BESTELAKO XEDAPENAK

HEZKUNTZA SAILA

5318

AGINDUA, 2018ko urriaren 16koa, Hezkuntzako sailburuarena, lanbide-heziketako lau espezializazio ezartzen dituena.

Euskal Autonomia Erkidegoko Autonomia Estatutuaren 16. artikuluaren arabera, Euskal Autonomia Erkidegoak du irakaskuntzaren gaineko eskumena –irismen, maila eta gradu guztietan eta modalitate eta espezialitate guztietan–, betiere Konstituzioaren 27. artikulua eta hori garatzen duten lege organikoak ezertan eragotzi gabe, baita Konstituzioaren 149.1.30.a artikuluak Estatuari esleitzen dizkion ahalmenak eragotzi gabe, eta berori betetzeko eta bermatzeko behar den ikuskapena ere ergotzi gabe.

Lanbide-heziketari eta kualifikazioei buruzko ekainaren 19ko 5/2002 Lege Organikoaren helburua, zehazki, honako hau da: lanbide-prestakuntza, kualifikazio eta akreditazioen sistema integrala antolatzea, prestakuntza-modalitate desberdinen bidez gizartearen eta ekonomikoaren eskariei eraginkortasunez eta gardentasunez erantzuteko. Era berean, funts publikoekin sostengatzen den prestakuntza-eskaintzak bizialdi osoko prestakuntzari bide eman behar diola eta hainbat asmo eta egoera pertsonal nahiz profesionaletara egokitu behar duela ezartzen du.

Lan-arloan, Autonomia Estatutuaren 12.2 artikuluan xedatutakoaren arabera, Euskal Autonomia Erkidegoko Administrazio Orokorrari dagokio estatuaren legeria betearazteko eskumena, batez ere hemen esanguratsuena den honetan, eta, horretarako, langileen kualifikazioa eta prestakuntza integrala bultzatuko ditu.

Pertsonen enplegagarritasuna hobetzeko, bai epe laburrean, bai epe luzean, estrategia eta mekanismo berriak eskatuko dira. Alde batetik, eskumenak eskuratzeko prozesuetan eman beharreko orduak areagotuko dira, geroz eta konplexuagoak diren eremuek eskatzen duten espezializazio-maila altuagoa lortzeko bide bakar gisa. Bestetik, gaur egungo lehiakortasun-egoerara egokitutako prestakuntza eta konpetentziak dituzten langileak eskatzen dira, eta horrek berekin dakar orain arteko eskemak haustea; hau da, «lanpostura» bideratutako prestakuntza-eredua atzean utzi eta «lanbide-eremura» bideratutako eredu berri bat hartzea. Paradigma-aldaketa horrek pertsona du ardatz, pertsonek gaitasun tekniko, pertsonal eta sozialak eskuratzea eta finkatzea sustatzen baitu. Hartara, bermatzen da pertsona horiek zenbait arlotarako balioko dutela eta funtzionalitate handiagoa izango dutela.

Produkzio-egituraren benetako beharrizanetara gehien egokitzen diren kualifikazioak ezarriz, hauek ahalbidetu behar dira: alde batetik, lanbide-heziketa ikasten ari diren pertsonen prestakuntza enpresen gero eta beharrizan espezializatuetara egokitzea, eta, bestetik, langileen kualifikazioa hobetzea, enplegua sortzen duten produkzio-sektoreek eskatzen dituzten gaitasunak emanez.

Lanbide-heziketa hobetzeko, eraginkortasunari dagokionez, eskaintza espezializatu, eta lan-merkatuaren beharrizanetara gehiago egokituta planifikatu behar da, bereziki azaleratzen ari diren sektore eta lanpostuetan. Hala, enplegu gehiago sortuko dute, eta estrategikoak izango dira Euskal Autonomia Erkidegoko ekonomiaren etorkizunerako.

Testuinguru horretan, lanbide-heziketa elementu giltzarria da egungo eta etorkizuneko lanpostuetarako eskatzen diren kualifikazioei erantzuteko.

Ekonomiarako esanguratsuak diren ekoizpen-sektoreetatik datorren eskari ugari dagoenez, pertsonen enplegagarritasuna egokitu eta hobetzeari nahiz ekoizpen-sarean espezializazio altuena duten eskariei erantzun azkarra emango dieten prestakuntza-programak bultzatzeko beharrizana sortzen da. Hala, Euskal Autonomia Erkidegoko Administrazioak prestakuntza-programa horien ziurtagiriak eman ahal ditu. Halaxe ziurtatutako programek, edonola ere, ez dute titulu edo ziurtagiri akademikorik, lanbide-ziurtagiririk edo ziurtagiri partzial metagarririk emango, eskumenak ez baitaude sartuta Lanbide Kualifikazioen Katalogo Nazionalean.

Hezkuntza Sistemako Lanbide Heziketaren antolamendu orokorra ezartzen duen otsailaren 26ko 32/2008 Dekretuan (otsailaren 2ko 14/2016 Dekretuaren bidez aldatua), zehazki, Euskal Autonomia Erkidegoko lanbide-espezializazioko programak ezartzen dira, lanbide-heziketaren eremuan, bai eta horien aitorpena eta ziurtapena ere, indarreko araudi-esparruan duten balioa egiaztatzeko.

Horregatik, ekainaren 28ko 4/2018 Legean –Euskal Autonomia Erkidegoko Lanbide Heziketari buruzkoa–, V. kapituluan dago ezarrita Lanbide Kualifikazio eta Espezializazioen euskal esparrua.

Legeak, lanbide-kualifikazio eta -espezializazioen euskal esparrua arautzen du, gure lan-merkatuari erantzun ahal izateko, lanbide-heziketako sistema orokorraren bidez. Esparru horretan sartuko dira Euskal Autonomia Erkidegoko lanbide-espezializazioko programen ziurtagiriak eta egiaztagiriak. Bizialdi Osoko Ikaskuntzari buruzko Legean ezarrita dago jada hainbat bide erabiliz ikaskuntza-jarduerak egiaztatzeko sistema. Lege honen bidez, orduan arautu zena osatu nahi da, eta berariaz aipatzen da bereziki sustatu nahi den jarduera bat: lanbidearen eremuko espezializazio-programak. Ezinbestekoa da jarduera horien balioa aitortzea eta ziurtatzea indarrean dagoen araudiaren esparruan.

Erreferente horiek gogoan izanda aztertu dira gure ekonomiako ekoizpen-sektore estrategikoen eskariak, eta, halaxe definitu dira agindu honetan jaso diren lanbide-espezializazioko programak.

Agindu honek Hezkuntza, Hizkuntza Politika eta Kulturako sailburuaren 2016ko uztailaren 27ko Aginduaren bidez argitaratutako lanbide-espezializazioko programen katalogoa osatzen du (Agindua, 2016ko uztailaren 27koa, Hezkuntza, Hizkuntza Politika eta Kulturako sailburuarena, zeinaren bidez lanbide-espezializazioko zazpi programa eta horiek baimendu eta emateko baldintza orokorrak ezartzen baitira), eta Hezkuntzako sailburuaren 2016ko abenduaren 23ko Agindua, zeinaren bidez lanbide-espezializazioko bost programa ezartzen baitira; izan ere, lanbide-espezializazioko beste lau programa eransten zaizkio.

Horregatik guztiagatik, honako hau

EBAZTEN DUT:

Artikulu bakarra.– Xedea.

1.– Agindu honen xedea da eranskinetan jasotako lanbide-espezializazioko lau programaren egitura ezartzea, Euskal Autonomia Erkidegoaren esparruan Hezkuntza Sistemako Lanbide Heziketaren antolamendu orokorra ezartzen duen otsailaren 26ko 32/2008 Dekretuaren 12.ter artikuluan ezarritakoaren arabera.

2.– Agindu honen eranskinean aipatzen diren espezializazio-programak, zeinen egitura zehazten baita, honako eranskin hauetan aipatzen dira:

I. eranskina: Enpresa txiki eta ertainetako zibersegurtasuna.

II. eranskina: Material metalikoen eta saiakuntza ez-suntsitzaileen bidez soldatutako junturen ikuskapena.

III. eranskina: Produkzio integrala produktu tubularrak fabrikatzeko lerroetan.

IV. eranskina: Industria aeroespazialerako soldadura.

3.– Programa horiek emateko baldintzak Euskal Autonomia Erkidegoaren esparruan Hezkuntza Sistemako Lanbide Heziketaren antolamendu orokorra ezartzen duen otsailaren 26ko 32/2008 Dekretuko 12.ter artikuluan ezarritakoak izango dira, bai eta lanbide-espezializazioko zazpi programa eta horiek baimendu eta emateko baldintza orokorrak ezartzen dituen Hezkuntza, Hizkuntza Politika eta Kulturako sailburuaren 2016ko uztailaren 27ko Aginduan ezarritakoak ere.

AZKEN XEDAPENETAKO LEHENENGOA.– Indarren jartzea.

Agindu hau Euskal Herriko Agintaritzaren Aldizkarian argitaratu eta hurrengo egunetik aurrera jarriko da indarrean.

AZKEN XEDAPENETAKO BIGARRENA.– Errekurtsoak.

Agindu honen aurka, aukerako berraztertze-errekurtsoa jar dakioke Hezkuntzako sailburuari, hilabeteko epean. Bestela, administrazioarekiko auzi-errekurtsoa jar daiteke Euskal Autonomia Erkidegoko Justizia Auzitegi Nagusian, Administrazioarekiko Auzien Salan, bi hileko epean. Bi kasuetan, errekurtsoak aurkezteko epea agindu hau Euskal Herriko Agintaritzaren Aldizkarian argitaratu eta hurrengo egunean hasiko da.

Vitoria-Gasteiz, 2018ko urriaren 16a.

Hezkuntzako sailburua,
CRISTINA URIARTE TOLEDO.

I. ERANSKINA, 2018KO URRIAREN 16KO AGINDUARENA

ESPEZIALIZAZIO-PROGRAMA: ENPRESA TXIKI ETA ERTAINETAKO ZIBERSEGURTASUNA

A) Identifikazio-datuak.

Izena: enpresa txiki eta ertainetako zibersegurtasuna.

Kodea: EP013.

Iraupena: 900 ordu.

B) Lanbide-profila.

Konpetentzia orokorra:

Sistemen eta aplikazioen segurtasuna bermatzea, kodea modu seguruan diseinatuta, segurtasun aktiboko eta ikerkuntza forentseko metodoak eta tresnak erabilita, eta, horretarako, ahuleziak eta mehatxuak identifikatzea eta zibersegurtasuneko plan estrategikoak definitzea.

Lanbide-eremua:

Lanbide-titulu hau duenak datuak kudeatzeko sistemak eta sare-azpiegiturak (Internet, intranet edo estranet) dituzten erakundeen informatika-arloan egiten du lan (organizazio guztietan, gaur egun). Oro har, sor daitezkeen ahuleziei aurrea hartzen eta konponbidea ematen dihardu, hala behar duten departamentuetan.

Hauek dira zeregin eta lanpostu aipagarrienak:

- Komunikazio-sareen eta informatika-sistemen segurtasuneko auditorea.
- DBLOaren gaineko aholkularia.
- Plataforma seguruen diseinatzailea edo muntatzailea.
- Industria-sareetako segurtasun-sistemen kontrolatzailea.
- Kode seguruen programatzailea.

Esku-hartze profesionalerako konpetentzia profesional tekniko, pertsonal eta sozialak:

a) Kodeak modu seguruan garatzea, programazio-ahuleziak ezagututa.

b) Ahuleziarik gabeko aplikazioak sortu eta ezartzea, segurtasun-tresnak erabilita.

c) Intrusio-proba erabiltzea, helburu izan daitezkeenak identifikatzeko eta lokalizatzeko.

d) Zenbait ahulezia eskaneatzea, emaitzak aztertzea eta dokumentuak egitea.

e) Ebidentziak biltzeko metodoak aplikatzea eta eurak ebaluatzeko analisi-teknikak erabiltzea.

f) Analisi forentseko tresnak instalatu, konfiguratu eta erabiltzea, sistema informatikoan sor daitezkeen ebidentziak detektatzeko.

g) Hardware-gailuak konfiguratu eta erabiltzea ekipo informatikoen analisi forentserako.

h) Sistema eragile jabeduneko artefaktuetako informazioa berreskuratzea.

i) Txosten forentseak egitea, analisietatik lortutako emaitzetan oinarrituta.

j) Zibersegurtasuneko plan estrategikoak definitzea.

k) Informazioaren segurtasunerako kudeaketa-sistema ezarri eta ziurtatzea.

l) Segurtasuna gobernatzeko nazioarteko erreferentzia-estandarrak identifikatzea eta datuen segurtasunari eta datuak babesteari buruzko legeak eta arauak jakitea, bai nazionalak bai nazioartekoak.

m) Arrisku-analisiari dagozkion faseak garatzea, informazio-segurtasunaren industrian arrisku-analisietarako gehien erabiltzen diren metodologiak aplikatuta, eta analisitik ondorioztatutako hondar-arriskua kudeatzeko plana egitea.

n) Informazioa segurtasunez tratatzeko jarraibideak eta jardunbideak ezartzea, sistema informatikoen ahuleziak ezagututa.

o) Segurtasun aktiboko mekanismoak ezartzea, kontraneurriak hautatu eta exekutatuta, sistemaren kontrako mehatxu edo erasorik badago.

p) Sistema informatikoan urrunetik sartzeko teknika seguruak ezartzea, segurtasun-plana interpretatu eta aplikatuta.

q) Sistema informatikoa segurtatzeko suebakiak ezartzea, euren prestazioak aztertuta eta barne-sarerako trafikoa kontrolatuta.

r) Proxy zerbitzariak ezartzea, zerbitzuaren funtzionamendu segurua bermatzen duten konfigurazio-irizpideak aplikatuta.

s) Erabilgarritasun handiko konponbideak ezartzea, birtualizazio-teknikak erabilita eta proba-inguruneak konfiguratuta.

t) Industriako kontrol-sistemen ahuleziak eta mehatxu espezifikoak identifikatzea eta nazioarteko ospea duten erreferentzia-jardunbide onak lokalizatzea.

u) Oinarrizko automatizazio- eta kontrol-ingurune bat ezarri eta hedatzea.

v) Internetetiko irisgarritasuna duten automatizazio-sistemak identifikatzea.

w) Automatizazio- eta kontrol-sistemen oinarrizko ahuleziak esplotatzea.

x) Industria-komunikazioak eta -protokoloak interpretatzea.

y) Oinarrizko industria-suebaki bat konfiguratu eta hedatzea.

z) Industria-inguruneetarako zenbait zibersegurtasun-teknologia eta antolamendu- edo prozedura-neurriak proposatzea inguruneon segurtasuna hobetzeko.

aa) Organizazioan, informazio-teknologiaren (IT) segurtasun-eremuaren eta automatika-eremuaren arteko bitartekoa izatea.

bb) Segurtasuna kudeatzeko sistema ezartzeko faseak garatzea.

cc) Etengabeko hobekuntzarako sistemak erabiltzea.

dd) Ingurune seguruak sortzea bere lana zein lantaldearena garatzeko, laneko eta ingurumeneko arriskuen prebentzioko prozedurak berrikusita eta aplikatuta, araudian ezarritakoa eta enpresen helburuetan adierazitakoa beteta.

ee) Lan-egoera berrietara egokitzea, kasuan kasuko lanbide-ingurunearekin loturiko ezagutzak eguneratuz, bizialdi osoko ikaskuntzarako nork bere prestakuntza nahiz eskura dauden baliabideak kudeatuz.

ff) Egoerak edo arazoak ekimenez eta autonomiaz konpontzea nork bere eskumen-esparruan, sormenez, jarrera berritzailez eta norberaren nahiz taldekideen lana hobetzea bilatuz.

gg) Maila berean dauden kideekin, gorago dauden kideekin, bezeroekin eta haren mende dauden kideekin komunikatzea, komunikatzeko bide eraginkorrak erabiliz, informazio edo ezagutza egokiak emanez eta lan-esparruan parte hartzen duten pertsonen autonomia eta gaitasuna errespetatuz.

hh) Lantaldeak arduraz antolatu eta koordinatzea eta horietan parte hartzea, eta, horretarako, haien garapena ikuskatzea, beharrezkoa denean, harreman arinak izanez, lidergoa hartuz eta sortzen diren talde-gatazketarako konponbideak ekarriz.

C) Prestakuntza.

Ikaskuntza-eremuak. Ordu-esleipena.

1.– Zibersegurtasunerako sarrera: sareak, objektuetara bideratutako programazioa eta informatika-segurtasuna: 100 ordu.

2.– Kode seguruko programazioa: 150 ordu.

3.– Segurtasun perimetrala: 150 ordu.

4.– Analisi forentsea: 100 ordu.

5.– Sistema industrialetako segurtasuna: 150 ordu.

6.– Sartze-proba (pentesting) eta web-auditoria: 150 ordu.

7.– Segurtasunaren kudeaketa eta gobernua: 100 ordu.

– Programaren ikaskuntzaren emaitzak:

Erantzukizuna eta autonomia jarduera profesionalean (programaren zeharkakoak).

Informatika-inguruneetako zibersegurtasun-neurriak ezartzeko aholkuak emateko erantzukizuna hartzen du; ahuleziarik ez izateko, eskura dauzkan mekanismo guztiak abiarazten ditu; intzidenterik izanez gero, ahalik eta inpakturik txikiena sortuko dela bermatzen du, eta berriro ez gertatzeko neurriak hartzen ditu. Halaber, organizazioetan, korporazioaren informatika-arloaren eta automatika-arloaren arteko bitartekaritza-lana egiten du, hala behar denean, eta hango langileen jarduerak gainbegiratzen ditu.

– 1. eremuari lotuta: Zibersegurtasunerako sarrera: sareak, objektuetara bideratutako programazioa eta informatika-segurtasuna

– Eskuratu beharreko gaitasunak eta trebeziak.

1.– Ordenagailuak eta periferikoak sare kableatuetan eta hari gabekoetan integratzea, eta haien funtzionamendua eta prestazioak ebaluatzea.

Ebaluazio-irizpideak:

a) Sare kableatuetarako eta hari gabekoetarako estandarrak identifikatu ditu.

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

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

2.– Bideratzaile baten oinarrizko funtzioak administratzea eta hura sarean integratzeko konfigurazio-aukerak ezartzea.

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, intzidentzien jarraipena egitea ahalbidetzen dutenak.

e) Trafikoa iragazteko ahalmenak deskribatu ditu.

f) ACL sarbide-kontroleko zerrendak kudeatzeko komandoak erabili ditu.

3.– Sare lokal birtualak konfiguratzea eta horien aplikazio-eremua identifikatzea.

Ebaluazio-irizpideak:

a) VLAN sare lokal birtualak inplementatu ditu.

b) Lotura nagusiak konfiguratu ditu.

c) Bideratzaileren bat edo maila askoko switchen bat erabili du VLAN sare lokal birtualak elkarrekin konektatzeko.

d) Administrazio zentralizatuko protokoloen arabera lan egiteko konfiguratu ditu kommutadoreak.

e) SNMP protokoloan oinarritutako aplikazioen bidez monitorizatu du sarea.

4.– Informazioa segurtasunez tratatzeko jarraibideak eta jardunbideak hartzea eta sistema informatiko baten ahuleziak ezagutzea, baita sistema segurtatu beharraz jabetzea 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) Babes perimetraleko plan integral bat ezarri beharraz jabetu da, batez ere sare publikoekin konektatutako sistemetan.

5.– Sistema informatiko batean urrunetik sartzeko teknika seguruak ezartzea eta segurtasun-plana interpretatu eta aplikatzea.

Ebaluazio-irizpideak:

a) Sistema bateko arriskuguneak sailkatu ditu, segurtasun perimetraleko irizpideen arabera.

b) Komunikazio-protokolo seguruak eta horien erabilera-esparruak identifikatu ditu.

c) Zerbitzari bat ezarri du urruneko kokalekuetatik barneko sarera sartzeko atebide gisa.

d) Urruneko erabiltzaileek atebidean zeharreko sarbidean erabil ditzaketen autentifikazio-metodoak identifikatu eta konfiguratu ditu.

6.– Sistema informatikoa segurtatzeko suebakiak ezartzea, euren prestazioak aztertuta eta barne-sarerako trafikoa kontrolatuta.

Ebaluazio-irizpideak:

a) Suebakien ezaugarriak, motak eta funtzioak deskribatu ditu.

b) Trafikoa iragazten duten mailak sailkatu ditu.

c) Sareko gune jakin batzuetarako sarbideak mugatzeko suebakien instalazioa planifikatu du.

d) Suebaki batean iragazkiak konfiguratu ditu iragazteko arauen zerrenda abiapuntutzat hartuta.

e) Suebakien gertakari-erregistroak berrikusi ditu.

7.– Programa sinpleak idatzi eta probatzea, eta, eginkizun horretan, objektuetara bideratutako programazioaren oinarriak aplikatzea.

Ebaluazio-irizpideak:

a) Objektuetara bideratutako programazio-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.

8.– Klaseka antolatutako programak garatzea, eta, eginkizun horretan, objektuetara bideratutako programazioaren printzipioak aplikatzea.

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 erabiltzen dituzten programak garatu ditu.

e) Klaseen eta kideen ikuspena 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.

9.– Programak garatzea eta, horretarako, objektuetara bideratutako lengoaien ezaugarri aurreratuak aplikatzea.

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 inplementatzen eta erabiltzen dituzten programak egin ditu.

– Ezagutzak (100 ordu).

Sare kableatuak eta hari gabeko sareak:

● IP helbideak eta azpisare-maskarak konfiguratzea.

● Sare-egokigailu kableatuak eta hari gabekoak zenbati sistema eragiletan konfiguratzea.

● Sare kableatuak eta hari gabekoak elkarrekin konektatzeko gailuak konfiguratzea.

Bideratzailearen oinarrizko konfigurazioa eta administrazioa:

● Bideratzailera iristeko metodo desberdinak.

● Bideratzailea konfiguratzeko eta administratzeko komandoak. Bide estatikoen konfigurazioa.

● Intzidentzien jarraipena egiteko eta bideratzailearen egoera monitorizatzeko komandoak.

● Bideratzailearen trafiko-iragazkien konfigurazioa.

● ACL sarbide-kontroleko zerrenden kudeaketa.

Sare birtualak:

● VLAN sare lokal birtualak inplementatzea.

● VLAN sare lokal birtualetan intzidentziak diagnostikatzea.

● Gailuen arteko lotura nagusia konfiguratzea.

● Bideratzaileak edo maila askoko switchak konfiguratzea VLAN sare lokal birtualak elkarrekin konektatzeko.

● VLAN sare lokal birtualetako protokoloak.

● Sarea SNMP protokoloan oinarritutako aplikazioen bidez monitorizatzea.

Informatika-segurtasuneko jarraibideak:

● Ahulezien arrazoi nagusiak eta ahulezien jatorria.

● Pasahitzen politika.

● Segurtasun fisikoa eta segurtasun logikoa.

Urrutiko sarbideko teknikak. Segurtasun perimetrala:

● Sistema informatikoetako arriskuguneak.

● Zerbitzari bat ezartzea barneko sarera sartzeko atebide gisa.

● Urruneko erabiltzaileen atebidean zeharreko sarbidean autentifikazio-metodoak konfiguratzea.

● Komunikazio-protokolo seguruak.

Suebakiak instalatzea eta konfiguratzea:

● Suebakien instalazioa planifikatzea.

● Suebaki batean iragazkiak konfiguratzea iragazteko arauen zerrenda abiapuntutzat hartuta.

● Arazoen diagnostikoa.

Objektuak erabiltzea:

● Objektuen eta klaseen ezaugarriak.

● Objektuen propietateak edo atributuak.

● Metodoaren kontzeptua.

● Klase bateko kideen sarbide-kontrola.

● Metodo estatikoaren kontzeptua.

● Parametro eta balio itzuliak. Objektu-liburutegiak.

● Eraikitzailearen kontzeptua.

● Objektuak suntsitzea eta memoria askatzea.

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.

Klase aurreratuak garatzea:

● Klase-hierarkia: superklasea eta azpiklaseak.

● Polimorfismoaren kontzeptua.

● Azpiklaseen eraikitzaileak eta suntsitzaileak. Superklasearen metodoetarako sarbidea. Superklasearen metodoen birdefinizioa.

– 2. eremuari lotuta: kode seguruko programazioa.

– Eskuratu beharreko gaitasunak eta trebeziak.

1.– Ahuleziarik gabeko aplikazioak sortzea, kanpoko erasorik ez izateko.

Ebaluazio-irizpideak:

a) Baliabideetarako sarbide-kontrola egin du.

b) Zerbitzarian eta bezeroan injekzio-erroreak aztertu ditu.

c) Autentifikazio-protokoloak identifikatu ditu.

d) Aplikazioa exekutatu bitartean erabiltzaile-saioak sortu, berritu eta suntsitu ditu.

e) Erasotzaileari saio-identifikatzailea finkatzen uzten dion sistema baten ahuleziak aztertu ditu.

f) Saioen kudeaketa zuzena ziurtatu du.

g) Bidaltzailearen identitate digitala egiaztatu du baliabideren edo funtzioren baterako sarbidean edo komunikazioan.

2.– Informazio zifratua bidaltzen duten aplikazioak ezartzea.

Ebaluazio-irizpideak:

a) Gako sekretu batean oinarrituta, informazioa babesteko edo baimenik gabeko behatzaileei informazioa ezkutatzeko teknikak aplikatu ditu.

b) Komunikazio idatzien pribatutasuna zaindu du eta bermatu du baimendunek baino ezin dutela ikusi jatorrizko mezua.

c) Egindako ziurtagiri digitaletan ageri diren datuen autentikotasuna eta egiazkotasuna bermatu du.

3.– Datu-ihesik ez izateko aplikazioak garatzea.

Ebaluazio-irizpideak:

a) Behar besteko baimena ez izatea kontrolatu du.

b) Erasoak murriztu ditu eta, horretarako, rolak esleitu dizkie aplikazioaren datuei eta funtzionalitateei.

c) Roletan oinarritutako sarbide-kontrola erabili du.

d) Sarbide-kontrolak egiaztatu ditu negozio-logikaren ikuspegitik.

e) Zerbitzariaren aldean baimenak kontrolatzeko mekanismoa ezarri du.

f) Errore-mezuetan behar den informazioa baino ez agertzea bermatu du.

g) Erabiltzaileak kontrolatzen dituen sarrerak balidatu ditu.

4.– Indarrean dauden arauetan oinarritzen diren garapen segururako segurtasun-tresnak aplikatzea.

Ebaluazio-irizpideak:

a) Aplikazio baten arrisku-maila identifikatu du eta Application Security Verification Standard (ASVS) –aplikazio-segurtasuna egiaztatzeko estandarra– deritzon arrisku-mailaren bidez mapeatu du.

b) ASVS aplikazio-segurtasuna egiaztatzeko estandarrean oinarritutako segurtasun-eskakizunak definitu ditu identifikazio-mailaren arabera.

– Ezagutzak (150 ordu).

Programazio seguruko teknikak:

● Programazioko oinarrizko segurtasun-printzipioak.

● Zerbitzariko eta bezeroko injekzio-erroreak.

● Inprimakietan oinarritutako protokoloen autentifikazioa.

● Sarbide-kontrol deklaratibo eta programatikoa.

● Saioen kontrol-kudeaketa.

● Datu-ihesen prebentzioa.

Aplikazioen inplementazioa:

● Kriptografiako tresna espezifikoak: informazioa zifratze bidez babesteko teknikak.

● Bildutako datuen autentikotasunerako eta egiazkotasunerako ziurtagiri digitalak.

● Aplikazioek informazioa modu seguruan transmititu ahal izateko segurtasun-protokoloak.

● Elektronikoki sortutako eta digitalki transmititutako dokumentuen autentikotasuna eta osotasuna bermatzeko sinadura digitalak.

Datu-ihesa:

● Behar besteko baimena ez izatea kontrolatzeko teknikak.

● Errore-mezuetan informazioa agerraraztea.

● Zeharkako patha.

Indarreko araudiak:

● OWASP Top 10 – web-aplikazioetako segurtasun-arriskuak.

● OWASP Application Security Verification Standard–Aplikazio-segurtasuna egiaztatzeko estandarra (ASVS).

● Security Verification Standard–Segurtasuna egiaztatzeko estandarra (ASVS).

● Web-aplikazioetako segurtasunarekiko konfiantza-mailak: planifikazioa, arrisku-mailaren araberako eskakizunen definizioa, arrisku-mailaren baterako diseinua, ezarpena eta egiaztapena.

– 3. eremuari lotuta: segurtasun perimetrala.

– Eskuratu beharreko gaitasunak eta trebeziak.

1.– Sare publikoetako segurtasuna bermatzeko neurriak hartzea solaskideen identitatea bermatuta.

Ebaluazio-irizpideak:

a) Informatika-sistemetako segurtasunaren printzipioak eta helburuak definitu ditu.

b) Informazioaren konfidentzialtasuna eta osotasuna bermatzeko protokoloak ezarri ditu.

c) Pasahitza kudeatzeko tresna bat baino gehiago ezarri du.

d) Zifratze-teknikak, sinadura elektronikoak eta ziurtagiri digitalak erabili ditu sare publikoen erabileran oinarritutako lan-inguruanean.

e) Informazioaren autentikotasunerako, konfidentzialtasunerako eta osotasunerako teknikak erabili ditu.

2.– Sistema informatiko bateko segurtasun perimetralaren eredua diseinatu eta ezartzea.

Ebaluazio-irizpideak:

a) Segurtasun perimetralaren eredua ezartzeko zenbait egoera identifikatu ditu.

b) Zenbait suebaki mota konfiguratu eta erabili ditu.

c) Suebakiaren iragazki-politika eta -arauak konfiguratu ditu eta gertakari-erregistroak auditatu ditu.

d) Zerbitzariak eta zerbitzuak modu seguruan konfiguratu ditu DMZ zonan.

3.– Proxya konfiguratzea eta ezartzea.

Ebaluazio-irizpideak:

a) Proxyek dituzten funtzionamenduak definitu ditu.

b) Zenbait proxy mota konfiguratu eta erabili ditu.

4.– Urrutiko sarbideko sistemetan identitateak autentifikatzeko eta kudeatzeko sistemak ezartzea.

Ebaluazio-irizpideak:

a) Autentifikazio-prozesuetarako segurtasun-politika eta prozedurak definitu ditu.

b) Komunikazio-protokolo seguruak eta horien erabilera-esparruak identifikatu ditu.

c) RADIUS zerbitzariak konfiguratu ditu erabiltzaileak urrunetik autentifikatzeko.

d) Barne-sarerako urrutiko sarbidea ezarri du VPN konexioen bidez.

e) Bi faktoreko autentifikazio-sistemak ezarri ditu.

5.– SIEM sistema ezarri du (Security Information and Event Management)

Ebaluazio-irizpideak:

a) Mehatxu-gertaerak identifikatu eta kalifikatu ditu.

b) Aplikazioak erabiltzeko direktibak inplementatu ditu.

c) Erregistratutako gertaerak aztertu eta dokumentatu ditu.

– Ezagutzak (150 ordu).

Informazioaren segurtasuna:

● Pasahitz-kudeatzaileak.

● Konfidentzialtasuna, informazioaren osotasuna.

● Informazioaren segurtasunean kriptografia aplikatzea.

● Informazio konfidentziala zifratzeko teknikak.

● Autentikotasuna.

● Sinadura digitalaren aplikazioa.

● Ziurtagiri digitalak. PKI kudeatzailea. PKCS.

● Errebokatze-protokoloak: CLR, OCSP.

Segurtasun perimetrala:

● Segurtasun-perimetroa ezartzeko ereduak diseinatzea eta definitzea.

● Suebakien iragazkietarako politika eta arauak konfiguratzea.

● Zerbitzariak eta zerbitzuak modu seguruan konfiguratzea DMZ zonan. Euspen- eta bastioi-suebakiak.

● DMZ zonako zerbitzarietarako sarbide segurua.

● UTM: forward (aurrera), reverse (atzera), transparent (gardena), cachea, proxyak.

Proxy zerbitzariak instalatzea eta konfiguratzea:

● Web-proxy-cache zerbitzari bat instalatzea eta konfiguratzea.

● Proxy zerbitzaria erabiltzea web-sarbidean murrizketak ezartzeko.

● Proxyaren funtzionamendu-probak egitea eta haren aktibitatea monitorizatzea.

● Bezeroetatik proxyra sartzeko probak. Proxy bat modu gardenean eta alderantzizko moduan konfiguratzea.

Urrunetik sartzeko teknikak ezartzea:

● Autentifikazio-prozesuetarako segurtasun-politika eta prozedurak.

● Bi faktoreko autentifikazioa. Txartel kriptografikoak erabiltzea. Sistemas de Single Sign On (SSO).

● Erabiltzaileen urruneko autentifikazioa, RADIUS zerbitzariak.

● Barne-sarera urrutitik VPN konexioen bidez sartzea (tunela).

● Barne-zerbitzariekiko komunikazio segurua ezartzea, IPSEC (CSP/HA) konexioen bidez.

● Delegazioen arteko konexioetarako tunel zifratuak ezartzea.

Makina birtualetan SIEM sistema bat ezartzea:

● Gertaeren oinarrizko teoria: SIM, SEM.

● Gertaeren analisia eta normalizazioa.

● Gertaerak eranstea. Log fitxategien kudeaketa eta jarduera-prozedura.

● Segurtasun- eta mehatxu-intzidentzien motorizazioa, dokumentazioa eta erantzuna.

– 4. eremuari lotuta: analisi forentsea.

– Eskuratu beharreko gaitasunak eta trebeziak.

1.– Analisi forentsearen etapak ezagutzea eta ebidentziak biltzeko faseak identifikatzea.

Ebaluazio-irizpideak:

a) Analisi forentseari buruzko kontzeptu orokorrak definitu ditu.

b) Ikerketa forentsearen eskakizunak zehaztu ditu.

c) Erregistro-agindua eskatu aurreko informazioa zehaztu du.

d) Erregistro-tokian sartzeko modua deskribatu du.

e) Zigilugabetze- eta klonatze-fasea espezifikatu du.

2.– Datu-biltegiragailuak klonatzea, software-aplikazioen eta hardware-ekipoen bidez.

Ebaluazio-irizpideak:

a) Zenbait datu-biltegiragailutan idazketa-blokeatzaileak erabili ditu.

b) Diskoak bikoiztu ditu zenbait euskarritan.

c) Kopien osotasuna egiaztatu du zenbait prozesuren bidez.

3.– Diskoetako irudiak zenbait tresnaren bidez aztertzea.

Ebaluazio-irizpideak:

a) Ostatatu gabeko espazioaren eta Slack espazioaren arteko aldea ezarri du fitxategien sisteman.

b) Ezabatutako fitxategiak berreskuratu ditu.

c) Fitxategiak eta metadatuak aztertu ditu.

4.– RAMen informazio hegakorra atzematea, eta exekuzioan dauden prozesuak aztertzea.

Ebaluazio-irizpideak:

a) Memoria-iraulketak egin ditu.

b) Memoria aztertu du beroan.

c) Exekuzioan dauden prozesuak identifikatu eta aztertu ditu.

5.– Sistema eragile jabeduneko artefaktuetako informazioa berreskuratzea.

Ebaluazio-irizpideak:

a) Erregistroaren egitura zehaztu du.

b) Lineako eta lineaz kanpoko erregistroa aztertu du.

c) Erregistroa aztertzeko zenbait tresna erabili ditu.

d) Ebidentzien azterketetarako karpeten diseinua eta egitura aztertu du.

e) Hive erregistro-fitxategiak aztertu ditu.

f) Gertaeren erregistro-fitxategiak aztertu ditu.

g) Nabigazioaren historia-fitxategiak aztertu ditu.

h) Erabiltzaile-profilen eta sistemaren jarduera-fitxategiak aztertu ditu.

– Ezagutzak (100 ordu).

Analisi forentsearen etapak:

● Etapak: eskuratzea, analisia, aurkezpena eta denbora-lerroa.

● Eskuratu aurreko kontsiderazioak.

● Hegakortasun-ordena. Ikerketa forentsearen eskakizunak: onargarritasuna, osotasuna, sinesgarritasuna kausa-efektu erlazioa, errepikagarria eta dokumentatua.

Ebidentzien bilketa:

● Erregistro-agindua eskatu aurreko informazioa.

● Erregistro-tokirako sarrera.

● Zigilugabetzea eta klonatzea.

Gailuak klonatzea:

● Hardware/software idazketa-blokeatzaileak.

● Bitez biteko edo disko-irudien bidezko kopiak eskuratzea.

● Diskoei, partizioei eta fitxategiei buruzko kontzeptuak.

● Kopiaren osotasuna egiaztatzea (laburpen edo hash prozesuak).

Irudien analisia:

● Fitxategi-sistema. Ostatatu gabeko espazioak eta Slack espazioak.

● Ezabatutako fitxategiak berreskuratzea.

● Datuen eta metadatuen analisia.

RAM memoriaren analisia:

● Memoria-iraulketa. Beroan egindako analisia.

● Exekuzioan dauden prozesuen analisia.

Sistema eragile jabeduneko artefaktuetako informazioa berreskuratzea:

● Erregistroaren egitura. Erregistroaren lineako eta lineaz kanpoko analisia.

● Erregistroa analizatzeko tresnak.

● Analisi forentsearen karpeta eta fitxategi garrantzitsuenak.

● Erabiltzailearen analisia eta informazioa. Posta elektronikoa, nabigazio-historia, bilaketen historia, jardueren historia eta programa-exekuzioen historia.

– 5. eremuari lotuta: sistema industrialetako segurtasuna.

– Eskuratu beharreko gaitasunak eta trebeziak.

1.– Zibersegurtasun industrialaren oinarrizko alderdiak aztertzea eta, horretarako, dauden araudi eta praktika onak identifikatzea, IT ingurunea (informazio-teknologia) eta OT ingurunea (operazio-teknologia) desberdintzea, eta ulertzea zein izan diren mundu zabaleko enpresa industrial handiak kaltetu dituzten zibereraso handienak.

Ebaluazio-irizpideak:

a) Zibersegurtasun industriala definitu du.

b) Automatizazio- eta kontrol-sistemen mugak identifikatu ditu, informazio-sistemek dituztenen aldean, segurtasuneko kontraneurriak ezarri behar izan dituenean.

c) Industria-inguruneko zibersegurtasunaren lehentasunak identifikatu ditu.

d) Enpresa-sare bateko diagramaren gainean, identifikatu du zer den OT ingurunea eta zer den IT ingurunea.

e) Segurtasuneko arauak eta segurtasuneko jardunbide onak desberdindu ditu.

f) Azpiegitura Kritikoak Babesteko Legearen eta bera garatzen duen dekretuaren irismena deskribatu du, baita hari buruzko informazioa non topatu ere.

g) IEC 62443 eta CCN-STIC jardunbide onak, beroriek osatzen dituzten dokumentuak eta aplikazio-eremua identifikatu ditu.

h) Mundu zabaleko industria-konpainiek izan dituzten eraso nagusiak identifikatu ditu, Stuxnet, Duqu, Night Dragon, Flame, Shamoon, Havex/Energetic Bear, Sandworm barnean hartuta.

i) Aurkeztutako eraso nagusietatik «irakaspenak» atera ditu.

2.– Oinarrizko industria-ingurune bat birsortzea eta, horretarako, gutxienez, gainbegiratzeko eta urrunetik kontrolatzeko software bat eta automata simulatu bat instalatu eta konfiguratzea.

Ebaluazio-irizpideak:

a) Automata bat simulatu du Raspberry Pi3 baten eta behar den softwarearen bidez.

b) Automatari oinarrizko kontrol-logika kargatu dio.

c) SCADA software bat (oinarrizko gainbegiratzea) instalatu eta konfiguratu du.

d) Gainbegiratze-softwarea eta automata konektatu ditu.

e) Gainbegiratze-softwarea begiratu du eta egiaztatu du kapaz dela denbora errealean automataren aldagaiak ikusteko eta balio horiek historikoen datu-basean biltegiratzeko.

3.– Zenbait osagai industrialen ezaugarriak aztertzea (PLC, RTU, PC industrialak, SIS, SCADA, DCS, MES, eta abar), baita horiek automatizazio-, funtzionamendu- eta ahulezia-eremuetan zer gune hartzen duten ere.

Ebaluazio-irizpideak:

a) ICS sistemen gunea deskribatu du OT sistemen eremuaren barruan.

b) Alde funtzionalak eta teknologikoak identifikatu ditu automatizazio-maila guztietan.

c) Zeharkako osagaiak aurkeztu ditu kontrol lokalerako: sentsoreak, eragingailuak, serboak eta erregulagailuak, PLC, RTU, PC industrialak eta DCS.

d) Gainbegiratze bidezko kontrol-sistemak aurkeztu ditu: DCS, SCADA, historizadoreak, etab.

e) Industria-inguruneetan, segurtasuna (safety) automatizatu eta kontrolatzen duten sistemak aurkeztu ditu, baita kontrol- eta segurtasun-bertsio hibridoak ere.

f) Sektorekako beste automatizazio- eta kontrol-osagai batzuk aurkeztu ditu: robotak, CNC, kontagailu adimendunak, MES, etab.

g) Aurkeztutako osagai guztiak ukitzen dituzten ahulezia nagusiak aurkeztu ditu.

4.– Ahuleziak esplotatzeko oinarrizko tresnak erabiltzea, automatizazio- eta kontrol-sistemetatik, batez ere, Shodan eta Kali-Moki sistemetatik.

Ebaluazio-irizpideak:

a) Shodan zer den eta nola erabili azaldu du.

b) Shodan erabiltzeko erakustaldi praktikoa egin du: objektiboaren lokalizazioa eta sarbide-proba.

c) Identifikatu du zer tresna erabili behar duen hauek aurkitzeko: ostalariak, ataka irekiak, argitaratutako zerbitzuak eta zerbitzu-bertsioak.

d) JohnTheRipper erabili du automatizazio- eta kontrol-sistema batean pasahitzak hausteko.

e) Metasploit erabili du ekipo industrial bateko ahulezia esplotatzeko.

5.– Industria-komunikazioen oinarrizko alderdiak, erabiltzen diren komunikazio-protokolo nagusiak (ModBUS, BACnet, Profinet, etab.), euren funtzionamendua eta ahuleziak aztertzea.

Ebaluazio-irizpideak:

a) Denbora errealaren, komunikazio kommutatuen eta seriearen kontzeptuak azaldu ditu.

b) Bezero-zerbitzariaren eta argitalpen-harpidetzaren paradigmak, komunikazio asinkronoak, marka-ikurra pasatzearen bidezkoak, etab. identifikatu ditu.

c) ModBUS, BacNet eta Profinet protokoloen funtzionamendua azaldu du.

d) Aurreko protokoloen oinarrizko segurtasun-alderdiak azaldu ditu.

e) Industria-inguruneetako sare tipikoen (eta segurtasun gabekoen) arkitektura aurkeztu du.

6.– Industria-komunikazio eta -osagaiei erasoak egitea, Kali-Moki banaketan edo antzekoetan dauden tresnen bidez.

Ebaluazio-irizpideak:

a) Wireshark edo TCPDump bidezko industria-trafikoa atzeman eta interpretatu du.

b) TCPReplay erabili du industria-sare batean trafikoa injektatzeko.

c) ModScan eta MBTGet erabili ditu automata bateko erregistroak manipulatzeko.

d) Metasploit erabili du pibot-eraso bat egiteko, txarto diseinatutako kontrol-sare batean, eta automata baten kontrol-parametroak aldatzeko.

7.– Kontraneurri teknikoak proposatzea, barnean hartuta datu-diodoak, industria-suebakiak, intrusioak detektatzeko sistemak; antolamendu-neurriekin batera, barnean hartuta segmentazioa, arriskurik gabeko auditoriak, eta baliabide mugikor eta ateragarrien erabilera seguruaren prozedurak.

Ebaluazio-irizpideak:

a) Neurri teknikoen eta antolamendu-neurrien beharra azaldu du.

b) Datu-diodoak edo noranzko bakarreko atebideak aurkeztu ditu, suebakiekiko desberdintasunekin batera.

c) Edukiera industrialeko suebakiak aurkeztu ditu, barnean hartuta DPI eta sendotasun industrial kontzeptuak.

d) Industria-eremuko intrusioak detektatzeko sistemak aurkeztu ditu, barnean hartuta DPBI teknikak.

e) Industria-komunikazioetako segmentazio- eta segregazio-jardunbide onak azaldu ditu.

f) Industria-inguruneetan arriskurik ez daukaten auditoria libreen oinarrizko printzipioak azaldu ditu.

g) Jardunbide onak proposatu ditu baliabide mugikor eta gailu ateragarriak erabiltzeko, esate baterako, USB gailuak, eramangarriak, mugikorrak, PDA, eta abar.

8.– Modbus industria-suebakia hedatzea eta konfiguratzea.

Ebaluazio-irizpideak:

a) IPTables suebakiaren oinarrizko – Ezagutzak aurkeztu ditu.

b) Modbus modulua aurkeztu du.

c) Irakurketa- eta idazketa-komandoetan iragazkiak egiteko arauak konfiguratu ditu, Modbus/TCP bidez komunikaturiko PLC baten memoria-hedabideetan.

d) Industria-suebakiaren funtzionamendu zuzena egiaztatu du automata batez eta MBTget eta ModScan tresnez.

– Ezagutzak (150 ordu).

Industria-azpiegituren oinarrizko kontzeptuak.

● Industria-segurtasunaren arauak eta jardunbide onak: Azpiegitura Kritikoak Babesteko Legea, CCN-STIC, IEC 62443. OT versus IT: segurtasun-helburuak eta mugak.

● Eraso nagusiak, talde kriminalak eta irakaspenak: Stuxnet, Duqu, Night Dragon, Flame, Shamoon, Energetic Bear, Sandworm.

Industria-ingurunea birsortzea:

● PLC simulatu bat instalatu eta konfiguratzea.

● Oinarrizko SCADA bat instalatu eta konfiguratzea.

● PLC eta SCADA arteko konektibitatea konfiguratzea.

Industria-osagaiak:

● Industria-kontroleko sistemetarako sarrera.

● Kontrol lokaleko sistemak: sentsoreak, eragingailuak, serboak eta erregulagailuak, PLC, RTU, PC industrialak eta DCS.

● Gako-alderdiak, puntu sendoak eta puntu ahulak. SCADA: funtzioak, arkitektura eta osagaiak.

● Segurtasun-sistemak, segurtasun-sistema instrumentalizatuak (SIS) eta kontrol- eta segurtasun-sistema integratuak (ICSS).

● Beste sektore-sistema espezifiko batzuk: CNC, kontagailu adimendunak, robotak, MES, etab.

Automatizazio-sistemetan eta industria-kontroleko sistemetan ahuleziak esplotatzeko tresnak.

● Shodan: helburua eta erabilera. Banaketa.

● Kali-Moki: automatizazio- eta kontrol-sistemei ostalari mailan eraso egiteko tresnak.

● JohnTheRipper programaren erabilera.

● Metasploit proiektuaren erabilera.

Industria-komunikazioei buruzko oinarrizko alderdiak:

● Denbora errealaren, komunikazio kommutatuen eta seriearen kontzeptuak.

● Bezero-zerbitzariaren eta argitalpen-harpidetzaren paradigmak, komunikazio asinkronoak eta marka-ikurra pasatzearen bidezkoak.

● ModBUS, BacNet eta Profinet protokoloen funtzionamendua.

● Aurreko protokoloen oinarrizko segurtasun-alderdiak.

● Industria-inguruneetako sare tipikoen (eta segurtasun gabekoen) arkitektura.

Industria-sarean eta -protokoloetan oinarritutako erasoak:

● Wireshark edo TCPDump tresnen erabilera industria-komunikazioetarako.

● TCPReplay tresnen erabilera industria-protokoloetan bilbeak injektatzeko.

● MBTGet eta ModScan tresnen erabilera.

● Metasploit proiektuaren erabilera pibot-erasoetan.

Kontraneurri teknikoak eta antolamenduko jardunbide onak:

● Neurri teknikoen eta antolamendu-neurrien definizioa eta osagarritasuna.

● Datu-diodoak edo noranzko bakarreko atebideak, eta suebakiekiko aldeak.

● Edukiera industrialeko suebakiak. DPI eta sendotasun industriala.

● Industria-eremuko intrusioak detektatzeko sistemak. DPBI. Industria-komunikazioetako segmentazio- eta segregazio-jardunbide onak.

● Industria-inguruneetan arriskurik ez daukaten auditoria libreen oinarrizko printzipioak.

● Baliabide mugikor eta gailu ateragarriak erabiltzeko jardunbide onak, esate baterako, USB gailuak, eramangarriak, mugikorrak, PDA, eta abar.

Modbus industria-suebakia:

● IPTableseko Modbus modulua. Modbus/TCPetarako irakurketa- eta idazketa-komandoetan iragazteko arauak.

● MBTget eta ModScan tresnen erabilera, Modbus suebakiaren funtzionamendu zuzena egiaztatzeko.

– 6. eremuari lotuta: sartze-proba (pentesting) eta web-auditoria.

– Eskuratu beharreko gaitasunak eta trebeziak.

1.– Segurtasun-auditoriaren faseak aztertzea.

Ebaluazio-irizpideak:

a) Segurtasun-auditoria baten printzipioak eta helburuak definitu ditu.

b) Hacking motak ezarri ditu.

c) Proba motak ezarri ditu. Intrusio-proba eta ahulezien analisia.

d) Intrusio-proben eta ahulezia-analisien erabilgarritasuna eta eskakizunak identifikatu ditu.

e) Segurtasun-auditoria baten faseak definitu ditu.

f) Segurtasun-auditorietarako estandarrak definitu ditu.

2.– Auditatutako sistemen ebidentziak bildu, taldekatu eta ebaluatzea.

Ebaluazio-irizpideak:

a) Iturri irekien adimena erabili du.

b) Informazioa ezagutzeko edo bilatzeko tresnak erabili ditu.

c) Ebidentziak bildu, taldekatu eta ebaluatu ditu.

d) Zerbitzuak eskaneatu eta identifikatu ditu.

e) Zerbitzariak eta zerbitzuak modu seguruan konfiguratu ditu.

1.– Sistemak edo webguneak ahulak diren egiaztatzea, ahuleziaren bat erabilita, eta beraietan intrusioren bat egiten saiatzea.

Ebaluazio-irizpideak:

a) Ahuleziaren analisian eta esplotazioan zenbait ekintza definitu ditu.

b) Ahuleziak aztertu ditu eta sistema edo webgunea ahula den ala ez adierazi du.

c) Ahulezia esplotatzeko zenbait ekintza definitu ditu.

d) Ahuleziak zenbait ingurunetan esplotatu dira, eta zenbait tresnaz baliatuta.

3.– Telefonia mugikorrerako aplikazioak seguruak diren ala ez egiaztatzea.

Ebaluazio-irizpideak:

a) Bezeroaren aldean, aplikazioaren analisi estatikoak egin ditu.

b) Komunikazioak aztertu ditu.

c) Portaera dinamikoki aztertu du.

d) Zerbitzariaren aldea aztertu du.

4.– Ahulezien txosten xehatua egitea.

Ebaluazio-irizpideak:

a) Txostena idazteko faseak deskribatu ditu.

b) Lortutako informazioa biltzeko ekintzak definitu ditu.

c) Egindako probetatik lortutako informazioa eratu du.

d) Aurkikuntzen, ondorioen eta gomendioen txostena egin du.

e) Ahuleziei buruzko txostenak eta dokumentuak egin ditu.

f) Ahulezia-eraso nagusiak minimizatzeko zenbait baliabide definitu ditu.

– Ezagutzak (150 ordu).

Segurtasunaren auditoria:

● Segurtasun-auditoria baten printzipioak eta helburuak.

● Ahulezien sailkapena eta tipifikazioa.

● Segurtasun-auditoria baten faseak.

● Proba motak: intrusio-proba eta ahulezien analisia.

● Segurtasun-auditoriarako estandarrak.

Auditoriaren prozesuak:

● Iturri irekien adimena. Portuen eskaneatzea.

● Aplikazioen eta sistemen fingerprinting prozesua (mugikorrak, webguneak, sareko gailuak.).

Ahulezien bilaketa eta esplotazioa.

● Ahulezien eta erasoen sailkapena.

● Eraso-tresnak, esplotazio-metodoak.

● Pentesting prozedurako tresnak.

● Zenbait sistema eragileren eta zerbitzuren auditoria.

● Web-aplikazioen auditoria.

Mugikorretarako aplikazioak:

● Bezeroaren aldeko aplikazioaren analisi estatikoak.

● Komunikazioen analisia.

● Portaeraren analisi dinamikoa.

● Zerbitzariaren aldeko analisia.

Ahulezien txostenak:

● Dokumentazio-tresnak. Txostenaren formatua eta egitura.

● Ekintza-plana.

● Ahuleziaren xehetasunak.

– 7. eremuari lotuta: segurtasunaren kudeaketa eta gobernua.

– Eskuratu beharreko gaitasunak eta trebeziak.

1.– Segurtasuna kudeatu eta gobernatzeko egungo legeak eta estandarrak aztertzea.

Ebaluazio-irizpideak:

a) Segurtasunaren eta haren kudeaketaren kontzeptuak identifikatu ditu.

b) Segurtasunaren gobernua ezartzeko puntu kritikoak identifikatu ditu (segurtasunaren politikaren definizioa, segurtasunaren antolamendua, arriskuak kudeatzera eta etengabeko hobekuntza-prozesuetara zuzendutako ikuskera).

c) Arauen (ISO, NIST...) garatzaile nagusiak, eurei lotutako arauak (esate baterako, ISO 2700x, COBIT, ISO 22301, PCI DSS, ENS, DBLO) eta euren arteko intererlazioa eta osagarritasuna identifikatu ditu.

d) Zibersegurtasunaren gobernuan dauden arauak eta jardunbide onak lokalizatu eta kontsultatu ditu.

2.– Informazioaren segurtasunerako kudeaketa-sistema baten faseak ezartzea.

Ebaluazio-irizpideak:

a) Segurtasunaren gobernua (SGSI) ezartzeko behar diren faseak eta jarduerak ezarri ditu.

b) Segurtasunaren gobernua ezartzeko erabili behar diren prozesuak, metodologiak eta tresnak aztertu ditu.

c) Segurtasunaren ebaluazioa garatzeko eta zibersegurtasun-planak definitzeko prozesuak eta jarduerak identifikatu ditu.

d) Etengabeko hobekuntzarako sistemak (PDCA) identifikatu eta erabili ditu, segurtasunaren gobernua ezartzeko, industriaren jardunbide onak oinarritzat hartuta.

e) Arriskuak analizatzeko metodologia nagusiak eta analisi-fase nagusiak identifikatu ditu.

3.– Arrisku-analisietarako metodologiak eta teknikak ezartzea.

Ebaluazio-irizpideak:

a) Industriako arriskuak analizatzeko metodologia nagusiak eta analisi-fase nagusiak identifikatu ditu.

b) Arrisku-analisi oso bat garatu du, aktiboak hasieran identifikatzetik egungo arriskuaren azken emaitza lortzeraino (hondarra).

c) Hondar-arriskua kudeatzeko plana prestatu du.

4.– Informazio pertsonala babesteko segurtasun-neurriak ezartzea eta datuak babesteko indarreko arauak betetzeko behar diren prozedurak egitea.

Ebaluazio-irizpideak:

a) Datuak Babesteko Lege Organikoaren (DBLO) artikulu nagusiak eta Datuak Babesteko Erregelamendu Orokorra berrikusi ditu, indar berezia jarrita DBEOak dakartzan berrikuntzetan.

b) Segurtasun-dokumentu bat egin du.

c) DBLOak eta DBEOak beharrezkotzat jotzen dituzten prozedurak prestatu ditu.

○ Informazio-klausulak

○ Hirugarrenekiko kontratuak.

○ Interesdunen eskubideak baliatzea.

d) Babestu beharreko datu pertsonalen mailaren arabera aplikatu beharreko segurtasun-neurri nagusiak identifikatu ditu.

– Ezagutzak (100 ordu).

Segurtasun-estandarrak eta -arauak:

● Kontzeptuak eta hurbilketa: arriskuaren kudeaketari buruzko ikuskera. Zibersegurtasunaren dimentsioak. Segurtasunaren gobernuaren eta antolamenduaren definizioa eta ezarpena. Arrakastaren bestelako faktore kritikoak.

● Segurtasun-organismo, -estandar eta -araudi nagusiak: Organismoak: ISO, ISACA, NIST. Araudi eta estandar nagusiak. Estandarrak: ISO27002, COBIT 5.0, ITIL, NIST 800. ISO 27002.–2013

● Jardunbide onen kodea: sarrera. ISO 27002.–2013 Domeinuak. Kontrolen xehetasuna.

● Segurtasunaren antolamendua. Betetzea eta auditoria.

Segurtasunaren gobernua eta ezarpena.

● Bizi-zikloa: Plan, Do, Check, Act: SGSI bat garatzeko faseak; SGSI bat garatzeko eskakizun dokumentalak.

Arrisku-analisia:

● Kontzeptuak, terminologia eta definizioak.

● Metodologiaren identifikazioa eta berrikusketa, MAGERIT metodologiarena, batez ere.

● Arrisku-analisia egitea.

● Azkeneko arriskua eskuratzea.

● Arriskua kudeatzeko plana egitea.

Informazio pertsonalaren babesa:

● Kontzeptuak, terminologia eta definizioak.

● DBLOaren eta DBEOaren gako-artikuluak.

● Segurtasun-dokumentu bat egitea.

● Informazio-klausulak egitea.

● Eragindakoen eskubideak baliatzeko prozedurak.

● Hirugarrenekiko kontratuak.

● Segurtasun-neurri aplikagarriak.

D) Programarekin lotutako tituluak.

● Sareko Informatika Sistemen Administrazioko goi-mailako teknikaria.

● Web Aplikazioen Garapeneko goi-mailako teknikaria.

● Plataforma Anitzeko Aplikazioak Garatzeko goi-mailako teknikaria.

Era berean, salbuespen gisa eta Lanbide Heziketako Sailburuordetzak aldez aurretik baimenduta, espezializazioko programa hauetan, gutxienez 3 urteko esperientzia duten profesionalek ere parte hartu ahal izango dute, baldin eta programa ematen laguntzen duten enpresek horretarako proposatzen badituzte.

E) Sektore ekonomikoa eta eskatzaileak.

Sare-azpiegituraren bat behar duten jardueretako edozein sektore ekonomiko.

Demandatzaileak izan daitezke: software-garapenean, sare-azpiegituren kudeaketan eta gain-begiratzean diharduten enpresak eta, oro har, informazioa babestu nahi duen edozein enpresa.

Negozio-helburuak lortzeko automatizazio-sistemak eta industria-kontroleko sistemak behar dituzten enpresak, barnean hartuta robotak, makina-erreminta, automatak, kontrolatzaileak, gain-begiratzeko eta kontrolatzeko softwarea (esate baterako, SCADA, DCS, MES), eta abar.

F) Irakasleen eta instruktoreen betekizunak.

1. atala.– Irakasleen espezialitateak eta irakaskuntza-atribuzioa, lanbide-espezializazioaren programako ikaskuntza-esparruetan.

Prestakuntza-zentroko irakasleek jarraian adierazten diren espezialitateetako batean araututako baldintzak bete beharko dituzte:

Ikaskuntza-eremuak. Irakasleen espezialitateak.

1.– Zibersegurtasunerako sarrera: sareak, objektuetara bideratutako programazioa eta informatika-segurtasuna. Lanbide Heziketako irakasle teknikoa:

● Sistema eta aplikazio informatikoak.

Bigarren Hezkuntzako irakaslea:

● Informatika.

2.– Kode seguruko programazioa. Lanbide Heziketako irakasle teknikoa:

● Sistema eta aplikazio informatikoak.

Bigarren Hezkuntzako irakaslea:

● Informatika.

3.– Segurtasun perimetrala. Lanbide Heziketako irakasle teknikoa:

● Sistema eta aplikazio informatikoak.

Bigarren Hezkuntzako irakaslea:

● Informatika.

4.– Analisi forentsea. Lanbide Heziketako irakasle teknikoa:

● Sistema eta aplikazio informatikoak.

Bigarren Hezkuntzako irakaslea:

● Informatika.

5.– Sistema industrialetako segurtasuna. Lanbide Heziketako irakasle teknikoa:

● Sistema eta aplikazio informatikoak.

Bigarren Hezkuntzako irakaslea:

● Informatika.

6.– Sartze-proba (pentesting) eta web-auditoria. Lanbide Heziketako irakasle teknikoa:

● Sistema eta aplikazio informatikoak.

Bigarren Hezkuntzako irakaslea:

● Informatika.

7.– Segurtasunaren kudeaketa eta gobernua. Lanbide Heziketako irakasle teknikoa:

● Sistema eta aplikazio informatikoak.

Bigarren Hezkuntzako irakaslea:

● Informatika.

2. atala.– Irakasleek egiaztatu beharko dute zibersegurtasunari buruzko prestakuntza espezifikoa izan dutela espezializazio-ikastaro honetan eskatutako moduluetarako (Kode seguruko programazioa, Segurtasun perimetrala, Analisi forentsea, Sistema industrialetako segurtasuna, Sartze-proba (pentesting) eta web-auditoria, eta Segurtasunaren kudeaketa eta gobernua).

3. atala.– Enpresak jarritako instruktoreen esperientzia- eta prestakuntza-baldintzak.

Prestakuntzan parte hartzen duten enpresek jarritako instruktoreek gutxienez 3 urteko lan-esperientzia izango dute programaren profilarekin loturiko ekintzetan, edo, bestela, gutxienez 5 urteko prestakuntza egiaztatuko dute programaren ikaskuntzaren emaitzekin lotuta.