad, como el Esquema Nacional de Seguridad (ENS), el RGPD en su dimensión de seguridad de la información, y la Directiva NIS2, con implicaciones prácticas para las investigaciones criminológicas.
- Analizar incidentes de ciberseguridad desde una perspectiva criminológica, conociendo cómo se planifica, ejecuta y responde a un incidente, y cuál es el papel de los profesionales de la criminología en estos procesos.
- Introducirse en los conceptos básicos del análisis forense digital, prestando atención a la cadena de custodia, la recogida de evidencias digitales y el uso inicial de herramientas forenses.
- Fomentar una cultura de ciberseguridad en contextos organizativos, comprendiendo los factores humanos, las políticas de seguridad, la formación de usuarios y el diseño de estrategias de prevención.

- Desarrollar una visión crítica sobre los desafíos emergentes de la ciberseguridad, como la protección frente a amenazas persistentes avanzadas (APT), la ciberinteligencia, la protección de infraestructuras críticas o el uso de inteligencia artificial en entornos de defensa y ataque.

- Identificar y clasificar los distintos tipos de ciberdelitos, con especial atención a aquellos de mayor impacto social como el ciberacoso, el fraude informático, el acceso no autorizado a sistemas, la pornografía infantil en línea, el ransomware y los delitos contra la privacidad.

Resultados de aprendizaje

1. CM34 (Competencia) Aplicar con precisión los modelos de prevención en situaciones concretas de criminalidad
2. CM37 (Competencia) Intervenir profesionalmente en actuaciones preventivas, en resolución de conflictos o en atención a las víctimas sobre la base de la evidencia científica y de acuerdo con los valores de la pacificación y la prevención de nuevos conflictos
3. CM38 (Competencia) Intervenir profesionalmente con perspectiva de género
4. KM30 (Conocimiento) Identificar el marco jurídico que regula la prevención primaria, secundaria y terciaria para las distintas formas de criminalidad
5. SM42 (Habilidad) Aplicar las formas de prevención más efectivas para abordar la problemática específica de criminalidad
6. SM43 (Habilidad) Identificar los factores de riesgo y de protección en referencia a las distintas formas de delincuencia

Contenido

El programa de la asignatura abarca un amplio espectro de conceptos y prácticas esenciales en el campo de la ciberseguridad y las tecnologías de la información. Comienza con una introducción a la metodología del curso, proporcionando a los estudiantes una base sólida en los conceptos fundamentales de TI y seguridad de la información. A medida que avanza el curso, se exploran incidentes de ciberseguridad conocidos, diversos tipos de ciberamenazas y el papel de la inteligencia artificial en la detección y respuesta a estos incidentes. También se discuten las estrategias de ciberdefensa y los planes nacionales diseñados para proteger infraestructuras críticas.

El curso también cubre la normativa estatal y europea relacionada con la ciberseguridad, así como la delincuencia tecnológica y la importancia de la prueba electrónica en la investigación de delitos informáticos. Además, se enseña cómo preparar una organización para investigaciones forenses digitales, incluyendo la protección de los activos de información y la aplicación de estándares de ciberseguridad reconocidos a nivel internacional. Por último, se aborda la protección de infraestructuras críticas y el desarrollo de planes de continuidad de negocio para garantizar que una organización pueda seguir operando durante y después de incidentes disruptivos. Este enfoque integral prepara a los estudiantes para enfrentar los desafíos en ciberseguridad de manera efectiva y competente.

BLOQUE 1 - INTRODUCCIÓN Y FUNDAMENTOS

Tema 1. Fundamentos de seguridad.
Tema 2. Conceptos básicos de seguridad de la información y ciberseguridad.
Tema 3. Gobernanza, gestión de riesgos y cumplimiento normativo.

BLOQUE 2 - PANORAMA DE LAS AMENAZAS

Tema 4. Ciberriesgo y amenazas.
Tema 5. Principales ciberataques.
Tema 6. La evaluación del riesgo.

BLOQUE 3 - ASEGURAMIENTO DE ACTIVOS, OPERACIONES DE SEGURIDAD Y RESPUESTA

Tema 7. Aseguramiento de los activos.
Tema 8. Arquitecturas, modelos y marcos.
Tema 9. Controles de seguridad.
Tema 10. Operaciones de seguridad y respuesta.

BLOQUE 4 - NORMATIVA DE CIBERSEGURIDAD

Tema 11. Normativa estatal y europea en materia de ciberseguridad.
Tema 12. Delincuencia tecnológica.
Tema 13. Preparación forense e investigación digital forense.

Actividades formativas y Metodología

Título	Horas	ECTS	Resultados de aprendizaje
Tipo: Dirigidas			
Clase magistral	19,5	0,78	CM34, CM37, CM38, KM30, SM42, SM43, CM34
Seminario	19,5	0,78	CM34, CM37, CM38, KM30, SM42, SM43, CM34
Tipo: Supervisadas			
Trabajo externo para la preparación de las actividades	5	0,2	CM34, CM37, CM38, KM30, SM42, SM43, CM34
Tipo: Autónomas			
Estudio	36	1,44	CM34, CM37, CM38, KM30, SM42, SM43, CM34
Investigación sobre materiales y preparación de actividades evaluables.	30	1,2	CM34, CM37, CM38, KM30, SM42, SM43, CM34
Preparación de escenario de ciberseguridad en el aula	35	1,4	CM34, CM37, CM38, KM30, SM42, SM43, CM34

La asignatura combina la exposición teórica con metodologías activas de aprendizaje colaborativo. Se basa principalmente en tres estrategias docentes complementarias: la clase magistral, la técnica del puzle (Jigsaw) y el aprendizaje basado en problemas.

En primer lugar, las clases magistrales servirán para introducir los principios básicos de cada tema, estructurar los contenidos y ofrecer un marco teórico sólido. El profesorado realizará una exposición clara y guiada de los conceptos fundamentales de la ciberseguridad (confidencialidad, integridad, disponibilidad, vectores de ataque, sistemas de protección, gestión del riesgo, etc.) con el apoyo de materiales visuales y ejemplos prácticos de actualidad.

A continuación, cada unidad se ampliará y consolidará mediante la metodología del puzle (Jigsaw). Esta técnica de aprendizaje cooperativo implica que el alumnado trabaje de forma autónoma y colaborativa en pequeños grupos. El proceso se organiza en dos fases:

- Fase de expertos: Cada miembro del grupo recibe una subtemática concreta del tema general (por ejemplo: un estudiante trabaja el phishing, otro el ransomware, otro el firewall, etc.). Los estudiantes que comparten la misma subtemática se reúnen en un "grupo de expertos" para estudiarla en profundidad y preparar una explicación clara para sus compañeros.
- Fase de grupo base (recomposición del puzle): Cada estudiante regresa a su grupo original y enseña a los demás miembros lo que ha aprendido. De este modo, cada grupo reconstruye el contenido completo del tema a través del intercambio entre iguales, fomentando la responsabilidad compartida, el aprendizaje activo y la consolidación crítica del conocimiento.

Esta metodología favorece una comprensión profunda de los contenidos, el desarrollo de competencias comunicativas y la capacidad de trabajo en equipo, aspectos clave para el abordaje multidisciplinar de la ciberseguridad en el ámbito criminológico.

Por otro lado, la asignatura utilizará el Aprendizaje Basado en Problemas (ABP) para el desarrollo de parte de sus actividades de evaluación. El ABP es una metodología educativa que utiliza problemas reales como punto de partida para la adquisición e integración de nuevos conocimientos. En el contexto de la ciberseguridad, este enfoque es especialmente adecuado debido a la naturaleza dinámica y multifacética de los riesgos cibernéticos.

Así, se presentará al estudiantado un escenario de riesgo en ciberseguridad, que podría incluir un ataque de ransomware a una empresa, una brecha de datos en una organización financiera, o una campaña de phishing dirigida. El problema debe ser complejo y abierto, permitiendo múltiples enfoques y soluciones posibles.

El alumnado se organizará en pequeños grupos colaborativos, que trabajarán de forma autónoma para analizar y comprender el problema. La colaboración fomentará el intercambio de ideas, el debate y la confrontación de diferentes perspectivas, enriqueciendo el proceso de aprendizaje.

Los estudiantes identificarán lo que saben y lo que necesitan aprender para abordar el problema. Esto implicará una investigación activa, donde buscarán información relevante sobre ciberseguridad, incluyendo técnicas de ataque y defensa, normativas aplicables y buenas prácticas. La investigación podrá incluir la revisión de literatura académica, análisis de estudios de caso previos y consulta con expertos en la materia.

Con la información recopilada, los grupos analizarán el problema en profundidad, identificando las vulnerabilidades explotadas y las posibles consecuencias. A partir de ese análisis, desarrollarán estrategias y planes de acción para mitigar el riesgo y prevenir futuros incidentes.

Este proceso requiere pensamiento crítico y la aplicación de conocimientos técnicos y prácticos adquiridos a lo largo del curso.

Nota: se reservarán 15 minutos de una clase dentro del calendario establecido por el centro o por la titulación para que el alumnado rellene las encuestas de evaluación de la actuación del profesorado y de evaluación de la asignatura o módulo.

Evaluación

Actividades de evaluación continuada

Título	Peso	Horas	ECTS	Resultados de aprendizaje
Actividad de análisis de una Advanced and Persistent Threat (APT)	30%	1,5	0,06	CM34, CM37, CM38, KM30, SM42, SM43
Exposición en clase de un escenario de riesgo relacionado con ciberseguridad	20%	1,5	0,06	CM34, CM37, CM38, KM30, SM42, SM43
Prova final	50%	2	0,08	CM34, CM37, CM38, KM30,

Las actividades de evaluación se pueden realizar a lo largo del curso en parte de forma individual y en parte, en grupo. La evaluación es continua y se organiza en función de las actividades formativas anteriormente descritas.

El sistema de evaluación continua combina la asistencia a las clases teóricas/magistrales, la participación activa en los seminarios, la realización de las actividades evaluables (con un peso global del 50%) y la superación de la prueba final (con un peso global del 50%). Atendiendo a que la prueba final implica la evaluación de los conocimientos adquiridos de forma acumulativa a través de las actividades de evaluación continua, es requisito imprescindible superar la prueba final con un 5/10.
Evaluación

1. Modelo de evaluación

El modelo de evaluación es continua y tiene el objetivo formativo de que alumnado y profesorado pueda conocer el grado de consecución de las competencias para orientar su proceso formativo. Valor de cada ítem de evaluación: trabajos individuales (20%); trabajo grupal (30%); prueba final (50%).

Es obligatoria la asistencia al 80% de las clases teóricas y de los seminarios para poder superar la asignatura.

2. Items de evaluación

a. Exposición en clase de un escenario de riesgo y entrega por escrito del trabajo (20%).

Esta actividad consiste en escoger un escenario de riesgo de los propuestos por el profesor, o de los que se propongan por los estudiantes/as y sean validados. Se debe realizar un análisis de riesgos y proponer unas recomendaciones. En el seminario se discutirá el resultado del análisis de riesgos y de las recomendaciones propuestas. Dependiendo dela complejidad del escenario propuesto se autorizará la realización por parejas.

b. Trabajo en el seminario. Se programará en cada seminario el análisis de un escenario relacionado con una amenaza. En este sentido, en cada seminario se dedicará a una de las principales amenazas actuales de cibersegurado (Ramsonware, DDoS, Ingeniería social, ATPs, etc.). Por la preparación de esta actividad se pondrá con antelación a disposición del estudiantado materiales relacionados con la materia. Al final de la sesión se realizará un cuestionario o prueba escrita, dependiendo de la actividad, para evaluar la adquisición de conocimientos. Cada actividad se evaluará sobre 10, la media de todas las notas tendrá una ponderación de un 30% sobre la nota final.

c. Cuestionario sobre el temario de 30 preguntas, 4 opciones, sólo una correcta, penalización de 0'25 sobre 30.

3. Condiciones para ser evaluado
El alumnado será evaluable siempre que haya realizado un conjunto de actividades cuyo peso equivalga a un mínimo de 2/3 partes de la calificación total de la asignatura. Si el valor de las actividades realizadas no llega a este umbral, el profesor/a de la asignatura puede considerar al estudiante como no evaluable,

4. Requisitos para superar la asignatura y recuperaciones

Es necesario tener una nota mínima de 5 en todos los ítems que conforman la evaluación. Si un alumno no supera la parte de evaluación correspondiente al trabajo individual, al trabajo grupal o la aprueba final tendrá la posibilidad de recuperar el día establecido para reevaluar. Los trabajos individual y los trabajos grupal se recuperarán a través de una o varias preguntas teóricas sobre los contenidos y materias trabajadas en las respectivas actividades.
Para aprobar la asignatura a re-evaluación es necesario tener igualmente un 5 en todos los ítems. Si no se obtiene esta calificación mínima en cada ítem, aunque la media aritmética de los cuatro ítems deevaluación supere el 5, la nota final en el acta será suspendido 4'5.

Atendiendo a que se trata de una segunda oportunidad, la nota máxima de pruebas y trabajos recuperados es de 5.

5. Presentaciones fuera de plazo

No se aceptan, salvando situaciones de fuerza mayor. El alumno obtendrá un 0 en la práctica no entregada.

6. Excusas

Las excusas para cumplir con las obligaciones debidas a enfermedad o razones de fuerza mayor podrán ser aceptadas siempre que se cuente con un certificado oficial. Ausencias por razones académicas tendrán que ser previamente aceptadas por el profesorado.

7. Conductas fraudulentas

Un alumno que copie o intente copiar a un examen tendrá un 0 en esta prueba. Un alumno que presente una práctica en el que haya indicios de plagio o que no pueda justificar los argumentos de su práctica obtendrá un 0 y recibirá una advertencia.

8. Puntualidad

Las clases comienzan puntualmente. No se admite la entrada en clase una vez ésta haya comenzado, ni la salida antes de su finalización, salvo justificación razonable.

9. Matrículas de Honor
El estudiantado que obtenga una calificación de 9 o superior a la nota final podrá obtar en la Matrícula de Honor por curso. Estos efectosse formará una comisión de evaluación entre todo el profesorado del grupo, la cual evaluará con criterios objetivos si algún/a estudiante cumple con los requerimientos de excelencia exigidos por la obtención de esta calificación. En todo caso, por normativa académica sólo se pueden otorgar como máximo un 5% de matrículas de honor sobre el total de estudiantes matriculados en un curso. La comisión de evaluación con criterios objetivos puede decidir no otorgarninguna matrícula de honor.

10. Evaluación única

Aquellos/as estudiantes que se acojan al sistema de evaluación única, después de ser aprobados por la facultad, realizarán las siguientes pruebas finales.

1. Examen final tipo test con valor del 50%. Este examen se realizará sobre el manual obligatorio de curso " ISACA, (2021), Fundamentos de Ciberseguridad, Guía de estudio, 3ª edición."
2. Realización de un trabajo de curso sobre los escenarios de riesgo y amenazas que se propondrán en el campus virtual al inicio del curso con un valor del 30%.
3. Presentación oral (ponencia) frente al profesor de un tema sobre las materias que se propondrá al inicio de curso con un valor del 20%.
No evaluable: Se aplicará el mismo criterio de no evaluable que por la evaluación continua.

11. Uso de la Inteligencia Artificial

Uso restringido: "Para esta asignatura, se permite el uso de tecnologías de Inteligencia Artificial (IA) exclusivamente en [tareas de apoyo, como la búsqueda bibliográfica o de información, la corrección de textos o las traducciones. El estudiante deberá identificar claramente qué partes han sido generadas con esta tecnología, especificar las herramientas utilizadas e incluir una reflexión utilizada y incluir una reflexión la actividad. La no transparencia del uso de la IA en esta actividad evaluable se considerará falta de honestidad académica y puede acarrear una penalización parcial o total en la nota de la actividad, o sanciones mayores en casos de gravedad

Bibliografía

Bibliografía obligatoria

ISACA (2021). *Fundamentos de Ciberseguridad. Guía de estudio (3ª ed.). Isaca.*

Otra bibliografía aconsejada

Alonso Lecuit, J. (2021). Directiva NIS2: valoraciones y posiciones desde el sector privado (Documento de trabajo DT6/2021). [Directiva NIS2 disponible en http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_

Communications-Electronics Security Group. (2009). Good Practice Guide18: Forensic Readiness, The National Archives - CESG.

DoménechPascual, G. (2006). *Derechos fundamentales y riesgos tecnológicos: el derecho del ciudadano a ser protegido por los poderes públicos*. Centro de Estudios Políticos y Constitucionales.

Fojón, E., Coz, J.R., & Miralles, R. (2011). *La ciberseguridad nacional, un compromiso de todos: de una cultura reactiva a una de prevención y resiliencia*. ISMS Forum.

Gómez-Vieites, A. (2018). *Enciclopedia de la seguridad informática* (2ª ed.). RA-Ma Editorial.

ISACA. (2019). COBIT2019: Framework - Governance and Management Objectives. ISACA. Sucesor de COBIT5 (2012), incorpora mejoras para integración y adaptación.

ISACA. (2024). CISM Study Guide 2024-2025: CISM exam prep. Kevin Sirius. ISACA Store.

ISACA. (2017). *CSX Cybersecurity Fundamentals Study Guide* (rev. ed.). Isaca.

ISACA. *Guía actualizada para la certificación CSX Fundamentals*. Isaca.

Ortiz Plaza, R., & Núñez Baroja, A. (2021). De la concienciación al riesgo humano en la ciberseguridad. *Revista SIC: Ciberseguridad, seguridad de la información yprivacidad,* 30(143), 72-73.

Piattini, M., del Peso, E., & del Peso, M. (2011). *Auditoría de tecnologías y sistemas de información.* RA-Ma Editorial.

Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence,* 2(3), 1-28.

Velasco Núñez, E. (2013). Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica. *Diario La Ley*, (8183), 1-9.

Velasco Núñez, E. (2015). Los delitos informáticos. *Práctica Penal: Cuaderno Jurídico*, (81), 14-28.

Recursos on-line:

ENISA (Agencia Europea para la ciberseguridad) - https://www.enisa.europa.eu/

Instituto Nacional de Ciberseguridad - www.incibe.es

Agencia Española de Protección de Datos www.agpd.es

SIC - Revista de Ciberseguridad, Seguridad de la Información y Privacidad - www.revistasic.es

Wired - www.wired.com

CIBER Elcano http://www.realinstitutoelcano.org/wps/portal/rielcano_es/publicaciones/ciber-elcano/

Software

Esta asignatura no requiere software.

Grupos e idiomas de la asignatura

La información proporcionada es provisional hasta el 30 de noviembre de 2025. A partir de esta fecha, podrá consultar el idioma de cada grupo a través de este enlace. Para acceder a la información, será necesario introducir el CÓDIGO de la asignatura

Nombre	Grupo	Idioma	Semestre	Turno
(SEM30) Seminaris (30 estudiants per grup)	1	Español	primer cuatrimestre	tarde
(TE) Teoría	1	Español	primer cuatrimestre	tarde