IRAKASKUNTZA-GIDA 2023/24

Ikastegia 363 - Bilboko Ingeniaritza Eskola **Zikl.** Zehaztugabea

Plana GIIGSI30 - Kudeaketaren eta Informazio Sistemen Informatikaren Ingeniaritza **Ikastaroa** 3. maila

IRAKASGAIA

26025 - Informazio Sistemen Segurtasuna Kudeatzeko Sistemak **ECTS kredituak:** 6

IRAKASGAIAREN AZALPENA ETA TESTUINGURUA ZEHAZTEA

Segurtasun informatikoa, informazio sistema seguru eta fidagarri bat lortzeko erabiltzen diren arauak, prozedurak, metodoak eta teknikak aztertzen dituen ezagutza arloa da.
Informazio Sistemetan erakundeen informazioarekin - publikoa eta pribatua - lan egiten da, berau aztertuz (ordenagailuen eta sistema informatikoen bidez), gordez (datuak gordetzeko baliabideak erabiliz), moldatuz, bihurtuz eta igorriz (sare informatikoak erabiliz). Sistema hauek hainbat jatorri dituzten mehatxuak eta arriskuak pairatzen dituzte. Arrisku fisikoak izan daitezke, ezbehar edo hondamendi naturalen eraginez, edo ez-baimendutako atzipen baten ondorioz; arrisku logikoak, aldiz, eraso informatiko baten ondorioz suertatzen direnak dira, birusak, zerbitzu ukapenerako erasak (DoS), etab.

Irakasgai honetan informazio sistemek pairatzen dituzten arrisku ezberdinak aztertuko dira, berauek sakonean ezagutu, kudeatu eta bere eragina txikiagotu ahal izateko.

GAITASUNAK / IRAKASGAIA IKASTEAREN EMAITZAK

Informazioaren eta komunikazioen teknologia eta enpresa prozesuetako soluzioak integratzeko gaitasuna erakundeen informazio premiak asetzeko, haien helburuak modu eraginkor eta efizientean betetzeko aukera emateko, eta horrela lehiatzeko abantailak eskaintzeko.

Antolakuntza baten informazio eta komunikazio sistemen eskakizunak zehazteko gaitasuna, kontuan izanik segurtasunaren eta indarrean diren araudiaren eta legeriaren betetze mailaren alderdiak.

Informazio eta komunikazio sistemak zehazten, diseinatzen, inplementatzen eta mantentzen modu aktiboan parte hartzeko gaitasuna.

Arriskuen ebaluazioaren printzipioak ulertzeko eta aplikatzeko gaitasuna, eta horiek zuzen aplikatzea jarduketa planak prestatzean eta gauzatzean.

CONTENIDOS TEÓRICO-PRÁCTICOS

1.- Sarrera
Gai honetan, erakunde batek aurre egin behar dien segurtasun-arriskuak aztertuko dira, eta arrisku horiek izan dezaketen eragina ebaluatzeko eta balioesteko modua aztertuko da.

I BLOKEA - Zifratzea

2.- Zifratzearen hastapenak
Informazioa zifratzearen helburu nagusia informazioa babestea da. Enkriptatzeari buruzko oinarrizko ideiak landuko dira, baita haien historia ere.

3.- Zifratze simetrikoa
Algoritmo ohikoenak eta horien aplikazioak.

4.- Zifratze asimetrikoa
Algoritmo ohikoenak eta horien aplikazioak.

5.- Komunikazio seguruak
Zifratzea aplikatzea komunikazio seguruetan: ziurtagiriak, SSH konexioak, etab.

6.- Bitcoin
Bitcoin zifratzearen aplikazio interesgarria da, baita beste kontzeptu batzuena ere, hala nola datu-base hedatuak. Bitcoin eta bere Blockchain-ari buruzko oinarrizko sarrera teknikoa eskainiko da.

II BLOKEA - Sistemak

7.- Backup-ak
Segurtasun-kopiek informazioaren osotasuna eta erabilgarritasuna ziurtatzen dute, jatorrizko informazioa galduz gero. Bertan, babeskopiak egiteko moduak eta sistemak aztertuko dira.

8.- Segurtasun fisikoa

Ez du ezertarako balio era guztietako arrisku logikoen aurka babestutako informazio-sisde bat edukitzeak, edonork eskura badezake fisikoki eta manipulatu. Informazio-sistemen eta datuen segurtasun fisikoa ezinbestekoa da.

9.- Sareetako segurtasuna
Informazioa gutxitan egoten da isolatuta makina batean, sarerik gabe. Komunikazio-sareak babesteko segurtasun-neurriak hartzea ezinbesteko urratsa da informazioa ziurtatzeko.

10.- Segurtasuna web sistemetan
Gero eta datu gehiago daude webera konektatutako sistemetan, eta planetako edozein puntutatik eskura daitezke. Segurtasunaren alderdi asko hartu behar dira kontuan sistema horiek ezartzean, nahi ez diren sarbideak saihesteko.

III BLOKEA - Gizartea

11.- Giza faktorea
Horretan zehar ingeniaritza soziala eta pertsonen informazioa babesteko moduak aztertuko dira, askotan informazioa babesteko katearen katebegirik ahulena baitira.

12.- Malwarea
Zer da kode maltzurra (malware)? Nola antzeman eta saihestu daiteke? Bertan, software maltzurretik eta haren ondorioetatik babesteko modu nagusiak ikusiko dira. Horretarako, malware motak, horietako bakoitzaren ezaugarriak eta informazio-sistemetan dituen ondorioak aztertuko dira.

13.- Legeria
Segurtasun informatikoaren arloan, ezinbestekoa da arlo horretan indarrean dagoen legeria ezagutzea. Bertan, indarrean dauden lege garrantzitsuenak aztertuko dira, baita informazio-sistemetan dituzten ondorioak ere.

14.- Informatika forentsea
Bertan, ekipo informatiko baten autopsiarako prozedurak aztertuko dira.

15.- Hitzaldiak (definitzeke)
Bitcoin, Pentest eta abarri buruzko hitzaldiak industriako adituen eskutik

METODOLOGIA

Eskola magistralak (M) segurtasun informatikoarekin lotutako kontzeptu teorikoak azaltzeko erabiliko dira batipat. Eskola horiek ikasleek planteatzen dituzten zalantzak argitzeko erabiliko dira baita ere. Dena den, zenbait eskola magistraletan eta ordenagailuekin egindako praktiketan (GO) ariketa praktikoen bidez teorian eman diren kontzeptuetan sakonduko da. Ariketa hauek banaka eta baita talde txikietan ere egingo dira, metodologia aktiboetan oinarrituta (Kasuaren Metodoa). Horrelako ariketetan, ikasleek enuntziatu bat jasoko dute non ebatzi nahi den kasua planteatuko zaien. Hiruzpalau taldekidez osatutako taldetan ebatzi beharko dituzte. Ikasgelan ordenagailu eramangarria erabiltzea gomendatzen da, bereziki GNU/Linux sistema eragile batekin.

Ordenagailuekin egindako praktiketan ere, Arazoetan Oinarritutako Irakaskuntza aplikatuko da. Bertan, ikasleek beste ariketa mota batzuk jasoko dituzte, bai banaka edo bai taldeka ebazteko modukoak.

IRAKASKUNTZA MOTAK

Eskola mota	M	S	GA	GL	GO	GCL	TA	TI	GCA
Ikasgelako eskola-orduak	45				15				
Horas de Actividad No Presencial del Alumno/a	67,5				22,5				

Legenda: M: Magistrala · S: Mintegia · GA: Gelako p. · GL: Laborategiko p. · GO: Ordenagailuko p. · GCL: P. klinikoak · TA: Tailerra · TI: Tailer Ind. · GCA: Landa p.

EBALUAZIO-SISTEMAK

- Ebaluazio jarraituaren sistema
- Azken ebaluazioaren sistema

KALIFIKAZIOKO TRESNAK ETA EHUNEKOAK

- Garatu beharreko proba idatzia % 10
- Test motatako proba % 20
- Praktikak (ariketak, kasuak edo buruketak) % 30
- Talde lanak (arazoen ebazpenak, proiektuen diseinuak) % 40

OHIKO DEIALDIA: ORIENTAZIOAK ETA UKO EGITEA

Ohiko deialdian, besterik adierazi ezean, ikasleek ebaluaketa jarraitua egingo dutela ulertzen da. Ikasle batek ebaluaketa finala egin nahiko balu, emailez jakinarazi beharko du 3. partziala baino 2 aste lehenago.
Ebaluaketa jarraituan, ebaluazioa 3 zatitan banatuko da, bakoitzak azterketa teoriko eta praktiko bat izango duelarik. Azterketa horien kalifikazioaren batazbestekoa kalkulatuko da zati horren nota zehazteko. Azterketa bakoitzaren edukia eskoletan landutakoari buruz eta zati horri dagokizon laborategiko edukian oinarrituko da.
Horrez gain, lauhilekoan zehar zenbait lan egingo dira, irakasgaiaren azken kalifikazioan eragina izango dutena.
Ebaluazketa jarraituari uko egin eta azterketa finala egitera aurkeztu nahi diren ikasleek, bi azterketa izango dituzte: bata teorikoa eta beste bat praktikoa, irakasgaiaren gaitegi osoa kontutan izango dutena. Irakasgaiaren azken nota bi azterketa horien batezbesteko notarekin kalkulatuko da.

LANEN EBALUAKETA:
Lan baten edozein zatitan plagio bat egon dela antzematen bada, lan horren kalifikazioa 0 puntokoa izango da.
Lan guztiek zuzen eta txukun idatzi behar dira. Beraz, lan batean 3 akats ortografiko larri edo gehiago aurkituz gero, lan horren zuzenketa bertan behera utziko da eta bere nota ordura arte kalifikatutako zatiaren nota izango da.

KOPIA KASUAK:
Bi talde ezberdinen artean kopia bat egon dela antzematen bada, bi lan horiek 0 batekin kalifikatuko dira.
Azterketa kasuetan, ikasleen ebaluazioari dagokion eta indarrean dagoen Ikasleen Ebaluaziorako Arautegiko 11.3 artikulua aplikatuko da.

DEIALDIARI UKO EGIN:
Ebaluaketa jarraituari atxikitako ikasle batek deialdiari uko egin eta "Ez aurkeztua" kalifikazioa lortu nahiko balu, 3.partzialera ez aurkeztea nahiko du. Ebaluaketa finalari atxikitako ikasleen kasuan, nahikoa izango da azterketa egunean ez aurkeztearekin.

EZOHIKO DEIALDIA: ORIENTAZIOAK ETA UKO EGITEA

Ohiko deialdian gainditzen ez duenak bigarren deialdiko azterketa egin beharko du (bi zatitan banatuta, alde praktiko eta teorikoa), irakasgaiko gaitegi osoan oinarrituta.

DEIALDIARI UKO EGIN:
Ikasle batek azterketa teorikoa edo praktikoa ez badu egiten, "Ez aurkeztua" kalifikazioa jarriko zaio.

NAHITAEZ ERABILI BEHARREKO MATERIALAK

- Irakasgaiaren apunteak (Teoria eta Praktika)
- Egelaplataforman "Informazio Sistemen Segurtasuna Kudeatzeko Sistemak" irakasgaian argitaratutako materiala.

BIBLIOGRAFÍA

Oinarrizko bibliografia

How Cybersecurity Really Works: A Hands-On Guide for Total Beginners, Sam Grubb, No Starch Press, 2021
Web Security for Developers: Real Threats, Practical Defense Illustrated Edition, Malcolm McDonald, 2020
Ruiz Manzanos,A., Software kaltegarria, Elhuyar, 2008

Gehiago sakontzeko bibliografia

Serious Cryptography: A Practical Introduction to Modern Encryption; Jean-Philippe Aumasson, No Starch Press, 2017
The governance of privacy. C.J. Bennett y C.D. Raab, Massachussets Institute of Technology Press 2006
Beyond Fear. B. Schneier, Beyond Fear: Thinking Sensibly About Security in an Uncertain World; 2006; Springer
Vigilancia permanente. Edward Snowden. Planeta, 2019
Social Engineering: The Science of Human Hacking. Christopher Hadnagy, Wiley 2018
El pequeño libro rojo del activista en la red. Marta Peirano, Roca 2015
Grokking Bitcoin. Kalle Rosenbaum, Manning 2019

Aldizkariak

Auditoría + Seguridad informática
IEEE Security & Privacy

Interneteko helbide interesgarriak

Basque Cybersecurity Centre - BCSC - Zibersegurtasun Euskal Zentroa
https://www.basquecybersecurity.eus/eu/

Bruce Schneier-en segurtasunari buruzko blog-a (2022/05/12 atzitua)
https://www.schneier.com/

Agencia Española de Protección de Datos (2022/05/12 atzitua)
http://www.agpd.es

Red temática de criptografía y seguridad de la información (2022/05/12 atzitua)
http://www.criptored.upm.es

Equipo de seguridad de rediris (2022/05/12 atzitua)
http://www.rediris.es/cert/

Instituto nacional de ciberseguridad (2022/05/12 atzitua)
https://www.incibe.es/

Blog sobre seguridad (2022/05/12 atzitua)
https://krebsonsecurity.com

Malware scanner (2022/05/12 atzitua)
https://www.virustotal.com

OHARRAK

Plagioa dela eta lan batean 0 puntu ateraz gero, irakasgai osoa ez-gainditua notarekin kalifikatuko da.