UAB
Universitat Autònoma de Barcelona

Ciberseguretat

Codi: 105746
Crèdits: 6

2025/2026

Titulació	Tipus	Curs
Prevenció i Seguretat Integral	FB	2

Professor/a de contacte

Nom: Miguel Angel Garcia Alvira

Correu electrònic: miguelangel.garcia@uab.cat

Equip docent

Laura Casas Diaz

Idiomes dels grups

Podeu consultar aquesta informació al final del document.

Prerequisits

No hi ha prerequisits.

Objectius

- Conèixer els conceptes bàsics informàtics i el funcionament d'un sistema d'informació que poden afectar la seguretat de les organitzacions o les persones.

- Conèixer els components físics d'un sistema informàtic u ordinador i xarxes.

- Conèixer el procés d'auditoria de sistemes d'informació.

- Analitzar el Govern i la Gestió de les Tecnologies de la Informació.

- Estudiar els aspectes fonamentals de la Gestió de la Seguretat de la Informació.

- Analitzar els principals estàndards de Seguretat de la informació.

- Conèixer els conceptes fonamentals de la Ciberseguretat.

- Analitzar les tipologies de la delinqüència tecnològica, prova electrònica i Forensic Readiness.

Competències

- Actuar amb responsabilitat ètica i amb respecte pels drets i deures fonamentals, la diversitat i els valors democràtics.
- Aplicar eines de programari específiques per a la resolució de problemes propis de la seguretat.
- Comunicar-se de manera eficaç en anglès, tant de manera oral com escrita.
- Comunicar-se i transmetre idees i resultats de forma eficient en l'entorn professional i no expert, tant de forma oral com escrita.
- Contribuir a la presa de decisions d'inversió en prevenció i seguretat.
- Desenvolupar el pensament científic i el raonament crític en temes de prevenció i seguretat.
- Fer un ús eficient de les TIC en la comunicació i transmissió d'idees i resultats.
- Generar propostes innovadores i competitives en la investigació i en l'activitat professional desenvolupant la curiositat i la creativitat.
- Gestionar de manera eficient la tecnologia en les operacions de seguretat.
- Que els estudiants hagin demostrat posseir i comprendre coneixements en un àrea d'estudi que parteix de la base de l'educació secundària general, i se sol trobar a un nivell que, si bé es recolza en llibres de text avançats, inclou també alguns aspectes que impliquen coneixements procedents de l'avantguarda del seu camp d'estudi.
- Que els estudiants hagin desenvolupat les habilitats d'aprenentatge necessàries per a emprendre estudis posteriors amb un alt grau d'autonomia.
- Que els estudiants puguin transmetre información idees, problemes i solucions a un públic tan especialitzat com no especialitzat
- Que els estudiants sàpiguen aplicar els seus coneixements al seu treball o vocació d'una forma professional i posseeixin les competències que solen demostrar-se per mitjà de l'elaboració i defensa d'arguments i la resolució de problemes dins de la seva àrea d'estudi.
- Que els estudiants tinguin la capacitat de reunir i interpretar dades rellevants (normalment dins de la seva àrea d'estudi) per emetre judicis que incloguin una reflexió sobre temes rellevants d'índole social, científica o ètica.
- Respectar la diversitat i la pluralitat d'idees, persones i situacions.
- Valorar l'impacte tècnic, social i legal dels nous descobriments científics i dels nous desenvolupaments tecnològics.

Resultats d'aprenentatge

1. Analitzar críticament els principis, valors i procediments que regeixen l'exercici de la professió
2. Aplicar eines i fer desenvolupaments de programari específics per a la resolució de problemes propis de la seguretat, el medi ambient, la qualitat o la responsabilitat social corporativa.
3. Aplicar els fonaments d'estadística, d'economia i finances, de marc legal aplicable i d'informàtica necessaris per aplicar la prevenció i la seguretat integral.
4. Comunicar-se de manera eficaç en anglès, tant de manera oral com escrita.
5. Comunicar-se i transmetre idees i resultats de forma eficient en l'entorn professional i no expert, tant de forma oral com escrita.
6. Desenvolupar el pensament científic i el raonament crític en temes de prevenció i seguretat.
7. Explicar el codi deontològic, explícit o implícit, de l'àmbit de coneixement propi.
8. Fer un ús eficient de les TIC en la comunicació i transmissió d'idees i resultats.
9. Formular estratègies de gestió en l'empresa.
10. Generar propostes innovadores i competitives en la investigació i en l'activitat professional desenvolupant la curiositat i la creativitat.
11. Proposar projectes i accions que estiguin d'acord amb els principis de responsabilitat ètica i de respecte pels drets i deures fonamentals, la diversitat i els valors democràtics.
12. Que els estudiants hagin demostrat posseir i comprendre coneixements en un àrea d'estudi que parteix de la base de l'educació secundària general, i se sol trobar a un nivell que, si bé es recolza en llibres de text avançats, inclou també alguns aspectes que impliquen coneixements procedents de l'avantguarda del seu camp d'estudi.
13. Que els estudiants hagin desenvolupat les habilitats d'aprenentatge necessàries per a emprendre estudis posteriors amb un alt grau d'autonomia.
14. Que els estudiants puguin transmetre información idees, problemes i solucions a un públic tan especialitzat com no especialitzat

15. Que els estudiants sàpiguen aplicar els seus coneixements al seu treball o vocació d'una forma professional i posseeixin les competències que solen demostrar-se per mitjà de l'elaboració i defensa d'arguments i la resolució de problemes dins de la seva àrea d'estudi.
16. Que els estudiants tinguin la capacitat de reunir i interpretar dades rellevants (normalment dins de la seva àrea d'estudi) per emetre judicis que incloguin una reflexió sobre temes rellevants d'índole social, científica o ètica.
17. Respectar la diversitat i la pluralitat d'idees, persones i situacions.
18. Valorar l'impacte tècnic, social i legal dels nous descobriments científics i dels nous desenvolupaments tecnològics.

Continguts

La informàtica i per extensió les tecnologies de la informació i comunicació (TIC en endavant) han transformat no només la nostra societat, sinó també les formes d'organització de les empreses i les institucions públiques, les maneres de fer negoci, l'oci i l'entreteniment, i en definitiva les vides de les persones. Per aquest motiu, el coneixement de com funcionen els elements bàsics de la informàtica, així com els principals conceptes del que podríem anomenar com un sistema d'informació complex formen part del contingut substancial d'aquesta assignatura.

D'altra banda, hem de situar als experts en seguretat integral en el què es coneix com "cicle de vida" d'un sistema d'informació d'una organització, des de la seva adquisició, on no només s'han de prendre decisions relacionades amb l'eficàcia o l'eficiència, o la reducció de costos, sinó també sobre la seva alineació amb les polítiques de seguretat de l'empresa. Igualment, la seva gestió, manteniment I operacions han d'estar directament en consonància amb les directrius de seguretat de l'organització.

Per tal d'aconseguir aquests objectius, aquesta assignatura vol oferir a l'estudiant eines d'auditoria de sistemes d'informació, que li permetran avaluar i mesurar si s'estan complint els nivells de seguretat a l'organització. Altrament, s'explicaran models de Govern i gestió de les Tecnologies d'Informació, així com els principals estàndards COBIT, ISO 27.000, NIST 800-53, Esquema Nacional de Seguridad, així com s'analitzarà l'Estrategia de Ciberseguridad Nacional.

Finalment, des del punt de vista jurídic es vol analitzar la delinqüència informàtica i la prova electrònica ja que suposen reptes per la seguretat de la informació. Com a mesures de prevenció es veurà que és un pla de preparació forense digital pel cas de sofrir un atac informàtic o un esdeveniment no desitjat, això es l'anomenat *Forensic Readiness*.

BLOC 1

Tema 1. Introducció i metodologia de lassignatura.

Tema 2. Conceptes bàsics de tecnologies de la informació.

Tema 3. Conceptes bàsics de seguretat de la informació i de cibersegure

BLOC 2

Tema 4. Esdeveniments de ciberseguretat coneguts

Tema 5. Ciberamenaces: definició i tipus

Tema 6. Intel·ligència Artificial i ciberseguretat.

Tema 7. Ciberdefensa i avions nacionals de ciberseguretat.

BLOC 3

Tema 8. Normativa estatal i europea en matèria de ciberseguretat.

Tema 9. Delinqüència tecnològica.

Tema 10. Prova electrònica.

Tema 11. Preparació Forense i Investigació forense digital.

BLOC 4

Tema 12. Protecció dels actius de sistemes dinformació.

Tema 13. Anàlisi dels principals estàndards de ciberseguretat.

Tema 14. Infraestructures crítiques i Pla de Continuïtat de Negoci.

Activitats formatives i Metodologia

	Resultats

Títol	Hores	ECTS	d'aprenentatge
Tipus: Dirigides			
CLASSE TEÒRICA	44	1,76	
Tipus: Supervisades			
TUTORIES DE SUPORT PEL SEGUIMENT DE LES UNITATS DIDÀCTIQUES	2	0,08	
Tipus: Autònomes			
ESTUDI I RESOLUCIÓ DELS ESCENARIS DE RISC	47	1,88	
PREPARACIÓ DE LES PRÀCTIQUES	47	1,88	

Llengua de docencia: Català
Les classes a l'aula corresponen a la metodologia magistral en la que el professor exposa la matèria objecte d'estudi, però també es suscita el debat i resolen problemes i situacions, la resta correspon a sessions practiques on els alumnes treballaran en grup, discutint sobre materials reflexius i resolent casos concrets. Els continguts treballats a les sessions teòriques (a més de la bibliografia bàsica obligatòria) seran avaluats mitjançant proves escrites. D'altra banda, els continguts treballats a les sessions practiques també seran avaluats mitjançant el lliurament de les tasques realitzades.
Alhora, els alumnes, fora de l'aula contribueixen a l'aprenentatge de la matèria amb la cerca de documentació de temes relacionats amb la matèria objecte d'estudi. Cada alumne, a més de la seva assistència a l'aula i l'estudi individual ha de realitzar cerca de documentació i treball personal de consolidació sobre l'exposat en classe.

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
EXAMEN FINAL	50%	2	0,08	1, 2, 3, 6, 7, 9, 11, 12, 13, 14, 15, 16
TREBALL DE GRUP	25%	4	0,16	1, 3, 6, 9, 12, 15, 16, 17, 18
TREBALLS PRÀCTICS	25%	4	0,16	1, 4, 5, 6, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18

A)AVALUACIÓ CONTINUADA

Primera i segona prova: treballs pràctics (25% de la nota final)

Aquests treballs pràctics s'aniran demanant en el decurs del semestre i es centraran en aspectes concrets que determinarà el professorat. Cadascun dels treballs haurà de ser avaluat per sobre del 5 (d'un total de 10) i haurà de ser lliurat en la data proposada segons el cronograma. La mitjana dels treballs pràctics suposarà el 25% de la nota del curs.

Ambdós treballs hauran de tenir una nota de 3 (d'un total de 10) com a mínim per poder sumar a l'avaluació continua.

Els treballs seran recuperables (a la setmana dedicada a tal efecte al final del semestre). Els alumnes que no hagin presentat cap dels treballs en el moment programat no seran avaluats i no podran recuperar-los, a excepció dels que aportin una justificació (document escrit).

Tercera prova: Treball en grup (25% de la nota final)

La pràctica consistirà en la presentació d'un treball en equip relatiu al temari de l'assignatura, on l'alumnat haurà de desenvolupar un programa de prevenció dirigit a col·lectius vulnerables.
Cal obtenir una nota de 3 (d'un total de 10) com a mínim per poder sumar l'activitat a l'avaluació continua.

B)AVALUACIÓ FINAL

a) 2 exàmens finals (50% de la nota final)

Els alumnes, de forma individual, realitzaran dos exàmens, un parcial alliberador durant el decurs de l'assignatura i un examen final que es farà en la data oficial del calendari establert per l'EPSI. En ambdues proves s'haurà d'obtenir una qualificació mínima d'un 5 (d'un total de 10). Ambdós exàmens consistiran en un test de trenta preguntes sobre el programa de l'assignatura i la resolució d'un cas pràctic sobre les matèries analitzades. Pel que fa a la prova tipus test consistirà en trenta preguntes amb múltiple opció (quatre respostes només una correcta), amb una penalització per pregunta incorrecta de 0,25/30 (o quatre incorrectes resta una correcta).

L'alumnat que no hagués superat la primera prova final d'acord als criteris anteriors haurà d'examinar-se de la totalitat del temari en l' examen final que es farà en la data oficial del calendari establert per l'EPSI. Els alumnes No Presentats no seran avaluats, a excepció dels que aportin una justificació (document escrit).

Els exàmens seran recuperables a la setmana dedicada a tal efecte al final del semestre.

Examen de recuperació

En cas de no superar l'assignatura d'acord amb els criteris abans esmentats i s'obtingui un resultat del conjunt de les avaluacions que no arribi a una nota de 5 (d'un total de 10) podrà presentar-se a un examen final sempre que l'alumne s'hagi avaluat en un conjunt d'activitats, el pes de les quals equivalgui a un mínim de dues terceres parts de la qualificació total de l'assignatura. Si no ha estat avaluat d'aquestes dues terceres parts per no haver-se presentat a les proves obtindrà una qualificació de *No Prese*ntat, sense que tingui la possibilitat de presentar-se a l'examen final de recuperació.

En aquest examen es tornarà a avaluar el conjunt dels continguts de l'assignatura que no s'hagin superat a l'avaluació continuada.

En cas de superar-se l'examen final l'assignatura quedarà aprovada amb un 5 com a màxim, independentment de la nota obtinguda a l'examen.

Les proves/exàmens podran ser escrits i/o orals a criteri del professorat.

Canvi de data d'una prova o examen

L'alumnat que necessiti canviar una data d'avaluació han de presentar la petició justificada emplenant el document que trobarà a l'espai moodle de Tutorització EPSI. Un cop emplenat el document s'ha d'enviar al professorat de l'assignatura i a la coordinació del Grau.

Revisió

En el moment de fer cada activitat avaluativa, el professorat informarà l'alumnat dels mecanismes de revisió de les qualificacions. Per a l'alumnat d'avaluació única el procés de revisió serà el mateix.

Avaluació Única

Els estudiants que optin per l'avaluació única faran una prova de síntesi final de tot el contingut de l'assignatura (50%) i lliuraran la feina de l'assignatura (50%)

La data per a aquesta prova i el lliurament del treball de lassignatura serà la mateixa programada en lhorari per a lúltim examen davaluació continuada.

S'aplica el mateix sistema de recuperació que per a l'avaluació continuada. Les proves/exàmens podran ser escrits i/o orals a criteri del professorat.

Avaluació de l'alumnat en segona convocatòria o més

L'alumnat que repeteixil'assignatura haurà de realitzar les proves i els exàmens programats i lliurar el treball de l'assignatura en les dates indicades a l'aula Moodle.

Les proves/exàmens podran ser escrits i/o orals a criteri del professorat.

Altres consideracions

Sense perjudici d'altres mesures disciplinàries que s'estimin oportunes, i d'acord amb la normativa acadèmica vigent, "en cas que l'estudiant faci qualsevol irregularitat que pugui conduir a una variació significativa de la qualificació d'un acte d'avaluació, es qualificarà amb un 0 aquest acte d'avaluació, amb independència del procés disciplinari que es pugui instruir. en cas que es produeixin diverses irregularitats en els actes d'avaluació duna mateixa assignatura, la qualificació final d'aquesta assignatura serà 0".

Si concorren circumstàncies sobrevingudes que impedeixin el desenvolupament normal de l'assignatura, el professorat podrà modificar tant la metodologia com l'avaluació de l'assignatura.

Ús de la IA

En aquesta assignatura, es permet l'ús de tecnologies d'Intel·ligència Artificial (IA) com a part integrant del desenvolupament del treball, sempre que el resultat final reflecteixi una contribució significativa de l'estudiant en l'anàlisi i la reflexió personal. 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 es considerarà falta d'honestedat acadèmica i pot comportar una penalització en la nota de l'activitat, sancions majors en casos de gravetat.

Bibliografia

Alonso Lecuit, Javier (2021). "Directiva NIS2: valoraciones y posiciones desde el sector privado", CIBER elcano No. 65 - abril de 2021: Entidades críticas y resileiencia en la UE | Directiva NIS2 (disponible en http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_

Communications-Electronics Security Group (2011). *Digital Continuity to Support Forensic Readiness.* London: The National Archives.

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

Fojon, E., Coz J. R., Linares, S., Miralles, R. (sin fechar) *La Ciberseguridad Nacional, un compromiso de todos. La necesidad de evolucionar de una cultura reactiva a una de prevención y resiliencia.* ISMS FORUM: Madrid.

Gómez Vieites, A. (2011). *Enciclopedia de la seguridad informática*. Madrid: Ra-Ma Editorial.

ISACA (2012). *COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT.* ISACA: Rolling Meadows.

ISACA (2014). *Manual de preparación para el examen de* CISM*.* ISACA: Rolling Meadows.

ISACA (2014).*CSX Cybersecurity Fundamentals Study Guide*. ISACA: Rolling Meadows.

ISACA (2014). *Transforming Cybersecurity*. ISACA: Rolling Meadows.

ISACA (2014). *Responding to Targeted Cyberattacks*. ISACA: Rolling Meadows.

ISACA (2016). *Manual de preparación para el examen de* CISA*.* ISACA: Rolling Meadows.

Martín Ávila, A.; Quinto Zumarraga, F. de. (2003). *Manual de seguridad en Internet: soluciones técnicas y jurídicas*. A Coruña: Netbiblo.

Ortiz Plaza, Roberto; Nuñez Baroja, Andrés (2021). "De la concienciación al riesgo humano en la ciberseguridad", Revista SIC: ciberseguridad, seguridad de la información y privacidad, ISSN 1136-0623, Vol. 30, Nº. 143 (Febrero 2021), 2021 (Ejemplar dedicado a: Ciberataques en 2021. Tiempos modernos), págs. 72-73

Piattini Velthuis, M., Peso Navarro, E. del, Peso M. del (2011). *Auditoría de tecnologías y sistemas de información.* Madrid: Ra-Ma Editorial.

Rowlingson R. (2004). "A Ten Step Process for Forensic Readiness". *International Journal of Digital Evidence* (Volume 2, Issue 3)

Velasco Núñez, E. (2013). "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica", *Diario La Ley (*Nº 8183)

Velasco Núñez, E. (2015). "Los delitos informáticos", *Práctica Penal: cuaderno jurídico* (núm.81) pp. 14 a 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

No és necessari programari per aquesta assignatura

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
(TE) Teoria	1	Català	segon quadrimestre	tarda
(TE) Teoria	2	Català	segon quadrimestre	tarda
(TE) Teoria	3	Català	segon quadrimestre	tarda