UAB
Universitat Autònoma de Barcelona

Ciberseguretat

Codi: 107929
Crèdits: 6

2025/2026

Titulació	Tipus	Curs
Criminologia	OP	4

Professor/a de contacte

Nom: Jose Cañabate Perez

Correu electrònic: josep.canabate@uab.cat

Idiomes dels grups

Podeu consultar aquesta informació al final del document.

Prerequisits

No hi ha prerequisits.

La docència de l'assignatura s'impartirà tenint en compte la perspectiva dels Objectius de Desenvolupament Sostenible.

Objectius

- Comprendre els principis essencials de la ciberseguretat, incloent els conceptes de confidencialitat, integritat, disponibilitat, autenticació i traçabilitat de la informació.
- Identificar els principals vectors d'atac i amenaces cibernètiques, com ara malware, ransomware, atacs de denegació de servei (DDoS), phishing, suplantació d'identitat o explotació de vulnerabilitats.
- Conèixer les mesures de protecció tècnica i organitzativa més comunes, com tallafocs, sistemes de detecció d'intrusions (IDS/IPS), antivirus, xifratge, autenticació multifactor, segmentació de xarxes i gestió de pegats
- Entendre el cicle de gestió del risc en ciberseguretat, incloent la identificació d'actius crítics, l'anàlisi d'amenaces i vulnerabilitats, l'avaluació de l'impacte i la definició de controls.
- Explorar el marc normatiu i regulador aplicable a la ciberseguretat, com l'Esquema Nacional de Seguretat (ENS), el RGPD en la seva dimensió de seguretat de la informació, i la Directiva NIS2, amb implicacions pràctiques per a les investigacions criminològiques.
- Analitzar incidents de ciberseguretat des d'una perspectiva criminològica, coneixent com es planifica, s'executa i es respon davant d'un incident, i quin és el paper dels professionals de la criminologia.
- Introduir-se en els conceptes bàsics de l'anàlisi forense digital, amb atenció a la cadena de custòdia, la recollida d'evidències digitalsi l'ús inicial d'eines forenses.
- Fomentar una cultura de ciberseguretat en contextos organitzatius, comprenent els factors humans, les polítiques de seguretat, la formació dels usuaris i el disseny d'estratègies de prevenció.

- Desenvolupar una visió crítica sobre els reptes emergents de la ciberseguretat, com la protecció davant d'amenaces persistents avançades (APT), la ciberintel·ligència, la protecció d'infraestructures crítiques o l'ús de la intel·ligència artificial en entorns de defensa i atac.

Resultats d'aprenentatge

1. CM34 (Competència) Aplicar amb precisió els models de prevenció en situacions concretes de criminalitat.
2. CM37 (Competència) Intervenir professionalment en actuacions preventives, en resolució de conflictes o en atenció a les víctimes sobre la base de l'evidència científica i d'acord amb els valors de la pacificació i la prevenció de nous conflictes.
3. CM38 (Competència) Intervenir professionalment amb perspectiva de gènere.
4. KM30 (Coneixement) Identificar el marc jurídic que regula la prevenció primària, secundària i terciària per a les diferents formes de criminalitat.
5. SM42 (Habilitat) Aplicar les formes de prevenció més efectives per abordar la problemàtica específica de criminalitat.
6. SM43 (Habilitat) Identificar els factors de risc i de protecció en referència a les diferents formes de delinqüència.

Continguts

El programa de l'assignatura abasta un ampli espectre de conceptes i pràctiques essencials en l'àmbit de la ciberseguretat i les tecnologies de la informació. Comença amb una introducció a la metodologia del curs, proporcionant a l'estudiantat una base sòlida en els conceptes fonamentals de TI i seguretat de la informació. A mesura que avança el curs, s'exploren incidents coneguts de ciberseguretat, diversos tipus de ciberamenaces i el paper de la intel·ligència artificial en la detecció i resposta davant d'aquests incidents. També es tracten les estratègies de ciberdefensa i els plans nacionals dissenyats per protegir les infraestructures crítiques.

El curs també cobreix la normativa estatal i europea relacionada amb la ciberseguretat, així com la delinqüència tecnològica i la importància de la prova electrònica en la investigació de delictes informàtics. A més, s'ensenya com preparar una organització per a investigacions forenses digitals, incloent-hi la protecció dels actius d'informació i l'aplicació d'estàndards de ciberseguretat reconeguts internacionalment. Finalment, s'aborda la protecció de les infraestructures crítiques i el desenvolupament de plans de continuïtat de negoci per garantir que una organització pugui continuar operant durant i després d'incidents disruptius.Aquest enfocament integral prepara l'estudiantat per afrontar de manera efectiva i competent els reptes de la ciberseguretat.

BLOC 1 - INTRODUCCIÓ I FONAMENTS

Tema 1. Fonaments de seguretat.
Tema 2. Conceptes bàsics de seguretat de la informació i ciberseguretat.
Tema 3. Governança, gestió de riscos i compliment normatiu.

BLOC 2 - PANORAMA DE LES AMENACES

Tema 4. Ciberrisc i amenaces.
Tema 5. Principals ciberatacs.
Tema 6. L'avaluació del risc.

BLOC 3 - ASSEGURAMENT D'ACTIUS, OPERACIONS DE SEGURETAT I RESPOSTA

Tema 7. Assegurament dels actius.
Tema 8. Arquitectures, models i marcs.
Tema 9. Controls de seguretat.
Tema 10. Operacions de seguretat i resposta.

BLOC 4 - NORMATIVA de CIBERSEGURETAT

Tema 11. Normativa estatal i europea en matèria de ciberseguretat.
Tema 12. Delinqüència tecnològica.
Tema 13. Preparació forense i investigació digital forense.

Activitats formatives i Metodologia

Títol	Hores	ECTS	Resultats d'aprenentatge
Tipus: Dirigides			
Classe magistral	19,5	0,78	CM34, CM37, CM38, KM30, SM42, SM43
Seminari	19,5	0,78	CM34, CM37, CM38, KM30, SM42, SM43
Tipus: Supervisades			
Treball extern per a la preparació de les activitats	5	0,2	CM34, CM37, CM38, KM30, SM42, SM43
Tipus: Autònomes			
Estudi	36	1,44	CM34, CM37, CM38, KM30, SM42, SM43
Preparació d'escenaris de ciberseguretat a l'aula	35	1,4	CM34, CM37, CM38, KM30, SM42, SM43
Recerca de materials i preparació activitats avaluables	30	1,2	CM34, CM37, CM38, KM30, SM42, SM43

L'assignatura combina l'exposició teòrica amb metodologies actives d'aprenentatge col·laboratiu. Es basa principalment en tres estratègies docents complementàries: la classe magistral, la tècnica del puzle (Jigsaw) i l'aprenentarge basat en problemes.

En primer lloc, les sessions magistrals serviran per introduir els principis bàsics de cada tema, estructurar els continguts i oferir un marc teòric sòlid. El professor farà una exposició clara i guiada dels conceptes fonamentals de la ciberseguretat (confidencialitat, integritat, disponibilitat, vectors d'atac, sistemes de protecció, gestió del risc, etc.) amb el suport de materials visuals i exemples pràctics extrets de l'actualitat.

A continuació, cada unitat s'ampliarà i consolidarà mitjançant la metodologia del puzle (Jigsaw). Aquesta tècnica d'aprenentatge cooperatiu implica que l'alumnat treballi de forma autònoma i col·laborativa en petits grups. El procés s'organitza en dues fases:

Fase d'experts: Cada membre del grup rep una subtemàtica concreta del tema general (per exemple: un estudiant treballa el phishing, un altre el ransomware, un altre el firewall, etc.). Els estudiants que comparteixen la mateixa subtemàtica es reuneixen en un "grup d'experts" per estudiar-la en profunditat i preparar una explicació clara per als companys.

Fase de grup base (recomposició del puzle): Cada estudiant retorna al seu grup original i ensenya als altres membres allò que ha après. D'aquesta manera, cada grup reconstrueix tot el contingut del tema a través de l'intercanvi entre iguals, fomentant la responsabilitat compartida, l'aprenentatge actiu i la consolidació crítica dels coneixements.

Aquesta metodologia afavoreix lacomprensió profunda dels continguts, el desenvolupament de competències comunicatives i la capacitat de treballar en equip, aspectes clau per a l'abordatge multidisciplinari de la ciberseguretat en l'àmbit criminològic

D'altra banda, l'assignatura utilitzarà l'Aprenentatge Basat en Problemes per al desenvolupament de la part de les seves activitats d'avaluació. L'aprenentatge basat en problemes (ABP) és una metodologia educativa que utilitza problemes reals com a punt de partida per a l'adquisició i la integració de nous coneixements. En el context de ciberseguritat, aquest enfocament s'adapta especialment bé a causa de la naturalesa dinámica i multifacètica dels riscos cibernètics. Aquí es descriu com es pot aplicar aquesta metodologia a escenaris de risc en ciberseguritat. En un entorn de ABP, es presenta als estudiants un escenari de risc en ciberseguritat. Aquest podria ser un atac de ransomware en una empresa, una bretxa de dades en una organització financera, o una campanya de phishing dirigida. El problema ha de ser complex i obert, permetent múltiples enfocaments i solucions. Els estudiants s'organitzen en petits grups col·laboratius. Cada grup treballa de manera autònoma per a analitzar i entendre el problema presentat. La col·laboració fomenta l'intercanvi d'idees, la discussió i la confrontació de diferents punts de vista, el que enriqueix el procés d'aprenentatge. Els estudiants identifiquen el que saben i el que necessiten aprendre per abordar el problema. Això implica una investigació activa, on els estudiants busquen informació rellevant sobre ciberseguretat, incloent tècniques d'atac i defensa, normatives aplicables, i millors pràctiques. La investigació pot incloure la revisió de literatura acadèmica, anàlisi de casos d'estudi previs,i consulta amb experts en la matèria. Amb la informació recopilada, els estudiants analitzen el problema en profunditat, identificant les vulnerabilitats explotades i les possibles conseqüències. A partir d'aquest anàlisi, desenvolupar estratègies i plans d'acció per mitigar el risc i prevenir futurs incidents. Finalment, s'ha d'indicar que aquest procés requereix pensament crític i l'aplicació de coneixements tècnics i tècnics adquirits durant el curs.

Nota: es reservaran 15 minuts d'una classe, dins del calendari establert pel centre/titulació, perquè els alumnes completin les enquestes d'avaluació de l'actuació del professorat i d'avaluació de l'assignatura.

Avaluació

Activitats d'avaluació continuada

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
Activitat d'anàlisi d'una Advanced and Persistent Threat (APT)	30%	1,5	0,06	CM34, CM37, CM38, KM30, SM42, SM43
Exposició a classe d'un escenari de risc relacionat amb cibersegurat	20%	1,5	0,06	CM34, CM37, CM38, KM30, SM42, SM43
Prova final	50%	2	0,08	CM34, CM37, CM38, KM30, SM42, SM43

Les activitats d'avaluació es poden realitzar al llarg del curs en part de manera individual i en part, en grup. L'avaluació és continuada i s'organitza en funció de les activitats formatives anteriorment descrites.

El sistema d' avaluació continuada combina l' assistència a les classes teòriques/magistrals, la participació activa als seminaris, la realització de les activitats avaluables (amb un pes global del 50%) i la superació de la prova final (amb un pes global del 50%). Atenent a que la prova final implica l'avaluació dels coneixements adquirits de manera acumulativa a través de les activitats d'avaluació continuada, és requisit imprescindible superar la prova final amb un 5/10.

Avaluació

1. Model d'avaluació

El model d'avaluació és continuada i té l'objectiu formatiu que alumnat i professorat pugui conèixer el grau d'assoliment de les competències per tal d'orientar el seu procés formatiu.

Valor de cada ítem d'avaluació: treballs individuals (20%); treball grupal (30%); prova final (50%).

És obligatòria l'assistència a 80% de les classes teòriques i dels seminaris per poder superar l'assignatura.

2. Items d'avaluació

a). Exposició a classe d'un escenari de risc i lliurament per escrit del treball (20%).

Aquesta activitat consisteix escollir un escenari de risc del proposats pel professor, o dels que es proposin pels estudiants/es i siguin validats. S'ha de fer una anàlisi de riscos i proposar unes recomanacions. Al seminari es discutirà el resultat de l'anàlisi de riscos i de les recomanacions proposades. Depenent de la complexitat de l'escenari proposat s'autoritzarà la realització per parelles.

b). Treball alseminari. Es programarà a cada seminari l'anàlisi d'un escenari relacionat amb una amenaça. En aquest sentit, a cada seminari es dedicarà a una de les principals amenaces actuals de cibersegurat (Ramsonware, DDoS, Enginyeria social, ATPs, etc.). Per la preparació d'aquesta activitat es posarà amb antelació a disposició de l'estudiantat materials relacionats amb la matèria. Al final de la sessió es realitzarà un qüestionari o prova escrita, depenen de l'activitat, per avaluar l'adquisició de coneixements. Cada activitat s'avaluarà sobre 10, la mitjana de totes les notes tindrà una ponderació d'un 30 % sobre la nota final.

c). Qüestionari sobre el temari de 30 preguntes, 4 opcions, només una correcta, penalització de 0'25 sobre 30.

3. Condicions par a ser avaluat

L'alumnat serà avaluable sempre que hagi realitzat un conjunt d'activitats el pes de les quals equivalgui a un mínim de 2/3 parts de la qualificació total de l'assignatura. Si el valor de les activitats realitzades no arriba a aquest llindar, el professor/a de l'assignatura pot considerar l'estudiant com a no avaluable,

4. Requisits per a superar l'assignatura y recuperacions

Cal tenir una nota mínima de 5 en tots els ítems que conformen l'avaluació. Si un alumne no supera la part d'avaluació corresponent al treball individual, al treball grupal o laprova final tindrà la possibilitat de recuperar el dia establert per re-avaluar. Els treballs individual i el treballs grupal es recuperan a través d'una o vàries preguntes teòriques sobre els continguts i matèries treballats a les respectives activitats.

Per aprovar l'assignatura a re-avaluació cal tenir igualment un 5 a tots els ítems. Si no s'obté aquesta qualificació mínima a cada ítem, encara que la mitja aritmètica dels quatre ítems d'avaluació superi el 5, la nota final a l'acta serà suspès 4'5.

Atenent a que es tracta d'una segona oportunitat, la nota màxima de proves i treballs recuperats és de 5.

5. Presentacions fora de termini

No s'accepten, salvant situacions de força major. L'alumne obtindrà un 0 en la pràctica no entregada.

6. Excuses

Les excuses per complir amb les obligacions degudes a malaltia o a raons de força major podran ser acceptades sempre que es compti amb un certificat oficial. Absències per raons acadèmiques hauràn de ser prèviament acceptades pel professorat.

7. Conductes fraudulentes

Un/a alumne que copiï o intenti copiar a un examen tindrà un 0 en aquesta prova. Un/a alumne que presenti una pràctica en el que hi hagi indicis de plagi o que no pugui justificar els arguments de la seva pràctica obtindrà un 0 i rebrà una advertència.

8. Puntualitat

Les classes comencen puntualment. No s'admet l'entrada a classe una vegada aquesta hagi començat, ni la sortida abans de la seva finalització, salvant justificació raonable.

9. Matrícules d'Honor

L'estudiantat que obtingui una qualifiació de 9 o superior a la nota final podrá obtar a la Matrícula d'Honor per curs. Aquests efectes es formarà una comissió d'avaluació entre tot el professorat del grup, la qual avaluarà amb criteris objectius si algun/a estudiant compleix amb els requeriments d'excel·lència exigits per l'obtenció d'aquesta qualificació. En totcas, per normativa acadèmica només es poden atorgar com un màxim un 5% de matrícules d'honor sobre el total d'estudiants matriculats en un curs. La comssió d'avaluació amb criteris objectius pot decidir no atorgar cap matrícula d'honor.

10. Avaluació única

Aquells/es estudiants que s'acullin al sistema d'avaluació única, després de ser aprovats per la facultat, realitzaran les proves finals següents.

1. Examen final tipus test amb un valor del 50%. Aquest examen es realitzarà sobre el manual obligatori de curs "ISACA, (2021), Fundamentos de Ciberseguridad, Guía de estudio, 3ª edición."

2. Realització d'un treball de curs sobre els escenaris de risc i amenaces que es proposaran al campus virtual a l'inici del curs amb un valor del 30%.

3. Presentació oral (ponència) davant del professor dun tema sobre les matèries que es proposarà a l'inici de curs amb un valor del 20%.

No avaluable: S'aplicarà el mateix criteri de no avaluable que per l'avaluació continuada.

10. Us intel·ligència artificial

Ús restringit: "Per a aquesta assignatura, es permet l'ús de tecnologies d'Intel·ligència Artificial (IA) exclusivament en [tasques de suport, com la cerca bibliogràfica o d'informació, la correcció de textos o les traduccions . L'estudiant haurà d'identificar clarament quines parts han estat generades amb aquesta tecnologia, especificar les eines emprades i incloure una reflexió crítica sobre com aquestes han influït en el procés i el resultat final de l'activitat. La no transparència de l'ús de la IA en aquesta activitat avaluable es considerarà falta d'honestedat acadèmica i pot comportar una penalització parcial o total en la nota de l'activitat, o sancionsmajors en casos de gravetat

Bibliografia

Bibliografia obligatòria

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

Altra bibliografia aconsellada

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

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. (2024). *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 y privacidad,* 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/

Programari

Aquesta assignatura no precisa programari.

Grups i idiomes de l'assignatura

La informació proporcionada és provisional fins al 30 de novembre de 2025. A partir d'aquesta data, podreu consultar l'idioma de cada grup a través daquest enllaç. Per accedir a la informació, caldrà introduir el CODI de l'assignatura

Nom	Grup	Idioma	Semestre	Torn
(SEM30) Seminaris (30 estudiants per grup)	1	Espanyol	primer quadrimestre	tarda
(TE) Teoria	1	Espanyol	primer quadrimestre	tarda