III. ERANSKINA, 2021EKO XXX(E)KO XXX DEKRETUARENA

ERAGIKETA-TEKNOLOGIEN INGURUNEETAN ZIBERSEGURTASUNEKO ESPEZIALIZAZIO-IKASTAROA

1. Identifikazioa.

Izena: Zibersegurtasuna eragiketa-teknologien inguruneetan.
Maila: Goi-mailako Lanbide Heziketa.
Iraupena: 990 ordu.
Lanbide-arloa: Elektrizitatea eta elektronika (Lanbide Heziketako irakaskuntzak sailkatzeko bakarrik).
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:

- Sistema elektroniko eta automatizatuetako goi-mailako teknikariaren titulua, urriaren 22ko 222/2011 Dekretuaren bidez ezarritakoa; dekretu horren bidez, Sistema elektroniko eta automatizatuetako goi-mailako teknikariaren tituluari dagokion curriculuma ezartzen da.
- Mekatronika Industrialeko goi-mailako teknikariaren titulua, apirilaren 22ko 340/2013 Dekretuaren bidez ezarritakoa; dekretu horren bidez, Mekatronika Industrialeko goi-mailako teknikariaren tituluari dagokion curriculuma ezartzen da.
- Automatizazioko eta Robotika Industrialeko goi-mailako teknikariaren titulua, azaroaren 27ko 254/2012 Dekretuaren bidez ezarritakoa; dekretu horren bidez, Automatizazioko eta Robotika Industrialeko goi-mailako teknikariaren tituluari dagokion curriculuma ezartzen da.
- Telekomunikazio- eta informatika-sistemetako goi-mailako teknikariaren titulua, uztailaren 3ko 118/2012 Dekretuaren bidez ezarritakoa; dekretu horren bidez, telekomunikazio- eta informatika-sistemetako goi-mailako teknikariaren tituluari dagokion curriculuma ezartzen da.
- Mantentze-lan elektronikoetako goi-mailako teknikariaren titulua, apirilaren 22ko 341/2013 Dekretuaren bidez 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 segurtasun-estrategiak definitu eta ezartzea industria-erakunde eta -azpiegituretan; horretarako, zibersegurtasuneko diagnostikoak egin behar dira, eta ahuleziak identifikatu eta arintzeko behar diren neurriak ezarri behar dira, indarrean dagoen araudia eta sektoreko estandarrak aplikatuz, kalitate, laneko arriskuen prebentzio eta ingurumen-babeseko protokoloak betez.

3.2. Lanbide-ingurunea:

Espezializazio-ikastaro hori gainditu izana egiaztatzen duen ziurtagiria lortu duten pertsonek hainbat sektoretako erakundeetan lan egin ahal izango dute, non beharrezkoa den industria-prozesuen segurtasuna ezarri eta bermatzea.

Hauek dira zeregin eta lanpostu aipagarrienak:

- Aditua eragiketa-teknologien inguruneetako zibersegurtasunean.
- Auditorea eragiketa-teknologien inguruneetako zibersegurtasunean.
- Aholkularia eragiketa-teknologien inguruneetako zibersegurtasunean.
- Zibersegurtasuneko analista eragiketen inguruneetan.

3.3. Konpetentzia profesionalak, pertsonalak eta sozialak:

a) Erakundeetan arrisku-profilak zehaztea eta praktika onak, estandarrak eta aplikatzekoa den araudia identifikatzea.

b) Erakundeen ekipoak eta sistemak lerrokatuta daudela egiaztatzea, segurtasun informatikoaren eta zibersegurtasun-arriskuen printzipioei dagokienez.

c) Industriako ingurune eta sistemei buruzko zibersegurtasuneko txostenak egitea (teknikoak eta antolaketakoak), erabilitako segurtasun-elementuak ebaluatuta.

d) Zibersegurtasuneko estrategiak erabiltzea industriako proiektuen faseetan, gerta litezkeen gorabeheren eragina gutxitzeko.

e) Industria-kontrolaren sistemen eboluzioaren ezaugarriak finkatzea eta erakundean duen eraginaren balorazioa egitea.

f) Industria-kontrolaren sistemen konfigurazioa ezartzea eta erakundean arriskuak gutxitzea.

g) Sektorean aitortuta dauden metodologiak aplikatzea eta industria-sareetako arrisku teknologikoko egoeren balorazioa egitea.

h) Ahuleziak identifikatzea eta sareetako gailuen konfigurazioa ezartzea, ahalik eta arrisku-egoera gutxien egoteko.

i) Auzitegi-analisiak egitea industria-sare eta -sistemetan eta erakundean ahuleziak detektatzea.

j) Segurtasun fisikoko, eragiketa-segurtasuneko eta zibersegurtasuneko arauak eta prozedurak eragiketen inguruneetan txertatzea eta arriskuak gutxitzea.

k) Dokumentazio teknikoa eta administratiboa lantzea, indarreko legeriari eta bezeroen eskakizunei jarraikiz.

l) Lan-egoera berrietara egokitzea, eguneratuta edukiz bere lan-inguruneko ezagutza zientifikoak, teknikoak eta teknologikoak, bere prestakuntza eta bizialdi osoko ikaskuntzarako baliabideak kudeatuz.

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

n) 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.

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

4. Espezializazio-ikastaroaren irakaskuntzak

4.1. Helburu orokorrak:

a) Praktika onak, aplikazioaren estandarrak eta araudia aztertzea arrisku-profilak zehazteko.

b) Zibersegurtasuneko betekizunak zehaztu eta txertatzea industria-proiektu baten fase guztietan, gorabeherak ekiditeko.

c) OT inguruneetan teknologia aurreratu aplikagarriak identifikatu eta aplikatzea, segurtasun informatikoko printzipioekin eta zibersegurtasuneko arriskuekin bat egiten dutela egiaztatzeko.

d) Praktika profesionalak OT eta IT inguruneetan nola uztartzen diren aztertzea, eta zibersegurtasuneko estrategiak erabiltzeko eta industria-kontrolaren sistemen eboluzioaren ezaugarriak finkatzeko eskakizunak aztertzea.

e) Industria-kontroleko sistemak betekizun jakin batzuekin eta auditoretza-kontrolekin bat definitu eta parametrizatzea, sistema horien konfigurazioa ezartzeko.

f) Industria-sareen ekipoak eta konfigurazioak identifikatzea eta haien ezaugarriak finkatzea, egon daitezkeen ahulezien zerrendak egiteko.

g) Industria-instalazioen sareei lotutako arrisku-mailak ebaluatzea, ahuleziak identifikatzeko.

h) Auzitegi-analisiak egiteko tresnak hautatzea eta erabiltzea.

i) Industria-sareetako konfigurazioak definitzea eta aplikatzea, segurtasun-eskakizunak txertatzean ahalik eta arrisku gutxien egon dadin.

j) Auzitegiko analisiaren metodologiak aplikatzea SCADA, DCS, PLC sistemetan, robotika industrialean, IoT gailuetan eta industria-sareetan, segurtasun-prozedurak integratzeko.

k) Txostenak egitea auzitegi-analisiaren emaitzak eta ondorioak aurkezteko, dokumentazio teknikoa eta administratiboa egiteko.

l) Segurtasun fisikoari, eragiketa-segurtasunari eta zibersegurtasunari aplikatu beharreko araudia eta prozedurak zehaztea, segurtasun-arauak eta -prozedurak integratzeko.

m) Eragiketaren inguruneetan segurtasun-arriskuen kudeaketa integralerako metodologiak definitzea eta aplikatzea.

n) Bulegotikako eta ordenagailuz lagundutako diseinuko tresnak erabilita, hartzaileentzako informazio-eskuliburuak garatzea, dokumentazio teknikoa eta administratiboa lantzeko.

ñ) Sormena eta berrikuntzarako gogoa garatzea, lanarekin eta norberaren bizitzarekin lotutako prozesuetan eta antolamenduan agertzen diren erronkei erantzuteko.

o) Sektoreko bilakaera zientifikoarekin, teknologikoarekin eta antolamendukoarekin lotzen diren ikaskuntza-baliabideak eta -aukerak aztertzea eta erabiltzea, baita informazioaren eta komunikazioaren teknologiak ere, eguneratze-izpirituari eusteko eta laneko egoera berrietara eta egoera pertsonal berrietara egokitzeko.

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

q) Irisgarritasun unibertsalari eta «guztiontzako diseinua»ri erantzuteko beharrezkoak diren

lanbide-ekintzak identifikatzea eta proposatzea.

r) Kalitate-parametroak identifikatzea eta aplikatzea ikaskuntza-prozesuan egindako lanetan eta jardueretan, ebaluazioaren eta kalitatearen kultura baloratzeko eta kalitate-kudeaketako prozedurak hobetzeko.

4.2. Lanbide-moduluak.

KODEA	LANBIDE-MODULUA	ORDU-KOPURUA
5027	Zibersegurtasuna industria-proiektuetan.	120
5028	Industria-kontroleko sistema seguruak.	144
5029	Industriako komunikazio-sare seguruak.	168
5030	Industriako zibersegurtasunari buruzko auzitegi-analisia.	192
5031	Segurtasun integrala.	96
E304	Prestakuntza praktiko duala enpresan	270
GUZTIRA		990

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

1. lanbide-modulua: Zibersegurtasuna industria-proiektuetan.

Kodea: 5027.
Iraupena: 120 ordu.
ECTS kredituak: 6.

Ikaskuntzaren emaitzak, ebaluazio-irizpideak eta edukiak.

RA1. Industria-proiektu baten diseinuan sartu beharreko zibersegurtasun-elementuak zehazten ditu, antolakuntzan ezarritako segurtasuna aztertuz.

Ebaluazio-irizpideak:

a) Industria-proiektuaren diseinua ebaluatu du: irismena, finantzako bideragarritasunari buruzko azterlanak eta betekizun teknikoak, antolaketakoak eta prozedurakoak.
b) Proiektuan parte hartzen duten eragileak eta arduradunak identifikatu ditu, bai eta zibersegurtasunaren arloko funtzioak eta eskumenak ere.
c) Mehatxuen ezaugarriak finkatu ditu eta proiektua automatizatzeko teknologien osagaien ahuleziak identifikatu ditu.
d) Zibersegurtasuna inplikatutako eragileetatik (bezeroa, ingeniaritza eta fabrikatzaileak) kontuan hartzen duten azterlanak garatu ditu.
e) Zibersegurtasuneko betekizunak, fluxuak eta interakzioak definitu ditu proiektuaren automatizazio-mailetarako.

Edukiak: Zibersegurtasun-jarduerak industria-proiektu baten diseinuan.

− Proiektuaren diseinu kontzeptuala. Proiektuaren eta erakundearen bizi-zikloa – PMBOKen oinarritutakoa.
− Bideragarritasunari buruzko proiektu-azterlanaren aldez aurreko diseinua.
− Oinarrizko ingeniaritza edo proiektuaren plan zehatza.
− Xehetasuneko ingeniaritza edo teknologien automatizazioko maila bakoitzean erabiltzen diren teknologien definizioa eta beraien arteko interakzioa.
− Zibersegurtasun-jarduerak diseinu fasean.

RA2. Erosketak kudeatzeko planak ezartzen ditu, eta hornitzaileek bete behar dituzten segurtasun-eskakizunak finkatu.

Ebaluazio-irizpideak:

a) Erosketak kudeatzeko prozesua ezarri du hornitzaileentzat.
b) Erosketak kudeatzeko prozesuaren oinarrizko dokumentuak ezarri ditu.
c) Hornitzaileen zibersegurtasun-eskakizunen ebaluazioa egin du.
d) Hornidura-katearekin lotutako arriskuen analisia eta kudeaketa egin du.
e) Zibersegurtasuneko eskakizunak ezarri ditu erosketak kudeatzeko prozesuan.
f) Horniduran ezarritako zibersegurtasuneko eskakizunen betetze-maila ebaluatu du.

Edukiak: Zibersegurtasuneko eskakizunak erosketak kudeatzeko prozesuan.

− Erosketak kudeatzeko prozesua ezartzea eta beraren oinarrizko dokumentuak egitea.
− Hornitzaileen zibersegurtasun-eskakizunen ebaluazioa. “Hornitzaileek bete beharreko zibersegurtasuneko eskakizunen ebaluazioa egiteko tresna”.
− Hornidura-katearen arriskuen analisia eta kudeaketa.
− «Muturretik muturrera» zibersegurtasun-neurriak ezartzea.

RA3. Industria-proiektu bat gauzatzeko eta abiarazteko zibersegurtasun-neurriak ezartzen ditu, kalitate eskakizunak beteta.

Ebaluazio-irizpideak:

a) Proiektua gauzatu eta abiaraztean, zibersegurtasuneko erantzukizunak eta funtzioak aztertu ditu.
b) Aldez aurretiko inpaktu-analisia egin du, zibersegurtasuneko neurriak identifikatzeko.
c) Zibersegurtasuneko neurrien plan zehatz bat ezarri du.
d) Segurtasunaren ebaluazioaren esparru metodologikoa ezarri du.
e) Ekonomia zirkularraren printzipioak kontuan hartu ditu.
f) Zibersegurtasun-irizpideak sartu ditu onarpen-probetan (FAT).
g) Segurtasun-irizpideak sartu ditu onarpen-probetan.
h) Kalitate eta auditorietako kontrol planak ezarri ditu.
i) Zibersegurtasunaren ebaluazioa kontuan hartu du.

Edukiak: Zibersegurtasun-neurriak industria-proiektua gauzatu eta abiaraztean.

− Proiektua eraikitzea.
− Ekonomia zirkularraren printzipioak 4.0. industrian.
− Euskarri-jarduerak proiektuaren eraikuntzan gehitzea.
− Segurtasun fisiko eta logikoaren plan zehaztua gauzatzea.
− Bideragarritasuna ebaluatzeko metodoak.
− Ingeniaritzari buruzko dokumentazioa eguneratzea.
− Lantegiko onarpen-probak
− Neurketak instalazioetan.
− Kalitate eta auditorietako kontrol planak gauzatzea.

RA4. Industria-proiektu baten eragiketa- eta mantentze-faseko zibersegurtasun-jarduerak ezartzen ditu, egindako jarduerak dokumentatuta.

Ebaluazio-irizpideak:

a) Instalazioan zibersegurtasun arloko hobekuntzak identifikatu ditu.
b) Instalazioan zibersegurtasun arloko hobekuntzak ezarri ditu.
c) Aldaketa-kudeaketako prozesu bat ezarri du, zibersegurtasunaren kudeaketari eragin ahal dioten eragiketa-hobekuntzak sartzeko.
d) Eragiketa-faseko zibersegurtasun-jarduerak ezarri ditu.
e) Mantentze-faseko zibersegurtasun-jarduerak ezarri ditu.
f) Zibersegurtasun-prozedurak dokumentatu ditu, industria-proiektu baten mantentze- eta

eragiketa-faserako.

g) Zibersegurtasun arloko kontzientziazio eta prestakuntzako planak ezarri ditu.

Edukiak: Zibersegurtasun-jarduerak industria-proiektu baten mantentze- eta eragiketa-fasean.

− Eragiketaren optimizazioaren eta hasierako jarraipenaren aldia.
− Aldaketa-kudeaketaren prozesua.
− Eragiketa- eta mantentze-faseko zibersegurtasun-jarduerak.
  - Eragiketa-faseko zibersegurtasun-jarduerak: hardware, software, sare eta sarbideen kontrola eta kudeaketa, ahulezien kudeaketa eta eraso-bektoreen monitorizazioa.
  - Mantentze-faseko zibersegurtasun-jarduerak: segurtasuneko eta lehengoratzeko kopiak, gorabeheren monitorizazioa eta kudeaketa, kontingentzia planak.
− Eragiketa- eta mantentze-faseko dokumentazioa.
− Kontzientziazio- eta prestakuntza-plana.

RA5. Zibersegurtasun-jarduerak ezartzen ditu instalazioak eraisteko lanetan, sistemen suntsipenean eta/edo kontserbazioan ezarritako eskakizunak modu seguruan betez.

Ebaluazio-irizpideak:

a) Zibersegurtasun-jarduerak definitu ditu proiektuaren instalazioak desmuntatzeko, deskontaminatzeko, desklasifikatzeko, eraisteko eta birjartzeko lanetan.

b) Sistemak suntsitzeko neurriak ezarri ditu.

c) Sistemak suntsitzeko neurriak egiaztatu ditu.

d) Sistemak kontserbatzeko neurriak ezarri ditu.

e) Sistemak kontserbatzeko neurriak egiaztatu ditu.

f) Ezarri eta egiaztatzeko prozesuetan antzemandako gorabeherak dokumentatu ditu.

g) Kontserbazio-prozesuan ezarritako neurriak dokumentatu ditu.

Edukiak: Zibersegurtasun-jarduerak instalazioen eraispenean.

− Desmuntatzeko, deskontaminatzeko, desklasifikatzeko, eraisteko eta birjartzeko jarduerak.
− Sistemen suntsipena kudeatzea, zibersegurtasunaren ikuspuntutik.
− Kontserbazioaren kudeaketa, zibersegurtasunaren ikuspuntutik.

2. lanbide-modulua: Industria-kontroleko sistema seguruak.

Kodea: 5028.
Iraupena: 144 ordu.
ECTS kredituak: 7.

Ikaskuntzaren emaitzak, ebaluazio-irizpideak eta edukiak.

RA1: *IT* (Informazioaren teknologiak) eta *OT* (eragiketaren teknologiak) teknologiak uztartzeko aldaketak ezartzen ditu, erakundeetan ingurune horien egoera aztertuz.

Ebaluazio-irizpideak:

a) Industrian eraldaketa digitaleko prozesuen ezaugarriak finkatu ditu.
b) Informazioaren teknologiak (IT) eta eragiketaren teknologiak (OT) kontzeptuak aztertu eta bereizi ditu.
c) IT eta OT inguruneetako beharrizan teknologikoak detektatu ditu.
d) Teknologia aurreratu aplikagarriak identifikatu ditu.
e) IT eta OT sailek teknologia aurreratuen arloan dituzten erronkak identifikatu ditu.
f) Teknologiak uztartzeko analisia egin du maila hauetan: lan-praktikak, antolaketa eta datuak ITrekin partekatzea.
g) Aldaketa nagusiak zehaztu ditu, profesionalizazio altua, etorkizuneko ikuspegia, lidergoa eta efizientzia eskatuko dituztenak.

Edukiak: *IT* eta *OT* teknologiak uztartzeko aldaketak.

− Eragiketa-teknologiak (OT), aldaketak egitea/antzematea prozesu fisikoetan, gailuen monitorizazioaren eta kontrolaren bidez.
− Informazioaren teknologiak (IT, datuen tratamendurako ekipo informatikoak).
− Teknologiak uztartzea errazteko aldaketa garrantzitsuak IT eta OT inguruneetan.

RA2: Sistema dinamikoen eta mugimendua kontrolatzeko sistemen kontrolean esku hartzen duten gailu programagarriak ezagutzen ditu, haien osagaiak, funtzionalitatea identifikatzen ditu eta industria-ingurune automatizatuetan dituzten aplikazioak zehazten ditu.

Ebaluazio-irizpideak:

a) Aplikazio automatikoak aztertu ditu seinale dinamikoak irakurtzeko eta kontrolatzeko, eta kontrol programatuko sistemaren egitura identifikatu du.
b) Gailu programagarrien ezaugarri teknikoak zehaztu ditu, behar den aplikazioaren arabera.
c) Identifikatutako industria-aplikazio batzuetan justifikatuta dago roboten eta mugimendua kontrolatzeko sistemen erabilera, eta roboten eta industria-manipulatzaileen tipologia eta ezaugarriak zehaztu ditu.
d) Gainbegiratzeko eta kontrolatzeko sistema batek eskaintzen dituen funtzioak automatizazioko industria-aplikazioekin lotu ditu.
e) Sistema automatiko osoa abiarazi du, eta sistema automatikoaren eskakizunen arabera diseinatutako kontrolatzeko, eskuratzeko eta gainbegiratzeko programen funtzionamendua egiaztatu du.

Edukiak: Gailu programagarriak eta industria-kontroleko sistemak.

− Kontrol-sistemen egitura.
- Automatizazio-piramidea.
- Automatizazio-teknologiak.

- Perdue eredua:
    - 0. maila: Instrumentazioko teknologia.
    - 1. maila: Kontrolagailuak eta DCS sistemak.
    - 2. maila: Scada, HMI.
    - 3. maila: EMS.
    - 4. maila: ERP.

− Seinale dinamikoak irakurtzeko eta kontrolatzeko aplikazio automatikoak.
− Gailu programagarrien ezaugarri teknikoak.
− Industria-sareak eta protokoloak.
− Mugimendua kontrolatzeko sistemak, eta industria-roboten tipologia eta ezaugarriak.
− Gainbegiratzeko eta kontrolatzeko sistemak automatizazioko industria-aplikazioekin.
− Sistema automatiko bat abian jartzea.
− Industriako zibersegurtasunaren arloko funtsezko termino eta kontzeptuen definizioa eta identifikazioa. Azpiegitura kritikoak, estrategikoak eta funtsezko zerbitzuak.

RA3. Arrisku teknologikoko egoeren balorazioa egiten du industria-instalazioetako kontrol-sistemetan, aitortuta dauden metodologiak erabiliz.

Ebaluazio-irizpideak:

a) Arriskuen Analisirako metodologia bat (AR) zehaztu du.
b) Industria-instalazio bat osatzen duten aktibo motak identifikatu ditu.
c) Aktiboetarako dauden mehatxu mota desberdinen ezaugarriak finkatu ditu.
d) Ahulezia ezagunei buruzko datu interesgarriak aurkitu ditu industria-kontroleko sistemetan.
e) Diagnostikorako tresnak alderatu ditu.
f) Egiaztagutunen segurtasuna eta sarbidea kontrolatzeko bideak identifikatu eta ebaluatu ditu.
g) Firmware eta/edo gailu baten konfigurazioa ebaluatu du alderantzizko ingeniaritzako prozeduren bitartez.
h) Gailu eta sistemen konfigurazioa egiaztatzeko ekintzak automatizatu ditu.
i) Industria-kontroleko sistema garrantzitsu baten testbed bat sortu du, beraren konfigurazioaren antzeko batekin.
j) Industria-instalazio baten kontrol-sistemei lotutako arrisku-zerrenda bat egin eta ordenatu du.

Edukiak: Arrisku teknologikoen egoeren ebaluazioa.

− Industria-kontroleko sistemen motak.
− Mehatxua eta mehatxu-motak.
− Arriskuaren ebaluazioa.
− Kanpo-arriskuak.
− Egiaztagutunen eta sarrerak kontrolatzeko sistemen motak.
− Ahulezia ezagunei buruzko informazioaren bilaketa industria-kontroleko sistemetan.
− Diagnostikorako tresnak.
− Testbed bikien sorrera.

RA4. Diagnostiko eta analisien prozesuak eta industria-instalazio baten beste prozesu batzuk dokumentatzen ditu, zibersegurtasunari dagokionez, konplexutasun-maila desberdinetako txostenak sortuz.

Ebaluazio-irizpideak:

a) Langile teknikoei eta zuzendaritzako kideei zuzendutako txostenen elementuak identifikatu ditu, haien arteko desberdintasunak ezarriz.

b) Zibersegurtasuneko diagnostikoari buruzko txosten tekniko bat egin du, zuzendaritzako kideei zuzenduta.

c) Zibersegurtasuneko diagnostikoari buruzko txosten tekniko bat egin du, eragiketen langile teknikoei zuzenduta.

d) Txosten teknikoaren komunikazioko tresnak eta teknikak identifikatu ditu hartzailearen arabera.

e) Emaitzei buruzko txostenak aurkezteko orduan gatazkak eta erretizentziak kudeatzeko erak garatu ditu.

f) Hobekuntzarako proposamenak jasotzeko diagnostikoko txosten teknikoak aztertu ditu.

Edukiak: Zibersegurtasun-prozesuen dokumentazioa.

− Txosten teknikoak egitea.
− Hizkuntza txostenaren hartzailearen arabera egokitzea.
− Zibersegurtasuneko diagnostikoari buruzko txosten teknikoak egitea, zuzendaritzako kideei eta eragiketen langile teknikoei zuzenduta.
− Txostenak egitea sareen arkitekturari, kontrol-sistemen konfigurazioari eta monitorizazioari buruz.
− Txostenak egitea SGCIren segurtasun-politikekin.
− Hobekuntzarako proposamenak jasotzeko diagnostikoko txosten teknikoak aztertzea.
− Txostenak egitea sareen arkitekturari, kontrol-sistemen konfigurazioari eta monitorizazioari buruzko txostenak aztertzea, hobekuntzarako proposamenak jasotzeko.
− Emaitzak aurkeztea.

RA5. Segurtasun-politikak diseinatzen ditu industria-kontroleko sistemetarako, kontuan hartuta egindako analisiak, sektorearen estandarrak eta aplikatzekoa den araudia.

Ebaluazio-irizpideak:

a) Pertsona, gailu eta sistemen autentifikazio-mekanismoak identifikatu ditu.

b) Sarbiderako egiaztagutunei alta, baja emateko eta mantentzeko prozedurak identifikatu ditu.

c) Industria-instalazio baten erabiltzaileak kudeatzeko prozesuak egin ditu, erakunde baten politikekin bat etorrita.

d) Industria-instalazio bateko eremu desberdinetan sartzeko kontrolerako eta segurtasun fisikorako politikak egin eta justifikatu ditu.

Edukiak: Segurtasun-politiken diseinua.

− Pertsona, gailu eta sistemen identifikazioa.
− Rolak, erabiltzaileak eta baimenak kudeatzea.
− Segurtasun fisikorako eta sarbide-kontrolerako politikak.

RA6. Industria-kontroleko sistemak konfiguratzen ditu, ahalik eta arrisku-egoera gutxien egon dadin.

Ebaluazio-irizpideak:

a) Industria-kontroleko sistemak eguneratzeko eta segurtasun-adabakiak jartzeko segurtasun-eskakizunak identifikatu ditu.
b) PCetan oinarritutako industria-kontroleko sistemen antibirusak kudeatzeko segurtasun-eskakizunak identifikatu ditu.
c) Industria-kontroleko sistemen konfigurazioen eta informazioaren segurtasun-kopien segurtasun-eskakizunak identifikatu ditu.
d) Industria-kontroleko sistemak konfiguratu eta parametrizatu ditu, ezarritako babes-eskakizunekin bat.
e) Industria-kontroleko sistemak konfiguratu eta parametrizatu ditu, ezarritako auditoretza-kontrolekin bat.

Edukiak: Industria-kontroleko sistemen konfigurazioa.

− Erabiltzaileen eta/edo sistemak kontrolatzeko gaitutako IP helbideen konfigurazioa.
− Erregistroak (Log-ak) kanpoko sistemetara bidaltzea.
− Sistemen eguneratzea kudeatzea.
− Nahi den konfigurazioaren eta haren zaintzaren segurtasun-kopiak.

RA7. Anomaliak aurkitzen ditu industria-kontroleko sistemetan, analisien monitorizazio- eta prozedura- tresnen bidez.

Ebaluazio-irizpideak:

a) Segurtasun-gertaeren monitorizazio-tresnak identifikatu ditu eta haien ezaugarriak finkatu.
b) Industria-kontroleko sistema konektatuak automatikoki aurkitzeko monitorizazio-tresnak konfiguratu ditu.
c) Monitorizazio-tresnen gaineko jardun-arauak definitu ditu, monitorizatu nahi diren gertaerak ezartzeko.
d) Segurtasun-gertaeren kudeatzaile baten portaeraren oinarrizko printzipioak identifikatu ditu (SIEM, Security Information and Event Management).
e) Portaera susmagarriak antzeman ditu.
f) Aurkitu diren anomaliak dokumentatu ditu.

Edukiak: Anomalien detekzioa industria-kontroleko sistemetan.

− Industria-kontroleko sistemen monitorizazioa.
− Segurtasun-gertaeren monitorizazio-tresnak.
− Aktiboak automatikoki aurkitzeko tresnak.
− Sinaduretan oinarritutako jardun- eta ikuskapen-arauak.

3. lanbide-modulua: Industriako komunikazio-sare seguruak.

Kodea: 5029
Iraupena: 168 ordu
ECTS kredituak: 9

Ikaskuntzaren emaitzak, ebaluazio-irizpideak eta edukiak.

RA1: Elementuak eta ekipamenduak sare kableatuetan eta hari gabekoetan integratzen ditu, eta haien aplikazio-eremua ebaluatzen du.

Ebaluazio-irizpideak:

a) Sare kableatuetarako eta hari gabekoetarako estandarrak identifikatu ditu.
b) Ekipoak eta sareen elementuak identifikatu ditu.
c) Sareen ekipoen funtzioak bereizi ditu.
d) IP helbideratze logikoko sistema erabili du sareko helbideak eta azpisare-maskarak esleitzeko.
e) Sare-moldagailu kableatuak eta hari gabekoak konfiguratu ditu hainbat sistema eragiletan.
f) Sare-zerbitzu eta aplikazioak identifikatu ditu.

Edukiak: Elementuak eta ekipamendua sare kableatuetan eta hari gabekoetan.

− Sareetan gehien erabiltzen diren estandarren eta protokoloen identifikazioa: TCP/IP, Ethernet, IEEE 802 eta haien eratorriak, ekipo informatikoen arteko komunikazioaren aplikazio-eremua ebaluatzeko.
− Sareko ekipoen eta gailuen identifikazioa, esaterako: Sare-txartelak, kommutadoreak (switch), routerrak, firewall sistemak, zerbitzariak... eta haien aplikazio-eremua.
− IP helbideratze-sistema.
− Sare-zerbitzu eta aplikazioen identifikazioa, esaterako, urruneko sarbide-sistema, http eta https web zerbitzuak, autentifikazio-zerbitzuak, IP helbideen (DHCP) esleipena, DNS zerbitzua...

RA2: Industria-ingurune automatizatu baten segurtasun-mailak zehazten ditu, erabilitako komunikazio eta protokoloen ezaugarriak aztertuz eta segurtasun-eskari berriei irtenbideak proposatuz.

Ebaluazio-irizpideak:

a) Fabrikatzaile desberdinen kontrol-gailuen ezaugarriak finkatu ditu industria-ingurune automatizatu batean.
b) Ikuskapenaren eta SCADA sistemen (datuak ikuskatu, kontrolatu eta eskuratzeko sistemak) elementuak deskribatu ditu.
c) Optimizazio eta kudeaketa-sistemak identifikatu ditu.
d) Industriaren automatizazio arlo desberdinetako segurtasun-mailak zehaztu ditu (eremua, kontrola, ikuskapena, optimizazioa eta kudeaketa).
e) Aztertutako sistemaren eta etorkizuneko sistemaren arteko aldeak ezarri ditu, segurtasunari dagokionez.
f) Egokitzeko proposamenak dokumentatu ditu, segurtasunari dagokionez eta eskari berriekin bat.

Edukiak: Segurtasun-mailak industria-ingurune automatizatu batean.

− Industria-automatizazioko prozesuak. Automatizazio-piramidea.
  - Prozesu-maila (gailu fisikoan, hala nola sentsoreak, jarduleak...).
  - Kontrol-maila (gailu logikoak, hala nola PCak, PLCak, DCS, UTR, PAC...).
  - Ikuskapen-maila (datuak ikuskatzeko eta eskuratzeko sistemak, hala nola SCADA edo HMI).
  - Plangintza-maila (MES fabrikazioaren exekuzio-sistemak).
  - Kudeaketa-maila (ERP kudeaketa- eta plangintza-sistemak).

− Merkatuan eskuragarri dauden kontrol- eta ikuskapen-gailuak.

− Merkatuan eskuragarri dauden industria-komunikazio eta -protokolo aurreratuen aukerak: Common Industrial Protocol (CIP), MODBUS, DNP3, Profibus, Profinet, Powerlink Ethernet, OPC, therCAT, besteak beste.

− OPC UA komunikazioa, zeinak ahalbidetzen baitu industria-ekipoen eta -sistemen arteko komunikazioa, datuen bilketa eta kontrolerako.

− ISA99/IEC62443 estandarra.

RA3: Arrisku teknologikoko egoeren balorazioa egiten du industria-sareetan, aitortuta dauden metodologiak erabiliz.

Ebaluazio-irizpideak:

a) Industria-instalazio baten sarea osatzen duten gailu motak identifikatu ditu.
b) Industria-instalazio baten sare fisiko eta logiko baten arkitekturaren ezaugarriak finkatu ditu.
c) Industria-instalazio baten sarean egon beharko liratekeen segurtasun-eremuak identifikatu ditu.
d) Industria-instalazio baten sareari lotutako arriskuak sailkatu ditu.
e) Industria-instalazio baten sareari lotutako arrisku-maila ebaluatu du.

Edukiak: Industria-sareetan arrisku teknologikoen egoeren ebaluazioa.

− Industria-sare baten gailu motak.
− Sare fisiko eta logikoaren arkitektura.
− Industria-sare baten elementuak eta ekipoak.
− Zonifikazioa (kontrol-sarea, ikuskapen-sarea, sare korporatiboa...).
− Arriskuaren ebaluazioa.

− Kanpoko arriskuak (droneen arriskua industria-inguruneetan, industria-eraikinen automatizazio-sistemen arriskua (IoT), pertsona enplegatuen jabetzako gailuen arriskua (BYOD), geolokalizazio aktibatuaren zerbitzua duten gailuen ondoriozko arriskua...).

RA4: Industria-sareak ezartzen ditu switching eta bideratze-teknikak erabiliz.

Ebaluazio-irizpideak:

a) Industria-sareetan switching teknikaren ezaugarriak finkatu ditu.
b) Topologiak ezarri ditu industriako Ethernet-en.
c) Eraztun-topologiak ezarri ditu.
d) Eraztunen artean segmentu-akoplamenduak ezarri ditu modu erredundantean.
e) OT sareak eta IT sareak elkarrekin konektatu ditu.
f) Sarearen trafikoa sareko analizatzaileekin aztertu du.
g) Industria-sareetan bideratze-teknikaren ezaugarriak finkatu ditu.
h) Konexio sinpleak sare ofimatikoekin ezarri ditu (OT eta IT).
i) Konexio erredundanteak sare ofimatikoekin ezarri ditu.
j) Legacy sareetarako konexioak ezarri ditu.
k) Sareetarako konexioak ezarri ditu, bidearen detekzio automatikoarekin.
l) Bideratzearen murrizketak ezarri ditu ACLen bidez.
m) Sare pribatu birtualetan (VPN) autentifikazio-gailuak eta -protokoloak konfiguratu ditu.
n) Esku-hartzeak dokumentatu ditu.

Edukiak: Industria-sareak ezartzea switching eta bideratze-teknikak erabiliz.

− Switching-aren teknikak aztertzea industria-sareetan.
− LAN, MAN, WAN, GAN.
− Ohiko topologiak Industriako Ethernet-en, sarearen eremu logikoak, haien arteko interkonexioak eta sistemak adierazita.
− Eraztun-topologiak HRP Hihg-Speep Redundancy Protocol-arekin.
− Eraztunen artean segmentu-akoplamenduak ezartzea modu erredundantean.
− RSTP (Rapid Spanning Tree Protocol).
− RSTP protokoloaren eta eraztunen arteko konexio erredundanteak.
- Automatizazio-segmentuen eta IT sareen arteko akoplamenduak.

− Topologiak PRP (Parallel Redundancy Protocol) eta HSR (High-Availability Seamless Redundancy Protocol) protokoloekin.
− Bideratzea industria-sareetan.
− Konexio sinpleak sare ofimatikoekin (OT eta IT).
− Bideratze-taulak.
− AAA eta 802.1x erabiltzea LAN terminalak eta terminal-guneak eta gailuak autentikatzeko.
− Konexio erredundanteak sare ofimatikoekin VRRP bidez (Virtual Router Redundancy Protocol).
− Legacy sareetarako konexioak RIP bidez (Routing Information Protocol).
− Latentzia-probak ping eta traceroute bezalako komandoekin.

RA5: Industria-sare hari gabekoak ezartzen ditu sektorearen estandarrak erabiliz.

Ebaluazio-irizpideak:

a) Hari gabeko teknologien ezaugarriak finkatu ditu.
b) Zelulen antolaera- eta sarbide-metodoak ezarri ditu.
c) Roaming ezarri du.
d) Sarbide-puntuen kokapena identifikatu du.

e) Antenak hautatu ditu.
f) Industria-instalazioetarako wifi sareak diseinatu ditu.
g) Industria-instalazioetarako wifi sareak ezarri ditu.

Edukiak: Hari gabeko industria-sareak ezartzea.

− Wireless teknologiak (WIMAX, IWLAN, Bluetooth, WirelessHart).
− WLAN estandarra.
− Zelulen antolaera- eta sarbide-metodoak.
− Roaming.
− Segurtasuna (TKIP eta WPA2) eta transmisio-tasak. Autentifikazio-teknikak.
− Enkriptatzea.
− WDS (Wireless Distribution System).
− PCF (Point Coordinated Function) eta DCF (Distributed Coordination Function) arteko desberdintasuna.
− Wifi komunikazioak denbora errealean – determinismoa wifi-n (iPCF).
− ARP taulak.
− Hari gabeko gailu faltsuak detektatzeko administrazio-sistemak.
− RADIUS sistemak eta sarbideak kontrolatzeko beste sistema batzuk.

RA6: Urruneko sarbideak ezartzen ditu industria-inguruneetan, komunikazioen segurtasuna bermatuta.

Ebaluazio-irizpideak:

a) Urruneko komunikazio erabilienen ezaugarriak finkatu ditu.
b) Komunikazio seguruak ezarri ditu komunikazio ez seguruen bidez.
c) Industriako sare pribatuak sare publikoetara konektatu ditu, hainbat teknologia aplikatuz.
d) Urruneko sarbideak ezarri ditu, gutxieneko azaleraren printzipioan oinarrituta.
e) Cloud zerbitzu erabilienak (IAAS, PAAS, SAAS eta beste batzuk) identifikatu eta haien ezaugarriak finkatu ditu.
f) Komunikazioen integritatea egiaztatu du.

Edukiak: Urruneko sarbide seguruak ezartzea industria-sareetan.

− Urruneko komunikazioak (LAN, WAN, MAN eta GAN).
− Komunikazio seguruak sare ez seguruen bidez (VPN).
− IPsec VPN eta OpenVPN.
− Industria-sare pribatuen eta sare publikoen interkonexioa: NAT (Network Address Translation).
− Gutxieneko eraso-azaleraren printzipioa urruneko sarbideak ezartzeko orduan.
− Paketeak ikuskatzeko sistema, egoera, ikusgaitasuna eta aplikazio-kontrola.
− URLren iragazketa.
− Urruneko sarbidearen aplikazioak, hala nola telnet, SSH eta HTTPS.

RA7: Automatizazio-sarea diseinatzen du beharrezko segmentazioa aplikatuz erakundearen sareetan.

Ebaluazio-irizpideak:

a) Segmentazioa automatizazio-sareetan ezarri du.
b) VLANak sareak egituratzeko ezarri ditu.
c) VLAN estatiko eta dinamikoetan ekipoak esleitu ditu.
d) VLANei lehentasuna eman die.
e) Automatizazioko zelulen segmentazioak egin ditu suebaki industrialen bidez.
f) IT eta OT inguruneen arteko segmentazioak egin ditu NGF bidez (Next Generation Firewall).

Edukiak: Automatizazio-sarearen diseinua segmentazioaren bidez.

− Segmentazioa automatizazio-sareetan.
− Segmentazioa eremuetan: gutxienez, 3 eremutan, Kontrol Sarea, DMZ eta LAN korporatiboa. Eremuak trusted edo untrusted (konfiantzazkoa edo ez) izan daitezke.
− Sareen egituraketa VLAN sareekin: estatikoak eta dinamikoak.
− Komunikazioaren zifratua eta sareko segmentuen arteko banaketa logikoa, VLAN eta VPN teknologiak erabiliz.
− Zelularen segmentazioa suebaki industrialen bidez.
− IT eta OT inguruneen arteko segmentazioa NGFrekin (Next Generation Firewall).
− ISA 99-IEC 62443 segmentazioa.

RA8: Ahuleziak, mehatxuak eta erasoak identifikatzen ditu industria-sareetako gailuetan, kontraneurriak proposatuz.

Ebaluazio-irizpideak:

a) Ahuleziak, mehatxuak eta erasoak identifikatu ditu industria-sare eta gailuetan.
b) Ahulezien, mehatxuen eta erasoen irismena baloratu du.
c) Diagnostikorako tresnen ezaugarriak finkatu ditu.
d) Diagnostikorako tresnak eta egoera desberdinetako aplikazioa erlazionatu ditu.
e) Gailuen konfigurazioa eta sareak egiaztatzeko ekintzak automatizatu ditu.
f) Industria-sare bateko segmentu garrantzitsu baten testbed biki bat sortu du, gailuen eta sarearen konfigurazioa imitatuz.
g) Sarpen-test sakonak egin ditu industria-instalazio bateko testbed biki batean.

Edukiak: Ahulezia eta erasoen identifikazioa industria-sareetako gailuetan.

− Ahulezia ezagunei buruzko informazioaren bilaketa industria-sareetako gailuetan.
− Diagnostikorako tresnak.
− Testbed bikiak sortzea.
− Sarpen-test ez intrusiboak, ekoizpen-prozesuaren jarraitutasuna bermatzen dutenak.
− MAC taulen aurkako erasoak eta helbideak ordezteko erasoak.
− DoS erasoak.

RA9. Gorabeherak antzematen ditu denbora errealean industria-sareetan, analisietarako prozedurak eta tresna egokiak erabiliz.

Ebaluazio-irizpideak:

a) Industria-inguruneetan trafikoaren analisirako tresnen ezaugarriak finkatu ditu.
b) Tresnak beren prestazioen arabera hautatu ditu.
c) Intrusioak antzemateko sistema bat diseinatu, konfiguratu eta ezarri du (IDS, Intrusion Detection System) industria-kontroleko sistemetarako.
d) Azpiegitura batean portaera susmagarriak antzeman eta ikertu ditu, sareko trafikoaren analisiaren bidez.
e) Antzemandako portaera anomaloak dokumentatu ditu.

Edukiak: Gorabeheren detekzioa industria-sareetan, denbora errealean.

− Trafikoaren analisia.
− Intrusioen detekziorako sistemak (IDS, IPS).
− Industria-protokoloen portaeretan oinarritutako detekzio-sistemak.

RA10: Egiaztatze- eta ikuskatze-prozedurak definitzen ditu, segurtasun-politiken betetzearen metrikak lortuz.

Ebaluazio-irizpideak:

a) Segurtasun-politikak betetzeko metrikak identifikatu ditu.
b) Industria-kontroleko sistemen erregistroak aztertu ditu, segurtasun politiketan baimendu gabeko aldaketak detektatzeko.
c) Industria-automatizazioko sareen monitorizazio-tresnen ezaugarriak finkatu ditu.
d) Sareen monitorizazio-tresnak instalatu ditu.
e) Monitorizazioaren emaitzak dokumentatu ditu.

Edukiak: Egiaztatze- eta ikuskatze-prozeduren definizioa.

− Politikak betetzearen metrikak.
− Erregistroen kudeaketa (Log-ak).
− Kommutadoreen eta sareetako beste gailu batzuen monitorizazioa.
− Sareko monitorizazio-sistemak (SNMP, SSH, web, etab.): eskuzkoa, automatikoa.
− Azpiegiturari eta zerbitzuaren kudeaketari buruzko informazioaren erregistro-sistemak, esaterako, CMDB eta informazioaren beste erregistro-sistema batzuk.

RA11: Industria-sareetako gailuak konfiguratzen ditu, ahalik eta arrisku-egoera gutxien egon dadin.

Ebaluazio-irizpideak:

a) Gailuen babeserako parametroak zehaztu ditu.
b) Sareko gailuak konfiguratu ditu, geroago haien auditoretza egin ahal izateko.
c) Segurtasun-eskakizunak identifikatu ditu sareko gailuetako firmware eguneratzeko.
d) Segurtasun-eskakizunak identifikatu ditu sareko gailuen konfigurazioen segurtasun-kopietarako.
e) Sareko gailuak konfiguratu ditu definitutako babes-parametroekin bat etorrita.

Edukiak: Industria-sareetako gailuen konfigurazioa.

− Erabiltzaileen eta/edo gailuak kontrolatzeko gaitutako IP helbideen konfigurazioa.
− Firewall sistemen eta ekitaldi-erregistroen (log) konfigurazioa.
− Gailuen firmware-aren eguneratzeen kudeaketa.
− Nahi den konfigurazioaren eta haren zaintzaren segurtasun-kopiak.

4. lanbide-modulua: Industriako zibersegurtasunari buruzko auzitegi-analisia.

Kodea: 5030.
Iraupena: 192 ordu
ECTS kredituak: 11.

Ikaskuntzaren emaitzak, ebaluazio-irizpideak eta edukiak.

RA1. Auzitegi-analisiaren metodologiak aplikatzen ditu, babes-, eskuraketa-, analisi- eta dokumentazio-faseen ezaugarriak finkatuz.

Ebaluazio-irizpideak:

a) Aztertu nahi diren gailuak identifikatu ditu, ebidentzien babesa bermatzeko.
b) Ebidentziak eskuratu eta ateratzeko tresna eta mekanismo egokiak erabili ditu.
c) Eszena segurtatu eta zaintza-katea kontserbatu du.
d) Egindako prozesua zehatz-mehatz dokumentatu du.
e) Ebidentzien denbora-lerroa kontuan hartu du.
f) Ondorioen txosten bat egin du maila tekniko eta exekutiboan.
g) Auzitegi-analisiaren ondorioak aurkeztu eta azaldu ditu.

Edukiak: Auzitegi-analisien metodologiak erabili dira.

− 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).
− Hegakortasunaren analisia.
– Informazioa ateratzea (Volatility).
− Logen analisia, tresnarik erabilienak.

RA2. Auzitegi-analisiaren prozesuak garatzen ditu industria-kontroleko sistemetan, aitortutako metodologiak erabiliz.

Ebaluazio-irizpideak:

a) Aztertu nahi diren gailuak identifikatu ditu, ebidentzien babesa bermatzeko.

b) Ebidentziak eskuratu eta ateratzeko tresna eta mekanismo egokiak erabili ditu.

c) Ebidentzien eskuzko analisiak egin ditu.

d) Ebidentzien analisiak tresna automatikoen bidez egin ditu, auzitegi-ikerketari erantzuna emateko.

e) Egindako analisiaren prozesua zehatz-mehatz dokumentatu du, urrats guztien erreprodukzioa bermatzeko.

f) Ebidentzien denbora-lerroa, zaintza-katea eta maila tekniko eta exekutiboko ondorioen elaborazioa kontuan hartu ditu.

g) Auzitegi-analisiaren ondorioak dagozkien solaskideei jakinarazi dizkie.

Edukiak: Auzitegi-analisiaren prozesua industria-kontroleko sistemetan.

− Locard-en printzipioa.
− Auzitegi-analisien motak.
− Zaintza-katea.
− Hash funtzioak.
− Ezkutatze-sistemak.
− Memoria-iraulketa.
− Ebidentzia hegakorrak, ez-hegakorrak eta bidean direnak ateratzea.
− Ebidentzia hegakorren, ez-hegakorren eta bidean direnen analisia eskuzko tresnen bidez.
− Ebidentzia hegakorren, ez-hegakorren eta bidean direnen analisia tresna automatizatuen bidez.
− Euskarrien ezabaketa segurua.

RA3. Auzitegi-analisiaren prozesua garatzen du kontroleko sistemetan eta kontrolagailu logiko programagarrietan, aitortutako metodologiak erabiliz.

Ebaluazio-irizpideak:

a) Gainbegiratzeko, kontrolatzeko eta datuak eskuratzeko sistemak (SCADA), kontrol banatuko sistemak (DCS) eta kontrolagailu logiko programagarriak (PLC) identifikatu ditu, ebidentziak babestea bermatzeko.

b) Ebidentziak eskuratzeko eta ateratzeko mekanismo eta tresna egokiak erabili ditu, haien autentikotasuna, osotasuna, fidagarritasuna eta legezkotasuna bermatzen dituztenak.

c) Ebidentziak eskuz eta tresna automatizatuen bidez aztertu ditu, auzitegi-ikerketei erantzuna emateko.

d) Egindako analisiaren prozesua dokumentatu du, urrats guztien erreprodukzioa bermatzeko.

e) Ebidentzien denbora-lerroa, zaintza-katearen mantentzea eta maila tekniko eta exekutiboko ondorioen elaborazioa kontuan hartu ditu.

f) Auzitegi-analisiaren ondorioen jakinarazpen formala egin die dagozkien solaskideei.

Edukiak: Auzitegi-analisiaren prozesua kontroleko sistemetan eta kontrolagailu logiko programagarrietan.

− Hash funtzioak sistemetan.
− Ezkutatze-sistemak sistemetan.
− Sistemetan ebidentzia hegakorrak, ez-hegakorrak eta bidean direnak ateratzea.

− Ebidentzia hegakorren, ez-hegakorren eta bidean direnen analisia sistemetan, eskuzko tresnen bidez.

− Ebidentzia hegakorren, ez-hegakorren eta bidean direnen analisia sistemetan, tresna automatizatuen bidez.

− Sistemen ezabaketa segurua.

RA4. Auzitegi-analisiaren prozesua industria-robotikan garatzen du, aitortutako metodologiak erabiliz.

Ebaluazio-irizpideak:

a) Aztertu nahi diren industria-gailuak identifikatu ditu, ebidentzien babesa bermatzeko.

b) Ebidentzia egokiak eskuratu eta ateratzeko beharrezko mekanismo eta tresnak erabili ditu, haien autentikotasuna, osotasuna, fidagarritasuna eta legezkotasuna bermatzen dituztenak.

c) Ebidentzien analisiak eskuz eta tresna automatikoen bidez egin ditu, auzitegi-ikerketei erantzuna emateko.

d) Egindako analisiaren prozesua zehatz-mehatz dokumentatu du, urrats guztien erreprodukzioa bermatzeko.

e) Ebidentzien denbora-lerroa, zaintza-katearen mantentzea eta maila tekniko eta exekutiboko ondorioen elaborazioa kontuan hartu ditu.

f) Auzitegi-analisiaren ondorioen jakinarazpen formala egin die dagozkien solaskideei.

Edukiak: Auzitegi-analisiaren prozesuaren garapena industria-robotikan.

− Hash funtzioak industria-gailuetan.

− Ezkutatze-sistemak industria-gailuetan.

− Ebidentzia hegakorrak, ez-hegakorrak eta bidean direnak ateratzea industria-gailuetan.

− Ebidentzia hegakorren, ez-hegakorren eta bidean direnen analisia industria-gailuetan, eskuzko tresnen bidez.

− Ebidentzia hegakorren, ez-hegakorren eta bidean direnen analisia industria-gailuetan, tresna automatizatuen bidez.

− Ezabatuta segurua industria-gailuetan.

RA5. Auzitegi-analisiaren prozesua garatzen du Gauzen Internet-eko gailuetan (IoT), industria-sektoreetako eta osasun, garraio, eraikuntza... sektoreko gailuetan, aitortutako metodologiak erabiliz.

Ebaluazio-irizpideak:

a) Aztertu nahi diren gailuak identifikatu ditu, ebidentzien babesa bermatzeko.

b) Ebidentzia egokiak eskuratu eta ateratzeko beharrezko mekanismo eta tresnak erabili ditu, haien autentikotasuna, osotasuna, fidagarritasuna eta legezkotasuna bermatzen dituztenak.

c) Ebidentzien analisiak eskuz eta tresna automatikoen bidez egin ditu, auzitegi-ikerketei erantzuna ematea ahalbidetzeko.

d) Analisiaren prozesua dokumentatu du, urrats guztien erreprodukzioa bermatzeko.

e) Ebidentzien denbora-lerroa, zaintza-katearen mantentzea eta maila tekniko eta exekutiboko ondorioen elaborazioa kontuan hartu ditu.

f) Auzitegi-analisiaren ondorioen jakinarazpen formala egin die dagozkien solaskideei.

Edukiak: Auzitegi-analisiaren prozesua Gauzen Internet-eko gailuetan (IoT), eta industria-sektoreetako eta beste sektore batzuetako gailuetan.

− Hash funtzioak gailuetan.
− Gailuen ezkutatze-sistemak.
− Ebidentzia hegakorrak, ez-hegakorrak eta bidean direnak ateratzea gailuetan.
− Ebidentzia hegakorren, ez-hegakorren eta bidean direnen analisia gailuetan, eskuzko tresnen bidez.
− Ebidentzia hegakorren, ez-hegakorren eta bidean direnen analisia gailuetan, tresna automatizatuen bidez.
− Ezabatuta segurua gailuetan.

RA6. Erakundeari eragiten dion zibersegurtasuneko gorabehera baten aurrean erantzuten du, beharrezko neurriak hartuz.

Ebaluazio-irizpideak:

a) Jardun-prozedura batzuk garatu ditu, industria-kontroleko sistemetan zibersegurtasun-gorabehera ohikoenei erantzuteko, arintzeko, desagerrarazteko edo gordetzeko.
b) Erantzun ziber-erresilenteak prestatu ditu, erakundearen zerbitzuak ematen jarraitzea ahalbidetzen dutenak, zibersegurtasun-gorabeheretan berehalako erantzuna emateko.
c) Gorabeherari egokitzen zaion erabakiak hartzeko fluxu bat eta barne eta/edo kanpoko eskala-faktore bat ezarri ditu.
d) Gorabeheraren eragina jasan duten zerbitzuei berrekiteko lanak egin ditu, normaltasunera itzuli dela berretsi arte.
e) Egindako ekintzak dokumentatu ditu, ikasbideen erregistro bat mantentzea ahalbidetzen duten ondorioak barne.
f) Gorabeheraren jakinarazpen formala egin die, une egokian, parte hartu duten edo eragindako guztiei: bezeroak, hornitzaileak, barne langileak, komunikabideak eta agintari eskudunak.
g) Gorabeheraren jarraipen egokia egin du, antzeko egoerarik berriz gerta ez dadin.

Edukiak: Erantzuna zibersegurtasuneko gorabehera baten aurrean.

− Jardun-prozedura xehatuak garatzea, hainbat motatako gorabeherei erantzuteko, arintzeko, desagerrarazteko edo eusteko.
− Zibererresilientziako ahalmenak ezartzea.
− Gorabeheren eragina jasan duten zerbitzuak berrezartzeko lanak.
− Dokumentazioa eta ikasbideak.
− Gorabeheraren jakinarazpena.
− Gorabeheraren segimendua.

5. lanbide-modulua: Segurtasun integrala.

Kodea: 5031.
Iraupena: 96 ordu.

ECTS kredituak: 10.

Ikaskuntzaren emaitzak eta ebaluazio-irizpideak.

RA1: Segurtasun fisikoko arauak eta prozedurak OT inguruneetako zibersegurtasunean txertatzen ditu, izan litezkeen arriskuak identifikatuta.

Ebaluazio-irizpideak:

a) Arrisku fisikoaren eta segurtasun fisikoaren ezaugarriak finkatu ditu.
b) Segurtasun fisikoko eskema baten oinarriak eta funtsezko tresnak deskribatu ditu.
c) OT inguruneetarako segurtasun fisikoko arauen oinarrizko kontzeptuak definitu ditu.
d) Garatuko den jardueraren arabera aplikatzekoak diren segurtasun fisikoaren arauen ezaugarriak finkatu ditu.
e) OT inguruneetarako segurtasun fisikoko prozedurak zehaztu ditu, aplikatzekoak diren arauen arabera.
f) Segurtasun fisikoko prozedura jakin batzuk ezarri ditu.
g) Egiaztatu du segurtasun fisikoko arau eta prozeduren integrazioak zibersegurtasun-eskakizunak betetzen dituela.

Edukiak: Segurtasun fisikoko arauak eta prozedurak OT inguruneetako zibersegurtasunean.

− Segurtasun fisikoko arriskuak OT ingurune batean.
− OT ingurune batean aplikatzekoak diren segurtasun fisikoko arauak.
− Segurtasun fisikoa OT segurtasunean txertatzea.

RA2: Eragiketa-segurtasun fisikoko arauak eta prozedurak OT inguruneetako zibersegurtasunean txertatzen ditu, eta izan litezkeen arriskuak identifikatzen ditu.

Ebaluazio-irizpideak:

a) Eragiketa-arriskuaren eta eragiketa-segurtasunaren ezaugarriak finkatu ditu.
b) Eragiketa-segurtasunaren eskema baten oinarriak eta funtsezko tresnak deskribatu ditu.
c) Eragiketa-segurtasuneko arauen oinarrizko kontzeptuak definitu ditu.
d) Garatuko den jardueraren arabera aplikatzekoak diren eragiketa-segurtasuneko arauen ezaugarriak finkatu ditu.
e) Ingurunean aplikatzekoak diren segurtasun-prozedurak zehaztu ditu, aplikatzekoak diren arauen arabera.
f) Eragiketa-segurtasuneko prozedura jakin batzuk ezarri ditu.
g) Egiaztatu du eragiketa-segurtasuneko arau eta prozeduren integrazioak zibersegurtasun-eskakizunak betetzen dituela.

Edukiak: Eragiketa-segurtasuneko arauak eta prozedurak OT inguruneetako zibersegurtasunean.

− Eragiketa-segurtasuneko arriskuak OT ingurune batekin.
− OT inguruneak.
− Eragiketa-segurtasuna OT segurtasunean txertatzea.

RA3: Kalitatearen arauak eta prozedurak OT inguruneetako zibersegurtasunean txertatzen ditu, eta izan litezkeen arriskuak identifikatzen ditu.

Ebaluazio-irizpideak:

a) Kalitateari eragiten dion arrisku eta galeraren kontzeptua definitu du.
b) Kalitate-eskema baten oinarriak eta funtsezko tresnak deskribatu ditu.
c) Kalitateari buruzko arauen oinarrizko kontzeptuak definitu ditu.
d) Garatuko den jardueraren arabera aplikatzekoak diren kalitate-arauen ezaugarriak finkatu ditu.
e) Ingurunean aplikatzekoak diren kalitate-prozedurak zehaztu ditu, arauak kontuan hartuta aplikatzekoak direnak.
f) Kalitate-prozedura jakin batzuk ezarri ditu.
g) Egiaztatu du kalitate-arau eta -prozeduren integrazioak zibersegurtasun-eskakizunak betetzen dituela.

Edukiak: Kalitate-arauak eta -prozedurak OT inguruneetako zibersegurtasunean.

− OT ingurune batean kalitateari eragiten dioten arriskuak.
− OT ingurune batean aplikatzekoak diren kalitate-arauak.
− Kalitatea OT zibersegurtasunean txertatzea.

RA4: Zibersegurtasun-arauak aplikatzen ditu segurtasun-sistema instrumentatuetan (SIS), aplikatzekoa den araudiaren arabera.

Ebaluazio-irizpideak:

a) Akats moten eta segurtasun-sistema instrumentatuen ezaugarriak finkatu ditu.
b) SIS teknologien plataformen artean bereizi eta erakundearen errealitate industrialari egokitzen zaizkionak hautatu ditu.
c) Garatuko den jardueraren arabera aplikatzekoak diren arauak hautatu ditu (IEC 61508 edo arau horren ordezkoak izan litezkeenak).
d) Ingurunean aplikatzekoak diren segurtasun-integritatearen mailak zehaztu ditu, aplikatzekoa den araudiaren arabera (IEC 61508 edo arau horren ordezkoak izan litezkeenak).
e) SIS sistemen segurtasun-teknikak eta -neurriak zehaztu ditu.
f) Egiaztatu du SIS sistemek zibersegurtasun-eskakizunak betetzen dituztela.

Edukiak: Zibersegurtasun-arauak segurtasun-sistema instrumentatuetan (SIS).

Akats motak eta segurtasun-sistema instrumentatuen motak.
− Segurtasun-sistema instrumentatuak (SIS) ezartzeko erabilgarri dauden teknologia-plataformak eta haien eskakizunak.
− Aplikatzekoa den araudia (IEC 61508 edo haren ordezkoak izan litezkeenak).
− Segurtasun-integritatearen mailak (SIL) zehazteko metodoak.
− Segurtasun-teknikak eta neurriak SISetan.
− Zibersegurtasun-eskakizunak segurtasun-sistema instrumentatuetan.

RA5: Segurtasun-arriskuak modu integralean kudeatzen ditu, aitortutako metodologiak erabiliz.

Ebaluazio-irizpideak:

a) Arriskuen kudeaketa integralaren ezaugarriak finkatu ditu.
b) Segurtasun-arriskuen kudeaketa integralaren arauak, esparruak eta metodologiak deskribatu ditu.
c) Arriskuak kudeatzeko esparru bat ezarri du aplikatzekoa den araudiaren arabera (ISO 31000 edo haren ordezkoak izan litezkeenak).
d) Arriskua identifikatu eta ebaluatu du aplikatzekoa den araudiaren arabera (ISO 31000 edo haren ordezkoak izan litezkeenak).
e) Arriskuaren tratamendua egin eta arriskua onartu eta jakinarazi du aplikatzekoa den araudiaren arabera (ISO 31000 edo haren ordezkoak izan litezkeenak).

Edukiak: Segurtasun-arriskuen kudeaketa integrala.

− Arriskuen Kudeaketa Esparrua, aplikatzekoa den araudiaren arabera (ISO 31000 edo haren ordezkoak izan litezkeenak).
− Arriskuaren eta zaintzaren identifikazioa, ebaluazioa, tratamendua, onarpena eta jakinarazpena, aplikatzekoa den araudiaren arabera (ISO 31000 edo haren ordezkoak izan litezkeenak).
− Industria Zibersegurtasuneko araudia. NIST SP800-X, NERC-ZIP, IEC 62443, BSI-100 araudia edo haren ordezkoak izan litezkeenak.

6. lanbide-modulua: Prestakuntza praktiko duala enpresan
Kodea: E304
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 jardueren barruan hauek egon behar dira:

− Zibersegurtasuneko estrategien erabilera industria-proiektuen faseetan.
− Industria-ingurune eta -sistemei buruzko txostenak egitea eta haien ebaluazioa.
− Industria-kontroleko sistemen konfigurazioa.
− Ahulezien detekzioa industria-sareetan eta haien gailuen konfigurazioa.
− Auzitegi-analisietarako lankidetza, industria-sare eta -sistemetan.
− Segurtasun integraleko arauak eta prozedurak eragiketa-inguruneetan txertatzea.

5. Espazioak eta ekipamenduak.

5.1. Espazioak:

PRESTAKUNTZA-ESPAZIOA	AZALERA (M2) / 30 IKASLE	AZALERA (M2) / 20 IKASLE
Erabilera anitzeko gela.	60	40
Informatika-gela.	120	80
Sistema automatikoen laborategia.	180	120
Sistema automatikoen lantegia.	200	130

5.2. Ekipamenduak:

PRESTAKUNTZA-ESPAZIOA	EKIPAMENDUA
Erabilera anitzeko gela.	Proiekzio-sistemak. Sarean konektatutako ordenagailuak, Internet sarbidearekin. Sarean biltegiragailuak. Eskanerra. Erreprografiako sistemak. Ikus-entzunezko tresneria.
Informatika-gela.	Proiekzio-sistemak. Sarean konektatutako ordenagailuak, Internet sarbidearekin. Eskanerra. Plotterra. Proiektuak kudeatzeko programak. Erreprografiako sistemak. Ikus-entzunezko ekipoak. Diseinuko softwarea eta industriako automatizazio eta robotikako sistemen simulazioa. SCADA eragiketaren kontrol-sistemak garatzeko softwarea.
Sistema automatikoen laborategia.	Proiekzio-sistemak. Sarean konektatutako ordenagailuak, Internet sarbidearekin. Erreprografiako sistemak. Aplikatzekoa den softwarea. Hartu eta neurtzeko elementuak, batez ere, IoT motako komunikazioen teknologia integratuen bidez Elementu jarduleak, batez ere, IoT motako komunikazioen teknologia integratuen bidez. Kommutadoreak. Ukipen-pantailak. Pasarelak. Haririk gabeko komunikazio-sistemetarako txartelak. Hainbat bus motatarako komunikazio-txartelak. Telekudeaketarako eta telemantentzerako komunikazio-txartelak. Bideratzaileak. Suebakiak. Aginte- eta maniobra-elementuak. Babes-elementuak. Transformadoreak. Polimetroak. Elikatze-iturriak. Frekuentzimetroak. Automata programagarriak. Osziloskopioak. Seinale-injektorea. Elektrizitaterako mekanizazio-tresna eta -makina eramangarriak. Makina elektriko estatikoen eta birakarien akoplamendu, erregulazio, kontrol eta saiakuntzetako bankua. Matxarda anperimetrikoak. Takometroak. Hainbat motatako motorrak. Abiagailu progresiboak. Industria-komunikazioko elementuak eta entrenagailuak. Neurketa eta kontroleko ekipamenduak eta elementuak. Entseguak egiteko ekipamendua.
Sistema automatikoen lantegia.	Proiekzio-sistemak. Sarean konektatutako ordenagailuak, Internet sarbidearekin. Erreprografiako sistemak. Eskuzko mekanizazioko erremintak eta tresneria. Neurketa eta kontroleko ekipamenduak eta elementuak. Elementuak neurtzeko eta egiaztatzeko ekipamendua. Mekanismoak. Sistemak muntatzeko panel modularrak. Sistema hidraulikoak, pneumatikoak, elektro-hidraulikoak eta elektro-pneumatikoak muntatzeko eta simulatzeko elementuak.

	Mekanizaziorako erreminta eramangarriak. Estazio-simulagailuak: banaketa, egiaztapena, prozesamendua, robota, eta abar. Automata programagarriak. Egiaztatzeko eta neurtzeko tresneriak. Aplikatzekoa den softwarea.

6. Irakasleak.

6.1. Eragiketa-teknologien inguruneetan zibersegurtasuneko espezializazio-ikastaroaren lanbide-moduluetan irakasteko eskumena duten irakasleen espezialitateak:

LANBIDE-MODULUA	IRAKASLEEN ESPEZIALITATEA	KIDEGOA
5027. Zibersegurtasuna industria-proiektuetan.	Ekipo elektronikoak. Instalazio elektroteknikoak. Fabrikazio mekanikoaren antolamendua eta proiektuak.	Bigarren Hezkuntzako irakaslea.
	Irakasle espezialista.	
5028. Industria-kontroleko sistema seguruak.	Fabrikazio mekanikoaren antolamendua eta proiektuak. Sistema elektronikoak. Sistema elektroteknikoak eta automatikoak.	Bigarren Hezkuntzako irakaslea.
	Irakasle espezialista.	
5029. Industriako komunikazio-sare seguruak.	Ekipo elektronikoak. Instalazio elektroteknikoak.	Lanbide Heziketako irakasle teknikoa.
	Irakasle espezialista.	
5030. Industria-zibersegurtasunari buruzko auzitegi-analisia.	Ekipo elektronikoak. Instalazio elektroteknikoak.	Lanbide Heziketako irakasle teknikoa.
	Irakasle espezialista.	
5031. Segurtasun integrala.	Fabrikazio mekanikoaren antolamendua eta proiektuak. Sistema elektronikoak. Sistema elektroteknikoak eta automatikoak.	Bigarren Hezkuntzako irakaslea.
	Irakasle espezialista.	
E304. Prestakuntza praktiko duala enpresan.	Fabrikazio mekanikoaren antolamendua eta proiektuak. Sistema elektronikoak. Sistema elektroteknikoak eta automatikoak.	Bigarren Hezkuntzako irakaslea.
	Ekipo elektronikoak. Instalazio elektroteknikoak.	Lanbide Heziketako irakasle teknikoa.

6.2. Irakasteko beharrezkoak diren titulazioak:

KIDEGOA	ESPEZIALITATEA	TITULAZIOAK
Bigarren Hezkuntzako irakaslea.	Fabrikazio mekanikoaren antolamendua eta proiektuak.	Ontzi-makinetan diplomaduna. Nekazaritzako ingeniari teknikoa: nekazaritza eta abeltzaintzako ustiapenetako espezialitatea, nekazaritzako elikagaien industrietako espezialitatea, nekazaritza-mekanizazioko eta landa-eraikuntzetako espezialitatea. Aeronautikako ingeniari teknikoa, aireontzietako espezialitatean, ekipo eta material aeroespazialetako espezialitatean. Industria-diseinuko ingeniari teknikoa. Industria-ingeniari teknikoa, espezialitate guztietan.

		Meatze-ingeniari teknikoa, espezialitate guztietan. Ontzigintzako ingeniari teknikoa, espezialitate guztietan. Herri-lanetako ingeniari teknikoa, eraikuntza zibiletako espezialitatean.
	Sistema elektronikoak. Sistema elektroteknikoak eta automatikoak.	Ontzietako irrati-elektronikan diplomaduna. Aeronautikako ingeniari teknikoa, Aireontzietako espezialitatean. Industria-ingeniari teknikoa, Elektrizitatea espezialitatean, Industria-elektronika espezialitatean. Sistema-informatikako ingeniari teknikoa. Telekomunikazioetako ingeniari teknikoa, espezialitate guztietan.

6.3. Espezializazio-ikastaroa osatzen duten lanbide-moduluak emateko behar diren titulazioak hezkuntzakoaz besteko administrazioetako titulartasun pribatuko ikastetxeetarako, eta hezkuntza-administraziorako orientabideak:

LANBIDE-MODULUAK	TITULAZIOAK
5027. Zibersegurtasuna industria-proiektuetan. 5028. Industria-kontroleko sistema seguruak. 5031. Segurtasun integrala.	Doktorea, lizentziaduna, ingeniaria, arkitektoa, edo dagokion mailako titulua edo irakaskuntzaren ondorioetarako beste zenbait titulu baliokide.
5029. Industriako komunikazio-sare seguruak. 5030. Industriako zibersegurtasunari buruzko auzitegi-analisia.	Doktorea, lizentziaduna, ingeniaria, arkitektoa, edo dagokion mailako titulua edo irakaskuntzaren ondorioetarako beste zenbait titulu baliokide. Unibertsitateko diplomaduna, arkitekto teknikoa edo irakaskuntzaren ondorioetarako beste zenbait titulu baliokide.

6.4. Espezializazio-ikastaroa osatzen duten lanbide-moduluak emateko eskatzen diren titulazioak hezkuntzakoaz besteko administrazioetako titulartasun pribatuko ikastetxeetarako, eta hezkuntza-administraziorako orientabideak:

LANBIDE-MODULUAK	TITULAZIOAK
5027. Zibersegurtasuna industria-proiektuetan. 5028. Industria-kontroleko sistema seguruak. 5031. Segurtasun integrala.	Ontzi-makinetan diplomaduna. Ontzietako irrati-elektronikan diplomaduna. Aeronautikako ingeniari teknikoa, Aireontzietako espezialitatean, Ekipo eta material aeroespazialetako espezialitatean, Aireontzietako espezialitatean. Nekazaritzako ingeniari teknikoa: nekazaritza eta abeltzaintzako ustiapenetako espezialitatea, nekazaritzako elikagaien industrietako espezialitatea, nekazaritza-mekanizazioko eta landa-eraikuntzetako espezialitatea. Industria-diseinuko ingeniari teknikoa. Industria-ingeniari teknikoa, espezialitate guztietan. Sistema-informatikako ingeniari teknikoa. Meatze-ingeniari teknikoa, espezialitate guztietan. Ontzigintzako ingeniari teknikoa, espezialitate guztietan. Herri-lanetako ingeniari teknikoa, eraikuntza zibiletako espezialitatean. Telekomunikazioetako ingeniari teknikoa, espezialitate guztietan.