I. ERANSKINA, 2021EKO XXXAREN XXX(E)KO XXX/XXXX DEKRETUARENA.

INFORMAZIO-TEKNOLOGIEN INGURUNEETAN ZIBERSEGURTASUNEKO ESPEZIALIZAZIO-IKASTAROA

1. Identifikazioa.

Izena: Zibersegurtasuna informazio-teknologien inguruneetan.
Maila: Goi-mailako Lanbide Heziketa.
Iraupena: 990 ordu.
Lanbide-arloa: Informatika eta Komunikazioa (Lanbide Heziketako irakaskuntzak sailkatzeko baino ez).
Jakintza-adarra: Ingeniaritza eta Arkitektura.
ECTS kredituak: 43.
Irakaskuntzaren Nazioarteko Sailkapen Normalizatuko erreferentea: P-5.5.4.

2. Sarbidea espezializazio-ikastarora.

Titulu hauetakoren bat edo ikasketetarako baliokidea den titulua edukitzea:
- Sareko informatika-sistemen administrazioko goi-mailako teknikaria, irailaren 21eko 244/2010 Dekretuak ezarritakoa; dekretu horren bidez, Sareko informatika-sistemen administrazioko goi-mailako teknikariaren tituluari dagokion curriculuma ezartzen da .
- Plataforma anitzeko aplikazioak garatzeko goi-mailako teknikaria, urriaren 7ko 207/2011 Dekretuak ezarritakoa; dekretu horren bidez, Plataforma anitzeko aplikazioak garatzeko goi-mailako teknikariaren tituluari dagokion curriculuma ezartzen da) .
- Web aplikazioen garapeneko goi-mailako teknikaria, azaroaren 29ko 245/2011 Dekretuak ezarritakoa; dekretu horren bidez, web aplikazioen garapeneko goi-mailako teknikariaren tituluari dagokion curriculuma ezartzen duena) .
- Telekomunikazio- eta informatika-sistemetako goi-mailako teknikaria, uztailaren 3ko 118/2012 Dekretuak ezarritakoa; dekretu horren bidez, Telekomunikazio- eta informatika-sistemetako goi-mailako teknikariaren tituluari dagokion curriculuma ezartzen da.
- Mantentze-lan elektronikoetako goi-mailako teknikaria, apirilaren 22ko 341/2013 Dekretuak ezarritakoa; dekretu horren bidez, Mantentze-lan elektronikoetako goi-mailako teknikariaren tituluari dagokion curriculuma ezartzen da.

3. Lanbide-profila.

3.1. Konpetentzia orokorra:

Espezializazio-ikastaro honen konpetentzia orokorra da informazio-sistemetan segurtasun-estrategiak definitzea eta ezartzea, eta, horretarako, zibersegurtasunaren diagnostikoak egin, ahuleziak identifikatu eta horiek arintzeko beharrezko neurriak ezartzea indarrean dagoen araudia eta sektoreko estandarrak aplikatuz, kalitate, laneko arriskuen prebentzio eta ingurumen-babeseko protokoloak betez.

3.2. Lanbide-ingurunea:

Profesional horrek informazio-sistemak eta komunikazio-sareak babesteko mekanismoak eta

neurriak ezarri behar diren sektoreetako erakundeetan jardungo du.

Hauek dira zeregin eta lanpostu aipagarrienak:
– Zibersegurtasuneko aditua.
– Zibersegurtasuneko auditorea.
– Zibersegurtasuneko aholkularia.
– Hacker etikoa.

3.3. Konpetentzia profesionalak, pertsonalak eta sozialak:

a) Erakundean zibersegurtasunaren arloko prebentzio eta kontzientziazio-planak egitea eta ezartzea, indarreko araudia aplikatuta.

b) Zibersegurtasun-gorabeherak detektatzea eta ikertzea, dokumentatzea eta erakundearen segurtasun-planetan sartzea.

c) Segurtasun-planak diseinatzea, sistemak eta sareak gotortzeko jardunbide onenak kontuan hartuta.

d) Sarbidea kontrolatzeko eta autentifikatzeko sistemak konfiguratzea sistema informatikoetan, segurtasun-baldintzak beteta eta erasoekiko arrisku-aukerak minimizatuta.

e) Sareko sistema informatikoak diseinatzea eta administratzea, eta ezarritako segurtasun-politikak aplikatzea, eskatutako funtzionaltasuna bermatuta, kontrolatutako arrisku-mailarekin.

f) Aplikazioek eta eraso-bektore ohikoenek eskatzen duten segurtasun-maila aztertzea, zibersegurtasun-gorabeherak saihestuta.

g) Softwarea hedatzeko sistema seguruak ezartzea, software-eragiketaren garatzaileen eta arduradunen arteko koordinazio egokiarekin.

h) Auzitegi-analisi informatikoak egitea, lotutako informazio garrantzitsua aztertuta eta erregistratuta.

i) Industriako sistemetan, sareetan, aplikazioetan eta kontrol-sistemetan ahuleziak hautematea, eta lotutako arriskuak ebaluatzea.

j) IT segurtasunaren arloa eta erakundearen automatizazioaren arloa koordinatzea, ingurune industrialen segurtasuna hobetzeko neurriak emanda.

k) Automatizazioko eta kontroleko oinarrizko ingurune seguruak ezartzea, oinarrizko suebaki industrialak konfiguratuta eta hedatuta.

l) Zibersegurtasunaren eta datu pertsonalen babesaren arloko araudia betetzeko prozedurak definitzea eta aplikatzea, bai barruan, bai hirugarrenei dagokienez.

m) Dokumentazio teknikoa eta administratiboa egitea, indarrean dagoen legeria eta ezarritako baldintzak beteta.

n) Laneko egoera berrietara egokitzea, egunean izanda lanbide-ingurunearen gaineko ezagutza zientifikoak, teknikoak eta teknologikoak, eta prestakuntza eta dauden baliabideak bizialdi osoko ikaskuntzan kudeatuta.

ñ) Egoerak, arazoak eta gorabeherak konpontzea, ekimenez eta autonomiaz dagokion eskumen-eremuan, eta sormenez, berrikuntzaz eta hobetzeko gogoaz norberaren eta taldekideen zereginetan.

o) Ingurune seguruak sortzea bere lana zein lantaldearena garatzeko, laneko arriskuen prebentzio eta ingurumen-babeseko prozedurak berrikusiz eta aplikatuz, araudian ezarritakoa eta erakundearen helburuetan adierazitakoa beteta.

p) Produkzioko edo zerbitzugintzako prozesuetan bildutako lanbide-jardueretan, kalitatea kudeatzeko prozedurak, irisgarritasun unibertsalekoak eta «denontzako diseinukoak» berrikustea eta aplikatzea.

4. Espezializazio-ikastaroko irakaskuntza

4.1. Helburu orokorrak:

a) Erakundearen printzipioak eta zibersegurtasunaren arloko babes-araudia identifikatzea, eta prebentzio- eta kontzientziazio-plana egiteko lanpostuan hartu behar diren ekintzak planifikatzea.

b) Erakundearen prebentzio- eta kontzientziazio-plana betetzen dela ikuskatzea, eta sor daitezkeen ekintza zuzentzaileak definitzea, erakundearen segurtasun-planean sartzeko.

c) Zibersegurtasun-gorabeherak detektatzea, eta horiek monitorizatzeko eta identifikatzeko beharrezko kontrolak, tresnak eta mekanismoak ezartzea.

d) Zibersegurtasun-gorabeherak aztertzea eta horiei erantzuna ematea, eta horiek arintzeko, ezabatzeko, eusteko edo berreskuratzeko behar diren neurriak identifikatu eta aplikatzea.

e) Industriako kontrol-sistemen ahulezia eta mehatxu espezifikoak identifikatzea eta antolaketa-neurriak proposatzea ingurune industrialetan.

f) Arriskuen analisiak egitea, aktiboak, mehatxuak, ahuleziak eta segurtasun-neurriak identifikatzeko.

g) Segurtasun-neurri teknikoen planak diseinatzea eta ezartzea, identifikatutako arriskuetatik abiatuta, eskatutako segurtasun-maila bermatzeko.

h) Sarbideak kontrolatzeko, pertsonak autentifikatzeko eta egiaztagutunak administratzeko sistemak konfiguratzea, datuen pribatutasuna babesteko.

i) Sistema informatikoen segurtasuna konfiguratzea, erasoekiko esposizio-aukerak minimizatzeko.

j) Informazioaren teknologien (IT) eta eragiketa-teknologien (OT) arteko integrazioa diseinatzea, OT gailuak bermatuta.

k) Sareko gailuak konfiguratzea, segurtasun-betekizunak betetzeko.

l) Sareko sistema informatikoen segurtasuna administratzea eta ezarritako segurtasun-politikak aplikatzea, behar den funtzionaltasuna bermatzeko kontrolatutako sarearen arrisku-mailarekin.

m) Aplikazioek eskatzen dituzten egiaztapen-estandarrak aplikatzea, segurtasun-gorabeherak saihesteko.

n) Softwarea hedatzeko planak automatizatzea, bertsioen, rolen, baimenen eta bestelakoen kontrolari buruzko betekizunak errespetatuta, hedapen segurua lortzeko.

ñ) Auzitegi-ikerketako teknikak aplikatzea, besteak beste, informazio ez-hegakorra, ordenagailu pertsonalak, gailu mugikorrak, Cloud eta IoT (Gauzen Internet) sistemak biltegiratzeko eremuetan, auzitegi-analisiak egiteko.

o) Auzitegi-txostenak aztertzea eta ikerketaren emaitzak identifikatzea, ondorioak ateratzeko eta txostenak egiteko.

p) Barneko eta kanpoko hacking etikoko teknikak konbinatzea, lotutako arriskuak ezabatzeko eta arintzeko aukera ematen duten ahuleziak detektatzeko.

q) Arauen aplikazioaren irismena identifikatzea erakundearen barruan nahiz hirugarrenei dagokienez, alderdi guztien eginkizunak eta erantzukizunak definitzeko.

r) Prozedurak berrikusi eta eguneratzea, arau eta estandar eguneratuen arabera, zibersegurtasunaren eta datu pertsonalen babesaren arloko araudia behar bezala betetzeko.

s) Bulegotikako eta ordenagailuz lagundutako diseinuko tresnak erabilita, informazio-eskuliburuak egitea, dokumentazio teknikoa eta administratiboa lantzeko.

t) Sektoreko bilakaera zientifikoarekin, teknologikoarekin eta antolamendukoarekin lotutako ikaskuntza-baliabideak eta -aukerak aztertzea eta erabiltzea, baita informazioaren eta komunikazioaren teknologiak ere, eguneratzeko gogoari eusteko eta laneko egoera berrietara eta egoera pertsonal berrietara egokitzeko.

u) Sormena eta berrikuntza-gogoa garatzea, lanaren eta norberaren bizitzaren prozesuetan eta antolamenduan agertzen diren erronkei erantzuteko.

v) Laneko arriskuen prebentzioko eta ingurumen-babeseko egoerak ebaluatzea, eta norberaren eta taldearen prebentziorako neurriak proposatu eta aplikatzea, lan-prozesuetan aplikatzekoa den araudiaren arabera, ingurune seguruak bermatzeko.

w) Irisgarritasun unibertsalari eta «guztiontzako diseinuari» erantzuteko beharrezkoak diren lanbide-ekintzak identifikatzea eta proposatzea.

x) Kalitate-parametroak identifikatzea eta aplikatzea ikaskuntza-prozesuan egindako lanetan eta jardueretan, ebaluazioaren eta kalitatearen kultura baloratzeko eta kalitate-prozedurak gainbegiratzeko eta hobetzeko gai izateko.

4.2. Lanbide-moduluak.

KODEA	LANBIDE-MODULUA	ORDU-ESLEIPENA
5021	Zibersegurtasun-gorabeherak.	84
5022	Sareak eta sistemak gotortzea.	192
5023	Ekoizpen seguruan jartzea.	120
5024	Auzitegi-analisi informatikoa.	96
5025	Hacking etikoa.	120
5026	Zibersegurtasunaren arloko araudia.	48
E300	Oinarrizko funtsak.	60
E301	Prestakuntza praktiko duala enpresetan.	270
GUZTIRA		990

4.3. Lanbide moduluak: Ikaskuntzaren emaitzak, ebaluazio-irizpideak eta edukiak.

1. lanbide-modulua: Zibersegurtasun-gorabeherak.

Kodea: 5021.
Iraupena: 84 ordu.
ECTS kredituak: 9.

Ikaskuntzaren emaitzak, ebaluazio-irizpideak eta edukiak.

RA1. Zibersegurtasun arloan prebentzio- eta kontzientziazio-planak garatzen ditu eta arauak eta babes-neurriak ezartzen ditu.

Ebaluazio-irizpideak:

a) Zibersegurtasunaren arloan erakundeak dituen printzipio orokorrak definitu ditu, zeinak erakundearen zuzendaritzak ezagutu eta babestu behar baititu.

b) Lanpostuaren babes-araua ezarri du.

c) Zibersegurtasunaren arloko kontzientziazio-plana definitu du enplegatuentzat.

d) Enplegatuentzako kontzientziazio-ekintzak gauzatzeko beharrezkoa den materiala egin du.

e) Ikuskaritza egin du erakundearen prebentzio- eta kontzientziazio-planaren betetze-maila egiaztatzeko.

Edukiak: Zibersegurtasunaren arloan prebentzio- eta kontzientziazio-planak garatzea.

- Zibersegurtasunaren printzipio nagusiak.
- Lanpostuaren babes-araudia.
- Zibersegurtasunaren arloko prestakuntza- eta kontzientziazio-plana.
- Prestakuntza- eta kontzientziazio-materialak.
- Prebentzioaren arloan betetze-maila egiaztatzeko barneko ikuskaritzak.

RA2. Zibersegurtasun-gorabeherak aztertzen ditu, eta, horretarako, segurtasunaren arloko detekzio- eta alerta-tresna eta mekanismoak erabiltzen ditu.

Ebaluazio-irizpideak:

a) Erakundeari eragin ahal dioten zibersegurtasun-gorabeheren taxonomia sailkatu eta definitu du.

b) Gorabeherak monitorizatzeko, identifikatzeko, detektatzeko eta horien alerta emateko kontrolak, tresnak eta mekanismoak ezarri ditu.

c) Segurtasun fisikoko gorabeherak detektatu eta identifikatzeko kontrolak eta mekanismoak ezarri ditu.

d) Gorabeherak monitorizatzeko, identifikatzeko, detektatzeko eta horien alerta emateko kontrolak, tresnak eta mekanismoak ezarri ditu, iturri irekien ikerketaren bidez (OSINT: Open Source Intelligence).

e) Erakundean detektatutako gorabeherak sailkatu, baloratu, dokumentatu eta horien jarraipena egin du.

Edukiak: - Zibersegurtasun-gorabeheren auditoria.

- Zibersegurtasun-gorabeheren taxonomia.
- Gorabeherak monitorizatzeko, identifikatzeko, detektatzeko eta horien alerta emateko tresnak eta mekanismoak: motak eta iturriak.
- Segurtasun fisikoko gorabeherak detektatu eta identifikatzeko kontrolak, tresnak eta mekanismoak.
- Gorabeherak monitorizatzeko, identifikatzeko, detektatzeko eta horien alerta emateko kontrolak, tresnak eta mekanismoak, iturri irekien ikerketaren bidez (OSINT).
- Zibersegurtasun-gorabeherak sailkatzea, balorazioa egitea, dokumentatzea eta hasierako jarraipena egitea.

RA3. Zibersegurtasun-gorabeherak ikertzen ditu, eta, horretarako, inplikatutako arriskuak aztertu eta hartu beharreko neurriak definitzen ditu.

Ebaluazio-irizpideak:

a) Ebidentziak bildu eta aztertzeko prozesuaren faseak aztertu ditu.
b) Erakundeari eragiten dioten zibersegurtasun-gorabeheren ebidentziak bildu eta jaso ditu modu seguruan.
c) Ebidentzien analisia egin du.
d) Zibersegurtasun-gorabeheren ikerketa egin du.
e) Gorabeherei buruzko informazioa trukatu du horri buruzko ekarpenak egin ditzaketen hornitzaile eta erakunde eskudunekin.
f) Abian jarri ditu gorabeherei eusteko hasierako neurriak, eragindako kalteak murrizteko.

Edukiak: Zibersegurtasun-gorabeherak ikertzea.

- Prozesuaren faseak.
- Ebidentziak biltzea.
- Ebidentziak aztertzea.
- Gorabeherak ikertzea.
- Gorabeherei buruzko informazioa trukatzea hornitzaile eta erakunde eskudunekin.
- Gorabeherei eusteko neurriak.

RA4. Sare eta sistemetan zibersegurtasun-neurriak ezartzen ditu, detektatutako gorabeherei erantzuna emanda eta babes-teknika egokiak erabilita.

Ebaluazio-irizpideak:

a) Jardun-prozedura xehatu batzuk garatu ditu, zibersegurtasun-gorabehera ohikoenei erantzuteko, arintzeko, desagerrarazteko edo geldiarazteko.
b) Gorabeheren aurreko erantzun ziber-erresilienteak prestatu ditu, batetik, erakundearen zerbitzuak ematen jarraitzeko eta, bestetik, identifikatzeko, detektatzeko, prebenitzeko, eusteko berreskuratzeko eta hirugarrenekin lankidetzan aritzeko gaitasunak sendotzen jarraitzeko.
c) Erabakiak hartzeko eta gorabeheren barneko zein kanpoko eskala-faktoreen fluxu egokia ezarri du.
d) Gorabehera batek kaltetutako zerbitzuak berrabiatzeko zereginak gauzatu ditu, zerbitzu horiek normaltasunez ematen direla egiaztatu arte.
e) Egindako ekintzak eta “ikasitako irakasgaien” erregistroa eramatea ahalbidetzen duten ondorioak dokumentatu ditu.
f) Gorabeheraren jarraipen egokia egin du, antzeko egoerarik berriz gerta ez dadin.

Edukiak: Zibersegurtasun-neurriak ezartzea.

− Jardun-prozedura xehatuak garatzea, hainbat motatako gorabeherei erantzuteko, arintzeko, desagerrarazteko edo geldiarazteko.
− Zibererresilientziako ahalmenak ezartzea.
- Erabakiak hartzeko eta barneko zein kanpoko eskala-faktoreen fluxuak ezartzea.
- Gorabeherek kaltetutako zerbitzuak berrabiatzeko zereginak.
- Dokumentazioa.
– Gorabeheren jarraipena egitea, antzeko egoerarik berriz gerta ez dadin.

RA5. Zibersegurtasun-gorabeherak detektatu eta dokumentatzen ditu, ezarritako jarduketa-prozedurei jarraikiz.

Ebaluazio-irizpideak:

a) Zibersegurtasun-gorabeherak garaiz jakinarazteko jarduketa-prozedura zehatza egin du.
b) Gorabehera modu egokian jakinarazi zaie erakundearen barnean erabakiak hartzeko ardura duten langileei.
c) Gorabehera modu egokian jakinarazi zaie zibersegurtasun-gorabeheren kudeaketa arloko agintari eskudunei, hala behar izan denean.
d) Gorabehera formalki jakinarazi zaie kaltetuei,barneko langileei, bezeroei, hornitzaileei eta abarrei, hala behar izan denean.
e) Gorabehera jakinarazi zaie komunikabideei, hala behar izan denean.

Edukiak: Zibersegurtasun-gorabeherak detektatu eta dokumentatzea.

- Gorabeherak jakinarazteko jarduketa-prozedurak egitea.
- Gorabeherak erakundearen barnean jakinaraztea.
- Gorabeherak dagokionari jakinaraztea.

2. lanbide-modulua: Sareak eta sistemak gotortzea.

Kodea: 5022.
Iraupena: 192 ordu.
ECTS kredituak: 10.

Ikaskuntzaren emaitzak, ebaluazio-irizpideak eta edukiak.

RA1: Bideratzaile baten oinarrizko funtzioak administratzen ditu, eta hura sarean integratzeko konfigurazio-aukerak ezartzen ditu.

Ebaluazio-irizpideak:

a) Hainbat metodo erabili ditu bideratzailea konfiguratzeko moduan sartzeko.
b) Bide estatikoak konfiguratu ditu.
c) Bideratzailearen konfigurazioa gordetzen duten fitxategiak identifikatu ditu eta dagozkien komandoen bidez kudeatu ditu.
d) Bideratzailearen sistema eragileak eskaintzen dituen komandoak erabili ditu, izan litezkeen gorabeheren jarraipena egitea ahalbidetzen dutenak.
e) Trafikoa iragazteko bideratzailearen ahalmenak deskribatu ditu.
f) Sarbide-kontroleko zerrendak (ACL) kudeatzeko komandoak erabili ditu.
g) Sareko helbideak itzultzeko sistemak konfiguratu ditu.
h) Ataken birbidalketa konfiguratu du.

Edukiak: Bideratzailea oinarrizko mailan konfiguratzea eta administratzea.

- Bideratzailera sartzeko hainbat metodo.

- Bideratzailea konfiguratzeko eta administratzeko komandoak.
- Bide estatikoak konfiguratzea.
- Komandoak erabiltzea gorabeheren jarraipena egiteko eta bideratzailearen egoera monitorizatzeko.
- Bideratzailearen trafiko-iragazkiak konfiguratzea.
- Sarbide-kontroleko zerrendak (ACL) kudeatzea.
- Sareko helbideak itzultzea: NAT eta PAT.
- Atakak birbidaltzea.

RA2: Sare lokal birtualak konfiguratzen ditu eta horien aplikazio-eremua identifikatzen du.

Ebaluazio-irizpideak:

a) Sare lokal birtualak (VLAN) ezarri ditu.
b) Lotura nagusiak konfiguratu ditu.
c) Bideratzaile edo switch multilayer bat erabili du hainbat sare lokal birtual elkarrekin konektatzeko.
d) Administrazio zentralizatuko protokoloen arabera lan egiteko konfiguratu ditu kommutadoreak.

Edukiak: Sare birtualak

- Sare lokal birtualak (VLAN) ezartzea.
- Sare lokal birtualetan gorabeherak diagnostikatzea.
- Gailuen arteko lotura nagusiak konfiguratzea.
- Hainbat sare lokal birtual elkarrekin konektatzeko bideratzailea edo switch multilayer konfiguratzea.
- Sare lokal birtualen protokoloak.

RA3. Segurtasun-planak diseinatzen ditu, sistemak eta sareak gotortzeko jardunbide onenak kontuan hartuta.

Ebaluazio-irizpideak:

a) Erakundearen aktiboak, mehatxuak eta ahuleziak identifikatu ditu.
b) Egungo segurtasun-neurriak ebaluatu ditu.
c) Erakundearen egungo egoeraren zibersegurtasun-arriskuen azterketa egin du.
d) Erakundean ezarri beharreko segurtasun-neurri teknikoak lehenetsi ditu, Ekonomia Zirkularraren printzipioak ere kontuan hartuta.
e) Erakundean ezarri beharreko segurtasun-neurri teknikoen plan bat diseinatu eta egin du, erakundearen arriskuen arabera, segurtasun-maila egokia bermatzeko.
f) Jardunbiderik onenak identifikatu ditu, erakundearen sistemak eta sareak gotortzeko egokiak diren estandarretan, gidetan eta segurtasun-politiketan oinarrituta.

Edukiak: Prestakuntza-planak diseinatzea.

- Arriskuen analisia.

- Industria 4.0ko Ekonomia Zirkularreko printzipioak.
- Segurtasun-neurri teknikoen plana.
- Ohikoenak diren babes-politikak.
- Sistemak eta sareak babesteko jardunbide egokien gida.
- Sistemak eta sareak babesteko estandarrak.
- Prozedurak, jarraibideak eta gomendioak karakterizatzea.
- Gorabeherei erantzuteko mailak, eskala-faktoreak eta protokoloak.

RA4. Sarbidea kontrolatzeko eta pertsonak autentifikatzeko sistemak konfiguratzen ditu, datuen konfidentzialtasunari eta pribatutasunari eutsiz.

Ebaluazio-irizpideak:

a) Autentifikazio-mekanismoak definitu ditu, dauden hainbat faktoretan (fisikoak, berezkoak eta ezagutzan oinarritutakoak) oinarrituta.
b) Pasahitzetan eta sarrera-esaldietan oinarritutako autentifikazio-protokoloak eta -politikak definitu ditu, ahulezia nagusietan eta eraso-motetan oinarrituta.
c) Ziurtagiri digitaletan eta txartel adimendunetan oinarritutako autentifikazio-protokoloak eta -politikak definitu ditu, ahulezia nagusietan eta eraso-motetan oinarrituta.
d) Tokenetan, OTPetan eta abarretan oinarritutako autentifikazio-protokoloak eta -politikak definitu ditu, ahulezia nagusietan eta eraso-motetan oinarrituta.
e) Ezaugarri biometrikoetan oinarritutako autentifikazio-protokoloak eta -politikak definitu ditu, ahulezia nagusietan eta eraso-motetan oinarrituta.
f) Pasahitzak kudeatzeko hainbat tresna ezarri ditu.

Edukiak: Sarbidea kontrolatzeko eta pertsonak autentifikatzeko sistemak konfiguratzea.

- Autentifikazio-mekanismoak. Faktore-motak.
- Autentifikazio-teknikak: pasahitzak, ziurtagiri digitalak, tokenak, behin bakarrik erabiltzeko pasahitzak (OTP), ezaugarri biometrikoak, aurrekoen konbinazioa, eta abar.

RA5. Sistema informatikoetara sartzeko kredentzialak administratzen ditu, ezarritako funtzionamendu- eta segurtasun-baldintzak aplikatuta.

Ebaluazio-irizpideak:

a) Ohikoenak diren kredentzial-motak identifikatu ditu.
b) Hainbat ziurtagiri digital sortu eta erabili ditu urruneko zerbitzari batera sartzeko.
c) Web-zerbitzu baten ziurtagiri digital baten baliozkotasuna eta benetakotasuna egiaztatu ditu.
d) Ziurtagiri digital baliodunak eta hainbat arrazoirengatik baliogabeak direnak alderatu ditu.
e) Kredentzialak emateko zerbitzari seguru bat instalatu eta konfiguratu du (RADIUS - Remote Access Dial In User Service motakoa).

Edukiak: Sistema informatikoetara sartzeko kredentzialak administratzea.

- Kredentzialak kudeatzea.
- Gako publikoaren azpiegiturak (PKI).

- Sinadura elektronikoaren bidezko sarbidea.
- Sinadura digitala aplikatzea.
- Sarbideak kudeatzea. NAC sistemak (Network Access Control, Sarerako sarbideen kudeaketa-sistemak).
- Kontu pribilegiatuak kudeatzea.
- RADIUS eta TACACS protokoloak, KERBEROS zerbitzuak, besteak beste.

RA 6. Konputagailu-sareak diseinatzen ditu aintzat hartuta segurtasun-betekizunak.

Ebaluazio-irizpideak:

a) Tokiko sare lau baten segurtasun-maila handitu du, fisikoki segmentatuta eta bideratze-teknikak eta -gailuak erabilita.
b) Sare lokal lau bat optimizatu du segmentazio logikoko tekniken (VLAN) bidez.
c) Tokiko sare operatibo baten segmentu bat egokitu du subnetting teknikak erabilita, dauden helbideratzeak errespetatuz segmentazioa handitzeko.
d) Hari gabeko sare baterako sarbidea ematen duten gailuetan (bideratzaileak, sarbide-puntuak, etab.) segurtasun-neurri egokiak konfiguratu ditu.
e) Geografikoki bereizita dauden bi egoitzen arteko komunikazio-tunel segurua ezarri du.
f) Suebaki birtualek perimetroan aseguratutako sare segmentatuak definitu eta konfiguratu ditu, eta, horretarako, zerbitzarien birtualizazio-inguruneak erabili ditu.

Edukiak: Konputagailu-sare seguruen diseinua.

- Sareen segmentazioa.
- Sareak muntatu eta konfiguratzea zerbitzarien birtualizazio-inguruneetan (Proxmox, OpenStack…).
- Subnetting.
- Sare birtualak (VLAN).
- Gune desmilitarizatuak (DMZ).
- Segurtasuna hari gabeko sareetan (WPA2, WPA3...).
- Sare seguruen protokoloa (IPSec...).
- Segurtasun-perimetroak ezartzeko ereduak diseinatu eta definitzea.
- Suebakiak iragazteko politikak eta arauak konfiguratzea.
- Zerbitzarien eta zerbitzuen konfigurazio segurua DMZren gainean. Euste-suebakiak eta gotortzea.
- Suebaki birtualak (adibidez, Sophos).
- “Honeynetak” ezartzea.
- "Web-proxy-cache" zerbitzari bat instalatzea eta konfiguratzea.
- Proxy zerbitzaria erabiltzea web sarbidean murrizketak ezartzeko.
- Proxy-aren funtzionamendu-probak egitea eta haren aktibitatea monitorizatzea.
- Bezeroetatik proxy-rako hainbat sarbide-arazo konpontzea. Proxy bat modu gardenean eta alderantzizko moduan konfiguratzea.

RA 7. Gailu eta sistema informatikoak konfiguratzen ditu eta segurtasun-betekizunak betetzen ditu.

Ebaluazio-irizpideak:

a) Segurtasun-betekizun jakin batzuen araberako segurtasun-gailu perimetralak konfiguratu ditu.
b) Hainbat suebaki-mota konfiguratu eta erabili ditu.
c) Suebaki bat iragazteko politikak eta arauak konfiguratu ditu, eta gertaeren erregistroa ikuskatu du.
d) DMZ gaineko zerbitzari eta zerbitzuak modu seguruan konfiguratu ditu.
e) Sareko gailuen konfigurazioan erroreak detektatu ditu, trafikoaren analisiaren bitartez.
f) Sare batean nahi ez diren portaerak identifikatu ditu, suebaki baten erregistroak (Logs) aztertuta.
g) Sare batean nahi ez diren portaeren aurkako neurriak ezarri ditu.
h) Monitorizazio-tresnen ezaugarriak finkatu, instalatu eta konfiguratu ditu.
i) Hainbat proxy-mota konfiguratu eta erabili ditu.

Edukiak: Gailu eta sistema informatikoak konfiguratzea.

- Segurtasun perimetrala. Hurrengo belaunaldiko suebakiak.
- Web-atari eta -aplikazioen segurtasuna. WAF (Web Application Firewall) konponbideak.
- Lanpostuaren segurtasuna eta “endpoint” finko eta mugikorra. AntiAPT, antimalware.
- Cloud inguruneen segurtasuna. CASB konponbideak.
- Posta elektronikoaren segurtasuna.
- DLP (Data Loss Prevention) konponbideak.
- Log-ak biltegiratzeko tresnak.
- Log-ak aztertzeko datuen analisi-tresnak (Elasticsearch, adibidez).
- Datuak bistaratzeko tresnak (Kibana, adibidez), aztertutako log-ak erakusteko.
- Banatutako zerbitzua ukatzeko erasoetatik babestea (DDoS).
- Suebakien, bideratzaileen eta proxieen konfigurazio segurua.
- Sare pribatu birtualak (VPN) eta tunelak (IPSec protokoloa).
- Sistemak eta gailuak monitorizatzea. SNMP protokoloa.
- Monitorizazio-tresnak (IDS, IPS).
- SIEMak (Segurtasuneko Ekitaldien eta Informazioaren Kudeatzaileak).
- Ekitaldien analisia eta normalizazioa.
- Ekitaldiak gehitzea. Log-en kudeaketa eta jarduteko prozedurak.
- Segurtasun-gorabeherak eta mehatxuak monitorizatzea, dokumentatzea eta erantzuna ematea.
- Sareko Eragiketa Zentroen eta Sareko Segurtasun Zentroen konponbideak: NOCak eta SOCak.

RA 8. Sistema informatikoen segurtasuna konfiguratzen ditu, erasoekiko esposizio-aukerak minimizatuta.

Ebaluazio-irizpideak:

a) Gailuaren eta haren edukiaren segurtasuna areagotzeko BIOS konfiguratu du, erasoekiko esposizio-aukerak minimizatuta.
b) Sistema informatiko bat prestatu du lehen aldiz instalatzeko, beharrezkoak diren segurtasun-neurriak kontuan hartuta.
c) Sistema informatiko bat konfiguratu du, eragile gaizto batek ezin izan dezan abio-sekuentzia

aldatu, legez kontrako sarbidea izateko.

d) Sistema informatiko bat instalatu du, eta, horretarako, fitxategi-sistemaren zifratze-gaitasunak erabili ditu, datuak fisikoki ateratzea saihesteko.

e) Sistema informatikoaren fitxategi-sistema zatikatu du, segurtasun-arriskuak minimizatzeko.

f) Oso eskuragarriak diren neurriak ezarri ditu, eta gailuren bat eroriz gero eragiketaren jarraitutasuna egiaztatu du.

g) Honeynet bat konfiguratu du balizko erasotzaileak erakarri eta haien jarduketetatik ikasteko.

h) Log-ak prozesatu eta bistaratzeko sistema integral bat instalatu eta konfiguratu du.

Edukiak: Sistema informatikoak instalatzeko gailuak konfiguratzea.

- Sistema informatiko bat instalatu aurreko arreta-neurriak: isolamendua, BIOSetarako sarbide-kontrolaren konfigurazioa, gailuak abiarazteko aginduaren blokeoa, besteak beste.
- Segurtasuna sistema informatikoak abiaraztean, abio segurua konfiguratzea.
- Segurtasuna fitxategi, zifratze-, zatikatze-sistemetan, besteak beste.
- Eskuragarritasun handia: klusterrak, diskoen erredundantzia, bonding-a...

RA 9. Sistema informatikoak konfiguratzen ditu erasoekiko esposizio-aukerak minimizatzeko.

Ebaluazio-irizpideak:

a) Sisteman besterik ezean instalatu diren alferrikako programak, zerbitzuak eta protokoloak zerrendatu eta ezabatu ditu.

b) Sistema informatikoaren berezko ezaugarriak konfiguratu ditu, legez kanpoko sarbideak eragozteko prozesuen ustiaketa-tekniken bidez.

c) SSH eta beste urruneko administrazio-sistema batzuen segurtasuna areagotu du.

d) Sistema informatikoan, host batean arrotzak detektatzeko sistema (HIDS) instalatu eta konfiguratu du.

e) Babeskopien sistema instalatu eta konfiguratu du.

Edukiak: Sistema informatikoak konfiguratzea.

- Zerbitzuen kopurua murriztea: Telnet, RSSH, TFTP, besteak beste.

- Prozesuen hardening-a (erroreak gertatuz gero, arazketari buruzko informazioa ezabatzea, exploit-ak saihesteko memoria birtuala ausazkotzea, eta abar).

- Sarean beharrezkoak ez diren protokolokoak ezabatzea (ICMP, besteak beste).
- Urruneko administrazio-sistemak babestea.
- Birus eta arrotzak prebenitu eta haietatik babesteko sistemak (antibirusak, HIDS, eta abar).
- Eguneratzeak eta adabaki automatikoak konfiguratzea.
- Babeskopien sistemak.
- Shadow IT eta segurtasun-politikak SaaS inguruneetan.

RA 10. IT zatiaren eta OT zatiaren arteko integrazioa diseinatu du, OT gailuak bermatu ditu erakundearen barneko zein kanpoko balizko erasoen aurka.

Ebaluazio-irizpideak:

a) Txosten bat egin du OT sare bateko mehatxu nagusiak eta balizko defentsa-neurriak zehaztuta.

b) Sarearen geruzen araberako segmentazioa diseinatu du, OT gailuak bermatuta mantentzeko.

c) Segurtasun-neurriak ezarri dira OT gailuetarako urruneko sarbidea segurua izan dadin.

d) Honeypot espezifiko bat instalatu eta konfiguratu du, gailu industrialen aurkako eraso-saiakeren berri izateko.

e) Zibersegurtasun industrialaren oinarrizko alderdiak aztertu ditu.

f) Oinarrizko ingurune industrial bat birsortu du, eta, horretarako, gutxienez kontrol industrialeko gailu bat eta gainbegiratzeko eta urruneko kontrolerako software bat instalatu eta konfiguratu ditu.

g) Osagai industrialen ezaugarriak aztertu ditu, baita automatizazioaren esparruan duten lekua, funtzionamendua eta ahuleziak ere.

h) Gailu industrialen ahuleziak ustiatzeko oinarrizko tresnak erabili ditu.

Edukiak: Kontrol-sistema industrialak: mehatxuak eta ahuleziak.

- Azpiegitura industrialen oinarrizko kontzeptuak.

  - Kontrol-sistema industrialak: sarrera.
  - OTetako komunikazio-protokoloak. Modbus, Profinet, eta abar.
  - PLC simulatu bat instalatzea eta konfiguratzea.
  - Oinarrizko SCADA bat instalatzea eta konfiguratzea.
  - PLC baten eta SCADA baten arteko konektagarritasuna konfiguratzea.
  - Tokiko kontrol-sistemak: sentsoreak, eragingailuak, serboak eta erregulagailuak, PLCak, RTUak, PC industrialak eta DCS. Gako alderdiak, alde indartsuak eta alde ahulak.
  - SCADA: funtzioak, arkitektura eta osagaiak.
  - Segurtasun-sistemak, segurtasun-sistema instrumentatuak (SIS) eta kontrol- eta segurtasun-sistema integratuak (ICSS).
  - Beste sistema sektorial espezifiko batzuk: CNC, kontagailu adimendunak, robotak, MES, eta abar.

- IT/OT sareak integratzea. OT sareen ahuleziak.

  - OT sare bateko mehatxu nagusiak.
  - Sareen segmentazioa. IT/OT banaketa.
  - OT gailuetarako urruneko sarbide segurua.
  - Honeypot industrialak konfiguratzea.
  - Shodan: xedea eta erabilera.
  - Kali-Moki banaketa: host mailan automatizazio- eta kontrol-sistemei eraso egiteko tresnak.
  - Metasploit erabiltzea.

3. lanbide-modulua: Ekoizpen seguruan jartzea.

Kodea: 5023
Iraupena: 120 ordu

ECTS kredituak: 7

Ikaskuntzaren emaitzak, ebaluazio-irizpideak eta edukiak.

RA1: Programa errazak egiten ditu eta objektuei orientatutako programazioaren oinarriak aplikatzen ditu.

Ebaluazio-irizpideak:

a) Objektuei orientatutako programazioaren oinarriak identifikatu ditu.
b) Objektuak instantziatu ditu klase aurredefinituak abiapuntutzat hartuta.
c) Objektuen propietateak eta metodoak erabili ditu.
d) Metodo estatikoetarako deiak idatzi ditu.
e) Parametroak erabili ditu metodoetarako deietan.
f) Objektu-liburutegiak gehitu eta erabili ditu.
g) Eraikitzaileak erabili ditu.

Edukiak: Objektuak erabiltzea

- Objektuen eta klaseen ezaugarriak.
- Objektuen propietateak edo atributuak.
- Metodoaren kontzeptua.
- Klase bateko kideen sarbide-kontrola.
- Metodo estatikoaren kontzeptua.
- Parametro eta balio itzuliak.

RA2: Hainbat klasetan antolatutako programak garatzen ditu, eta, eginkizun horretan, objektuei orientatutako programazioaren printzipioak aplikatzen ditu.

Ebaluazio-irizpideak:

a) Klase baten sintaxia, egitura eta osagaiak identifikatu ditu.
b) Klaseak definitu ditu.
c) Eraikitzaileak sortu ditu.
d) Lehenago sortutako klaseetako objektuak ezarri eta erabiliko dituzten programak garatu ditu.
e) Klaseen ikuspena eta haietako kideena kontrolatzeko mekanismoak erabili ditu.
f) Herentziaren kontzeptua definitu du.
g) Klase heredatuak definitu eta erabili ditu.
h) Metodo estatikoak sortu eta erabili ditu.
i) Klase-liburutegiak sortu eta erabili ditu.
j) Interfazeak sortu eta definitu ditu.

Edukiak: Klaseak garatzea

- Klasearen kontzeptua.
- Klase baten egitura eta kideak.

- Atributuak eta sarbide-kontrola definitzeko tresnak.
- Metodoak eta argumentuak deklaratzeko tresnak.
- Eraikitzaileak diseinatzeko tresnak.
- Kapsulatzea eta ikuspena.
- Herentziaren kontzeptua.
- Klase heredatuaren kontzeptua.

RA3: Programak garatzen ditu, eta, horretarako, objektuei orientatutako lengoaien ezaugarri aurreratuak aplikatzen ditu.

Ebaluazio-irizpideak:

a) Superklasearen eta azpiklasearen kontzeptuak identifikatu ditu.
b) Klase-hierarkiak diseinatu eta aplikatu ditu.
c) Klase-hierarkiak probatu eta araztu ditu.
d) Klase-hierarkiak ezartzen eta erabiltzen dituzten programak egin ditu.

Edukiak: Klase aurreratuak garatzea.

- Klase-hierarkia: superklaseak eta azpiklaseak.
- Polimorfismoaren kontzeptua.
- Azpiklaseen eraikitzaileak eta suntsitzaileak.
- Superklasearen metodoak eskuratzea.
- Superklasearen metodoen birdefinizioa.

RA4: Gailu mugikorretarako web-aplikazioak eta aplikazioak probatzen ditu, eta kodearen egitura eta exekuzio-eredua aztertzen ditu.

Ebaluazio-irizpideak:

a) Programazio-lengoaiak alderatu ditu, ezaugarri nagusien arabera.
b) Softwarea gauzatzeko hainbat eredu deskribatu ditu.
c) Iturburu-kodearen oinarrizko elementuak ezagutu ditu, eta esanahia eman die.
d) Softwarearen hainbat proba gauzatu ditu.
e) Programazio-lengoaiak ebaluatu ditu, ematen duten segurtasun-azpiegituraren arabera.

Edukiak: Web-aplikazioak eta gailu mugikorretarako aplikazioak probatzea:

- Programazioaren oinarriak.
- Programazio-lengoaia interpretatuak eta konpilatuak.
- Iturburu-kodea eta garapen-inguruneak.
- Softwarea exekutatzea.
- Programen elementu nagusiak.
- Probak. Motak.
- Segurtasuna programazio-lengoaian eta gauzatze-inguruneetan (“sandboxak”).

RA5: Aplikazioek eskatzen duten segurtasun-maila zehazten du eta ohikoenak diren eraso-

bektoreak eta haiekin lotutako arriskuak identifikatzen ditu.

Ebaluazio-irizpideak:

a) Nazioarteko estandarrek (ASVS, "Application Security Verification Standard") ezarritako aplikazioetako segurtasuna egiaztatzeko mailen ezaugarriak finkatu ditu.
b) Aplikazioek eskatzen duten segurtasuna egiaztatzeko maila identifikatu du haien arriskuen arabera, onartutako estandarren bat etorriz.
c) Ezarritako segurtasun-mailari lotutako beharrezko egiaztapen-betekizunak zerrendatu ditu.
d) Garatutako aplikazioen arrisku nagusiak identifikatu ditu, haien ezaugarrien arabera.

Edukiak: Aplikazioek eskatzen duten segurtasun-maila zehaztea.

- Garapen segururako iturri irekiak.
- Ohiko segurtasun-arriskuen zerrenda: OWASP Top Ten (web eta mugikorra).
- Ezarritako segurtasun-mailari lotutako beharrezko egiaztapen-betekizunak.
- Segurtasun-egiaztapenak aplikazio mailan: ASVS (Application Security Verification Standard).

RA6: Web-aplikazioen ahuleziak detektatzen eta zuzentzen ditu, eta, horretarako, iturburu-kodea aztertu eta web-zerbitzariak konfiguratzen ditu.

Ebaluazio-irizpideak:

a) Erabiltzaileen sarrerak baliozkotu ditu.
b) Zerbitzarian eta bezeroarengan injekzio-arriskuak detektatu ditu.
c) Erasotzaileari saioaren identifikatzailea finkatzeko aukera ematen dion sistema baten ahuleziak aztertu ditu.
d) Erabiltzailearen saioa behar bezala kudeatu du aplikazioa erabiltzean.
e) Erabiltzailearen benetakotasuna egiaztatu du baliabideak eta funtzionaltasunak eskuratzean.
f) Datuen ihesa saihestu du horiei emandako baimena kontrolatuz.
g) Sarbidea kontrolatzeko rolak erabili ditu.
h) Algoritmo kriptografiko seguruak erabili ditu erabiltzailearen pasahitzak biltegiratzea.
i) Web-zerbitzariak konfiguratu ditu eraso ezagunak jasateko arriskua murrizteko.
j) Neurriak txertatu ditu programa automatikoen bidez (bot-ak) pasahitzei, mezuen bidalketa masiboari edo erabiltzaileen erregistroei egindako erasoak saihesteko.

Edukiak: Web-aplikazioen ahuleziak detektatu eta zuzentzea.

- Web-aplikazioen garapen segurua.
- Web-aplikazioen ahulezien zerrenda publikoak. OWASP Top Ten.
- Datu-orrietan oinarritutako sarrera. Injekzioa. Sarrerak baliozkotzea.
- Autentifikazio- eta baimentze-estandarrak.
- Saioa lapurtzea.
- Web-ahuleziak.
- Datuen ihesa. Informazioa ezagutaraztea errore-mezuetan. Path traversal.
- Pasahitzak modu seguruan biltegiratzea.
- Kontraneurriak. HSTS, CSP, CAPTCHAk, besteak beste.

- Kriptografiako berariazko tresnak. Ziurtagiri digitalak, protokolo seguruak eta sinadura digitalak.
- Web-atari eta -aplikazioen segurtasuna. WAF (Web Application Firewall) konponbideak.

RA7: Gailu mugikorretarako aplikazioetan segurtasun-arazoak detektatzen ditu, eta, horretarako, horien exekuzioa monitorizatu eta fitxategiak eta datuak aztertzen ditu.

Ebaluazio-irizpideak:

a) Plataforma mugikorren baimen-ereduak alderatu ditu.
b) Datuak gailuetan segurtasunez biltegiratzeko teknikak deskribatu ditu, informazioak ihes egin ez dezan.
c) Aplikazioan integratutako erosketak baliozkotzeko sistema bat ezarri du, zerbitzarian balidazioa erabilita.
d) Sareko trafikoa monitorizatzeko tresnak erabili ditu, aplikazio mugikorretan komunikazio-protokolo ez-seguruen erabilera detektatzeko.
e) Aplikazio mugikorren bitarrak ikuskatu ditu, bereziki babestutako informazioaren ihesak bilatzeko.

Edukiak: Gailu mugikorretarako aplikazioetan segurtasun-arazoak detektatzea.

- Plataforma mugikorretan baimen-ereduak. Sistemara egindako dei babestuak.
- Aplikazioak sinatzea eta egiaztatzea.
- Datuak modu seguruan biltegiratzea.
- Aplikazioan integratutako erosketak baliozkotzea.
- Informazioaren ihesa exekutagarrietan.
- CASB konponbideak.

RA8: Softwarea hedatzeko sistema seguruak ezartzen ditu, eta, horretarako, bere elementuen eraikuntza automatizatzeko tresnak erabiltzen ditu.

Ebaluazio-irizpideak:

a) Softwarearen garapenaren eta eragiketaren integrazioaren ezaugarriak, printzipioak eta helburuak identifikatu ditu.
b) Bertsioak kontrolatzeko sistemak ezarri ditu, eskatutako rolak eta baimenak administratuta.
c) Etengabeko integrazio-sistemak instalatu, konfiguratu eta egiaztatu ditu, eta bertsioak kontrolatzeko sistemekin konektatu ditu.
d) Softwarea hedatzeko planak planifikatu, ezarri eta automatizatu ditu.
e) Hedatze-sistemak akatsei automatikoki erantzuteko duen gaitasuna ebaluatu du.
f) Hondamenen aurrean egindako eragiketak eta lehengoratzeko jarraitu beharreko metodoak dokumentatu ditu.
g) Atzeraelikadurako begiztak sortu dituzte taldekideen artean.

Edukiak: Softwarea hedatzeko sistema seguruak ezartzea:

- Ekoizpen seguruan jartzea.

- Softwarea garatzeko eta erabiltzeko praktika bateratuak (DevOps).
- Bertsioak kontrolatzeko sistemak:
- Eraikuntza (build) automatizatzeko sistemak.
- Probak etengabe integratzea eta automatizatzea.
- Zerbitzarien eskala-faktoreak. Birtualizazioa. Edukiontziak.
- Sistemen konfigurazioaren kudeaketa automatizatua.
- Akatsak simulatzeko tresna.
- Edukiontzien orkestrazioa.

4. lanbide-modulua: Auzitegi-analisi informatikoa.

Kodea: 5024.
Iraupena: 96 ordu
ECTS kredituak: 7.

Ikaskuntzaren emaitzak, ebaluazio-irizpideak eta edukiak.

RA1. Auzitegi-analisirako metodologiak aplikatzen ditu, eta babeste-, eskuratze-, analisi- eta dokumentatze-faseen ezaugarriak finkatzen ditu.

Ebaluazio-irizpideak:

a) Ebidentzien babesa bermatzeko aztertu beharreko gailuak identifikatu ditu.
b) Ebidentziak eskuratzeko eta ateratzeko mekanismo eta tresna egokiak erabili ditu.
c) Eszena ziurtatu du eta zaintza-kateei heldu die.
d) Egindako prozesua modu metodikoan dokumentatu du.
e) Ebidentzien denbora-lerroa kontuan hartu du.
f) Ondorioen txosten bat egin du maila teknikoan eta exekutiboan.
g) Egindako auzitegi-analisiaren ondorioak aurkeztu eta azaldu ditu.

Edukiak: Auzitegi-analisien metodologiak aplikatzea.

− Aztertuko diren gailuen identifikazioa.
− Auzitegi-ikerketaren eskakizunak: onargarritasuna, integritatea, sinesgarritasuna, kausa-ondorioa erlazioa, errepikagarria eta dokumentatua.
− Auzitegi-analisiaren etapak.
− Eskuraketaren aurreko oharrak.
− Hegakortasun-hurrenkera.
− Ebidentzien bilketa (eszenatokia lantzea).
− Denbora-lerro baten analisia (TimeStamp).
– Hegakortasuna aztertzea.
– Informazioa ateratzea (Volatility).
− Logen analisia, tresnarik erabilienak.

RA2. Auzitegi-analisiak egiten ditu ordenagailu pertsonaletan, ezarritako, eguneratutako eta onartutako metodologiak aplikatuta.

Ebaluazio-irizpideak:

a) Fitxategi-sistemak, horiek dituzten datuak eta metadatuak aztertu ditu.
b) Ezabatutako fitxategiak berreskuratu ditu.
c) Ransomwarearen eta, oro har, malwarearen portaera aztertu du.
d) Diskoak aztertu ditu.
e) Sistemen RAM memoria aztertu du.
f) Sistemaren erregistroa aztertu du.
g) Erabiltzaileak sisteman duen informazioa eta jarduera aztertu ditu.

Edukiak: Auzitegi-analisiak egitea ordenagailu pertsonaletan.

- Fitxategi-sistemak. Datuak eta metadatuak.
- Ezabatutako fitxategiak berreskuratzea.
- Ransomwarearen eta malwarearen portaera.
- Diskoak aztertzea.
- Memoria aztertzea. Iraulketak. - Gauzatzen ari diren prozesuak.
- Erregistroa aztertzea.
- Erabiltzailearen analisia eta informazioa: nabigatzaileak, posta elektronikoa, bilaketak, jarduera...

RA3. Auzitegi-analisiak egiten ditu gailu mugikorretan, ezarritako, eguneratutako eta aitortutako metodologiak aplikatuta.

Ebaluazio-irizpideak:

a) Gailu mugikor batean ebidentziak hartzeko prozesua bete du.
b) Probak atera, deskodetu eta aztertu ditu, zaintza-kateari eutsita.
c) Datu mugikorrei buruzko txostenak egin ditu, telefonia mugikorreko auzitegi-industriaren eskakizunak beteta.
d) Egindako auzitegi-analisiaren ondorioak aurkeztu eta azaldu dizkie dagokienei.

Edukiak: Auzitegi-analisiak egitea gailu mugikorretan.

- Ebidentziak ateratzeko metodoak.
- Merkatuko tresna ohikoenak.
- SIM txartelak eta memoria-txartelak aztertzea.

RA4. Auzitegi-analisiak egiten ditu Clouden, ezarritako, eguneratutako eta aitortutako metodologiak aplikatuta.

Ebaluazio-irizpideak:

a) Clouden auzitegi-analisiaren estrategia bat garatu du, eta, gorabehera gertatu ondoren, beharrezko baliabideak eta gaitasunak eskura izatea bermatu du.

b) Gorabeheraren kausak, irismena eta hark benetan eragindako eragina identifikatzea lortu du.
c) Clouden auzitegi-analisiaren faseak bete ditu.
d) Hodeiaren berezko ezaugarriak identifikatu ditu (elastikotasuna, ubikuotasuna, abstrakzioa, hegakortasuna eta baliabideen partekatzea).
e) Indarrean dauden lege-eskakizunak, DBEO (Datuak Babesteko Erregelamendu Orokorra) eta NIS zuzentaraua (sareen eta informazio-sistemen segurtasunari buruzko EBren Zuzentaraua) edo horiek ordezka ditzaketenak bete ditu.
f) Egindako auzitegi-analisiaren ondorioak aurkeztu eta azaldu ditu.

Edukiak: Auzitegi-analisiak egitea Clouden.

- Hodei pribatua eta hodei publiko edo hibridoa.
- Clouden analisi baten legezko eta antolakuntzako erronkak eta tekniko partikularrak.
- Clouden auzitegi-analisiaren estrategiak.
- Clouden auzitegi-analisiaren fase garrantzitsuak egitea.
- Clouden analisi-tresnak erabiltzea (Cellebrite UFED Cloud Analizer, Cloud Trail, Frost, OWADE...).

RA5. Auzitegi-analisia egiten du IoT-eko gailuetan, ezarritako, eguneratutako eta aitortutako metodologiak aplikatuta.

Ebaluazio-irizpideak:

a) Ebidentzien babesa bermatzeko aztertu beharreko gailuak identifikatu ditu.
b) Ebidentziak eskuratzeko eta ateratzeko mekanismo eta tresna egokiak erabili ditu.
c) Ateratako ebidentzien egiazkotasuna, osotasuna, fidagarritasuna eta legezkotasuna bermatu ditu.
d) Ebidentziak eskuz eta tresnen bidez aztertu ditu.
e) Prozesua modu metodikoan eta xehatuan dokumentatu du.
f) Ebidentzien denbora-lerroa kontuan hartu du.
g) Zaintza-katea mantendu du.
h) Ondorioen txostena egin du maila teknikoan eta exekutiboan.
i) Egindako auzitegi-analisiaren ondorioak aurkeztu eta azaldu ditu.

Edukiak: Auzitegi-analisiak egitea IoT-en.

− Aztertuko diren gailuen identifikazioa.
– Ebidentziak eskuratzea eta ateratzea.
– Ebidentziak eskuz eta automatikoki aztertzea.
– Egindako prozesuaren dokumentazioa osatzea
– Denbora-lerroa ezartzea.
– Zaintza-kateari eustea.
– Ondorioak ateratzea.
– Ondorioak aurkeztea eta azaltzea.

RA6. Auzitegi-analisiak dokumentatzen ditu; horretarako, aplikatu beharreko araudia jasotzen

duten txostenak egiten ditu.

Ebaluazio-irizpideak:

a) Peritu-txostenaren helburua eta justifikazioa definitu ditu.
b) Peritu-txostenaren aplikazio-eremua definitu du.
c) Aurrekariak dokumentatu ditu.
d) Egindako auzitegi-analisian bete diren lege-arauak eta erregelamenduak bildu ditu.
e) Bezeroak ezarritako betekizunak jaso ditu.
f) Ondorioak eta justifikazioa atxiki ditu.

Edukiak: Auzitegi-analisien txostenak dokumentatzea eta egitea. Txostena osatzen duten atalak.
- Peritu-txostenen hastapenak. Legeak. Erregistro-ordenak. Judizioak.
- Identifikazio-orria (izenburua, sozietate-izena, izen-abizenak, sinadura).
- Memoriaren aurkibidea.
- Xedea (peritu-txostenaren helburua eta justifikazioa).
- Irismena (aditu-txostenaren aplikazio-eremua – edukia eta emaitzak azkar gainbegiratzeko laburpen exekutiboa).
− Aurrekariak (aztertutako alternatibak eta azken ondorioak ulertzeko beharrezkoak diren alderdiak).

- Arauak eta erreferentziak (ataletan aipatutako lege-dokumentuak eta -arauak eta erregelamenduak).
- Definizioak eta laburdurak (txostenean erabili diren definizioak, laburdurak eta adierazpen teknikoak).
- Betekizunak (bezeroak, legediak, erregelamenduak eta araudi aplikagarriak ezarritako abiapuntuko baseak eta datuak).
- Konponbideen analisia – peritu-txostenaren ondorioen laburpena (aztertutako alternatibak, haietara iristeko jarraitu diren bideak, bakoitzaren abantailak eta eragozpenak, eta azkenean aukeratutako konponbidea eta justifikazioa).
– Eranskinak.

5. lanbide-modulua: Hacking etikoa.

Kodea: 5025.
Iraupena: 120 ordu.
ECTS kredituak: 7.

Ikaskuntzaren emaitzak, ebaluazio-irizpideak eta edukiak.

RA1: Ahuleziak detektatzeko monitorizazio-tresnak zehazten ditu, hacking etikoko teknikak aplikatuta.

Ebaluazio-irizpideak:

a) Hacking etikoaren funtsezko terminologia definitu du.
b) Ziberdelituaren aurkako kontzeptu etikoak eta legalak identifikatu ditu.
c) Intrusio-testaren irismena eta baldintzak definitu ditu.

d) Segurtasunaren funtsezko elementuak identifikatu ditu: konfidentzialtasuna, benetakotasuna, osotasuna eta erabilgarritasuna.

e) Erasotzaile batek jarraitutako eraso baten faseak identifikatu ditu.

f) Ahulezia-motak aztertu eta definitu ditu.

g) Eraso-motak aztertu eta definitu ditu.

h) Dauden ahuleziak zehaztu eta horien ezaugarriak finkatu ditu.

i) Merkatuan eskuragarri dauden monitorizazio-tresna egokiak zehaztu ditu, erakunde motaren arabera.

Edukiak: Ahuleziak detektatzeko monitorizazio-tresnak zehaztea.

- Hacking etikoaren funtsezko elementuak.
- Hacking-aren, hacking etikoaren, sartze-testen eta hacktibismoaren arteko desberdintasunak.
- Intrusio-test baten aurretiko baimenak biltzea.
- Hacking-aren faseak.
- Kutxa beltzaren eta kutxa zuriaren auditoretzak.
- Ahuleziak dokumentatzea.
- Segurtasun- eta hacking-tresnak sailkatzea.
- ClearNeta, Deep Web, Dark Web, Darknets. Ezagutza, desberdintasunak eta sarbide-tresnak: Tor, ZeroNet, FreeNet.

RA2: Proba-inguruneetan, hari gabeko komunikazioak erasotzen eta defendatzen ditu, eta sareetarako sarbidea lortzen du ahuleziak frogatzeko.

Ebaluazio-irizpideak:

a) Hari gabeko txartelen funtzionamendu-moduak konfiguratu ditu.

b) Hari gabeko sareak eta horien puntu kalteberak enkriptatzeko teknikak deskribatu ditu.

c) Hari gabeko sareak detektatu ditu, eta sareko zirkulazioa antzeman du, erasoaren aurretik.

d) Hari gabeko sare ahuletara sartu da.

e) Hari gabeko beste komunikazio-sistema batzuen eta haien ahulezien ezaugarriak finkatu ditu.

f) "Ekipo gorri eta urdinaren" teknikak erabili ditu.

g) Detektatutako ahuleziei buruzko txostenak egin ditu, eta horiek arintzeko moduak gehitu ditu.

Edukiak: Proba-inguruneetan hari gabeko komunikazioen erasoa eta defentsa.

- Hari gabeko komunikazioa.
- Azpiegitura, ad-hoc eta monitore modua.
- Hari gabeko sareetan datuak aztertzea eta biltzea.
- Hari gabeko sareak erasotzeko eta aztertzeko teknikak.
- Hari gabeko beste eraso batzuen aurkako erasoak.
- Auditoria-txosten teknikoak egitea eta emaitzak aurkeztea.

RA3: Proba-inguruneetan, sareak eta sistemak erasotzen eta defendatzen du, eta hirugarrenen informaziorako eta sistemetarako sarbidea lortzen du.

Ebaluazio-irizpideak:

a) Sareari eta xede-sistemei buruzko informazioa bildu du teknika pasiboen bidez.
b) Sarearen eta xede-sistemen ekipoen, erabiltzaile-kontuen eta balizko ahulezien inbentarioa egin du, teknika aktiboen bidez.
c) Bereziki babestutako informazioa bilatzeko hirugarrenen sare-trafikoa moztu du.
d) Bitartekari-eraso bat egin du, urrutiko bi muturretatik trukatutako trafikoa irakurrita, txertatuta eta nahierara aldatuta.
e) Urruneko sistemak konprometitu ditu, eta haien ahuleziak ustiatu ditu.
f) Detektatutako ahuleziei buruzko txostenak egin ditu, eta horiek arintzeko moduak gehitu ditu.

Edukiak: Proba-inguruneetan, sareak eta sistemen erasoa eta defentsa hirugarrenen sistemetara sartzeko.

- Ezagutze-fasea (footprinting).
- Eskaneaketa-fasea (fingerprinting)
- Trafikoa monitorizatzea.
- Komunikazioak moztea, hainbat teknika erabilita.
- Trafikoa manipulatzea eta injektatzea.
- Ahuleziak aurkitu eta ustiatzeko tresnak.
- Ingeniaritza soziala. Phishing.
- Pribilegioak mailakatzea.
- Sareetako eta sistemetako ahuleziei buruzko txostenak eta hobetzeko proposamenak.

RA4: Sistema konprometituak finkatu eta erabiltzen ditu, eta etorkizuneko sarbideak bermatzen ditu.

Ebaluazio-irizpideak:

a) Urrutiko sistemak administratu ditu, komando-lerroko erreminten bidez.
b) Pasahitzak konprometitu ditu, hiztegien, rainbow taulen eta indar handiko erasoen bidez, enkriptatutako bertsioen aurka.
c) Sistema gehigarrietara sartu da, sistema konprometituen bidez.
d) Atzeko ateak instalatu ditu, etorkizunean konprometitutako sistemetarako sarbideak bermatzeko.

Edukiak: Sistema konprometituak finkatzea eta erabiltzea.

- Sistemak urrunetik administratzea.
- Pasahitzen erasoak eta auditoretzak.
- Sarean pibotatzea.
- Atzeko ateak troiarrekin (Rat, Remote Access Trojan) instalatzea

RA5: Proba-inguruneak eta web-aplikazioak erasotzen eta defendatzen ditu, eta baimendu gabeko datu edo funtzionaltasunetarako sarbidea lortzen du.

Ebaluazio-irizpideak:

a) Web-autentifikazioko sistemak identifikatu ditu, eta ahuleziak eta indarrak nabarmendu ditu.
b) Web-aplikazio baten zerbitzua ematen duten ekipoen, protokoloen, zerbitzuen eta sistema eragileen inbentarioa egin du.
c) Erabilera normalean nabigatzailearen eta aplikazioaren artean egindako interakzioen fluxua aztertu du.
d) Web-aplikazioak eskuz aztertu ditu, ohikoenak diren ahuleziak bilatzeko.
e) Web-ahuleziak bilatu eta ustiatzeko tresnak erabili ditu.
f) Web-ahuleziak bilatu eta ustiatu ditu software-tresnen bidez.
g) Detektatutako ahuleziei buruzko txostenak egin ditu, eta horiek arintzeko moduak gehitu ditu.

Edukiak: Proba-inguruneetan web-aplikazioen erasoa eta defentsa.

- Web-aplikazioetan kredentzialak ukatzea.
- Informazioa biltzea.
- Web-zerbitzarietarako konexioak automatizatzea (adibidez: Selenium).
- Trafikoa aztertzea, mozte-proxien bidez.
- Web-aplikazioetan ohikoak diren ahuleziak bilatzea.
- Web-ahuleziak ustiatzeko tresnak.
- Web-aplikazioen ahuleziei buruzko txostenak eta hobetzeko proposamenak.

RA6: Telefonia mugikorreko aplikazioak aztertzen ditu, eta seguruak diren ala ez frogatzen du.

Ebaluazio-irizpideak:

a) Aplikazioaren analisi estatikoak egin ditu bezeroaren aldean.
b) Komunikazioak aztertu ditu.
c) Aplikazioak bezeroaren aldean duen portaera modu dinamikoan aztertu du.
d) Pentesting-tresnak erabili ditu aplikazio mugikorrak aztertzeko.

Edukiak: Mugikorretarako aplikazioak aztertzea.

- Mugikorretarako aplikazioen iturburu-kodea aztertzeko tresnak, eskuzkoak zein automatikoak.
- Sareko trafikoa aztertzeko tresnak.
- Aplikazioen analisi dinamikorako tresnak (adibidez, DROZER)
- Mugikorretarako pentesting-tresnak (OWASP - ZAP)

6. lanbide-modulua: Zibersegurtasunaren arloko araudia.

Kodea: 5026.
Iraupena: 48 ordu.
ECTS kredituak: 3.

Ikaskuntzaren emaitzak, ebaluazio-irizpideak eta edukiak.

RA1: Arauak betetzen direla ziurtatzeko, aplikazio-puntu nagusiak eta funtzioak eta erantzukizunak identifikatzen ditu.

Ebaluazio-irizpideak:

a) Erakundeetan kontuan hartu beharreko araudia betetzeko oinarriak identifikatu ditu.
b) Gobernu onaren printzipioak eta etika profesionalarekin duten lotura deskribatu eta aplikatu ditu.
c) Erakundeen barruan araudia betetzeko kultura ezartzen duten politikak eta prozedurak definitu ditu, baita egitura antolatzailea ere.
d) Erakundearen barruan araudia betetzeko arduradunaren eginkizunak edo eskumenak deskribatu ditu.
e) Hirugarrenekiko harremanak ezarri ditu, araudia behar bezala betetzeko.

Edukiak: Araudia behar bezala betetzeko aplikatu beharreko puntu nagusiak.

- Araudia betetzeari buruzko hastapena (Compliance: helburua, definizioa eta kontzeptu nagusiak).
- Gobernu onaren eta enpresa-etikaren printzipioak.
- Compliance Officer: funtzioak eta erantzukizunak.
- Hirugarrenekiko harremanak Compliance barruan.

RA2: Aplikatu beharreko legeria eta jurisprudentzia hautatu eta araudia betetzeko sistemak diseinatzen ditu.

Ebaluazio-irizpideak:

a) Erakunde-mota guztiei eragiten dieten araudi nagusiak jaso ditu.
b) Indarrean dagoen araudiaren arabera (ISO 19600, besteak beste), hainbat erakunde motatarako balio duten gomendioak ezarri ditu.
c) Indarrean dagoen araudiaren arabera (31000, besteak beste), hainbat erakunde motatarako balio duten gomendioak ezarri ditu.
d) Araudia betetzeko diseinatutako sistema dokumentatu du.

Edukiak: Araudia betetzeko sistemak diseinatzea.

- Complianceren kudeaketa-sistemak.
- Aplikatzeko erregulazio-ingurunea.
- Arriskuak aztertzea eta kudeatzea, arriskuen mapa.
- Araudia betetzeko diseinatutako sistema dokumentatzea.

RA3: Erakundeen eta pertsona juridikoen erantzukizun penala betetzeko indarrean dagoen araudia eta ezarritako prozedurak lotzen ditu, eta indarrean dauden arauak biltzen eta aplikatzen ditu.

Ebaluazio-irizpideak:

a) Hainbat erakunderi aplika dakizkiekeen arrisku penalak identifikatu ditu.
b) Identifikatutako arriskuak ezabatzeko edo minimizatzeko beharrezko neurriak ezarri ditu.
c) Araudi penala betetzeko kudeaketa-sistema bat ezarri du, indarreko legeriarekin eta araudiarekin bat etorriz (Zigor Kodea eta UNE 19601, besteak beste).

d) Erakundeetan eroskeriari aurre egiteko eta enpresa-kultura etikoa sustatzeko oinarrizko printzipioak zehaztu ditu, indarreko legeriarekin eta araudiarenkin bat etorriz (ISO 37001, besteak beste).

Edukiak: Erantzukizun penala betetzeko legeria.

- Erakundeari eragiten dioten arrisku penalak.
- Compliance penala kudeatzeko sistemak.
- Ustelkeriaren aurkako kudeaketa-sistemak.

RA4: Datu pertsonalak babesteko legeria nazionala aplikatzen du, eta ezarritako prozedurak indarreko legeekin eta gaiari buruzko jurisprudentziarekin lotzen ditu.

Ebaluazio-irizpideak:

a) Zuzenbideko iturriak identifikatu ditu, datu pertsonalen babesaren arloko ordenamendu juridikoaren arabera.
b) Nazioan zein nazioartean datu pertsonalen babesarekin lotutako printzipioak aplikatu ditu.
c) Diseinuaren oinarrietatik bertatik pribatutasunari aurre egiteko beharrezkoak diren betekizunak ezarri ditu.
d) Tresna korporatiboak konfiguratu ditu, araudia lehenetsia betetzen dela kontuan hartuta.
e) Datuak babesteko eskubideak tratatzeko arriskuak aztertu ditu.
f) Datuak babesteko arloan identifikatutako arriskuak ezabatzeko edo minimizatzeko beharrezko neurriak ezarri ditu.
g) Erakundearen barruan araudia betetzeko ordezkariaren eginkizunak edo eskumenak deskribatu ditu.

Edukiak: Datuen babesaren arloko legeria eta jurisprudentzia.

- Datuen babesaren printzipioak.
- DBEO.
- Pribatutasun lehenetsia edo diseinutik abiatuta.
- Pribatutasunaren gaineko Eraginaren Analisia (PIA) eta segurtasun-neurriak.
- Datuak babesteko ordezkaria (DBO).
- IGMEZL (Informazioaren Gizartearen eta Merkataritza Elektronikoaren Zerbitzuei buruzko Legea).

RA5: Nazioko eta nazioarteko zibersegurtasunari buruzko indarreko araudia biltzen eta aplikatzen du, eta ezarritako prozedurak eguneratzen ditu, gaiari buruzko legeekin eta jurisprudentziarekin bat etorriz.

Ebaluazio-irizpideak:

a) Erakundeari eragin diezaioketen araudia, jurisprudentzia, jakinarazpenak eta abar berrikusteko plana ezarri du.
b) Datu-base juridikoak kontsultatu ditu, ezarritako berrikuspen-planari jarraituz, eta araudi berria identifikatu du.

c) Araudi berria aztertu du, erakundearen jarduerak aplikatzen duen zehazteko.

d) Erakundeari aplikatu beharreko araudi berriaren gainean egin beharreko aldaketak sartu ditu berrikuspen-planean, araudia behar bezala betetzeko.

e) Berrikuspen-planean sartutako araudi berriak behar bezala betetzen direla bermatzeko beharrezko kontrolak zehaztu eta ezarri ditu.

f) Informazioaren osotasuna, erabilgarritasuna eta konfidentzialtasuna ziurtatzeko, jardunbide egokien ISO 27002 arauan zehaztutako kontrolak zehaztu eta ezarri ditu.

g) ISKS (Informazioaren Segurtasuna Kudeatzeko Sistema) garatzeko faseak deskribatu ditu.

h) Zonak, eroaleak eta kanalak diseinatu ditu, IEC 62443 arauaren arabera.

Edukiak: Nazioan eta nazioartean zibersegurtasunari buruz indarrean dagoen araudia.

- Nazioko eta nazioarteko arauak.
- Informazioaren Segurtasuna Kudeatzeko Sistemak (nazioarteko estandarrak, ISO 27001).
- ISO 27002 Jardunbide Egokien Kodea.
-Herritarrak Zerbitzu Publikoetara Bitarteko Elektronikoz Sartzea. Segurtasun Eskema Nazionala (SEN).
- Negozioaren Jarraipen Planak (nazioarteko estandarrak) (ISO 22301).
- IEC 62443
- NIS Zuzentaraua
- Azpiegitura kritikoak babesteari buruzko legeria. PIC Legea (Azpiegitura kritikoen babesa).

7. lanbide-modulua: Lanbide-modulua Oinarrizko funtsak.

Kodea: E300

Iraupena: 60 ordu

Ikaskuntzaren emaitzak, ebaluazio-irizpideak eta edukiak.

RA1: Ordenagailuak eta periferikoak sare kableatuetan eta hari gabekoetan integratzen ditu, eta haien funtzionamendua eta prestazioak ebaluatzen ditu.

Ebaluazio-irizpideak:

a) Sare kableatuetarako eta hari gabekoetarako estandarrak identifikatu ditu.

b) IP helbideratze logikoko sistema erabili du sareko helbideak eta azpisare-maskarak esleitzeko.

c) Sare-egokigailu kableatuak eta hari gabekoak konfiguratu ditu hainbat sistema eragiletan.

Edukiak: Sare kableatuak eta hari gabekoak.

- IP helbideak eta azpisare-maskarak konfiguratzea.
- Sare-egokigailu kableatuak eta hari gabekoak hainbat sistema eragiletan konfiguratzea.
- Sare kableatuak eta hari gabekoak elkarrekin konektatzeko gailuak konfiguratzea.

RA2: Informazioa segurtasunez tratatzeko jarraibideak eta jardunbideak hartzen ditu, eta informatika-sistema baten ahuleziak identifikatzen ditu, baita sistema segurtatzeko beharra ere.

Ebaluazio-irizpideak:

a) Segurtasun fisikoaren eta logikoaren arteko aldeak deskribatu ditu.
b) Ingeniaritza sozialeko teknikek informatika-iruzurretan duten eragina kontrastatu du.
c) Sistema biometrikoak erabiltzeak dakartzan abantailak baloratu ditu.
d) Teknika kriptografikoak aplikatu ditu informazioa biltegiratzeko eta transmititzeko.
e) Komunikazio-protokolo seguruak eta horien erabilera-esparruak identifikatu ditu.

Edukiak: Informatika segurtasuneko jarraibideak.

- Segurtasun fisikoa eta segurtasun logikoa.
- Ahulezien kausa nagusiak eta horien jatorria.
- Pasahitzen politikak.
- Sistema biometrikoak.
- Pasahitzen kudeatzaileak.
- CIDAN propietateak.
- Kriptografia simetrikoa eta asimetrikoa.
- Sinadura digitala eta ziurtagiriak.
- Gako publikoaren azpiegiturak (PKI).

RA3: Sistema eragileen funtzio aurreratuak administratzen ditu, barne-funtzionamendua kontuan hartuta.

Ebaluazio-irizpideak:

a) Segurtasun-politikak modu zentralizatuan ezarri ditu domeinuaren ekipo eta erabiltzaile guztientzat.
b) Sistema abiaraztean inplikatutako prozesuak eta fitxategiak identifikatu ditu.
c) Sistemaren konfigurazio-fitxategiak administratu ditu.
d) Sisteman exekutatzen diren prozesuak identifikatu ditu.
e) Log fitxategiak aztertu ditu.

Edukiak: Sareko Sistema Eragileak.

- Domeinuak. - Segurtasuna. Talde-direktibak.
- Sistema eragileen barne-funtzionamendua.
    - Abiaraztea.
    - Konfigurazio-fitxategiak.
    - Prozesuak.
    - Log fitxategiak.

RA4: Programa errazak egiten ditu datu-baseetan sartuta.

Ebaluazio-irizpideak:

a) Hainbat motatako aldagaiak definitu ditu eta haiekin hainbat eragiketa egin ditu.
b) Egitura baldintzatzaileak eta errepikakorrak erabili ditu.

c) Datu-egiturak definitu eta erabili ditu.

d) Aurrez definitutako funtzioak erabili ditu eta erabiltzaileak definitutako funtzioak definitu eta erabili ditu.

e) Moduluak eta/edo paketeak sortu eta erabili ditu, bai eta liburutegi estandarrak ere.

f) Erroreak eta salbuespenak kudeatu ditu.

g) Datu-baseetara sartu da, eta erregistroak txertatzeko, hautatzeko, eguneratzeko eta ezabatzeko oinarrizko eragiketak egin ditu.

Edukiak: Oinarrizko programak egitea.

- Aldagaiak, motak eta eragileak.
- Egitura baldintzatzaileak eta errepikakorrak.
- Datuen egiturak.
- Aurrez definitutako funtzioak eta erabiltzaileak definitutako funtzioak.
- Moduluak eta/edo paketeak. Liburutegi estandarrak.
- Erroreak eta salbuespenak.
- Datu-baseak: erregistroak txertatzea, hautatzea, eguneratzea eta ezabatzea.
- Herentziaren kontzeptua.
- Klase heredatuaren kontzeptua.

8. lanbide-modulua: Prestakuntza praktiko duala enpresetan.
Kodea: E301
Iraupena: 270 ordu

- Enpresan egin beharreko jarduerak programatuko dira espezializazio-ikastaroko konpetentziak eta helburu nagusiak, ikastetxean eskuratutakoak zein ikastetxean eskuratzen zailak direnak, osatzeko helburuarekin. Diseinatutako jarduerek honako hauek izan beharko dituzte:

- Gorabeherak prebenitzeko eta antzemateko planak egitea, neurri zuzentzaileak monitorizatzeko eta ezartzeko tresnetan oinarrituta.
- Segurtasun-planak diseinatzea eta ezartzea, konputagailu-sareak diseinatzea eta sarbidea kontrolatzeko eta autentifikatzeko sistemak administratzea.
- Aplikazioek eta gailu mugikorrek eskatzen duten segurtasun-maila aztertzea, baita eraso-bektore ohikoenak ere, eta softwarea hedatzeko sistema seguruak ezartzea.
- Auzitegi-analisi informatikoen proiektuetan laguntzea.
- Sistema, sare eta aplikazioetan ahuleziak detektatzea.
- Arauak betetzeko eta datu pertsonalak babesteko prozedurak definitzea eta aplikatzea.

5. Espazioak eta ekipamenduak.

5.1. Espazioak:

PRESTAKUNTZA-ESPAZIOA	AZALERA (M2) / 30 IKASLE	AZALERA (M2) / 20 IKASLE
Gela teknikoa	60	40
Laborategia.	180	140
Erabilera anitzeko gela	60	40

5.2. Ekipamenduak:

PRESTAKUNTZA-ESPAZIOA	EKIPAMENDUA
Gela teknikoa.	Irakaslearen ordenagailua. Ikus-entzunezko baliabideak. Ikasleen ordenagailuak. Erreprografia-sistemak. Sare-instalazioa, Internet sarbidearekin. Urruneko kontroleko softwarea. Oinarrizko softwarea (sareko sistema eragileak). Bulegotika-aplikazioen softwarea, irudien tratamendua, besteak beste. Birtualizaziorako software espezifikoa, SNMP protokoloan oinarritutako monitorizazio-tresnak, erabilgarritasun handiko zerbitzuak monitorizatzeko tresnak, besteak beste. Fitxategien, webguneen, datu-baseen eta aplikazioen zerbitzariak. Ekipoak klonatzeko tresnak. Suebakiak, arrotzen detektagailuak, Interneteko aplikazioak, proxieak, besteak beste. Datu-baseak kudeatzeko sistemak. Zerbitzariak eta bezeroak. Garapen-inguruneak, konpiladoreak eta interpretatzaileak, iturburu-kodearen analistak, paketatzaileak, laguntza-sortzaileak, besteak beste. Sareen eta zerbitzuen ahuleziak aztertu, monitorizatu eta ustiatzeko software espezifikoa. Diagnosirako, segurtasunerako, antibiruserako eta pasahitzaren kudeatzaileetarako software espezifikoa, besteak beste.
Laborategia	Banakako lan-mahaiak, tailer motakoak (80-90 cm-ko altuera). Zerbitzariak eta gailu gehigarriak instalatzeko bastidorea (rack). Sareko sistema eragilea eta Internet konexioa duten ordenagailuak. Diagnosirako, segurtasunerako, antibiruserako eta komunikazioetarako software espezifikoa, honeypot-ak/honeynet-ak, besteak beste. Kontrolatzaile logiko programagarriak, horien simulatzaileak eta sentsoreak. Kontrolatzaile logiko programagarriak, simulatzaileak eta datuen bistaratzea programatzeko software espezifikoa. Automatizazio industrialeko eta prozesuetako ekipoa, eragingailu elektroniko eta pneumatikoekin. Erreprografia- eta eskaner-sistemak. Hainbat eszenatoki birtualizatzeko gaitasuna duten zerbitzariak, teknologia aurreratuenekin. Biltegiratzeko euskarriak (diskoak, USB memoriak, memoria-txartelak, SIM txartelak...).

	Switchak eta bideratzaileak. Etenik gabeko elikatze-sistemak. Ikus-entzunezko baliabideak. 8-12 LAN atakako hardware suebakiak, 2-4 WAN ataka, karga-kulunka, edukien iragazketa, erabiltzaileen autentifikazioa, berehalako mezularitzaren eta P2P aplikazioen blokeoa, zerbitzua ukatzearen babesa, VPN bidezko urruneko konexio segurua, besteak beste. Hari gabeko sareetara konektatzeko sarbide-puntuak eta gailu ateragarriak. Gailu mugikorrak eta IoT. Sarbide fisikoa kontrolatzeko sistemak: NAN elektronikoaren irakurgailuak, RFID txartelak (irrati-maiztasun bidezko identifikazioa), besteak beste. Fitxategien, webguneen, datu-baseen eta aplikazioen zerbitzariak. Datu-baseak kudeatzeko sistemak. Zerbitzariak eta bezeroak. Garapen-inguruneak, konpiladoreak eta interpretatzaileak, iturburu-kodearen analistak, bertsioen kontrola, paketatzaileak, laguntza-sortzaileak, besteak beste. Bertsioak kontrolatzeko sistemak. Mugikorren simulatzaileak eta IoT. Sareen eta zerbitzuen ahuleziak aztertu, monitorizatu eta ustiatzeko software espezifikoa.
Erabilera anitzeko gela.	Irakaslearen ordenagailua. Ikus-entzunezko baliabideak. Ikasleen ordenagailuak. Erreprografia-sistemak. Sare-instalazioa, Internet sarbidearekin.

6. Irakasleak.

6.1. Informazioaren Teknologien Inguruneetan Zibersegurtasuneko Espezializazio ikastaroko lanbide-moduluetan irakasteko eskumena duten irakasleen espezialitateak:

LANBIDE-MODULUA	IRAKASLEEN ESPEZIALITATEA:	KIDEGOA
5021. Zibersegurtasun-gorabeherak.	Informatika. Sistema elektronikoak. Sistema elektroteknikoak eta automatikoak.	Bigarren Hezkuntzako irakaslea.
	Irakasle espezialista.	
5022. Sareak eta sistemak gotortzea	Ekipo elektronikoak. Informatika-sistemak eta aplikazioak	Lanbide Heziketako irakasle teknikoa.
5023. Ekoizpen seguruan jartzea.	Informatika-sistemak eta aplikazioak	Lanbide Heziketako irakasle teknikoa.
	Irakasle espezialista.	
5024. Auzitegi-analisi informatikoa.	Informatika-sistemak eta aplikazioak.	Lanbide Heziketako irakasle teknikoa.

	Irakasle espezialista.	
5025. Hacking etikoa.	Informatika. Sistema elektronikoak. Sistema elektroteknikoak eta automatikoak.	Bigarren Hezkuntzako irakaslea.
	Irakasle espezialista.	
5026. Zibersegurtasunaren arloko araudia.	Informatika. Sistema elektronikoak. Sistema elektroteknikoak eta automatikoak.	Bigarren Hezkuntzako irakaslea.
	Irakasle espezialista.	
E300. Oinarrizko funtsak.	Informatika.	Bigarren Hezkuntzako irakaslea.
E301. Prestakuntza praktiko duala enpresetan.	Informatika. Sistema elektronikoak. Sistema elektroteknikoak eta automatikoak.	Bigarren Hezkuntzako irakaslea.
	Ekipo elektronikoak. Informatika-sistemak eta aplikazioak.	Lanbide Heziketako irakasle teknikoa.

6.2. Irakatsi ahal izateko baliokideak diren titulazioak:

KIDEGOA	ESPEZIALITATEA	TITULAZIOAK
Bigarren Hezkuntzako irakaslea.	Informatika.	Estatistikan diplomaduna. Kudeaketa-informatikako ingeniari teknikoa. Sistema-informatikako ingeniari teknikoa. Telekomunikazio-ingeniari teknikoa, Telematikako espezialitatea.
	Sistema elektronikoak. Sistema elektroteknikoak eta automatikoak.	Ontzietako irrati-elektronikan diplomaduna. Aeronautikako ingeniari teknikoa, Aire-nabigazioko espezialitatea. Industria-ingeniari teknikoa, Elektrizitatea espezialitatea, Industria-elektronikako espezialitatea. Sistema-informatikako ingeniari teknikoa. Telekomunikazioetako ingeniari teknikoa, espezialitate guztietan.

Edo araudi erregulatzailean ager daitekeen beste edozein titulazio.

6.3. Hezkuntzaz bestelako administrazioetako titulartasun pribatuko ikastetxeetarako espezializazioa eta hezkuntza-administraziorako orientabideak ikastaroa osatzen duten lanbide-moduluak emateko behar diren titulazioak:

.

LANBIDE-MODULUAK	TITULAZIOAK
5021. Zibersegurtasun-gorabeherak. 5025. Hacking etikoa. 5026. Zibersegurtasunaren arloko araudia.	Doktorea, lizentziaduna, ingeniaria, arkitektoa, edo dagokion graduko titulua edo irakatsi ahal izateko beste zenbait titulu baliokide.

E300. Programazioaren, sareen eta sistema eragileen (eta kriptografiaren) oinarrizko funtsak.	
5022. Sareak eta sistemak gotortzea 5023. Ekoizpen seguruan jartzea. 5024. Auzitegi-analisi informatikoa.	Doktorea, lizentziaduna, ingeniaria, arkitektoa, edo dagokion graduko titulua edo irakatsi ahal izateko beste zenbait titulu baliokide. Unibertsitateko diplomaduna, arkitekto teknikoa edo irakatsi ahal izateko beste zenbait titulu baliokide.

6.4. Hezkuntzaz bestelako administrazioetako titulartasun pribatuko ikastetxeetarako espezializazioa eta hezkuntza-administraziorako orientabideak ikastaroa osatzen duten lanbide-moduluak emateko behar diren titulazioak:

LANBIDE-MODULUAK	TITULAZIOAK
5021. Zibersegurtasun-gorabeherak. 5025. Hacking etikoa. 5026. Zibersegurtasunaren arloko araudia.	Estatistikan diplomaduna. Ontzietako irrati-elektronikan diplomaduna. Aeronautikako ingeniari teknikoa, Aire-nabigazioko espezialitatea. Industria-ingeniari teknikoa, Elektrizitatea espezialitatea, Industria-elektronikako espezialitatea. Kudeaketa-informatikako ingeniari teknikoa. Sistema-informatikako ingeniari teknikoa. Telekomunikazioetako ingeniari teknikoa, espezialitate guztietan.
E300. Oinarrizko funtsak.	Estatistikan diplomaduna. Kudeaketa-informatikako ingeniari teknikoa. Sistema-informatikako ingeniari teknikoa. Telekomunikazio-ingeniari teknikoa, Telematikako espezialitatea.