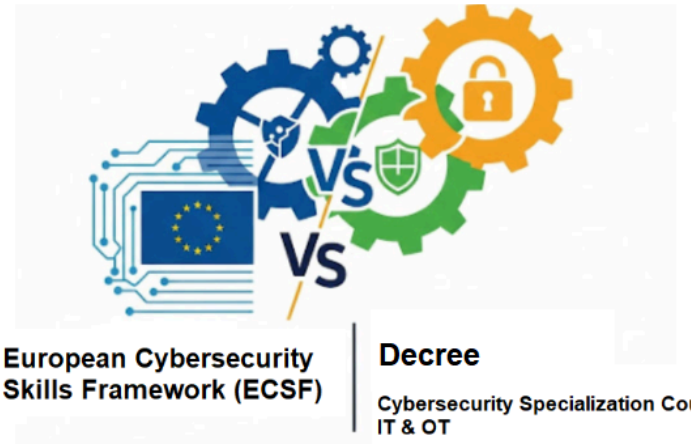

IT/OT Zibersegurtasuneko Espezializazio Ikastaroen Europako Gaitasunak eta Edukiak

2025-2026

indizea

1. Konparazio Dokumentuaren Helburua eta Esparrua

Enisa Europako Zibersegurtasun Agentzia da , eta enpresetan eta erakundeetan zibersegurtasun arloa estaltzeko beharrezkoak diren zibersegurtasun teknikarien eginkizunak eta profilak definitu ditu. Esparru honen helburu nagusia EBko estatu kideetako pertsonen, enpresaburuen eta prestakuntza programa hornitzaileen arteko ulermen komun bat sortzea da.

12 profil definitu dira talde ezberdinetan sailka ditzakegun izenburu, misio, zeregin, trebetasun, ezagutza eta gaitasunekin batera , kudeaketa-profil batzuk (CISO) eta araudiak, arriskuen kudeatzaileen profilak, gorabeherak eta mehatxuak, arkitektura-diseinuaren profil teknikoak, auditoria teknikoa, auzitegi-analisia edo pentesting-a eta prestatzaile eta ikertzaileen profilak.

Tknika **zibersegurtasun taldeak profil hauek aztertu eta IT eta OT arloetako zibersegurtasun espezializazio ikastaroak arautzen dituzten dekretuekin alderatu zituen** , profilen misioa, zereginak, trebetasunak eta ezagutzak modulu ezberdinen gaitasunekin, ikaskuntza-emaitzekin eta edukiekin alderatuz.

2. ENISAREN ETA EUROPAKO ZIBERSEGURTASUN GAITASUN ESPARRUAREN (ECSF) AURKEZPENA

2.1. ENISA

ENISA (Zibersegurtasunerako Europar Batasuneko Agentzia) Europar Batasunaren zibersegurtasun agentzia da. 2004an sortu zen eta Atenasen eta Heraklionen (Grezian) du egoitza. **Europar Batasuneko zibersegurtasuna hobetzeaz arduratzen den erakunde ofiziala da. Bere eginkizun nagusia estatu kideei, Europako erakundeei eta sektore pribatuari zibermehatxuen aurkako gaitasunak indartzen** laguntzea da, segurtasun digitalaren kultura komun bat sustatuz.

ENISAren zeregin nagusiak :

1. Aholkularitza estrategikoa eta teknikoa
    - Europako Batzordeari eta gobernu nazionalei zibersegurtasun-politikei buruzko aholkuak ematen dizkie.
    - NIS2 Erregelamendua eta Zibererresilientzia Legea bezalako lege garrantzitsuen garapenean eta ezarpenean kolaboratzen du.
2. Arriskuen eta politikaren kudeaketa
    - Arrisku teknologikoak eta segurtasunekoak kudeatzeko gidak, estandarrak eta jardunbide egokiak garatzen ditu.
    - Gaitasun-esparruak argitaratzen ditu, hala nola ECSF (Europako Zibersegurtasun Trebetasunen Esparrua).
3. Prestakuntza eta sentsibilizazioa
    - Profesionalen prestakuntza babesten du eta zibersegurtasunaren inguruko sentsibilizazio publikoa areagotzeko kanpainak sustatzen ditu.
    - Europako Zibersegurtasun Hilabetea bezalako ekitaldiak antolatzen ditu.
4. CSIRTentzako laguntza
    - Kide diren herrialdeetako Ordenagailu Segurtasun Intzidenteen Erantzun Taldeekin (CSIRT) lankidetzan aritzen da.
    - Mugaz gaindiko zibererasoen kasuan koordinazioa hobetzen du.
5. Mehatxuen ikerketa eta analisia
    - Zibermehatxuen, ahultasunen eta eraso berrien joerei buruzko txosten erregularrak argitaratzen ditu.

- Gobernuen eta enpresen artean ziberinteligentziari buruzko informazioa trukatzea errazten du.

6. Zibersegurtasun Ziurtagiria
    - Europako Zibersegurtasun Ziurtapen Esparrua gainbegiratzen eta koordinatzen du, eta horrek IKT produktu, zerbitzu eta prozesuetarako estandar komunak sustatzen ditu.

2.2. Europako Zibersegurtasun Gaitasun Esparrua (ECSF)

Europako Zibersegurtasun Trebetasunen Esparrua (ECSF) ENISAk (Zibersegurtasunerako Europar Batasuneko Agentzia) garatutako ekimena da, Europan zibersegurtasunaren arloan beharrezkoak diren eginkizun, trebetasun eta ezagutzari buruzko hizkuntza komun bat ezartzeko.

ECSF zibersegurtasuneko lanbide-rolak definitu eta sailkatzen dituen egituratutako eredua da, eta bakoitzerako honako hauek deskribatzen ditu:

- Bere funtzio eta zeregin nagusiak,
- Beharrezko trebetasun teknikoak eta ez-teknikoak,
- Lotutako oinarrizko ezagutza.

Hezkuntza-eskaintza, lan-merkatuaren beharrak eta zibersegurtasun-prestakuntza publikoko politikak lerrokatzeko diseinatuta dago.

ECSFren helburuak:

A. Enpresen, hezkuntza-erakundeen eta administrazio publikoen artean hizkuntza komuna ezartzea.
B. Zibersegurtasuneko lanbide-eginkizunak identifikatu eta sailkatu.
C. Sektorearen benetako beharretan oinarritutako prestakuntza-programak eta ziurtagiriak diseinatzea erraztea.
D. Profesionalentzako karrera-plangintza eta enplegatzaileentzako kontratazioa laguntzea.
E. Zibersegurtasuneko talentu-hutsuneak gainditzea Europan.

Norentzat da?

- Enpresak eta enplegatzaileak: lanpostuen deskribapenak eta kontratazio beharrak definitzeko.
- Prestatzaileak eta unibertsitateak: hezkuntza-programak lan-merkatuarekin lerrokatzeko.
- Profesionalak: beren trebetasunen eta karrera-ibilbidearen garapena gidatzeko.

- Politikariak eta arautzaileak: gaitasun digitalei buruzko politika koherenteak sortzeko.

ECSFren edukia

ECSF-k zibersegurtasuneko 12 lanbide-rol nagusi identifikatzen ditu. Bakoitzak eginkizunen, beharrezko trebetasunen, ezagutzaren eta lotutako tresnen deskribapen zehatza dakar.

1. **Informazioaren Segurtasuneko Zuzendari Nagusia(**CISO**)** (**Chief Information Security Officer (CISO))**

   Zibersegurtasun estrategia zuzentzen du eta politikak eta baliabideak negozio helburuekin lerrokatzen ditu.

2. **Ziber-intzidenteen erantzuna (Cyber Incident Responder)**
   Intzidenteak detektatu, aztertu, eduki eta berreskuratu, eragiketa- eta ospe-inpaktua minimizatzeko.
3. **Ziber-Lege, Politika eta Betetze Arduradunak (Cyber Legal, Policy & Compliance Officer)**
   Segurtasunarekin lotutako legeak, araudiak eta barne-politikak betetzen direla ziurtatzen du.
4. **Zibermehatxuen Inteligentzia Espezialista (Cyber Threat Intelligence Specialist**)

   Erasoei aurrea hartzeko, aktoreei, taktikei eta kanpainei buruzko informazioa bildu eta erlazionatzen du.

5. **Zibersegurtasuneko arkitektoak (Cybersecurity Architect)**
   Negozio-eskakizunak betetzen dituzten arkitektura, kontrol eta irtenbide seguruak diseinatzen ditu.
6. **Zibersegurtasun-ikuskatzaileak (Cybersecurity Auditor)**
   Kontrolen eraginkortasuna ebaluatzen du eta segurtasun-jarrera hobetzeko gomendioak egiten ditu.
7. **Zibersegurtasuneko Hezitzaileak (Cybersecurity Educator)**
   Zibersegurtasuneko prestakuntza, sentsibilizazio eta gaitasun-garapen programak garatu eta eskaintzen ditu.
8. **Zibersegurtasuneko Inplementatzaileak (Cybersecurity Implementer)**
   Irtenbide teknikoak (suebakiak, IAM, EDR, etab.) integratzen, konfiguratzen eta mantentzen ditu erakundearen politikaren arabera.
9. **Zibersegurtasuneko ikertzaileak (Cybersecurity Researcher)**
   Oinarrizko ikerketa eta ikerketa aplikatua egiten du, berrikuntza sortzen du eta egungo egoera zabaltzen duten emaitzak argitaratzen ditu.

10. **Zibersegurtasun Arriskuen Kudeatzaileak (Cybersecurity Risk Manager)**
    Zibersegurtasun arriskuak identifikatu, aztertu eta tratatzen ditu onargarri diren mugak mantentzeko.
11. **Auzitegi Digitaleko Ikertzaileak (Digital Forensics Investigator)**
    Ebidentzia digitala bildu eta aztertzen du, aurkikuntzak dokumentatzen ditu eta interesdunei aurkezten dizkie.
12. **Penetrazio-probatzaileak (Penetration Tester**)

    Kontrolatutako penetrazio-probak egiten ditu ahultasunak aurkitzeko eta zuzentzeko neurriak gomendatzeko.

Laburpena

ECSF (Europako Zibersegurtasun Gaitasun Esparrua) EBren tresna estrategiko bat da, Europako zibersegurtasun ekosistema harmonizatzeko, profesionalizatzeko eta indartzeko, kontinenteak gero eta mehatxu digitalei aurre egiteko behar dituen adituak trebatzen, kontratatzen eta garatzen lagunduz.

3. Informazio Teknologien Inguruneetako Zibersegurtasuneko Espezializazio Ikastaroaren Aurkezpena

479/2020 Errege Dekretua, apirilaren 7koa, Informazioaren Teknologien Inguruneetako Zibersegurtasuneko Espezializazio Ikastaroa ezartzen eta curriculumaren oinarrizko alderdiak ezartzen dituena.

83/2023 BOPV DEKRETUA, ekainaren 6koa, Informazioaren Teknologien Inguruneetako Zibersegurtasuneko espezializazio ikastaroari dagozkion curriculumak ezartzen dituena.

NAN

Izena : Zibersegurtasuna informazio-teknologiako inguruneetan.

Maila : Goi Mailako Lanbide Heziketa.

Iraupena : 900 ordu

Lanbide Familia : Informazioaren Teknologia eta Komunikazioak (Lanbide Heziketako ikastaroak sailkatzeko soilik).

Jakintza adarra : Ingeniaritza eta Arkitektura.

ECTS kredituak : 43.

Gaitasun orokorra:

Espezializazio ikastaro honen gaitasun orokorra informazio sistemetan segurtasun estrategiak definitzean eta ezartzean datza, zibersegurtasun diagnostikoak eginez, ahultasunak identifikatuz eta horiek arintzeko beharrezko neurriak ezarriz, egungo araudia eta industria estandarrak aplikatuz, kalitate, lan arriskuen prebentzio eta ingurumen babes protokoloak jarraituz.

Modulu profesionalak.

Kodea	Modulu Profesionala	Denbora-esleipena
5021	Zibersegurtasuneko gertakariak	105
5022	Sare eta sistemaren babesa	240
5023	Ekoizpenaren abiaraztea segurua	150
5024	Ordenagailu forentsea	120
5025	Hacking etikoa	150
5026	Zibersegurtasun araudia	60
E300	Oinarrizko oinarriak	75
	Guztira	900

4. Ingurune Teknologiko Operatiboetan Zibersegurtasuneko Espezializazio Ikastaroaren Aurkezpena

478/2020 Errege Dekretua, apirilaren 7koa, Eragiketa Teknologiko Inguruneetako Zibersegurtasuneko Espezializazio Ikastaroa ezartzen duena

83/2023 BOVP DEKRETUA, ekainaren 6koa, Ingurune Teknologiko Operatiboetako Zibersegurtasuneko espezializazio ikastaroaren curriculumak ezartzen dituena

NAN

Izenburua : Zibersegurtasuna Eragiketa Teknologikoko Inguruneetan. **Maila** : Goi Mailako Lanbide Heziketa.

Iraupena : 900 ordu.

Lanbide Familia : Elektrizitatea eta Elektronika (Lanbide Heziketako ikastaroak sailkatzeko soilik).

Jakintza adarra : Ingeniaritza eta Arkitektura.

ECTS kredituak : 43.

Gaitasun orokorra

Espezializazio ikastaro honen gaitasun orokorra erakundeetan eta industria azpiegituretan segurtasun estrategiak definitzean eta ezartzean datza, zibersegurtasun diagnostikoak eginez, ahultasunak identifikatuz eta horiek arintzeko beharrezko neurriak ezarriz, egungo araudia eta industria estandarrak aplikatuz, kalitate, lan arriskuen prebentzio eta ingurumen babes protokoloak jarraituz.

Modulu profesionalak

Kodea	Modulu Profesionala	Denbora-esleipena
5027	Zibersegurtasuna industria-proiektuetan	150
5028	Industria-kontrol sistema seguruak	180
5029	Industria-komunikazio sare seguruak	210
5030	Zibersegurtasun industrialeko analisi forentsea	240
5031	Segurtasun integrala	120
	Guztira	900

5. EUROPAKO ESPARRUAREN PROFILEN ETA IT/OT DEKRETUEN GAITASUN PROFESIONALEN ARTEKO ERLAZIOA AZTERTU.

ENISAren Zibersegurtasunerako Europako Gaitasun Esparruaren (ECSF) eta Informazioaren Teknologien Inguruneetako Zibersegurtasuneko Espezializazio Ikastaroaren curriculumaren edukiaren (Dekretua) arteko konparazio-analisi bat egin da.

Profil bakoitzean, zeregin nagusiak (Zeregin nagusia) modul bakoitzaren ikaskuntza-emaitzekin (RA) erlazionatu dira, trebetasun nagusiak (Trebetasun nagusiak) gaitasun pertsonal eta sozial profesionalekin, eta ezagutza nagusiak (Ezagutza nagusiak) modul bakoitzaren edukiekin.

- Zeregin nagusia > Modulua (RA)
- Gaitasun nagusiak > Trebetasun pertsonalak, sozialak eta profesionalak
- Ezagutza gakoak > Moduluak (Edukiak)

5.1. ECSFren analisia eta IT dekretua

5.1.1. Ikuspegi orokorrak

Egindako azterketaren ondoren —eta hurrengo ataletan xehetasunetan sartu aurretik—, ikuspegi orokor gisa, azalduko dugu zer neurritan ondorioztatzen dugun gure Dekretuak ECSF profilak jorratzen dituela.

ECSF	Zeregin nagusia(k)	Trebetasun gakoa(k)	Ezagutza gakoa	Guztira %
Dekretua	%55	%54	%63	%58

Ikusiko dugunez, puntuazio altuenak dituzten profilak ezagutza teknikoagoekin lotuta daude, eta puntuazio baxuagoak dituztenak, berriz, kudeaketa edo irakaskuntza rolekin lotuta daude, eta hori guztiz ulergarria da espezializazio ikastaroen izaera kontuan hartuta.

5.1.2. Informazio zehatzagoa

Profil bakoitzeko puntuazio osoak (zereginen, trebetasunen eta ezagutzen batura) lerrokatzea kalkulatzeko aukera ematen digu. Balio altuagoek Dekretua Europako esparruarekin lerrokatze handiagoa adierazten dute. Jarraian, profilaren araberako lerrokatze osoaren ehunekoaren arabera ordenatutako taula bat ageri da:

Profila	Zeregin nagusia(k)	Trebetasun gakoa(k)	Ezagutza gakoa	Guztira %
Penetrazio Analista	%81	%77	%88	%82
Zibersegurtasun Arriskuen Kudeatzailea	%75	%92	%65	%77
Auzitegi Digitaleko Ikertzailea	%88	%70	%73	%77
Zibersegurtasun Inplementatzailea	%70	%64	%75	%70
Lege, Politika eta Ziberbetetze arduraduna	%56	%53	%70	%60
Zibersegurtasuneko Ikertzailea	%58	%64	%50	%58
Ziber-intzidenteen erantzun arduraduna	%61	%46	%63	%57
Zibersegurtasun Auditorea	%38	%50	%72	%53
Zibersegurtasun Arkitektoa	%46	%40	%62	%49
Informazio Segurtasuneko zuzendaria	%32	%41	%52	%42
Zibermehatxuen Inteligentzia Espezialista	%46	%33	%42	%40
Zibersegurtasuneko hezitzailea	%13	%19	%47	%26

5.1.3. Lerrokatzearen araberako sailkapena

Lerrokatze sendoagoa: funtzio teknikoak eta praktikoak

Bat etortze-tasarik altuenak ikasgelan praktikan jar daitezkeen ezagutza tekniko handiagoak behar dituzten profiletan aurkitzen dira.

Profila	Zeregin nagusia(k)	Trebetasun gakoa(k)	Ezagutza gakoa	Guztira %
Penetrazio Analista	%81	%77	%88	%82
Zibersegurtasun Arriskuen Kudeatzailea	%75	%92	%65	%77
Auzitegi Digitaleko Ikertzailea	%88	%70	%73	%77
Zibersegurtasun Inplementatzailea	%70	%64	%75	%70

Lerrokatze moderatua: profil estrategikoak eta gobernantza-orientatuak

Hainbat profilek lerrokatze-maila moderatua erakusten dute; profil hauek xehetasunez landu ahal izan dira ikasgelan, baina zailagoak dira ikasgelan erabiltzen diren bezalako ingurune simulatuetan lantzen.

Profila	Zeregin nagusia(k)	Trebetasun gakoa(k)	Ezagutza gakoa	Guztira %
Lege, Politika eta Ziberbetetze arduraduna	%56	%53	%70	%60
Zibersegurtasuneko Ikertzailea	%58	%64	%50	%58
Ziber-intzidenteen erantzun arduraduna	%61	%46	%63	%57
Zibersegurtasun Auditorea	%38	%50	%72	%53
Zibersegurtasun Arkitektoa	%46	%40	%62	%49

Beheko lerroa: profil espezializatuak edo kudeaketa profilak

Espero bezala, profil zehatzagoek, kudeaketa osagai handiagoa dutenek edo irismen estrategikoarekin lotutakoek, lerrokatze maila txikiagoa dute.

Profila	Zeregin nagusia(k)	Trebetasun gakoa(k)	Ezagutza gakoa	Guztira %
Informazio Segurtasuneko zuzendaria	%32	%41	%52	%42
Zibermehatxuen Inteligentzia Espezialista	%46	%33	%42	%40
Zibersegurtasuneko hezitzailea	%13	%19	%47	%26

5.1.4. Ondorioak

Datuen arabera, Dekretuak ECSFk definitutako profilen xehetasunen % 50 baino gehiago hartzen ditu barne, oro har. Zehazki, lau profil oso lerrokatuta daude (% 70 edo gehiago), bost neurriz lerrokatuta daude (% 45 edo gehiago), eta hiru ahulki lerrokatuta daude (% 45 baino gutxiago). Gainera, 12 profiletatik, zortzi % 50etik gora lerrokatuta daude, eta hiru % 75etik gora.

Uste dugu espezializazio ikastaro oso baterako, datuek erakusten dutela curriculuma oso egokituta dagoela eta Europako zibersegurtasuneko funtzio tekniko gakoekin lerrokatuta dagoela.

5.2. ECSFren analisia eta OT dekretua

5.2.1. Ikuspegi orokorrak

Egindako azterketaren ondoren —eta hurrengo ataletan xehetasunetan sartu aurretik—, ikuspegi orokor gisa, azalduko dugu zer neurritan ondorioztatzen dugun gure Dekretuak ECSF profilak jorratzen dituela.

ECSF	Zeregin nagusia(k)	Trebetasun gakoa(k)	Ezagutza gakoa	Guztira %
Dekretua	%54	%56	%59	%56

Datuek profil profesionalen eta OT ingurunearen beharren arteko lerrokatze maila desberdinak erakusten dituzte. Puntuazio konbinatu altuagoak dituzten funtzioek eragiketa teknikoekin lerrokatze sendoagoa adierazten dute, eta beste batzuk beren osagai estrategikoengatik edo espezializazio tematikoagatik nabarmentzen dira.

5.2.2. Informazio zehatza

Rolaren araberako puntuazio osoak (zereginen, trebetasunen eta ezagutzen batura) lerrokatzea kalkulatzeko aukera ematen digu. Balio altuagoek OT arloarekin egokitasun handiagoa adierazten dute, bai teknikoki bai funtzionalki. Rolaren araberako guztizkoa behean erakusten da, beheranzko ordenan ordenatuta:

OT	Zeregin nagusia(k)	Trebetasun gakoa(k)	Ezagutza gakoa	Guztira %
Zibersegurtasun Arriskuen Kudeatzailea	%94	%88	%75	%86
Zibersegurtasun Inplementatzailea	%83	%75	%68	%75
Penetrazio Ebaluatzailea	%78	%70	%77	%75
Auzitegi Digitaleko Ikertzailea	%58	%70	%52	%60
Zibersegurtasun Arkitektoa	%67	%48	%62	%59
Ziber-intzidenteen kudeatzailea	%59	%50	%65	%58
Zibersegurtasuneko Ikertzailea	%52	%71	%45	%56
Zibermehatxuen Inteligentzia Espezialista	%46	%48	%48	%47
Informazio Segurtasuneko zuzendaria	%37	%47	%57	%47
Lege, Politika eta Ziberbetetze Aholkularitza	%35	%34	%70	%46
Zibersegurtasun Auditorea	%27	%38	%53	%39
Zibersegurtasuneko hezitzailea	%6	%28	%41	%25

5.2.3. Lerrokatzearen araberako sailkapena

Lerrokatze sendoagoa: funtzio teknikoak eta praktikoak

OT-n inplementazioan eta funtzionamenduan oinarritutako puntuazio oso altuena duten rolak:

Bat etortze-tasarik altuenak ikasgelan praktikan jar daitezkeen ezagutza tekniko handiagoak behar dituzten profiletan aurkitzen dira.

Zibersegurtasun Arriskuen Kudeatzailea	%94	%88	%75	%86
Zibersegurtasun Inplementatzailea	%83	%75	%68	%75
Penetrazio Ebaluatzailea	%78	%70	%77	%75

Lerrokatze moderatua: Estrategikoa eta gobernantzan oinarritua

Teknika eta kudeaketa politikoaren arteko ikuspegi mistoa duten rolak:

Hainbat profilek lerrokatze-maila moderatua erakusten dute; profil hauek xehetasunez landu ahal izan dira ikasgelan, baina zailagoak dira ikasgelan erabiltzen diren bezalako ingurune simulatuetan lantzen.

Auzitegi Digitaleko Ikertzailea	%58	%70	%52	%60
Zibersegurtasun Arkitektoa	%67	%48	%62	%59
Ziber-intzidenteen kudeatzailea	%59	%50	%65	%58
Zibersegurtasuneko Ikertzailea	%52	%71	%45	%56
Zibermehatxuen Inteligentzia Espezialista	%46	%48	%48	%47
Informazio Segurtasuneko zuzendaria	%37	%47	%57	%47
Lege, Politika eta Ziberbetetze Aholkularitza	%35	%34	%70	%46

Beheko lerrokatzea: Rol espezializatuak edo nitxoak

Testuinguru zehatzetara bideratua, hezkuntzakoak edo entzumenekoak, eta, oro har, OT pisu gutxiagorekin:

Espero bezala, profil zehatzagoek, kudeaketa osagai handiagoa dutenek edo irismen estrategikoarekin lotutakoek, lerrokatze maila txikiagoa dute.

Zibersegurtasun Auditorea	%27	%38	%53	%39
Zibersegurtasuneko hezitzailea	%6	%28	%41	%25

5.2.4. Ondorioak

Datuen arabera, Dekretuak ECSFk definitutako profilen xehetasunen % 50 baino gehiago hartzen ditu barne, oro har. Zehazki, hiru profil daude oso lerrokatuta (% 70 edo gehiago), zazpi neurriz lerrokatuta (% 45 edo gehiago) eta bi ahulki lerrokatuta (% 45 baino gutxiago). Gainera, 12 profiletatik zazpik % 50eko lerrokatzea gainditzen dute, eta hiruk % 75.

Aztertutako rol gehienek OT eskakizunekin bat datoz ondo, batez ere inplementazio teknikoan, segurtasun arkitekturan eta intzidenteei erantzunean oinarritutakoak. Kudeaketa tekniko eta politikoaren arteko profil mistoak tarteko nonbait kokatuko lirateke, hezkuntzan, politikan edo analisi forentsean oinarritutako profilek, berriz, ekarpen mugatuagoa dute, nahiz eta testuinguru zehatzetan garrantzitsuak izan.

IT balioen arteko aldea logikoa da instalazioen izaera desberdina kontuan hartuta. OT arloan, arkitekturak, gertakarien kudeaketak eta arriskuen kudeaketak dute lehentasuna, ekoizpen instalazio bat baita. Kudeaketa eta auditoria bigarren mailakoak dira.

Uste dugu espezializazio ikastaro oso baterako, datuek erakusten dutela curriculuma oso egokituta dagoela eta Europako zibersegurtasuneko funtzio tekniko gakoekin lerrokatuta dagoela.

6. Profilen eta Dekretuaren arteko erlazio-taulak

CHIEF INFORMATION SECURITY OFFICER (CISO) Informazioaren Segurtasuneko Zuzendari Nagusia

KONTZEPTUA	IT Dekretuaren BAT ETORTZEKO TASA	PARTIDAZIO-TASA Dekretu OT-N
Zeregin nagusia(k)	%32	%37
Trebetasun Nagusia(k)	%41	%47
Ezagutza gakoa	%52	%57
	%42	%47

CYBER INCIDENT RESPONDER Zibermehatxuen Inteligentzia Espezialista

KONTZEPTUA	IT Dekretuaren BAT ETORTZEKO TASA	PARTIDAZIO-TASA Dekretu OT-N
Zeregin nagusia(k)	%61	%59
Trebetasun Nagusia(k)	%46	%50
Ezagutza gakoa	%63	%65
	%57	%58

CYBER LEGAL, POLICY & COMPLIANCE OFFICER Ziberlege politika, betetze eta gai juridikoen arduraduna

KONTZEPTUA	IT Dekretuaren BAT ETORTZEKO TASA	PARTIDAZIO-TASA Dekretu OT-N
Zeregin nagusia(k)	%56	%35
Trebetasun Nagusia(k)	%53	%34
Ezagutza gakoa	%70	%70
	%60	%46

CYBER THREAT INTELLIGENCE SPECIALIST Zibermehatxuen Inteligentzia Espezialista

KONTZEPTUA	IT Dekretuaren BAT ETORTZEKO TASA	PARTIDAZIO-TASA Dekretu OT-N
Zeregin nagusia(k)	%46	%46
Trebetasun Nagusia(k)	%33	%48
Ezagutza gakoa	%42	%48
	%40	%47

CYBERSECURITY ARCHITECT Zibersegurtasuneko arkitektoak

KONTZEPTUA	IT Dekretuaren BAT ETORTZEKO TASA	PARTIDAZIO-TASA Dekretu OT-N
Zeregin nagusia(k)	%46	%67
Trebetasun Nagusia(k)	%40	%48
Ezagutza gakoa	%62	%62
	%49	%59

CYBERSECURITY AUDITOR Zibersegurtasun auditorea

KONTZEPTUA	IT Dekretuaren BAT ETORTZEKO TASA	PARTIDAZIO-TASA Dekretu OT-N
Zeregin nagusia(k)	%38	%27
Trebetasun Nagusia(k)	%50	%38
Ezagutza gakoa	%72	%53
	%53	%39

CYBERSECURITY EDUCATOR Zibersegurtasun hezitzailea

KONTZEPTUA	IT Dekretuaren BAT ETORTZEKO TASA	PARTIDAZIO-TASA Dekretu OT-N
Zeregin nagusia(k)	%13	%6
Trebetasun Nagusia(k)	%19	%28
Ezagutza gakoa	%47	%41
	%26	%25

ZIBERSEGURTASUN INPLEMENTATZAILEA Zibersegurtasun Inplementatzailea

KONTZEPTUA	IT Dekretuaren BAT ETORTZEKO TASA	PARTIDAZIO-TASA Dekretu OT-N
Zeregin nagusia(k)	%70	%83
Trebetasun Nagusia(k)	%64	%75
Ezagutza gakoa	%75	%68
	%70	%75

CYBERSECURITY RESEARCHER Zibersegurtasun ikertzailea

KONTZEPTUA	IT Dekretuaren BAT ETORTZEKO TASA	PARTIDAZIO-TASA Dekretu OT-N
Zeregin nagusia(k)	%58	%52
Trebetasun Nagusia(k)	%64	%71
Ezagutza gakoa	%50	%45
	%58	%56

CYBERSECURITY RISK MANAGER Zibersegurtasun arriskuen kudeatzailea

KONTZEPTUA	IT Dekretuaren BAT ETORTZEKO TASA	PARTIDAZIO-TASA Dekretu OT-N
Zeregin nagusia(k)	%75	%94
Trebetasun Nagusia(k)	%92	%88
Ezagutza gakoa	%65	%75
	%77	%85

DIGITAL FORENSICS INVESTIGATOR Auzitegi Digitaleko Ikertzailea

KONTZEPTUA	IT Dekretuaren BAT ETORTZEKO TASA	PARTIDAZIO-TASA Dekretu OT-N
Zeregin nagusia(k)	%88	%58
Trebetasun Nagusia(k)	%70	%70
Ezagutza gakoa	%73	%52
	%77	%60

PENETRATION TESTER Penetrazio-probatzaileak

KONTZEPTUA	IT Dekretuaren BAT ETORTZEKO TASA	PARTIDAZIO-TASA Dekretu OT-N
Zeregin nagusia(k)	%81	%78
Trebetasun Nagusia(k)	%77	%70
Ezagutza gakoa	%88	%77
	%82	%75

Laburpen taula %

	ELEMENTUA					OT			
	Zeregin nagusia(k)	Trebetasun gakoa(k)	Ezagutza gakoa	Guztira %		Zeregin nagusia(k)	Trebetasun gakoa(k)	Ezagutza gakoa	Guztira %
Informazioaren Segurtasuneko Zuzendari Nagusia (CISO)	%32	%41	%52	%42		%37	%47	%57	%47
Ziber-intzidenteen erantzuna	%61	%46	%63	%57		%59	%50	%65	%58
Ziberpolitika, Betetze eta Gai Juridikoen arduraduna	%56	%53	%70	%60		%35	%34	%70	%46
Zibermehatxuen Inteligentzia Espezialista	%46	%33	%42	%40		%46	%48	%48	%47
Zibersegurtasun Arkitektoa	%46	%40	%62	%49		%67	%48	%62	%59
Zibersegurtasun-ikuskatzailea	%38	%50	%72	%53		%27	%38	%53	%39
Zibersegurtasuneko hezitzailea	%13	%19	%47	%26		%6	%28	%41	%25
Zibersegurtasun Inplementatzailea	%70	%64	%75	%70		%83	%75	%68	%75
Zibersegurtasuneko ikertzailea	%58	%64	%50	%58		%52	%71	%45	%56
Zibersegurtasun Arriskuen Kudeatzailea	%75	%92	%65	%77		%94	%88	%75	%85
Auzitegi Digitaleko Ikertzailea	%88	%70	%73	%77		%58	%70	%52	%60
Penetrazio-probatzailea	%81	%77	%88	%82		%78	%70	%77	%75

Profilak (ECSF) % IT

ELEMENTUA	Zeregin nagusia(k)	Trebetasun gakoa(k)	Ezagutza gakoa	Guztira %
Penetrazio Analista	%81	%77	%88	%82
Zibersegurtasun Arriskuen Kudeatzailea	%75	%92	%65	%77
Auzitegi Digitaleko Ikertzailea	%88	%70	%73	%77
Zibersegurtasun Inplementatzailea	%70	%64	%75	%70
Lege, Politika eta Ziberbetetze arduraduna	%56	%53	%70	%60
Zibersegurtasuneko Ikertzailea	%58	%64	%50	%58
Ziber-intzidenteen erantzun arduraduna	%61	%46	%63	%57
Zibersegurtasun Auditorea	%38	%50	%72	%53
Zibersegurtasun Arkitektoa	%46	%40	%62	%49
Informazio Segurtasuneko zuzendaria	%32	%41	%52	%42
Zibermehatxuen Inteligentzia Espezialista	%46	%33	%42	%40
Zibersegurtasuneko hezitzailea	%13	%19	%47	%26

Profilak (ECSF) % OT

OT	Zeregin nagusia(k)	Trebetasun gakoa(k)	Ezagutza gakoa	Guztira %
Zibersegurtasun Arriskuen Kudeatzailea	%94	%88	%75	%86
Zibersegurtasun Inplementatzailea	%83	%75	%68	%75
Penetrazio Ebaluatzailea	%78	%70	%77	%75
Auzitegi Digitaleko Ikertzailea	%58	%70	%52	%60
Zibersegurtasun Arkitektoa	%67	%48	%62	%59
Ziber-intzidenteen kudeatzailea	%59	%50	%65	%58
Zibersegurtasuneko Ikertzailea	%52	%71	%45	%56
Zibermehatxuen Inteligentzia Espezialista	%46	%48	%48	%47
Informazio Segurtasuneko zuzendaria	%37	%47	%57	%47
Lege, Politika eta Ziberbetetze Aholkularitza	%35	%34	%70	%46
Zibersegurtasun Auditorea	%27	%38	%53	%39
Zibersegurtasuneko hezitzailea	%6	%28	%41	%25

7. Literatura

Enisa *:* https://www.enisa.europa.eu/

Europako Zibersegurtasun Gaitasun Esparrua (ECSF)

https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf

Lanbide Heziketako Ezagutzarako Institutua IVAC EEI

https://ivac-eei.eus/es/

INFORMAZIO TEKNOLOGIA INGURUNETAN ZIBERSEGURTASUNERAKO ESPEZIALIZAZIO IKASTAROA

https://ivac-eei.eus/es/familias-profesionales/informatica-y-comunicaciones-ifc/especializaciones/curso-de-especializacion-en-ciberseguridad-en-entornos-de-las-tecnologias-de-la-informacion.html

ESPEZIALIZAZIO IKASTAROA ERAGIKETA TEKNOLOGIA INGURUNETAN

https://ivac-eei.eus/es/familias-profesionales/electricidad-y-electronica-ele/especializaciones/curso-de-especializacion-en-ciberseguridad-en-entornos-de-las-tecnologias-de-operacion.html

➢ ERANSKINA : *PROFILEN ZERRENDA OSOA ETA DEKRETUA*

Betetze maila (RATE) ECSFren "Xehetasun" bakoitzaren dekretuan kuantifikatu da, eskala hau kontuan hartuta: % 0 - % 25 - % 50 - % 75 - % 100

1- Chief Information Security Officer Informazioaren Segurtasuneko arduradun nagusia

	Xehetasuna	ELEMENTUA	IT TASA	OT	OT TASA
Zeregin nagusia	Zibersegurtasun helburuak, eskakizunak, estrategiak eta politikak definitu, ezarri, komunikatu eta mantendu, negozio-estrategiarekin lerrokatuta, erakundearen helburuak laguntzeko.	M1:RA1(Ea);M2:RA 3(Ef)	%50	M1:RA1(Ea,Eb, Ed),RA2(Ec.Ed); M2:RA5(Ed)	%50
	Zibersegurtasun ikuspegia, estrategiak eta politikak prestatu eta aurkeztea erakundeko goi zuzendaritzak onar dezan, eta horien exekuzioa bermatzea.		%0	M4:RA1(Ef,Eg)	%25
	Informazioaren Segurtasun Kudeaketa Sistemaren (ISKS) aplikazioa eta hobekuntza kontrolatzea		%0	M1:RA4(Ea,Ec, Ef);M5:RA5(Ea, Eb,Ec,Ee)	%25
	Goi-zuzendaritzari zibersegurtasun-arriskuei, mehatxuei eta erakundean duten eraginari buruzko informazioa eman.	M1:RA1(Eb,Ec);M2: RA3(Ea),RA10(Ea)	%75	M5:RA2(Ea,Ed, Eg)	%25
	Ziurtatu goi-zuzendaritzak erakundearen zibersegurtasun-arriskuak onartzen dituela.	M2:RA3(Ec);M6:RA 2(Ec)	%50	M5:RA5(Ed,eE)	%25
	Zibersegurtasun planak garatu		%0	M1:RA1(Ee),RA 3(EC)	%75
	Zibersegurtasunarekin lotutako agintariekin eta komunitateekin harremanak garatu	M1:RA3(Ee); M6:RA1(Ee)	%50	M5:RA2(Ef,Eg); RA3(Ec,Ed)	%50
	Zibersegurtasun-intzidenteen, arriskuen eta aurkikuntzen berri eman goi-zuzendariari	M1:RA2(Ec,Ed,Ee),R A5(Eb)	%50	M4:RA1(Ef),RA 4(Ef)	%50
	Zibersegurtasunean aurrerapenak kontrolatu	M1:RA2(Eb,Ed);M2: RA7(Eh); M3:RA7(Ed);M5:RA 1(Ei)	%100	M3:RA9(Ea,Ed, EE)	%100

	Zibersegurtasun estrategia ezartzeko baliabideak ziurtatu	M2:RA3(e)	%25	M1:RA2(Ea,Eb)	%25
	Negoziatu zibersegurtasun aurrekontua goi-zuzendaritzarekin		%0	M1:RA2(Ed,Ef)	%0
	Ziber-intzidenteen aurrean erakundearen erresilientzia bermatzea	M1:RA4(Ea,Eb,Ed)	%50	M4:RA6(Eb,Ec, Eg)	%50
	Kudeatu etengabeko gaitasunak eraikitzea erakundearen barruan		%0	M5:RA1(Ea,Ee), RA2(Ee,Ef)	%25
	Zibersegurtasun baliabide egokiak berrikusi, planifikatu eta esleitu		%0	M1:RA2(Eb,Ed)	%0
	BETETZE MAILA		%32		%38
Trebetasun gakoa(k)	Erakunde baten zibersegurtasun-jarrera ebaluatu eta hobetu	Aire girotua	%25	Ca,Cb	%35
	Zibersegurtasun politikak, ziurtagiriak, estandarrak, metodologiak eta esparruak aztertu eta ezartzea	Ce,Ck	%75	Cb,Cg	%75
	Zibersegurtasunarekin lotutako legeak, araudiak eta legedia aztertu eta bete	Ca,Cl,Cm	%100	Ck	%100
	Zibersegurtasun gomendioak eta jardunbide egokiak ezartzea	Cb,Cc	%100	Cj,Ch	%100
	Zibersegurtasun baliabideak kudeatu		%0	Cl,Cm	%25
	Zibersegurtasun estrategia bat garatu, bultzatu eta gauzatzea zuzendu	Cb,Cc	%25	Cm,Cn	%25
	Erakunde baten zibersegurtasun-kulturan eragina izan	Ca,Cl	%25	Cn	%25
	Informazioaren Segurtasun Kudeaketa Sistema (ISKS) diseinatu, aplikatu, monitorizatu eta berrikusi, zuzenean edo bere azpikontratazioa zuzenduz.		%0	Ch,Cc	%25
	Segurtasun dokumentuak, txostenak eta SLAk berrikusi eta hobetu, eta segurtasun helburuak bermatu.		%0	Cc,Ck	%25
	Zibersegurtasunarekin lotutako arazoak identifikatu eta konpondu	Cf,Ci	%100	Ci,Cm	%75
	Zibersegurtasun plan bat ezarri	Ca,Cc	%50	Cd,Ca	%50
	Barneko eta kanpoko interesdunekin komunikatu, koordinatu eta lankidetzan aritu	Cñ	%50	Cg,Cn	%50
	Erakundearen informazio-segurtasun estrategian beharrezkoak diren aldaketak aurreikusi eta plan berriak formulatu	DC	%50	Ce,Cf	%50
	Zibersegurtasun kudeaketarako heldutasun ereduak definitu eta aplikatu		%0	Cf	%25

	Aurreikusi zibersegurtasun mehatxuak, beharrak eta etorkizuneko erronkak		%0	EE	%50
	Jendea motibatu eta animatu	Cñ	%50	Zentimetroak	%25
	BETETZE MAILA		%41		%48
Ezagutza gakoa	Zibersegurtasun politikak	M2:RA3(C4),RA6(C9),RA9(C8);M7:RA2(C3)	%100	M2:RA5(C1,C2,C3);M5:RA1(C1,C2,C3),RA2(C1,C2,C3,RA3(C1,C2,C3)	%100
	Zibersegurtasuneko estandarrak, metodologiak eta esparruak	M2:RA3(C6);M3:RA6(C4);M6:RA5(C2,C5)	%100	M3:RA2(C10);M5:RA5(C1,C2,C3)	%100
	Zibersegurtasuneko gomendioak eta jardunbide egokiak	M2:RA3(C5,C7);M6:RA5(C3);	%50	M3:RA7(C1,C5,C6);M5:RA5(C1,C3)	%100
	Zibersegurtasunarekin lotutako legeak, araudiak eta legedia	M6:RA3(C1,C2,C3),RA4(C*),RA5(C8)	%100	M5:RA5(C2,C3)	%50
	Zibersegurtasunarekin lotutako ziurtagiriak		%0	M1:RA2(C1,C2,C4);M5:RA5(C3)	%0
	Zibersegurtasun etikoaren erakundearen eskakizunak	M6:RA1(C1)	%25	M2:RA1(C1,C3);M5:RA5(C1,C3)	%25
	Zibersegurtasuneko heldutasun ereduak		%0	M1:RA1(C1,C5)	%25
	Zibersegurtasun prozedurak	M1:RA4(C1),RA5(C1);M2:RA3(C7),RA7(C17)	%100	M1:RA5(C2,C3);M4:RA6(C1,C5)	%100
	Baliabideen kudeaketa		%0	M1:RA2(C1,C3);M5:RA1(C3)	%25
	Kudeaketa praktikak		%0	M1:RA2(C2,C3);M5:RA5(C1,C2,C3)	%25
	Arriskuen kudeaketarako estandarrak, metodologiak eta esparruak	M2:RA3(C1);M3:RA5(C2);M6:RA2(C3)	%100	M5:RA5(C1,C2,C3)	%75
	BETETZE MAILA		%52		%57

2- **Cyber Incident Responder** Ziber-intzidenteen erantzuna

	Xehetasuna	ELEMENTUA	IT TASA	OT	OT TASA
	Istripuen Erantzun Planaren garapenean, mantentzean eta ebaluazioan lagundu	M1:RA5(Ea)	%25	M4:RA6(Ea,Eb),M5:RA5(Ea,Eb,Ec,Ee)	%25
	Intzidenteen kudeaketarekin lotutako prozedurak garatu, ezarri eta ebaluatu	M1:RA4(Ea,Eb),RA5(Ea)	%50	M4:RA6(Ea,Eb,Ec,Ee)	%50
	Zibersegurtasun-intzidenteak identifikatu, aztertu, arindu eta komunikatu	M1:RA2(Eb),RA3(Ea,Ed),RA5(Eb,Ec,Ed,Ee)	%100	M4:RA1(Ec,Ed),RA6(Ea,Ef,Eg)	%100
	Ahultasun teknikoak ebaluatu eta kudeatu	M2:RA3(Ea),RA4(Eb,Ec,Ed,Ee),RA9(Eg,Eh);M3:RA6(Ec);M5:RA1(Ef,Eh),RA2(Eb,Ed,Ee,Eg),RA3(Eb,Ee,Ef),RA5(Ed,Ee,Ef,Eg)	%100	M3:RA8(Ea,Ed,Ee)	%100
	Zibersegurtasun-intzidenteen detekzio eta erantzunaren eraginkortasuna neurtu	M1:RA2(Eb,Ed),RA3(Eb,Ef),RA4(Ea,Eb,Ed),	%100	M3:RA9(EA;Ed,Ee)	%75
Zeregin nagusia(k)	Zibersegurtasun edo datu-urraketa gertakari baten ondoren hartutako zibersegurtasun-kontrolen eta arintze-ekintzen erresilientzia ebaluatu.	M1:RA4(Ea,Eb)	%25	M4:RA6(Eb,Ec,Eg)	%25
	Intzidenteak kudeatzeko probak egiteko teknikak hartu eta garatu	M1:RA2(Eb,Ec,Ed),RA3(Ed),R4(Ea,Ec)	%100	M4:RA6(Ee,Ef)	%75
	Gertaeren emaitzen analisia eta gertaeren kudeaketaren berri emateko prozedurak ezartzea	M1:RA2(Ee),RA5(E*)	%75	M4:RA4(Ea,Ec,Ed)	%75
	Dokumentatu gertakarien emaitzen azterketa eta gertakarien kudeaketa ekintzak	M1:RA5(Ea)	%25	M4;RA5(Ef)	%75
	Lankidetzan aritu Operazio Seguru Zentroekin (SOC) eta Segurtasun Informatikoko Intzidenteen Erantzun Taldeekin (CSIRT)	M1:RA5 (Ed.)	%25	M5:RA5(Ef,Eg)	%25
	Lankidetzan aritu funtsezko langileekin	M1:RA3(Eb,Ee)	%50	M4:RA6(Ef.Eg)	%25

	segurtasun-intzidenteen berri emateko, aplikagarri den lege-esparruaren arabera.				
	BETETZE MAILA		%61		%59
Trebetasun Nagusia(k)	Zibersegurtasun-intzidenteen alderdi tekniko, funtzional eta operatibo guztiak landu manipulazioa eta erantzuna	Cf	%75	Cc, Cd, Cm, Cj, Cn	%75
	Hainbat iturritatik sortutako zibermehatxuen informazioa bildu, aztertu eta erlazionatu	Cb	%75	Ca, Ch, Ci, Cg	%75
	Sistema eragileetan, zerbitzarietan, hodeietan eta azpiegitura garrantzitsuetan lan egin		%0	Cb, Cf, Ch	%0
	Presiopean lan egin	Cñ	%75	Cb, Cf, Ch	%75
	Komunikatu, aurkeztu eta txostenak egin dagokion interesdunei	Cñ	%50	Cl,Cm	%50
	Erregistro fitxategiak kudeatu eta aztertu		%0	Cc, Ck, Cn	%25
	BETETZE MAILA		%46		%50
Ezagutza gakoa	Intzidenteen kudeaketarako estandarrak, metodologiak eta esparruak		%0	M4:RA1(C2,C3,C4);M5:RA5(C1,C3)	%50
	Intzidenteak kudeatzeko gomendioak eta jardunbide egokiak	M1:RA4(C6)	%75	M3:RA10(C1,C2,C3);M4:RA6(C1,C2,C4,C6)	%75
	Intzidenteak kudeatzeko tresnak	M1:RA2(C2,C3,C4)	%50	M3:RA9(C1,C2);M4:RA2(C7,C9)	%50
	Intzidenteak kudeatzeko komunikazio prozedurak	M1:RA3(C5),RA4(C3),RA5(C*)	%100	M4:RA6(C4,C5,C6);M5:RA5(C3,C5)	%75
	Sistema eragileen segurtasuna	M7:RA3(C1,C2)	%75	M2:RA6(C1,C4);M3:RA11(C2,C3)	%75
	Ordenagailu sareen segurtasuna	M2:RA1(C*),RA3(C*),RA6(C*);M7:RA1(C1,C2,C3)	%100	M3:RA5(C1,C2,C4),RA6(C1,C3)	%100
	Zibermehatxuak	M1:RA3(C4);M2:RA3(C1);M	%100	M3:RA8(C5,C6	%100

		3:RA5(C2)		);M4:RA2(C2,C6,C7)	
	Zibersegurtasun erasoen prozedurak	M5:RA2(C4,C5),RA3(C6,C7,C8),RA5(C6),RA6(C4)	%100	M3:RA8(C3,C4);M4:RA6(C2,C6)	%100
	Ordenagailu sistemen ahultasunak	M2:RA10(C10);M3:RA6(C2,C6);M5:RA3(C6,C9),RA5(C5,C6,C7)	%100	M4:RA2(C7,C9)	%100
	Zibersegurtasunarekin lotutako ziurtagiriak		%0	M1:RA2(C2,C3);M5:RA5:C1,C3)	%0
	Zibersegurtasunarekin lotutako legeak, araudiak eta legedia	M6:RA3(C1,C2,C3),RA4(C*),RA5(C8)	%100	M5:RA5(C2,C3)	%100
	Operazio Zentro Seguruen (SOC) funtzionamendua	M2:RA7(C19)	%25	M3:RA9(C1,C2);M4:RA6(C1,C5,C6)	%25
	Ordenagailu Segurtasun Intzidenteen Erantzun Taldeen (CSIRT) funtzionamendua		%0	M4:RA6(C3,C4,C5)	%0
	BETETZE MAILA		%63		%65

3- Cyber Legal, Policy & Compliance Officer Ziber-Lege, Politika eta Betetze Arduraduna

	Xehetasuna	ELEMENTUA	IT TASA	OT	OT TASA
Zeregin nagusia(k)	Datuen pribatutasun eta datuen babeserako estandarren, legeen eta araudien betetzea bermatzea eta aholkularitza juridikoa eta orientazioa ematea	M2:RA4(E*);M3:RA6(Ef);M4:RA4(Ee);M6:RA4(E*)	%100	M5:RA5(Ea,Eb,Ec,Ee)	%50
	Betetze-hutsuneak identifikatu eta dokumentatu	M1:RA1(Ee);M6:RA1(Ea,Ec,Ed,Ee);RA2(Ed);RA3(Ec),RA4(Ed)	%100	M5:RA3(Ea,Eb,Ef),RA5(Ed,Ee)	%75
	Pribatutasunaren gaineko eraginaren ebaluazioak egin eta pribatutasun-politikak eta prozedurak garatu, mantendu, komunikatu eta horien inguruan trebatu.	M1:RA1(Eb,Ec,Ed); M6:RA3(Eb),RA4(Ec)	%75	M5:RA1(Ee,Ef,Eg),RA2(Eb,Ee,Eg)	%50
	Erakundearen datuen pribatutasun eta babes programa betearazi eta defendatu	M1:RA1(Ea); M6:RA4(Ea,Eb,Ec,Ed,Ee,Ef)	%100	M5:RA1(Ec,Ef),RA5(Eb,Ed,Ee)	%50
	Ziurtatu datuen jabeek, titularrek, kontrolatzaileek, prozesatzaileek, subjektuek, barneko edo kanpoko bazkideek eta erakundeek beren datuen babeserako eskubideei buruz informatuta daudela,	M6:RA4(E1)	%25	M5:RA2(Ea,Ed,Eg),RA5(Ee,Ef)	%25
	Datuen tratamenduari buruzko kontsultak eta kexak kudeatzeko harremanetarako puntu nagusi gisa jardun	M6:RA4(Ee)	%25	M4:RA1(Ea,Ef,Eg),RA3(Ef,Eg)	%25
	Zibersegurtasuna eta pribatutasuna betetzen direla bermatzeko, zibersegurtasuna eta pribatutasuna diseinatzen, ezartzen, auditoretza egiten	M1:RA1(Ee);M6:RA4(Ec)	%50	M4:RA1(Eb,Ec,Ee),RA3(Ec,Ee)	%25

	eta betetze-probak egiten laguntzea.				
	Datuen babesarekin lotutako auditoriak eta prestakuntza jarduerak gainbegiratu	M1:RA1(Ec,Ed,Ee)	%50	M5:RA3(Ed,Ef,Eg),RA4(Ea,Ec)	%25
	Lankidetzan aritu eta informazioa partekatu agintariekin eta talde profesionalekin	M1:RA5(Ee)	%25	M5:RA2(Ef,Eg)	%25
	Lagundu erakundearen zibersegurtasun estrategia, politika eta prozedurak garatzen.	M1:RA1(Ec)	%25	M1:RA1(Ea,Eb,Ed)	%25
	Langileen sentsibilizazio prestakuntza garatu eta proposatu, betetzea lortzeko eta erakundearen barruan datuen babesaren kultura sustatzeko.	M6:RA1(Ec),RA3(Ed)	%50	M5:RA2(Ee,Eg), RA3(Ea,Eb)	%25
	Informazioaren segurtasunaren erantzukizunen eta hirugarrenekiko harremanen alderdi legalak kudeatu, legezko, arauzko eta estandarren eskakizunetan kontuan hartzeko gaitasuna izan dezan.	M6:RA1(Ee),RA4(Ea)	%50	M5:RA5(Eb,Ec,Ee)	%25
	BETETZE MAILA		%56		%35
Trebetasun Nagusia(k)	Negozio-estrategiaren, ereduen eta produktuen ulermen osoa eta legezko, arauzko eta estandarren eskakizunak kontuan hartzeko gaitasuna	Ca, Cj	%50	Ca,Ck	%25
	Erakundearen prozesuen, finantzen eta negozio estrategiaren ezarpenarekin lotutako datuen babesaren eta pribatutasunaren gaiei buruzko lan-bizitzako praktikak burutzea.	Cd,Ce	%100	Ca, Cd, Ck	%25

	Zibersegurtasun eta pribatutasun politika eta prozedura egokiak garatzea lideratu, negozioaren beharrak eta legezko eskakizunak osatuz; gainera,	Ca	%25	Ca, Cb, Cj, Cl	%25
	Pribatutasunaren gaineko eraginaren ebaluazioak egin, kontrolatu eta berrikusi, estandarrak, esparruak, metodologiak eta tresnak erabiliz.	Cj	%50	Ca, Cc, Ch, Cj	%25
	Datuen babesaren eta pribatutasunaren gaiak azaldu eta jakinarazi interesdunei eta erabiltzaileei	Cñ	%50	Cl,Cm	%50
	Baldintza eta estandar etikoak ulertu, praktikatu eta bete		%0	Cl	%25
	Ulertu erakundearen zibersegurtasun eta datuen babeserako estrategia eta politiketan lege-esparruaren aldaketen ondorioak.	Ca,Cm	%75	Ca,Ck	%25
	Beste taldekideekin eta lankideekin elkarlanean aritu	Cñ	%75	Cm,Cl	%75
	BETETZE MAILA		%53		%34
Ezagutza gakoa	Zibersegurtasunarekin lotutako legeak, araudiak eta legedia	M6:RA3(C1,C2,C3),RA4(C*),RA5(C8)	%100	M4:RA6(C5,C6); M5:RA5(C3)	%100
	Zibersegurtasuneko estandarrak, metodologiak eta esparruak	M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5)	%100	M2:RA3(C1);M5:RA5(C1,C3)	%100
	Zibersegurtasun politikak	M2:RA3(C4),RA9(C8)	%50	M1:RA4(C3,C5); M2;RA5(C1,C3)	%75
	Legezko, arauzko eta legegintzako betekizunak, gomendioak eta jardunbide egokiak	M2:RA3(C3,C5);M6:RA5(C3)	%75	M5:RA1(C1,C2), RA5(C2,C3)	%50
	Pribatutasunaren gaineko eraginaren ebaluazio-arauak,	M6:RA4(C3,C4)	%25	M4:RA2(C5,C7); M5:RA5(C1,C3)	%25

	metodologiak eta esparruak				
	BETETZE MAILA		%70		%70

4- Cyber Threat Intelligence Specialist Zibermehatxuen Inteligentzia Espezialista

	Xehetasuna	ELEMENTUA	IT TASA	OT	OT TASA
Zeregin nagusia(k)	Erakundearen zibermehatxuen inteligentzia estrategia garatu, ezarri eta kudeatu	M1:RA4(Ea,Ec),RA5(Ea)	%50	M1:RA1(Ea,Eb,Ed);M5:RA5(Ea,Ec,Ee)	%50
	Mehatxuen adimena kudeatzeko planak eta prozedurak garatzea	M1:RA4(Ea,Ec),RA5(Ea)	%50	M5:RA5(Eb,Ed,Ef)	%50
	Negozio-eskakizunak adimen-eskakizunetan bihurtu		%0	M1:RA1(Ea,Ec,Ee)	%25
	Mehatxu-inteligentzia biltzea, aztertzea eta ekintzarako adimena ekoiztea eta segurtasun-interesdunei zabaltzea ezartzea		%0	M4:RA2(Ea,Ec,Ef)	%25
	Erakundearen jomugan dauden zibermehatxu-eragileak identifikatu eta ebaluatu	M1:RA2(Eb,Ec,Ed);M2:RA3(Ea),RA7(Ef);M3:RA5(Ea,Eb)	%100	M3:RA8(Ea,Eb,Ed)	%75
	Zibermehatxu-eragileek erabiltzen dituzten Taktikak, Teknikak eta Prozedurak (TTP) identifikatu, kontrolatu eta ebaluatu, datu eta informazioa iturri irekikoak eta jabedunak aztertuz.	M1:RA2(Eb,Ec,Ed,Ee)	%50	M3:RA7(Ea,Ec),RA8(Ee,Eg)	%50
	Mehatxuen inteligentzia datuetan oinarritutako txosten erabilgarriak sortu	M4:RA1(Ef),Ra3(Ec),RA5(Eh),RA6(Ea,Eb),M5:RA2(Eg),RA3(Ef)	%100	M4:RA4(Eb,Ec,Ed)	%75
	Arintze-planak landu eta aholkuak eman maila taktiko, operatibo eta estrategikoan.	M1:RA4(Ea);M5:RA2(Eg),RA3(Eg),RA5(Eg)	%100	M5:RA5(Ed,Ee)	%100
	Zibermehatxu garrantzitsuei buruzko informazioa partekatu eta	M1:RA3(Ee)	%25	M5:RA2(Ef,Eg)	%25

	kontsumitzeko interesdunekin koordinatzea.				
	Erabili inteligentzia-datuak mehatxuen modelizazioa, Arriskuen Arintzeari buruzko gomendioak eta zibermehatxuen bilaketa laguntzeko.	M1:RA4(Ea),M6:RA3(Eb)	%50	M4:RA3(Eb, Ed,Ee),RA6(Ea,Eg)	%50
	Inteligentzia maila guztietan ireki eta publikoki artikulatu eta komunikatu		%0	M4:RA1(Adi b.)	%0
	Segurtasun-larritasun egokia jakinarazi, arriskuen esposizioa eta haren ondorioak azalduz interesdun ez-teknikoei.	M2:RA3(Ec,Ee)	%25	M4:RA4(Ea, Ef)	%25
	BETETZE MAILA		%46		%46
Trebetasun gakoa (k)	Beste taldekideekin eta lankideekin elkarlanean aritu	Cñ	%75	Cl,Cm	%75
	Hainbat iturritatik sortutako zibermehatxuen informazioa bildu, aztertu eta erlazionatu	Cb	%50	Ca, Cb, Cc, Ch	%75
	Mehatxu-eragileak, TTPak eta kanpainak identifikatu	Cb	%25	Ca,Cb	%50
	Mehatxuen adimenaren kudeaketa prozedurak automatizatu		%0	Cg,Cl	%0
	Azterketa teknikoak eta txostenak egin	Cf	%75	Cc,Ck	%100
	Ziber-jardueretan eragina duten ziber-gertaerak ez direnak identifikatu		%0	Ca,Cd	%50
	Mehatxu eredugarriak, aktoreak eta TTPak	Cb	%25	Ca,Cc	%25
	Barneko eta kanpoko interesdunekin komunikatu, koordinatu eta lankidetzan aritu	Cñ	%50	Cm,Cn	%50
	Komunikatu, aurkeztu eta txostenak egin dagokion interesdunei	Cm	%25	Cc,Ck	%50
	CTI plataformak eta tresnak erabili eta aplikatu		%0	Cg,Ch	%0
	BETETZE MAILA		%33		%48

	Sistema eragileen segurtasuna	M7:RA3(C1,C2)	%25	M2:RA6(C1,C4);M3:RA11(C2,C3)	%25
	Ordenagailu sareen segurtasuna	M2:RA3(C5,C6),RA6(C1)	%50	M3:RA5(C1,C2),RA6(C3)	%100
	Zibersegurtasuneko kontrolak eta irtenbideak	M1:RA2(C2,C3,C4)	%50	M2:RA4(C3,C4);M3:RA10(C3,C5)	%50
	Ordenagailu programazioa	M3:RA1(C*),RA2(C*),RA3(C*),M7:RA4(C*)	%100	M2:RA2(C2,C6)	%75
	Zibermehatxuen Inteligentzia (CTI) estandarrak, metodologiak eta esparruak partekatzeko		%0	M4:RA6(C1,C3,C5)	%0
	Informazioa arduraz zabaltzeko prozedurak	M1:RA3(C5)	%25	M4:RA6(C4,C5)	%25
Ezagutza gakoa	Zibersegurtasunari lotutako domeinu arteko eta mugako domeinuen ezagutza		%0	M1:RA1(C1,C4)	%25
	Zibermehatxuak	M1:RA3(C4);M2:RA3(C1);M3:RA5(C2)	%100	M3:RA8(C3,C5);M4:RA2(C2,C6)	%100
	Zibermehatxuen eragileak	M1:RA3(C4);M2:RA3(C1);M3:RA5(C2)	%100	M3:RA9(C1,C2)	%100
	Zibersegurtasun erasoen prozedurak	M5:RA1(C4),RA2(C4,C5),RA3(C5,C6,C7,C8,C9),RA4(C2),RA5(C3,C6)	%100	M3:RA8(C4,C6)	%100
	Zibermehatxu aurreratu eta iraunkorrak (APT)		%0	M4:RA3(C5)	%25
	Mehatxu-eragileen Taktikak, Teknikak eta Prozedurak (TTPak)		%0	M4:RA4(C4,C5)	%25
	Zibersegurtasunarekin lotutako ziurtagiriak		%0	M5:RA5(C3)	%0
	BETETZE MAILA		%42		%50

5- Cybersecurity Architect Zibersegurtasuneko arkitektoak

	Xehetasuna	ELEMENTUA	IT TASA	OT	OT TASA
Zeregin nagusia(k)	Erakundearen estrategia ezartzeko arkitektura seguru bat diseinatu eta proposatu	M2:RA3(Ee),RA10(Eb)	%50	M1:RA1(Ea,Ee),RA3(Eb,Ec,Ed); M5:RA5(Eb,Ec,Ed)	%50
	Garatu erakundearen zibersegurtasun-arkitektura segurtasun eta pribatutasun eskakizunak betetzeko	M6:R4(Cc),RA5(Eg)	%50	M5:RA4(Ec,Ed),RA5(Ea,Ee)	%75
	Arkitektura-dokumentazioa eta zehaztapenak sortzen ditu	M2:RA3(Ee)	%25	M4:RA4(Eb,Ed,Ef)	%100
	Goi-mailako segurtasun-arkitekturaren diseinua aurkeztu interesdunei		%0	M4:RA4(Ea,Ec,Ef)	%50
	Ezarri ingurune seguru bat sistemen, zerbitzuen eta produktuen garapen-zikloan zehar.	M2:RA6(Ef),RA10(Ef)	%50	M2:RA6(Ea,Eb,Ee)	%75
	Zibersegurtasun osagaien garapena, integrazioa eta mantentzea koordinatzea, zibersegurtasun espezifikazioak bermatuz.	M2:RA10(Adib.)	%25	M2:RA7(Eb,Ed,Eg)	%50
	Erakundearen arkitekturaren zibersegurtasuna aztertu eta ebaluatu	M1:RA1(Ee),M2:RA3(Eb);M3:RA8(Ee)	%100	M3:RA3(Ea,Eb,Ed,Ee)	%100
	Segurtasun-berrikuspenen eta ziurtagirien bidez irtenbide-arkitekturen segurtasuna bermatzea		%0	M5:RA5(Ea,Ed,Ee)	%25
	Beste talde eta lankideekin elkarlanean aritu	M4:RA1 (Adibidez), RA3 (Ed), RA4 (Ef), RA5 (Ei)	%100	M5:RA2(Ef,Eg)	%100
	Zibersegurtasun-irtenbideek erakundearen arkitekturaren diseinuan eta errendimenduan duten eragina ebaluatu.		%0	M3:RA7(Ec,Ee,Ef)	%25
	Egokitu erakundearen arkitektura mehatxu berrietara	M1:RA2(Ea),M2:RA3(Ea),RA10(Ea)	%75	M1:RA4(Ea,Ed,Ef)	%75
	Segurtasun maila egokia mantentzeko,	M2:RA3(Ee),RA	%75	M5:RA5(Ec,Ee,	%75

	inplementatutako arkitektura ebaluatu.	6(Ea);M3:RA5(Eb)		Ef)	
	BETETZE MAILA		%46		%67
Trebetasun gakoa (k)	Erabiltzaileen eta negozioen segurtasun-eskakizunen azterketa egin	Cb	%50	Ca, Cb, Cd	%50
	Zibersegurtasun arkitektura eta funtzionalitate zehaztapenak marraztu	DC	%50	Cc,Ck	%50
	Sistemak deskonposatu eta aztertu segurtasun eta pribatutasun eskakizunak garatzeko eta irtenbide eraginkorrak identifikatzeko.	Cf	%50	Ca, Cg, Ch	%50
	Diseinu bidezko segurtasunean eta pribatutasunean oinarritutako sistemak eta arkitekturak, eta zibersegurtasun printzipio lehenetsiak.	Cc,Ce	%75	Cb,Cj	%75
	Gidatu eta komunikatu inplementatzaileekin eta IT/OT langileekin	Cñ	%25	Cl,Cm	%25
	Komunikatu, aurkeztu eta txostenak egin dagokion interesdunei		%0	Cc,Ck	%25
	Zibersegurtasun arkitekturak proposatu interesdunen beharretan eta aurrekontuan oinarrituta		%0	Ca,Cb	%25
	Hautatu zehaztapen, prozedura eta kontrol egokiak	Cc,Ce	%100	Cj,Cg	%100
	Eraiki erresilientzia arkitektura osoan zehar huts egiten duten puntuen aurka	CDa	%50	Ce,Cn	%50
	Segurtasun-irtenbideen integrazioa koordinatzea		%0	Cd,Cj	%25
	BETETZE MAILA		%40		%48
Ezagutza gakoa	Zibersegurtasunarekin lotutako ziurtagiriak		%0	M1:RA2(C2,C3);M5:RA5(C3)	%0
	Zibersegurtasuneko gomendioak eta jardunbide egokiak	M2:RA3(C5);M6:RA5(C3)	%50	M2:RA5(C1,C3);M3:RA7(C1,C2)	%50
	Zibersegurtasuneko estandarrak, metodologiak eta esparruak	M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5)	%100	M2:RA3(C4);M5:RA5(C3)	%100
	Zibersegurtasunarekin lotutako		%0	M1:RA1(C2,C5)	%25

	eskakizunen analisia				
	Garapen-ziklo segurua		%0	M1:RA4(C3)	%50
	Segurtasun arkitekturaren erreferentzia ereduak	M2:RA6(C6);M3:RA7(C1)	%50	M3:RA2(C1,C6)	%50
	Zibersegurtasunarekin lotutako teknologiak	M1:RA2(C2,C3,C4);M2:RA5(C5),RA8(C1),RA10(C1,C6,C8);M3:RA2(C3)	%100	M2:RA2(C3);M3:RA5(C1,C4)	%100
	Zibersegurtasuneko kontrolak eta irtenbideak	M1:RA2(C2,C3,C4);M2:RA5(C5),RA8(C1),RA10(C1,C6,C8);M3:RA2(C3)	%100	M2:RA4(C4);M3:RA10(C2,C5)	%100
	Zibersegurtasun arriskuak	M2:RA3(C1),M3:RA5(C2);M6:RA2(C3)	%100	M2:RA3(C4);M5:RA5(C2,C3)	%100
	Zibermehatxuak	M1:RA3(C4);M2:RA3(C1);M3:RA5(C2)	%100	M3:RA8(C1,C5);M4:RA2(C2,C7)	%100
	Zibersegurtasun joerak	M2:RA7(C1)	%25	M3:RA2(C8,C10)	%50
	Legezko, arauzko eta legegintzako betekizunak, gomendioak eta jardunbide egokiak	M2:RA3(C3,C5);M6:RA5(C3)	%50	M5:RA1(C2)	%50
	Zibersegurtasun prozedura zaharrak	M6:RA1(C1,C3),RA3(C*),RA5(C3,C4,C5,C6,C7,C8)	%100	M1:RA5(C1,C2)	%100
	Pribatutasuna Hobetzeko Teknologiak (PET)	M2:RA4(C1,C2);M6:RA4(C3,C4)	%75	M5:RA5(C3)	%25
	Pribatutasun-diseinuaren estandarrak, metodologiak eta esparruak	M6:RA4(C2),RA5(C2,C4,C6,C7,C8)	%75	M5:RA5(C1,C3)	%25
	BETETZE MAILA		%62		%62

6- Cybersecurity Auditor Zibersegurtasun-ikuskatzaileak

	Xehetasuna	ELEMENTUA	IT TASA	OT	OT TASA
Zeregin nagusia(k)	Erakundearen auditoria-politika, prozedurak, estandarrak eta jarraibideak garatzea	M1:RA1(Ee);M2:RA2(Ec)	%50	M1:RA5(Ef,Eg);M5:RA5(Eb,Ee)	%25
	Sistemen auditorietarako erabiltzen diren metodologiak eta praktikak ezartzea	M3:RA7(Ec),M5:RA2(Ei),RA4(Eb)	%75	M2:RA3(Ea,Ec);M5:RA3(Ec,Ef)	%50
	Helburu-ingurunea ezarri eta auditoria-jarduerak kudeatu	M3:RA7(Ec),M5:RA2(Ei),RA4(Eb)	%75	M4:RA1(Ee,Eg);M5:RA1(Ef,Eg)	%50
	Auditoriaren esparrua, helburuak eta irizpideak definitzen ditu	M6:RA2(Ec)	%25	M2:RA5(Ed,Ee);M5:RA4(Ed,Ef)	%25
	Garatu auditoria-plan bat, markoak, estandarrak, metodologia, prozedurak eta auditoria-probak deskribatzen dituena.		%0	M1:RA3(Ed,Eh);M3:RA10(Ea,Ec)	%0
	Berrikusi ebaluazioaren helburua, segurtasun helburuak eta eskakizunak arrisku-profilaren arabera.	M2:RA3(Ec,Ee),RA8(Ee);M3:RA5(Eb,Ed),RA6(Eb)	%100	M1:RA1(Ec,Ee);M2:RA3(Eb,Ej)	%50
	Zibersegurtasunarekin lotutako lege eta araudi aplikagarrien betetzea ikuskatzea	M1:RA1(Ee)	%25	M3:RA3(Ed,Ee);M5:RA5(Ee,Ed)	%25
	Zibersegurtasunarekin lotutako aplikagarri diren estandarren betetzea ikuskatzea		%0	M1:RA5(Ec,Ee);M2:RA5(Ec,Ef)	%0
	Auditoria plana gauzatu eta frogak eta neurketak bildu	M1:RA3(Ea,Eb,Ec)	%50	M3:RA10(Eb,Ed);M4:RA2(Ee,Eg)	%50
	Auditoria-erregistroen osotasuna mantendu eta babestu	M2:RA8(Eh)	%25	M4:RA1(Ec,Ed);M5:RA5(Ef,Eg)	%25
	Adostasun-ebaluazio, berme, auditoria, ziurtapen eta mantentze-lanen txostenak garatu eta komunikatu		%0	M2:RA4(Eb,Ed);M4:RA1(Ef,Eg)	%0
	Arriskuen konponketa jarduerak kontrolatu	M1:RA1(Ei)	%25	M3:RA8(Eb,Ef);M5:RA5(Ed,Ee)	%25
	BETETZE MAILA		%38		%27
Trebe	Antolatu eta lan egin modu	Cc,Ce	%75	Cc,Cg	%75

tasun gakoa (k)	sistematiko eta deterministan, ebidentzian oinarrituta.				
	Jarraitu eta praktikatu auditoria-esparruak, estandarrak eta metodologiak	Cc,Ce	%75	Tx, Tx	%50
	Aplikatu auditoria tresnak eta teknikak	Cb,Cf	%75	Ca, Cb, Ci	%50
	Negozio-prozesuak aztertzea, softwarearen edo hardwarearen segurtasuna ebaluatzea eta berrikustea, baita kontrol teknikoak eta antolakuntzazkoak ere	Cg	%25	Ca, Ch, Cj	%25
	Sistemak deskonposatu eta aztertu ahuleziak eta kontrol eraginkorrak identifikatzeko	Cb,Cf	%50	Ck,Cm	%25
	Lege- eta araudi-eskakizunak eta negozio-beharrak komunikatu, azaldu eta egokitu	Cm	%25	Cd,Cl	%25
	Auditoria-informazioa bildu, ebaluatu, mantendu eta babestu	Cb,Cf	%75	Ca,Cm	%50
	Osotasunezko auditoria, inpartziala eta independentea izatea		%0	Cb,Cj	%0
	BETETZE MAILA		%50		%38
Ezagutza gakoa	Zibersegurtasuneko kontrolak eta irtenbideak	M1:RA2(C2,C3,C4); M2:RA5(C5),RA8(C1),RA10(C1,C6,C8); M3:RA2(C3)	%100	M2:RA4(C3,C4);M3:RA10(C2,C3,C5)	%100
	Legezko, arauzko eta legegintzako betekizunak, gomendioak eta jardunbide egokiak	M2:RA3(C3,C5);M6:RA5(C3)	%75	M5:RA5(C2,C3)	%50
	Zibersegurtasun-kontrolen eraginkortasuna monitorizatzea, probatzea eta ebaluatzea	M1:RA2(C2,C4);M2:RA7(C13,C14,C18)	%100	M3:RA9(C1,C2);M5:RA5(C1,C2)	%75
	Adostasun-ebaluaziorako arauak, metodologiak eta esparruak	M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5)	%100	M5:RA5(c3)	%75
	Auditoria-arauak, metodologiak eta esparruak	M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,	%100	M3:RA10(C3,C4);M4:RA6(C5,	%75

		C4),RA6(C4);M6:RA5(C2,C5)		C6)	
	Zibersegurtasuneko estandarrak, metodologiak eta esparruak	M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5)	%100	M2:RA3(C4);M5:RA5(C3)	%50
	Auditoriarekin lotutako ziurtagiria		%0	M5:RA5(C3)	%0
	Zibersegurtasunarekin lotutako ziurtagiriak		%0	M1:RA2(C1,C2);M5:RA5(C3)	%0
	BETETZE MAILA		%72		%53

7- Cybersecurity Educator Zibersegurtasuneko Hezitzaileak

	Xehetasuna	ELEMENTUA	TASA	OT	TASA
Zeregin nagusia(k)	Zibersegurtasun eta datuen babeserako curriculumak eta hezkuntza-materiala garatu, eguneratu eta eman, prestakuntzarako eta sentsibilizaziorako, edukian, metodoan, tresnetan eta ikasleen beharretan oinarrituta.		%0	M1:RA3(Eh); M5:RA5(Eb,Ee)	%0
	Zibersegurtasunari eta datuen babesari buruzko sentsibilizazio jarduerak, mintegiak, ikastaroak eta prestakuntza praktikoa antolatu, diseinatu eta ematea	M1:RA1(Ec,Ed,Ee)	%50	M2:RA4(Ed,Ee);M5:RA5(Ef,Eg)	%25
	Prestakuntzaren eraginkortasuna kontrolatu, ebaluatu eta jakinarazi		%0	M4:RA1(Ee,Ef),M5:RA3(Ef,Eg)	%0
	Praktikatzailearen errendimendua ebaluatu eta jakinarazi		%0	M5:RA5(Ef,Eg)	%0
	Hezkuntza, prestakuntza eta sentsibilizaziorako ikuspegi berriak aurkitzea	M1:RA1(Ec,Ed,Ee)	%50	M1:RA5(Ee,Ef);M3:RA8(Ef,Eg)	%25
	Zibersegurtasun simulazioak, laborategi birtualak edo ziber-eremu inguruneak diseinatu, garatu eta entregatu		%0	M2:RA2(Ec.Ed);M4:RA3(Ec,Ef)	%0
	Zibersegurtasun ziurtagiri programetarako orientazioa eman norbanakoentzat		%0	M1:RA3(Eh,Ei);M5:RA5(Ee,Ef)	%0
	Esperientzia etengabe mantendu eta hobetu; zibersegurtasun gaitasunak eta gaitasunen eraikuntza etengabe hobetzea bultzatu eta ahalbidetu		%0	M2:RA3(Ej,Ee);M5:RA3(Eg,Ef)	%0
	BETETZE MAILA		%13		%6
	Zibersegurtasun-kontzientziazio, prestakuntza eta hezkuntzaren beharrak identifikatzea	Ca	%50	Ca,Cl	%25

Trebetasun gakoa (k)	Zibersegurtasun beharrak asetzeko ikaskuntza programak diseinatu, garatu eta eman	Cm	%25	Ck,Cl	%25
	Zibersegurtasun ariketak garatu, ziber-eremu inguruneak erabiliz simulazioak barne.		%0	Cd,Cg	%25
	Zibersegurtasun eta datuen babeserako ziurtagiri profesionaletarako prestakuntza eskaintzea		%0	Ck,Cl	%50
	Erabili dauden zibersegurtasunarekin lotutako prestakuntza baliabideak		%0	Ca,Cl	%0
	Sentsibilizazio, prestakuntza eta hezkuntza jardueren ebaluazio programak garatzea		%0	Ck,Cl	%25
	Komunikatu, aurkeztu eta txostenak egin dagokion interesdunei	Cñ	%25	Cm,Cl	%25
	Helburu-publikoarentzat egokiak diren pedagogia-ikuspegiak identifikatu eta hautatu	Cñ	%25	Ck,Cl	%25
	Jendea motibatu eta animatu	Cñ	%50	Cl,Cm	%50
	BETETZE MAILA		%19		%28
Ezagutza gakoa	Pedagogia-arauak, metodologiak eta esparruak		%0	M5:RA1(C1)	%0
	Zibersegurtasuneko kontzientziazio, hezkuntza eta prestakuntza programaren garapena	M1:RA1(C3,C4)	%25	M1:RA4(C7); M5:RA1(C3)	%25
	Zibersegurtasunarekin lotutako ziurtagiriak		%0	M1:RA2(C2); M5:RA5(C3)	%0
	Zibersegurtasuneko hezkuntza eta prestakuntza estandarrak, metodologiak eta esparruak		%0	M5:RA5(C1,C3)	%0
	Zibersegurtasunarekin lotutako legeak, araudiak eta legedia	M6:RA3(C1,C2,C3),RA4(C*),RA5(C8)	%100	M5:RA5(C3)	%100
	Zibersegurtasuneko gomendioak eta jardunbide egokiak	M2:RA3(C5,C7);M6:RA5(C3)	%50	M2:RA5(C3); M3:RA7(C2,C5)	%50
	Zibersegurtasuneko estandarrak, metodologiak eta esparruak	M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5)	%100	M5:RA5(C3)	%75

	Zibersegurtasuneko kontrolak eta irtenbideak	M1:RA2(C2,C3,C4);M2:RA5(C5),RA8(C1),RA10(C1,C6,C8);M3:RA2(C3)	%100	M2:RA4(C3,C4);M3:RA10(C3,C5)	%75
	BETETZE MAILA		%47		%41

8-Cybersecurity Implementer Zibersegurtasuneko Inplementatzaileak

	Xehetasuna	ELEMENTUA	IT TASA	OT	OT TASA
Zeregin nagusia(k)	Zibersegurtasun produktuak garatu, ezarri, mantendu, eguneratu eta probatu	M1:RA2(Eb,Ec,Ed),RA4(Ed);M2:RA1(Ec,Ed,),RA2(Ea),RA4(Ef),RA5(Ee),RA6(Ef),RA8(Ef,Eh),RA9(Ed,Ee),RA10(Ef,Eh);M3:RA6(Eh,Ej),7(Ec,Ed);M4:RA2(*),RA3(Ea,Eb),Ra4(Cc),RA5(Eb,Ed);M5:RA1(Eh,Ej),RA2(Ea,Ed),RA3(Ec,Ee),RA4(E*),RA5(Ec,Ed,Ee,Ef),RA5(Ec,Ed,Ee,Ef),RA6,(Ed	%100	M1:RA3(Ec,Ef); M5:RA5(Ef,Eg)	%100
	Zibersegurtasunarekin lotutako laguntza eman erabiltzaileei eta bezeroei		%0	M2:RA4(Ec,Ed); M5:RA5(Ee,Ef)	%50
	Zibersegurtasun-irtenbideak integratzea eta haien funtzionamendu egokia bermatzea		%0	M1:RA3Ec,Ei); M3:RA4(Eg,Eh)	%50
	Sistemak, zerbitzuak eta produktuak modu seguruan konfiguratu	M2:RA4(Ea,Eb,Ec,Ed,Ee),Ra5(Ee),RA6(Ef),RA7(Ea,Eb,Ec,Ed,Ee,Eh,Ei),Ra8(Ec,Eg,Eh),	%100	M2:RA6(Ed,Ee);M5:RA4(Ec,Ef)	%100

		Ra9(Eb,Ed),RA10(Ed);M3:RA6(Ec),M3:RA6(Ec),RA8:(Ec);			
	Sistemen, zerbitzuen eta produktuen segurtasuna mantendu eta hobetu	M1:RA2(Eb,Ec,Ed),RA4(Ed);M2:RA1(Ec,Ed,),RA2(Ea),RA4(Ef),RA5(Ee),RA6(Ef),RA8(Ef,Eh),RA9(Ed,Ee),RA10(Ef,Eh);M3:RA6(Eh,Ej),7(Ec,Ed);M4:RA2(*),RA3(Ea,Eb),Ra4(Cc),RA5(Eb,Ed);M5:RA1(Eh,Ej),RA2(Ea,Ed),RA3(Ec,Ee),RA4(E*),RA5(Ec,Ed,Ee,Ef),RA5(Ec,Ed,Ee,Ef),RA6,(Ed	%100	M1:RA4(Eb,Ef);M5:RA3(Ee,Eg)	%100
	Zibersegurtasun prozedurak eta kontrolak ezartzea	M1:RA4(Ea),RA5(Ea);M3:RA8(Ef);M6:RA1(Ec),RA5(Ee,Ef)	%100	M2:RA3(Ef,Eh);M5:RA1(Eg,Eg)	%100
	Zibersegurtasun-kontrolak ezartzearen errendimendua kontrolatu eta bermatu	M1:RA2(Eb,Ec,Ed)	%25	M3:RA7(Ed,Ee);M5:RA3(Ef,Eg)	%50
	Sistemen, zerbitzuen eta produktuen segurtasunari buruzko dokumentazioa eta txostena egin	M1:RA2(Ee),RA4(Ee);M3:RA8(Ef);M4:RA1(Ed),RA5(Ee),RA6(Ec)	%100	M2:RA4(Eb,Ed);M4:RA1(Ed,Ef)	%100
	Zibersegurtasunarekin lotutako ekintzetan IT/OT langileekin estuki lan egin	M2:RA10(E*)	%75	M1:RA1(Eb,Ed);M2:RA1(Ef,Eg)	%75
	Produktuetan adabakiak ezarri, aplikatu eta kudeatu ahultasun teknikoak konpontzeko.	M2:RA4(Eb,Ec,Ed,Ee),RA10Eg,Eh);M3:RA6(Ec);M5:RA2(Ee),RA3(Ee),RA5(Ed,Ee,Ef),	%100	M2:RA6(Ea,Ed);M3:RA8(Ea,Eb)	%100

	BETETZE MAILA		%70		%83
Trebetasun gakoa (k)	Komunikatu, aurkeztu eta txostenak egin dagokion interesdunei	Cñ	%25	Cm,Ck	%25
	Zibersegurtasun-irtenbideak erakundearen azpiegituretan integratzea	Cd, Ce, Cg, Ch	%100	Cj,Cb	%100
	Konfiguratu irtenbideak erakundearen segurtasun-politikaren arabera	CDa	%25	Cf,Ch	%100
	Ebaluatu irtenbideen segurtasuna eta errendimendua	Cf,Ci	%50	Cc, Cd	%50
	Kodea, script-ak eta programak garatu	Cg	%75	Cl,Ce	%75
	Zibersegurtasunarekin lotutako arazoak identifikatu eta konpondu	Cf,Ci	%100	Cm,Cg	%100
	Beste taldekideekin eta lankideekin elkarlanean aritu	Cñ	%75	Cn,Cl	%75
	BETETZE MAILA		%64		%75
Ezagutza gakoa	Garapen-ziklo segurua	M3:RA8(C*)	%50	M1:RA1(C1,C5),RA4(C3)	%50
	Ordenagailu programazioa	M3:RA1(C*),RA2(C*),RA3(C*), M7:RA4(C*)	%100	M2:RA2(C2,C6)	%75
	Sistema eragileen segurtasuna	M7:RA3(C1,C2)	%25	M2:RA6(C1,C4);M3:RA11(C2,C3)	%25
	Ordenagailu sareen segurtasuna	M2:RA3(C5,C6), RA6(C1)	%50	M3:RA5(C1,C2, C4),RA6(C1,C3)	%75
	Zibersegurtasuneko kontrolak eta irtenbideak	M1:RA2(C2,C3,C4);M2:RA5(C5), RA8(C1),RA10(C1,C6,C8);M3:RA2(C3)	%100	M2:RA4(C4),M3:RA10(C2,C3,C5)	%100
	Segurtasun praktika erasokorrak eta defentsiboak	M5:RA1(C4),RA2(C*),RA3(C*)	%100	M3:RA8(C3,C5);M4:RA6(C2,C6)	%50
	Kodetze seguruaren gomendioak eta jardunbide egokiak	M3:RA5(C1,C2,C3,C4),RA6(C1,C3,C4,C5,C6,C7,C8,C9,C10,C11),RA	%100	M2:RA2(C2,C3)	%75

		7(C1,C2,C3,C4,C5,C6),RA8(C1,C2,C3,C4,C5,C6,C7,C8,C9)			
	Zibersegurtasuneko gomendioak eta jardunbide egokiak	M2:RA3(C5,C7); M6:RA5(C3);	%75	M5:RA5(C2,C3)	%75
	Probatzeko estandarrak, metodologiak eta esparruak	M2:RA3(C6);M3:RA6(C4);M6:RA5(C2,C5)	%100	M3:RA9(C1,C2)	%100
	Proba-prozedurak	M5:RA1(C2,C3)	%25	M3:RA5(C1,C4)	%25
	Zibersegurtasunarekin lotutako teknologiak	M1:RA2(C2,C3,C4);M2:RA5(C5), RA8(C1),RA10(C1,C6,C8);M3:RA2(C3)	%100	M2:RA2(C2);M3:RA5(C1,C4)	%100
	BETETZE MAILA		%75		%68

9- Cybersecurity Researcher Zibersegurtasuneko ikertzaileak

	Xehetasuna	ELEMENTUA	IT TASA	OT	OT TASA
Zeregin nagusia(k)	Zibersegurtasun-teknologiak, irtenbideak, garapenak eta prozesuak aztertu eta ebaluatu	M1:RA2(Eb,Ec,Ed),RA3(Eb,Ec,Ed);M2:RA10(Ee,Eg);M5:RA6(Eb,Ec)	%100	M2:RA3(Ea,Ec); M5:RA5(Ed,Ef)	%75
	Zibersegurtasunarekin lotutako gaietan ikerketa, berrikuntza eta garapen lana egitea	M1:RA2(Ed),RA3(Ed); M5:RA5(Ee,Ef)	%100	M1:RA3(Ec,Eh); M4:RA3(Ec,Ef)	%75
	Ikerketa eta berrikuntza ideiak agerian utzi eta sortu		%0	M5:RA5(Ee,Eg)	%25
	Zibersegurtasunarekin lotutako gaien egungo egoera aurreratzea		%0	M1:RA1(Ed,Ee); M4:RA3(Ed,Eg)	%25
	Zibersegurtasunarekin lotutako irtenbide berritzaileak garatzen	M3:RA4(Ee),RA5(Eb,Ec),RA6(E*),RA7(Ec,Ed)	%100	M3:RA8(Ef,Eg);	%75

	laguntzea			M5:RA3 (Ef,Eg)	
	Zibersegurtasun-irtenbideetarako esperimentuak egin eta kontzeptuaren froga, proba pilotuak eta prototipoak garatu.	M5:RA2(E*),RA3(E*),RA5(E*)	%100	M2:RA3 (Ej,Eh); M4:RA2 (Ee,Eg)	%75
	Hautatu eta aplikatu esparruak, metodoak, estandarrak, tresnak eta protokoloak, proiektuak laguntzeko kontzeptu-froga bat eraiki eta probatzea barne.	M5:RA2(E*),RA3(E*),RA5(E*)	%100	M1:RA3 (Ed,Ei); M3:RA10(Ea,Ed)	%100
	Zibersegurtasun negozio ideia, zerbitzu eta irtenbide berritzaileetan laguntzen du		%0	M1:RA5 (Ef,Eg); M5:RA5 (Eg,Eh)	%0
	Zibersegurtasunarekin lotutako gaitasunak eraikitzen laguntzea, besteak beste, sentsibilizazioa, prestakuntza teorikoa, prestakuntza praktikoa, probak, tutoretza, gainbegiratzea eta partekatzea.	M1:RA1(Ec,Ed,Ee);M5:RA2(E*),RA3(E*),RA5(E*)7	%100	M1:RA5 (Ef,Eg); M5:RA5 (Eg,Eh)	%100
	Sektore arteko zibersegurtasun lorpenak identifikatu eta testuinguru desberdinetan aplikatu edo ikuspegi eta irtenbide berritzaileak proposatu.		%0	M1:RA5 (Adibidez,Ef);M5:RA5(Adibidez,Ef)	%0
	Berrikuntza-prozesuak eta -proiektuak zuzendu edo horietan parte hartu, proiektuen kudeaketa eta aurrekontua barne.		%0	M2:RA1 (Ef,Eg); M3:RA2 (Ef,Eg)	%0
	Lan zientifikoak eta ikerketa eta garapen emaitzak argitaratu eta aurkeztu	M1:RA5(Eb,Ec,Ed,Ee), M4:RA1(Ef,Eg),RA3(Ed),RA4(Ef),RA5(Ei)	%100	M1:RA3 (Ed,Eh); M5:RA5 (Ee,Ef)	%75
	BETETZE MAILA		%58		%52
Trebetasun gakoa	Ideia berriak sortu eta teoria praktikara eraman	Cn	%25	Ca,Cl	%75
	Sistemak deskonposatu eta	Cb, Cf, Ci	%100	Cb, Ch	%100

(k)	aztertu ahuleziak eta kontrol eraginkorrak identifikatzeko				
	Sistemak deskonposatu eta aztertu segurtasun eta pribatutasun eskakizunak garatzeko eta irtenbide eraginkorrak identifikatzeko.	Ce,Cf	%75	Cc, Cd, Cf	%75
	Zibersegurtasunarekin lotutako teknologien aurrerapen berriak kontrolatu	Cg,Ck	%75	Ce,Cl	%75
	Komunikatu, aurkeztu eta txostenak egin dagokion interesdunei	Cñ	%25	Ck,Cm	%25
	Zibersegurtasunarekin lotutako arazoak identifikatu eta konpondu	Cf,Ci	%75	Cm,Cg	%75
	Beste taldekideekin eta lankideekin elkarlanean aritu	Cñ	%75	Cn,Cm	%75
	BETETZE MAILA		%64		%71
Ezagutza gakoa	Zibersegurtasunarekin lotutako ikerketa, garapena eta berrikuntza (I+G)	M6:RA1(Cd)	%25	M1:RA1 (C1,C4); M4:RA2 (C7,C9)	%25
	Zibersegurtasuneko estandarrak, metodologiak eta esparruak	M1:RA4(C1);M2:RA3(C6);M3:RA5(C2,C4),RA6(C4);M6:RA5(C2,C5)	%100	M2.RA3(C4);M5:RA5(C3)	%100
	Zibersegurtasunarekin lotutako teknologiak kaleratzeko edo erabiltzeko legezko, arauzko eta legegintzako eskakizunak	M4:RA4(C2);M6:RA4(C*),RA5(C3,C6,C7,C8)	%100	M5:RA5 (C2,C3)	%75
	Zibersegurtasunaren alderdi multidiziplinarra		%0	M1:RA1 (C2,C5); M5:RA1 (C1,C3)	%0
	Informazioa arduraz zabaltzeko prozedurak	M1:RA3(C5)	%25	M4:RA6 (C4,C5)	%25
	BETETZE MAILA		%50		%45

10- Cybersecurity Risk Manager Zibersegurtasun Arriskuen Kudeatzailea

	Xehetasuna	ELEMENTUA	IT TASA	OT	OT TASA
Zeregin nagusia(k)	Erakunde baten zibersegurtasun arriskuen kudeaketa estrategia garatu	M2:RA3(Ec,Ee), M3:RA5(Eb);M6:RA4(Ee)	%100	M1:RA1(Ed,Ee); M5:RA5(Ea,Ec)	%100
	Erakundearen aktiboen inbentarioa kudeatu	M5:RA3(Eb),RA5(Eb)	%50	M1:RA1(Eb,Ec); M2:RA3(Eb,Ec)	%100
	IKT sistemen zibersegurtasunarekin lotutako mehatxuak eta ahultasunak identifikatu eta ebaluatu	M1:RA2(Eb,Ec, Ed);M2:RA3(Ea),RA7(Ef);M3:RA5(Ea,Eb)	%100	M2:RA3(Ec,Ed); M3:RA8Ea,Eb)	%100
	Mehatxu-paisaiaren identifikazioa, erasotzaileen profilak eta erasoen potentzialaren estimazioa barne.	M1:RA2(Eb,Ec, Ed,Ee)	%50	M4:RA2(Ef,Eg); M5:RA5(Ee,Eg)	%75
	Zibersegurtasun-arriskuak ebaluatu eta arriskuen tratamendurako aukera egokienak proposatu, segurtasun-kontrolak eta erakundearen estrategiari hobekien erantzuten dioten arriskuen arintzea eta saihestea barne.	M5:RA2(Eg),RA3(Ef),RA5(Eg)	%75	M1:RA3(Ed,Eh); M5:RA5(Ed,Ef)	%75
	Zibersegurtasun-kontrolen eraginkortasuna eta arrisku-mailak kontrolatzea	M1:RA2(Eb,Ed); M2:RA7(Eh);M3·:RA7(Ed);M5:RA1(Ei)	%100	M3:RA7(Ed,Ee); M5:RA3(Ef,Eg)	%100
	Ziurtatu zibersegurtasun-arrisku guztiak erakundearen aktiboetarako maila onargarri batean mantentzen direla.	M2:RA3(Ec,Ee)	%25	M5:RA5(Ee,Ef)	%100
	Arriskuen kudeaketa ziklo osoaren jarraibideak garatu, mantendu, jakinarazi eta komunikatu, eta araudi eta estandarren betetzea ziurtatu.	M2:RA3(Ec,Ee), M3:RA5(Eb);M6:RA4(Ee)	%100	M1:RA3(Ei,Eh); M4:RA1(Ef,Eg)	%100
	BETETZE MAILA		%75		%94
Trebetasun Nagusia(k)	Zibersegurtasun arriskuen kudeaketarako esparruak, metodologiak eta jarraibideak eta araudi eta estandarrak betetzen direla	Ce, Cf, Ci	%100	Ca, Cb, Cj, Cn	%100

	ziurtatu				
	Erakundearen kalitate eta arriskuen kudeaketa praktikak aztertu eta bateratu	Ce, Cf, Ci, Cp	%100	Cg,Cñ	%100
	Negozioetako aktiboen jabeei, zuzendariei eta beste interesdun batzuei arriskuak kudeatzeko eta arintzeko erabaki informatuak hartzeko aukera eman.	Ce, Cf, Ci	%100	Cm,Cl	%100
	Zibersegurtasun arriskuen inguruko ingurune bat eraiki	Ce, Cf, Ci	%100	Ce,Cc	%100
	Komunikatu, aurkeztu eta txostenak egin dagokion interesdunei	Cñ	%75	Ck,Cm	%25
	Arriskuak partekatzeko aukerak proposatu eta kudeatu	Ce, Cf, Ci	%75	Cd,Ch	%100
	BETETZE MAILA		%92		%88
Ezagutza gakoa	Arriskuen kudeaketarako estandarrak, metodologiak eta esparruak	M2:RA3(C1); M3:RA5(C2);M6:RA2(C3)	%25	M2:RA3(C3);M5:RA5(C1)	%50
	Arriskuen kudeaketa tresnak	M6:RA2(C3)	%25	M2:RA3(C7);M3:RA3(C2)	%50
	Arriskuen kudeaketarako gomendioak eta jardunbide egokiak	M2:RA3(C1);M3:RA5(C2),M6:RA2(C3)	%100	M5:RA5(C2)	%100
	Zibermehatxuak	M1:RA3(C4);M2:RA3(C1);M3:RA5(C2)	%100	M2:RA3(C2)	%100
	Ordenagailu sistemen ahultasunak	M2:RA10(C10); M3:RA6(C2,C6);M5:RA3(C6,C9),RA5(C5,C6,C7)	%100	M3:RA8(C1)	%100
	Zibersegurtasuneko kontrolak eta irtenbideak	M1:RA2(C2,C3,C4);M2:RA5(C5),RA8(C1),RA10(C1,C6,C8);M3:RA2(C3)	%100	M2:RA4(C5,C6)	%100
	Zibersegurtasun arriskuak	M2:RA3(C1); M3:RA5(C2);M6:RA2(C3);	%25	M1:RA2(C3);M5:RA5(C3)	%75
	Zibersegurtasun-kontrolen	M1:RA2(C2,C4)	%75	M1:RA4(C5);M3	%75

	eraginkortasuna monitorizatzea, probatzea eta ebaluatzea	;M2:RA7(C13,C14,C18)		:RA9(C2)	
	Zibersegurtasunarekin lotutako ziurtagiriak		%0	M5:RA5(C3)	%0
	Zibersegurtasunarekin lotutako teknologiak	M1:RA2(C2,C3,C4);M2:RA5(C5),RA8(C1),RA10(C1,C6,C8);M3:RA2(C3)	%100	M1:RA3(C4);M2:RA1(C3)	%100
	BETETZE MAILA		%65		%75

11-Digital Forensics Investigator Auzitegi Digitaleko Ikertzailea

	Xehetasuna	ELEMENTUA	IT TASA	OT	OT TASA
Zeregin nagusia(k)	Garatu auzitegi digitaleko ikerketa politika, planak eta prozedurak	M4:RA1(Ea,Eb,Ec,Ed,Ee),RA2(E*),RA3(Ea,Eb),RA4(Ea,Eb,Ec),RA5(Ea,Eb,Ec,Ed,Ee,Ef,Eg)	%100	M4:RA1(Ea,Ed);M5:RA5(Ec,Ef)	75
	Froga digitalak identifikatu, berreskuratu, atera, dokumentatu eta aztertu	M4:RA1(Ea,Eb,Ee),RA3(Ea),RA5(Ea,Eb,Ec,Ed,Ef)	%75	M3:RA9(Ea,Ed);M4:RA2(Eb,Ec)	75
	Babestu eta gorde froga digitalak, eta jarri eskuragarri baimendutako interesdunen esku.	M4:RA1(Ea,Eb,Ee),RA3(Ea),RA5(Ea,Eb,Ec,Ed,Ef)	%75	M4:RA1(Ec,Ee);M5:RA1(Ef,Eg)	25
	Inguruneak ikuskatu baimenik gabeko eta legez kanpoko ekintzen zantzurik dagoen ikusteko.	M4:RA1(Ea,Eb,Ee),RA3(Ea),RA5(Ea,Eb,Ec,Ed,Ef)	%75	M3:RA8(Eb,Ee);M4:RA3(Ea,Ec)	50
	Sistematikoki eta deterministaki dokumentatu, txostendu eta aurkeztu analisi forentse digitalaren aurkikuntzak eta emaitzak	M4:RA1(Ef,Eg),RA3(Ec,Ed),RA4(Ef),RA5(Eh,Ei),RA6(E*)	%100	M2:RA4(Eb,Ed);M4:RA1(Ef,Eg)	75
	Hautatu eta pertsonalizatu forentsearen probak, analisiak eta txostenak egiteko teknikak aktoreak	M4:RA1(Ea,Eb,Ec,Ed,Ee),RA2(E*),RA3(Ea,Eb),RA4(Ea,Eb,Ec),	%100	M1:RA3(Eh,Ei):M4:RA2(Ed,Ef)	50

		RA5(Ea,Eb,Ec,Ed,Ee,Ef,Eg)			
	BETETZE MAILA		%88		58,33
Gako Trebetasunak	Lan egin modu etiko eta independentean; barneko edo kanpoko eraginpean eta alborapenik gabe aktoreak	Ch,Co	%75	Cl,Cn	25
	Informazioa bildu, haren osotasuna mantenduz	Ch	%75	Ci,Ck	75
	Zibersegurtasun gertaerak identifikatu, aztertu eta erlazionatu	Ch	%75	Ca, Cb, Ch	75
	Azaldu eta aurkeztu froga digitalak modu sinple, zuzen eta erraz ulertzeko moduan	Cm	%50	Cc,Ck	100
	Ikerketa-txosten zehatzak eta arrazoituak garatu eta komunikatu	Cm	%75	Cc,Cj	75
	BETETZE MAILA		%70		70
Ezagutza gakoa	Forentse digitalaren gomendioak eta jardunbide egokiak	M4:RA1(C2,C4),RA4(C3)	%75	M4:RA1(C2),RA4(C6)	50
	Auzitegi digitaleko estandarrak, metodologiak eta esparruak	M4:RA1(C4),RA3(C1,C2),RA4(C3)	%100	M4:RA1(C3)	50
	Auzitegi digitaleko analisi prozedurak	M4:RA1(C7,C8,C10),RA2(C4,C5,C6,C7),RA3(C3),RA5(C3)	%100	M4:RA1(C6);M4:RA1(C3)	75
	Proba-prozedurak	M5:RA1(C2,C3)	%50	M4:RA2(C10)	50
	Ikerketa kriminalen prozedurak, estandarrak, metodologiak eta esparruak		%0	M4:RA2(C3),RA5(C4)	25
	Zibersegurtasunarekin lotutako legeak, araudiak eta legedia	M6:RA3(C1,C2,C3),RA4(C*),RA5(C8)	%100	M5:RA5(C2,C3)	0
	Malwarearen analisi tresnak	M4:RA2(C3)	%50	M4:RA1(C9,C10),RA6(C2,C6)	75
	Zibermehatxuak	M1:RA3(C4);M2:RA3(C1);M3:RA5(C2)	%100	M4:RA3(C6)	50

	Ordenagailu sistemen ahultasunak	M2:RA10(C10); M3:RA6(C2,C6) ;M5:RA3(C6,C9),RA5(C5,C6,C7)	%100	M3:RA8(C1,C5); M4:RA5(C2,C3)	75
	Zibersegurtasun erasoen prozedurak	M5:RA1(C4),RA 2(C4,C5),RA3(C 5,C6,C7,C8,C9), RA4(C2),RA5(C 3,C6)	%100	M3:RA8(C5,C6)	75
	Sistema eragileen segurtasuna	M7:RA3(C1,C2)	%75	M2:RA6(C3,C4); M3:RA11(C3,C4)	75
	Ordenagailu sareen segurtasuna	M2:RA1(C*),RA 3(C*),RA6(C*); M7:RA1(C1,C2, C3)	%100	M3:RA2(C10),R A10(C2)	75
	Zibersegurtasunarekin lotutako ziurtagiriak		%0	M5:RA5(C3)	0
	BETETZE MAILA		%73		51,92

12- **Penetration Tester** Penetrazio-probatzailea

	Xehetasuna	ELEMENTUA	IT TASA	OT	OT TASA
Zeregin nagusia(k)	Zibersegurtasun-ahultasun teknikoak eta antolakuntzazkoak identifikatu, aztertu eta ebaluatu	M1:RA2(Eb,Ec,Ed);M2:RA3(Ea),RA7(Ef);M3:RA5(Ea,Eb)	%100	M2:RA3(Ec,Ee);M3:RA8(Ea,Eb)	%100
	Eraso bektoreak identifikatu, zibersegurtasuneko ahultasun teknikoen ustiapena aurkitu eta erakutsi	M2:RA10(Eh);M3:RA5(E*);M5:RA3(Ee),RA5(Ee,Ef)	%100	M3:RA8(Ec,Eg);M4:RA2(Eb,Ed)	%100
	Sistemak eta eragiketak arauzko estandarren arabera betetzen direla probatzea	M2:RA3(Ef),M3:RA5(Ea,Eb);M6:RA5(Ef)	%100	M1:RA3(Eh,Ei);M5:RA5(Ee,Ef)	%100
	Penetrazio-probak egiteko teknika egokiak hautatu eta garatu	M5:RA1(Ee,Ef,Eg,Eh),RA2(Ea,Ec,Ed,Ee,Ef),RA3(Ea,Eb,Ec,Ed,Ee),RA4(E*),RA5(Ea,Eb,Ec,Ed,Ee,Ef),RA6(E*)	%100	M3:RA8(Ed,Ef);M4:RA3(Ee,Eg)	%100
	Antolatu penetrazio-probetarako proba-planak eta prozedurak	M5:RA1(Ec),RA2(Ef),RA3(Eb),R5(Ea)	%75	M1:RA3(Ed,Eh);M5:RA5(Ec,Ef)	%50
	Sartze-proben emaitzen analisi eta txostenak egiteko prozedurak ezartzea	M5:RA2(Eg),RA3(Ef),RA5(Eg)	%75	M2:RA4(Ed,Ef);M4:RA1(Ef,Eg)	%75
	Dokumentatu eta jakinarazi penetrazio-proben emaitzak interesdunei	M1:RA3(Ee),RA4(Ee);M5:RA2(Eg),RA3(Ef),RA5(Eg)	%100	M2:RA4(Eb,Ed);M4:RA2(Ee,Ef)	%100
	Sartze-probak egiteko tresnak eta proba-programak zabaldu		%0	M3:RA8(Ee,Ef);M4:RA2(Eb,Ed)	%0
	BETETZE MAILA		%81		%78
Trebetasun gakoa(k)	Kodeak, gidoiak eta programak garatu	Cg	%75	Ch, Ck, Cl	%75
	Gizarte-ingeniaritza egin	Cb	%75	Ca,Cd	%75
	Ahultasunak identifikatu eta ustiatu	Cc, Cf, Ci	%100	Ch,Ci	%100
	Hacking etikoa egin	Cf	%100	Cg,Cj	%75

	Pentsatu modu sortzailean eta kutxatik kanpo	Cn,Cñ	%75	Zentimetroak	%75
	Zibersegurtasunarekin lotutako arazoak identifikatu eta konpondu	Cf,Ci	%75	Zentimetroak	%75
	Komunikatu, aurkeztu eta txostenak egin dagokion interesdunei	Cñ	%25	Cc,Ck	%25
	Erabili penetrazio-proben tresnak eraginkortasunez	Cb,Cf	%100	Cb,Cj	%75
	Azterketa teknikoak eta txostenak egin	Cf	%75	Cc,Cl	%75
	Sistemak deskonposatu eta aztertu ahuleziak eta kontrol eraginkorrak identifikatzeko	Cb, Cf, Ci	%100	Ce,Cf	%75
	Berrikuspen kodeek haien segurtasuna ebaluatzen dute	Cg	%50	Cb,Ck	%50
	BETETZE MAILA		%77		%70
Ezagutza gakoa	Zibersegurtasun erasoen prozedurak	M5:RA1(C4),RA2(C4,C5),RA3(C5,C6,C7,C8,C9),RA4(C2),RA5(C3,C6)	%100	M3:RA8(C5);M4:RA6(C1,C2)	%100
	Informazio-teknologiako (IT) eta eragiketa-teknologiako (OT) gailuak	M2:RA10(C*)	%75	M2:RA1(C1,C2,C3)	%75
	Erasoko eta defentsako segurtasun prozedurak	M5:RA1(C4),RA2(C*),RA3(C*)	%100	M3:RA8(C5,C6);M5:RA1(C3)	%75
	Sistema eragileen segurtasuna	M7:RA3(C1,C2)	%75	M2:RA6(C3,C4);M3:RA11(C3,C4)	%75
	Ordenagailu sareen segurtasuna	M2:RA1(C*),RA3(C*),RA6(C*);M7:RA1(C1,C2,C3)	%100	M3:RA10(C2,C4)	%75
	Penetrazio-proben prozedurak	M5:RA1(C3,C4),RA2(C5),RA3(C*),RA4(C2,C3),RA5(C3,C5,C6),RA6(C4)	%100	M3:RA8(C4);M4:RA2(C10)	%75
	Penetrazio-proben estandarrak, metodologiak eta esparruak	M5:RA1(C3,C4),RA2(C5),RA3(C*),RA4(C2,C3),RA5	%100	M4:RA2(C9,C10)	%75

		(C3,C5,C6),RA6(C4)			
	Penetrazio-proba tresnak	M2:RA10(C15);M3:RA6(C10),RA8(C8);M5:RA1(C7,C8),RA3(C6),RA5(C6),RA6(C*)	%100	M3:RA6(C3)	%75
	Ordenagailu programazioa	M3:RA1(C*),RA2(C*),RA3(C*),M7:RA4(C*)	%100	M3:RA5(C2,C3),RA8(C1,C2)	%100
	Ordenagailu sistemen ahultasunak	M2:RA10(C10);M3:RA6(C2,C6);M5:RA3(C6,C9),RA5(C5,C6,C7)	%100	M5:RA5(C2,C3)	%100
	Zibersegurtasuneko gomendioak eta jardunbide egokiak	M2:RA3(C5);M6:RA5(C3)	%100	M5:RA5(C3)	%100
	Zibersegurtasunarekin lotutako ziurtagiriak		%0		%0
	BETETZE MAILA		%88		%77