Gestió de la Seguretat dels Sistemes d'Informació

Codi: 102161
Crèdits: 6

2026/2027

Titulació	Tipus	Curs
Empresa i Tecnologia	OP	4
Gestió Aeronàutica	OP	4

Professor/a de contacte

Nom : Miguel Angel Cara Ruiz

Correu electrònic : miguelangel.decara@uab.cat

Equip docent

Miguel Angel Cara Ruiz

Idiomes dels grups

Podeu consultar aquesta informació al final del document.

Prerequisits

Tot i no haver prerequisits, es recomana cursar l'assignatura 102169-Xarxes.

Objectius

Objectius de l'assignatura

L'assignatura té com a objectiu proporcionar a l'alumnat una visió global, aplicada i progressiva de la seguretat de la informació en les organitzacions, combinant fonaments tècnics, govern de la seguretat, gestió del risc i aplicació pràctica mitjançant un cas de treball continu.

- Comprendre els fonaments de la ciberseguretat i de la seguretat de la informació en un context organitzatiu.
- Analitzar l'estat de la seguretat de la informació d'una organització des d'una perspectiva global, tenint en compte actius, processos, riscos, controls i necessitats del negoci.
- Dotar l'alumnat de les habilitats tècniques i de gestió necessàries per comprendre l'entorn tecnològic de la seguretat de la informació.
- Entendre les necessitats de seguretat de la informació en les organitzacions i transmetre-les a la Direcció.
- Conèixer els marcs legals, estàndards internacionals, normatives i bones pràctiques que afecten la seguretat de la informació.
- Identificar i valorar riscos de seguretat de la informació, proposant mesures de mitigació adequades i prioritzades.
- Comprendre els principals àmbits tècnics de la seguretat: gestió d'identitats, contrasenyes i criptografia,

xarxes, protecció de les dades, núvol, IoT, seguretat en aplicacions i resposta a incidents.
- Avaluar l'impacte de la seguretat de la informació en la continuïtat del negoci, la protecció de les dades, el compliment normatiu i la presa de decisions de la Direcció.
- Aplicar els coneixements adquirits en un cas pràctic mitjançant lliurables progressius: inventari d'actius i processos, valoració inicial, anàlisi de riscos, pla de projectes, arquitectura de seguretat i propostes de millora.

Competències detallades:

- Demostrar una visió global de la seguretat de la informació en les organitzacions.
- Comprendre l'alineament entre els objectius de l'organització i els objectius de seguretat de la informació.
- Identificar l'estat de la seguretat tant des d'un punt de vista de gestió organitzativa com des d'un punt de vista tècnic.
- Identificar mancances en el govern de la seguretat corporativa i proposar línies d'actuació per a la seva millora.
- Identificar riscos de seguretat de la informació i plantejar mesures de tractament adequades.
- Comprendre els principals àmbits tècnics de la seguretat de la informació, incloent-hi identitat, criptografia, xarxes, protecció de les dades, núvol, IoT, aplicacions i resposta a incidents.
- Demostrar habilitats per comunicar conceptes tècnics de seguretat a destinataris sense coneixement especialitzat, tant de forma oral com escrita.
- Aplicar els coneixements adquirits en exercicis d'avaluació continuada, presentacions i lliurables vinculats al cas pràctic de l'assignatura.

Resultats d'aprenentatge detallats

- Avaluar l'estat de la seguretat de la informació d'una organització, en coherència amb el seu sector d'activitat, context legal, exposició i nivell de risc assumible per la Direcció.
- Definir l'estratègia inicial d'implantació o millora d'un sistema de gestió de la seguretat de la informació.
- Aplicar una metodologia bàsica d'anàlisi de riscos per identificar amenaces, vulnerabilitats, impactes i mesures de mitigació.
- Definir un pla de projectes de seguretat prioritzat, justificant les accions proposades segons criteris de risc, impacte i alineament amb el negoci.
- Explicar el paper dels marcs de referència, estàndards i bones pràctiques en l'organització, gestió i millora contínua de la seguretat de la informació.
- Valorar la importància de la protecció de les dades, la gestió d'identitats, la criptografia i la seguretat en aplicacions dins d'una estratègia corporativa de seguretat.
- Comprendre els riscos i criteris de seguretat associats a l'ús de solucions al núvol, entorns IoT i tecnologies emergents, incloent-hi la seguretat en intel·ligència artificial.
- Analitzar situacions de resposta a incidents des d'una perspectiva organitzativa i tècnica, identificant necessitats de detecció, contenció, comunicació i millora posterior.

Resultats d'aprenentatge

Empresa i Tecnologia

- CM26 (Complir els principis ètics, legals i relatius a la propietat intel·lectual amb relació al tractament de la informació privada en l'àmbit empresarial.) Complir els principis ètics, legals i relatius a la propietat intel·lectual amb relació al tractament de la informació privada en l'àmbit empresarial.
- KM22 (Identificar, a partir de les necessitats d'una organització, els sistemes de gestió i comunicació de dades, així com la seva governança.) Identificar, a partir de les necessitats d'una organització, els sistemes de gestió i comunicació de dades, així com la seva governança.
- SM16 (Distingir les activitats de gestió de la seguretat i la seva implicació en el disseny i la implementació de sistemes d'informació.) Distingir les activitats de gestió de la seguretat i la seva implicació en el disseny i la implementació de sistemes d'informació.

Continguts

Seguretat de la Informació i Ciberseguretat

- Comprendre què s'entén per seguretat de la informació i ciberseguretat en el context de les organitzacions.
- Identificar la importància de la seguretat de la informació en entorns corporatius, considerant-ne l'impacte en el negoci, la continuïtat operativa, la protecció de dades i la presa de decisions.
- Analitzar els principals conceptes de confidencialitat, integritat, disponibilitat, autenticació, traçabilitat i responsabilitat.
- Comprendre l'evolució de les amenaces i els riscos de ciberseguretat en les organitzacions actuals.

Govern, marcs de referència i gestió de la seguretat

- Conèixer els principals marcs de referència, estàndards i bones pràctiques aplicables a la seguretat de la informació.
- Comprendre el paper dels marcs de referència en l'organització, la gestió i la millora contínua de la seguretat.
- Identificar com s'alineen els objectius de seguretat de la informació amb els objectius estratègics i operatius de l'organització.
- Analitzar les mancances de seguretat d'una organització i proposar línies d'actuació per a la seva millora.

Anàlisi i gestió de riscos

- Comprendre la importància de l'anàlisi de riscos en la gestió de la seguretat de la informació.
- Identificar actius, processos, amenaces, vulnerabilitats, impactes i controls dins d'un entorn corporatiu.
- Aplicar una metodologia bàsica d'anàlisi de riscos per valorar l'estat de seguretat d'una organització.
- Definir mesures de mitigació i plans d'actuació prioritzats segons criteris de risc, impacte i viabilitat.

Gestió d'identitats, contrasenyes i criptografia

- Comprendre la importància de la gestió d'identitats i accessos en la seguretat corporativa.
- Analitzar els riscos associats a l'ús de contrasenyes, l'autenticació feble i la mala gestió de privilegis.
- Conèixer els principis bàsics de la criptografia i la seva aplicació en la protecció de la informació.
- Diferenciar entre xifratge simètric, xifratge asimètric, funcions hash, certificats digitals i signatura digital.

Seguretat en xarxes i entorns tecnològics

- Comprendre els fonaments de la seguretat en xarxes de comunicacions.
- Identificar riscos habituals en arquitectures de xarxa corporatives i possibles mesures de protecció.
- Analitzar el paper dels controls de seguretat en xarxes, segmentació, monitorització i protecció perimetral.
- Relacionar la seguretat de xarxa amb la resta d'àmbits de la seguretat corporativa.

Protecció de dades i compliment normatiu

- Comprendre la importància de la protecció de dades dins d'una estratègia de seguretat de la informació.
- Identificar els principals requisits legals, normatius i regulatoris que afecten la seguretat i la protecció de la informació.
- Analitzar l'impacte del compliment normatiu en la gestió de la seguretat corporativa.
- Comprendre la relació entre protecció de dades, govern de la seguretat, riscos i controls tècnics.

Seguretat al núvol, IoT i tecnologies emergents

- Comprendre els principals riscos associats a l'ús de solucions cloud en entorns corporatius.
- Identificar criteris de seguretat aplicables a serveis cloud, models de responsabilitat compartida i protecció de la informació al núvol.
- Analitzar els riscos específics d'entorns IoT i dispositius connectats.
- Comprendre els riscos emergents vinculats a noves tecnologies, incloent-hi la seguretat en intel·ligència artificial.

Seguretat en aplicacions

- Comprendre els fonaments de la seguretat en aplicacions i la seva importància en el cicle de vida tecnològic.
- Identificar riscos habituals en aplicacions corporatives i serveis exposats.
- Relacionar la seguretat en aplicacions amb la protecció de dades, la identitat, la xarxa i la gestió de vulnerabilitats.

Resposta a incidents

- Comprendre el cicle de gestió i resposta davant d'incidents de seguretat.
- Identificar les fases principals de detecció, anàlisi, contenció, erradicació, recuperació i millora posterior.
- Analitzar incidents de seguretat des d'una perspectiva tècnica i organitzativa.
- Comprendre la importància de la comunicació, la documentació i la presa de decisions durant un incident.

Cas pràctic aplicat

- Aplicar els coneixements adquirits en un cas pràctic continu de seguretat de la informació.
- Elaborar un inventari d'actius, processos i valoració inicial del cas.
- Realitzar una valoració de riscos i definir un pla de projectes de seguretat.
- Proposar una arquitectura de seguretat coherent amb les necessitats del cas.
- Identificar millores addicionals i justificar-ne la prioritat en funció del risc, l'impacte i l'alineament amb el negoci.
- Presentar i defensar les conclusions del cas pràctic de forma clara, estructurada i orientada a perfils tècnics i no tècnics.

Activitats formatives i Metodologia

Títol	Hores	ECTS	Resultats d'aprenentatge
Treball en Grup	20	0,8	
Estudi	50	2	
Problemes i exercicis	15	0,6	
Classes Magistrals i casos	30	1,2	
Redacció de treballs i preparació de casos	32	1,28	

Aspectes generals

1. Relació professorat-alumnat

La informació general i rellevant de l'assignatura es publicarà al Campus Virtual, o a l'espai equivalent habilitat per la universitat. En aquest espai es detallaran els continguts de la guia docent, les dates d'avaluació continuada, les dates i condicions de lliurament dels treballs, els materials de suport i qualsevol altra informació necessària per al seguiment de l'assignatura.

La planificació de l'assignatura podrà estar subjecta a ajustos per motius organitzatius, acadèmics o per

incidències sobrevingudes. En cas que es produeixin canvis en la programació, aquests seran comunicats a través del Campus Virtual, que es considerarà el canal habitual de comunicació entre el professorat i l'alumnat.

2. Idiomes

Les classes es realitzaran majoritàriament en català o castellà, tot i que serà habitual l'aparició de termes tècnics en anglès. El material escrit o de suport a l'assignatura, com ara apunts, bibliografia, referències, enunciats de pràctiques, exercicis o casos, es podrà facilitar en català, castellà o anglès. En aquest sentit, l'ús de la llengua anglesa podrà ser habitual, especialment en materials tècnics o referències especialitzades.

La prova final i la reavaluació estaran redactades en català o castellà. Les respostes a les proves, exercicis, pràctiques i presentacions es podran lliurar indistintament en català, castellà o anglès.

Activitats durant el curs

Classes magistrals, casos i sessions de resolució d'exercicis

Durant les sessions teòriques es presentaran els continguts fonamentals de l'assignatura, necessaris per comprendre els principals àmbits de la seguretat de la informació en les organitzacions.

Aquestes sessions abordaran, entre altres aspectes, els fonaments de la ciberseguretat, els marcs de referència, l'anàlisi de riscos, la gestió d'identitats, la criptografia, la seguretat en xarxes, la protecció de dades, la seguretat al núvol i IoT, la seguretat en aplicacions, la resposta a incidents i les tecnologies emergents, incloent-hi la seguretat en intel·ligència artificial.

Les classes podran combinar explicació teòrica, anàlisi d'exemples, resolució d'exercicis, discussió de casos i activitats d'avaluació continuada. Així mateix, s'indicaran les vies necessàries per ampliar o aprofundir els continguts tractats a classe.

Aprenentatge basat en problemes, aprenentatge cooperatiu, tallers i exercicis pràctics

Una part de l'assignatura utilitzarà metodologies d'aprenentatge actiu i exercicis de caràcter aplicat, en què l'alumnat haurà d'afrontar situacions properes a la pràctica professional de la seguretat de la informació en entorns corporatius.

Durant el curs es podran realitzar activitats individuals i en grup, supervisades per l'equip docent de l'assignatura. Aquestes activitats estaran orientades a l'aplicació pràctica dels continguts treballats a classe, especialment mitjançant el desenvolupament del cas pràctic de l'assignatura.

Es fomentarà el treball en equip i l'intercanvi col·laboratiu d'informació i eines per a la resolució de problemes. No obstant això, el procés final d'aprenentatge haurà de ser individual, recolzat en l'activitat autònoma de cada estudiant, que haurà de complementar i enriquir el treball iniciat en les sessions dirigides del curs.

L'activitat supervisada, mitjançant tutories reglades i consultes efectuades durant el curs, serà igualment una eina important per a l'adquisició dels coneixements i competències que proporciona l'assignatura.

Nota: es reservaran 15 minuts d'una classe, dins del calendari establert pel centre/titulació, perquè l'alumnat completi 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
Pràctiques, Exercicis i Participació	60%	0	0	CM26, KM22, SM16
Examens	40%	3	0,12	CM26, KM22, SM16

Aquesta assignatura no contempla la posibilitat de avaluació única.

L'avaluació consta de dues parts diferenciades:

(1) Pràctiques, Exercicis i Participació (6 punts): Exercici(s) d'aprenentatge basat en problemes, treball en equip o individual, presentació a classe dels resultats i altres proves que es determinin. Si el pes de la activitat és de 1 punts o més, es publicarà un avis al campus virtual amb una anticipació de al menys una setmana.

Les activitats d'aquest grup, per ser d'avaluació continuada, no es podran recuperar. S'han de lliurar en els terminis i condicions establertes que es faran públiques al Campus Virtual de l'assignatura.

(2) Teoria (4 punts): Prova escrita final sobre conceptes i aspectes tractats al llarg del curs que es farà el dia que determini la facultat en el calendari d'exàmens.

Durant el curs es poden fer proves parcials alliberadores de matèria. Per cadascuna d'elles es publicarà un avis al campus virtual amb una anticipació de al menys una setmana

Condicions generals per superar l'assignatura:

Per aprovar l'assignatura cal obtenir 5 punts havent assolit els mínims següents:

- Part de Pràctiques Exercicis i Participació: mínim de 2.5 punts de 6 possibles
- Part Teoria: mínim de 1.5 punts de 4 possibles

Es considerarà Avaluable aquell qui hagi fet al menys dues entregues en l'avaluació continuada.

Càlcul de la nota final:

- Si s'assoleixen els mínims serà al menys la suma de la obtinguda en les dues parts. El professor podrà, noobstant, augmentar-la atenent a criteris objectius i equitatius. Si després de la suma dels resultats obtinguts a ambdues parts no s'assolissin els 5 punts necessaris per aprovar l'assignatura, l'alumne podrà optar pel efectuar el procés de recuperació en les condicions que es descriu més avall.
- Si no s'assoleixen els mínims de la part Pràctiques, Exercicis i Participació la nota final de l'assignatura serà la de aquesta part i per tant l'assignatura quedarà suspesa.
- Si no s'assoleixen els mínims de la part Teoria i la suma de les parts és inferior a 3,5 punts la nota final serà la suma de les parts i per tant l'assignatura quedarà suspesa
- Si no s'assoleixen els mínims de la part Teoria i la suma de les parts és superior o igual a 3,5 punts es podrà fer la prova de recuperació en les condicions descrites més endavant.

Calendari d'activitats d'avaluació

Les dates de les diferents activitats d'avaluació (exercicis, lliurament de treballs, ...) s'anunciaran amb suficient antelació durant el semestre.

Les dates de les proves parcial i final de l'assignatura estan programades en el calendari d'exàmens de la Facultat.

\"*La programació de les proves d'avaluació no es podrà modificar, tret que hi hagi un motiu excepcional i degudament justificat pel qual no es pugui realitzar un acte d'avaluació. En aquest cas, les persones*

responsables de les titulacions, prèvia consulta al professorat i a l'estudiantat afectat, proposaran una nova programació dins del període lectiu corresponent.\" ***Apartat 1 de l'Article 115. Calendari de les activitats d'avaluació (Normativa Acadèmica UAB)***

Els estudiants i les estudiantes de la Facultat d'Economia i Empresa que d'acord amb el paràgraf anterior necessitin canviar una data d'avaluació han de presentar la petició omplint eldocument Sol·licitud reprogramació prova https://eformularis.uab.cat/group/deganat_feie/reprogramacio-proves

Procediment de revisió de les qualificacions

Coincidint amb l'examen final s'anunciarà el dia i el mitjà en que es publicaran les qualificacions finals. De la mateixa manera s'informarà del procediment, lloc, data i hora de la revisió d'exàmens d'acord amb la normativa de la Universitat.

Procés de Recuperació

*"Per participar al procés de recuperació l'alumnat ha d'haver estat prèviament avaluat en un conjunt d'activitats que representi un mínim de dues terceres parts de la qualificació total de l'assignatura o mòdul."****Apartat 3 de l'Article 112 ter. La recuperació (Normativa Acadèmica UAB).*** Els estudiants i les estudiants han haver obtingut una qualificació mitjana de l'assignatura entre 3,5 i 4,9.

La data d'aquesta prova estarà programada en el calendari d'exàmens de la Facultat. L'estudiant que es presenti i la superi aprovarà l'assignatura amb una nota de 5. En cas contrari mantindrà la mateixa nota.

Irregularitats en actes d'avaluació

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 0 aquest acte d'avaluació, amb independència del procés disciplinari que s'hi pugui instruir. En cas que es produeixin diverses irregularitats en els actes d'avaluació d'una mateixa assignatura, la qualificació final d'aquesta assignatura serà 0\". ***Apartat 10 de l'Article 116. Resultats de l'avaluació. (Normativa Acadèmica UAB)***

La realització de les activitats d'avaluació està subjecta al que estableix aquesta guia docent, així com a la "Política de la Facultat d'Economia i Empresa davant la detecció d'irregularitats durant la realització d'activitats avaluatives", que regula les condicions de desenvolupament de les proves d'avaluació i els procediments aplicables en cas de detectar-se irregularitats. Es recomana a l'estudiantat consultar-ne el contingut.

Bibliografia

Veure Campus Virtual

Programari

No es fa servir cap programa que no sigui part de la ofimàtica convencional

Grups i idiomes de l'assignatura

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

Tipus de docència	Grup	Idioma	Semestre	Torn
(TE) Teoria	20	Català	primer quadrimestre	tarda
(PAUL) Pràctiques d'aula	201	Català	primer quadrimestre	tarda