UAB
Universitat Autònoma de Barcelona

Ciberseguretat

Codi: 105779
Crèdits: 6

2024/2025

Titulació	Tipus	Curs
2502501 Prevenció i Seguretat Integral	FB	2

Professor/a de contacte

Nom: Jose Cañabate Perez

Correu electrònic: josep.canabate@uab.cat

Equip docent

Laura Casas Diaz

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

- 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

El programa de l'assignatura inclou un ampli espectre de conceptes i de pràctiques essencials en el camp de la ciberseguretat i les tecnologies de la informació. Comença amb una introducció a la metodologia del curs, proporcionant als estudiants una base sòlida als conceptes fonamentals de TI i seguretat de la informació. A mesura que avança el curs, s'exploren incidents de ciberseguretat coneguts, diversos tipus de ciberamenaces i el paper de la intel·ligència artificial en la detecció i la resposta a aquests incidents. També es discuteixen les estratègies de ciberdefensa i els plans nacionals dissenyats per protegir 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. Per acabar, s'aborda la protecció d'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 els estudiants per enfrontar els desafiaments en ciberseguretat de manera efectiva i competent.

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 ciberseguretat.

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 plans 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. Forensic Readiness i Investigació digital forense.

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

Títol	Hores	ECTS	Resultats d'aprenentatge
Tipus: Dirigides			
Videoconferencies amb la participació activa de l'alumnat	12	0,48	
Tipus: Supervisades			
RESOLUCIÓ DE DUBTES SOBRE TEMARI i PRÀCTIQUES	6	0,24	
Tipus: Autònomes			
ESTUDI I RESOLUCIÓ DELS ESCENARIS DE RISC	60	2,4	
PREPARACIÓ DE LES PRÀCTIQUES	60	2,4	

Llengua de docència: espanyol.

Atenent a que la modalitat de la classe és en línia, amb l'objectiu d'aconseguir els objectius d'aprenentatge descrits en el present. de alguns documentals.Cada tema tindrà un fòrum de dudas, i s'establirà un fòrum de "Aportaciones" on els alumnes poden introduir lectures, articles, webs, documentals, i tot tipus de materials i recursos relacionats amb l'assignatura. Per altra part, hauran de realitzar la resolució dels dos casos pràctics relacionats amb els temes estudiats a l'assignatura. els fòrums i sessions en línia es van dedicar a aprofundir sobre els temes tractats així com a resoldre possibles duda.

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, per a la complementació per part de l'alumnat de les enquestes d'avaluació de l'actuació del professorat i d'avaluació de l'assignatura/mòdul.

Avaluació

Activitats d'avaluació continuada

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
EXAMEN FINAL	50%	2	0,08	3, 2, 6, 1, 18, 7, 9, 10, 5, 8, 11, 17, 15, 16, 14, 13, 12
PARTICIPACIÓ A FÒRUM I A CLASSE	10%	5	0,2	2, 15, 16, 14, 13, 12
TREBALLS PRÀCTICS	40%	5	0,2	3, 2, 4, 6, 1, 18, 7, 9, 10, 5, 8, 11, 17, 15, 16, 14, 13, 12

L'avaluació de l'assignatura es realitzarà mitjançant:

1. AVALUACIÓ CONTINUADA

- Realització de quatre Pràctiques d'Avaluació Continuada (40%)

  - Treball Indiduals:

Consisteix en dos PAC.

PAC 1: Sobre conceptes bàscis de cibersegurat.

PAC 2. Sobre conceptes bàsics de criptologia.

  - Treball en grup:

Consisteix en dos PAC grupals:

PAC 3: Definicions i característiques principals d'una *Advanced and Persistent Threat (APT)*.

PAC 4: Escenari de risc relacionat amb una *Advanced and Persistent Threat (APT)*.

- Participació als fòrums de debat i a classe (10%)

Per superar aquest apartat cada alumne haurà de realitzar una participació de qualitat, en cada fòrum de debat (hi haurà 4 fòrums, dividits per àrees temàtiques) Per tant de cada alumne s'esperen un mínim de 4 intervencions de qualitat (és a dir, aportant nocions i comentaris que vagin més enllà del que recull en els manuals incloent bibliografia i referències) Al seu torn cada alumne haurà d'introduir un mínim de 4 aportacions en l'apartat destinat a aquests efectes de l'assignatura. Cada intervenció en el fòrum i cada aportació suposen un 10% de l'avaluació d'aquest apartat, la qualificació s'establirà en base a criteris de

qualitat, originalitat, coherència i interacció, si cap. Les intervencions o aportacions extra, es valoraran positivament, però recordem que mai es podrà excedir dels 1 punt que té aquest apartat en relació a la nota global.

-Examen tipus test de tot el temari (50%)

Consistirà en un examen tipus test de30 preguntes sobre el temari amb quatre opcions possibles. La pregunta correcta suma 1 sobre 30, la pregunta incorrecta resta 0'25 sobre 30, la no contestades ni sumen ni resten.

REVISIÓ DE LA QUALIFIACIÓ FINAL: Es concertarà dia i hora de revisió amb els professors en un termini màxim de 48 hs. després de la publicació de les qualificacions finals.

RECUPERACIÓ

En cas de no superar l'assignatura d'acord amb els criteris abans esmentats (avaluació continuada), es podrà fer una prova de recuperació en la data programada a l'horari, i que versarà sobre la totalitat dels continguts del programa.

Per participar a la recuperació l'alumnat ha d'haver estat prèviament 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. No obstant això, la qualificació que constarà a l'expedient de l'alumne és d'un màxim de 5-Aprovat.

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.

PLAGI

Sense perjudici d'altres mesures disciplinàries que s'estimin oportunes, i d'acord amb la normativa acadèmica vigent, "en cas que l'estudiant realitzi 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 d'una mateixa assignatura, la qualificaciófinal d'aquestaassignatura serà 0".

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

Si durant la correcció es tenen indicis que una activitat o treball s'han realitzat amb respostes assistides per intel·ligència artificial, el/la docent podrà complementar l'activitat amb una entrevista personal per a corroborar l'autoria del text.

NO AVALUABLE:

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.

2. AVALUACIÓ ÚNICA.

Els/les estudiants que optin per l'avaluació única faran les següents proves.

- Realització de quatre Pràctiques (40%)

PAC 1: Sobre conceptes bàscis de cibersegurat.

PAC 2. Sobre conceptes bàsics de criptologia.

PAC 3: Definicions i característiques principals d'una *Advanced and Persistent Threat (APT)*.

PAC 4: Escenari de risc relacionat amb una *Advanced and Persistent Threat (APT)*.

- Realització de comentari de text sobre un tema de cibersegurat relacionat amb el programa (10%)

- Examen tipus test de tot el temari (50%)

Consistirà en un examen tipus test de 30 preguntes sobre el temari amb quatre opcions possibles. La pregunta correcta suma 1 sobre 30, la pregunta incorrecta resta 0'25 sobre 30, la no contestades ni sumen ni resten.

Recuperació: "S'aplicarà el mateix sistema de recuperació que per l'avaluació continuada."

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

Revisió de la qualificació final: "La revisió de la qualificació final segueix el mateix procediment que per a l'avaluació continuada".

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

L'assignatura no requereix programari.

Llista d'idiomes

Nom	Grup	Idioma	Semestre	Torn
(TE) Teoria	1	Espanyol	segon quadrimestre	tarda