Universitat Autònoma de Barcelona

2019/2020

Ciberseguretat

Codi: 105746
Crèdits: 6

Titulació	Tipus	Curs	Semestre
2502501 Prevenció i Seguretat Integral	FB	2	2

Professor/a de contacte

Nom: Josep Cañabate Pérez
Correu electrònic: Josep.Canabate@uab.cat

Utilització d'idiomes a l'assignatura

Llengua vehicular majoritària: espanyol (spa)
Grup íntegre en anglès: No
Grup íntegre en català: Sí
Grup íntegre en espanyol: No

Equip docent

Xavier Rubiralta Costa

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

- Aplicar eines de programari específiques per a la resolució de problemes propis de la seguretat.
- Assumir la responsabilitat social, ètica i professional que es derivi de la pràctica de l'exercici professional.
- 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.
- 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. 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.
2. Aplicar els fonaments d'estadística, deconomia i finances, de marc legal aplicable i dinformàtica necessaris per aplicar la prevenció i la seguretat integral.
3. Assumir la responsabilitat social, ètica i professional que es derivi de la pràctica de l'exercici professional.
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. Fer un ús eficient de les TIC en la comunicació i transmissió d'idees i resultats.
8. Formular estratègies de gestió en l'empresa.
9. Generar propostes innovadores i competitives en la investigació i en l'activitat professional desenvolupant la curiositat i la creativitat.
10. Respectar la diversitat i la pluralitat d'idees, persones i situacions.
11. 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 a l'assignatura i definició de conceptes bàsics.

Tema 2. Components físics d'un sistema informàtic o ordinador i xarxes.

Tema 3. Programari d'un sistema informàtic o ordinador (sistema operatiu, aplicacions, llicències).

Tema 4. Adquisició, desenvolupament i implementació de sistemes d'Informació.

Tema 5. Govern i Gestió de TI / COBIT (***Control Objectives for Information and Related Technology***).

BLOC 2

Tema 6. Procés d'auditoria de sistemes d'informació.

Tema 7. Delinqüència tecnològica.

Tema 8. Prova electrònica.

Tema 9. ***Forensic Readiness*** i Investigació digital forense.

BLOC 3

Tema 10. Protecció dels actius de sistemes d'informació.

Tema 11. Gestió de la seguretat de la informació i compliment

Tema 12. Desenvolupament del programa de seguretat de la informació.

BLOC 4

Tema 13. Gestió d'incidents de seguretat de la informació.

Tema 14. Anàlisi de la ISO 27000 (Sistema de Gestió de la Seguretat de la Informació) i la NIST 800_53.

Tema 15. Infraestructures crítiques i Pla de Continuïtat de Negoci.

BLOC 5

Tema 16. Tendències: ***Cloud Computing***, BYOD, ***Big Data***, mobilitat, xarxes socials, Internet of Things, etc.

Temi 17. Diferències i abast de la ciberseguridad i la seguretat de la informació. Planes Nacionals de Ciberseguridad.

Tema 18. Recomanacions i bones pràctiques en la gestió de la seguretat en l'àmbit empresarial i particular.

Metodologia

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.

Activitats formatives

Títol	Hores	ECTS	Resultats d'aprenentatge
Tipus: Dirigides			
CLASSE TEÒRICA	44	1,76	1, 2, 6, 8
Tipus: Supervisades			
TUTORIES DE SUPORT PEL SEGUIMENT DE LES UNITATS DIDÀCTIQUES	2	0,08	1, 2, 8
Tipus: Autònomes			
ESTUDI I RESOLUCIÓ DELS ESCENARIS DE RISC	47	1,88	1, 2, 8
PREPARACIÓ DE LES PRÀCTIQUES	47	1,88	1, 2, 5, 6, 8

Avaluació

A) 2 EXÀMEN FINAL (50% DE LA NOTA FINAL)

Els alumnes, de forma individual, realitzaran un examen final, aquest es farà en la data oficial del calendari establert per l'EPSI. En aquest exàmen s'haurà d'obtenir una qualificació mínima d'un 40%. Aquest examen consistirà 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).

Els exàmens seran recuperables a la setmana dedicada a tal efecte al final del semestre. Els alumnes No Presentats no seran avaluats, a excepció dels que aportin una justificació (document escrit).

B) TREBALLS PRÀCTICS (20% 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 40% i haurà de ser lliurat en la data proposada segons el cronograma. La mitjana dels treballs pràctics suposarà el 20% de la nota del curs.

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).

C) PRESENTACIÓ D'ESCENARIS DE RISC RELACIONAT AMB EL SISTEMA D'INFORMACIÓ (20% DE LA NOTA FINAL)

Durant el semestre s'aniran proposant problemes a classe que s'hauran de resoldre individualment i presentar la solució per escrit. El lliurament dels informes corresponents suposarà la seva avaluació i la mitjana d'ambdues suposarà el 10% de la nota final. Aquestes tasques poden ser també reflexions individuals, exercicis, presentacions de casos, etc. Atesa la seva naturalesa, no són susceptibles de recuperació al final del semestre

D) PARTICIPACIÓ ALS FÒRUMS I A CLASSE (10% DE LA NOTA FINAL)

Durant el semestre s'aniran proposant temes de debat/opinió tant a classe com als fòrums previstos al web de l'assignatura (MOODLE). L'objectiu és que els estudiants debatin entre ells de manera pública i moderada amb el professors sobre aquestes qüestions. La avaluació suposarà el 10% de la nota final. Atesa la seva naturalesa, no són susceptibles de recuperació al final del semestre.

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 qualificació final d'aquesta assignatura serà 0".

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

Activitats d'avaluació

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
EXAMEN FINAL	40%	2	0,08	1, 2, 5, 6, 7, 8, 9, 10, 11
PARTICIPACIÓ A FÒRUM I A CLASSE	10%	2	0,08	1, 2, 5, 6, 7, 8, 9, 10, 11
PRESENTACIÓ D'ESCENARIS DE RISC RELACIONATS AMB SISTEMES D'INFORMACIÓ	20%	3	0,12	1, 2, 3, 5, 6, 11
TREBALLS PRÀCTICS	30%	3	0,12	1, 3, 4, 5, 6, 7, 9, 10, 11

Bibliografia

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.

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.