



Zerbitzuen katalogoa



Aurkibidea

01. Sarrera	4
1.1. Helburua	4
1.2. Dokumentuaren edukia	4
1.3. Erlazionatutako dokumentuak	4
02. Zerbitzuen katalogoa	5
2.1. Katalogoko zerbitzuen oinarria eta funtsa	5
2.2. Zerbitzuen eskaintzaren segmentazioa	6
2.3. Zerbitzuen jardura-eremuak	6
2.4. CyberOrratz	7
2.5. Katalogoa mantentzea	7
03. Erakundeen eskubideak eta betebeharrak	8
3.1. Erakundearen eskubideak	8
3.2. Erakundearen betebeharrak	8
3.3. Gorabeheren jakinarazpena	9
3.4. Zerbitzuaren kalitatea eta konpromisoak	9
04. Zerbitzu-lerroak	10
4.1. Auditoretza	10
4.2. Kontzientziazioa	11
4.3. Koordinazio estrategikoa	11
4.4. Arriskuaren gobernu	12
4.5. Mehatxuen inteligentzia	12
4.6. Euskadiko segurtasun eredua	13
4.7. Segurtasun-eragiketak (SOC)	13
4.8. Gertakariei erantzutea (CSIRT)	14
4.9. Erasoko segurtasuna	15
4.10. Ezagutzaren transferentzia	15

05. Zerbitzu-fitxak	16
5.1. Auditoreta	
5.1.1. Segurtasunaren ebaluazioa	17
5.1.2. OAT - Auditoreta Teknikoko Organoa	18
5.1.3. Jarraitutasun-planak gainbegiratzea	19
5.2. Kontzientziazioa	
5.2.1. Kontzientziazioa	20
5.2.2. Phishing kanpainak	21
5.3. Koordinazio estrategikoa	
5.3.1. Euskadiko zibersegurtasun estrategiaren hedapena	22
5.3.2. Zerbitzuak kudeatzeko bulegoa	23
5.4. Arriskuaren gobernu	
5.4.1. Arriskuaren ebaluazioa	24
5.4.2. Arriskuaren kudeaketa	25
5.4.3. Harmonizazio bulegoa	26
5.4.4. Proiektu berezien kudeaketa	27
5.5. Mehatxuen inteligentzia	
5.5.1. Alerta goiztiarra	28
5.5.2. Ziber mehatxuei buruzko informazioa trukatzeko	29
5.6. Euskadiko segurtasun eredu	
5.6.1. Euskadiko segurtasun ereduaren hedapenean laguntzea eta jarraipena egitea	30
5.7. Segurtasun-eragiketak (SOC)	
5.7.1. SOC	31
5.7.2. Threat hunting	32
5.8. Gertakariei erantzutea (CSIRT)	
5.8.1. Aholkularitza	33
5.8.2. Koordinazioa	34
5.8.3. DFIR	35
5.8.4. Krisien kudeaketa	36
5.8.5. Takedown	37
5.8.6. Zibersegurtasun arloko gertakariei erantzuteko prestakuntza	38
5.9. Erasoko segurtasuna	
5.9.1. Auditoreta tekniko	39
5.9.2. EASM	40
5.9.3. Red team	41
5.10. Ezagutzaren transferentzia	
5.10.1. Prestakuntza	42
5.10.2. Entrenamendua	43

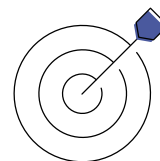
01.

Sarrera

1. 1.

Helburua

Zerbitzuen katalogoaren helburua Zibersegurtasunaren Euskal Agentziak (Cyberzaintza) emandako zerbitzuen ikuspegi orokorra aurkeztea da. Horrela, zerbitzuen eskaintza ulertzen eta eskuratzen laguntzen da, eta erakunde bakoitzak bere behar espezifikoetara egokitzen direnak identifikatu ahal izatea bermatzen da.



1. 2.

Dokumentuaren edukia

Sarrerako kapitulu horrez gain, Zerbitzuen katalogoak honako eduki hauek ditu:



Zerbitzuen katalogoaren [deskribapena](#).



Katalogoko zerbitzu bakoitzaren definizioa, ezaugarri nagusiak eta tipologiak islatzen dituzten [fitxen multzoa](#).



Zerbitzu-lerro bakoitzaren eta bertan jasotako zerbitzuen [definizioa](#).



Zerbitzu-maila estandarreko [akordioak](#).

1. 3.

Erlazionatutako dokumentuak

Jarraian, Zerbitzuen katalogoa egiteko kontuan hartu diren erreferentziazko arau nagusiak aurkezten dira:

Kalitatea kudeatzeko sistemak. Betekizunak (UNE-EN ISO 9001).

Informazioaren teknologia. Zerbitzua Kudeatzeko Sistema (SGS). 1. atala: Baldintzak (UNE ISO/IEC 20000-1).

Zerbitzu-kartak. Betekizunak (UNE 93200).

CyberOrratz.

Haren aplikazioak katalogoan sartutako zerbitzuek nazioartean onartutako estandarrei erantzutea eta sektoreko jardunbide egokienetara egokitzea bermatzen du.

02.

Zerbitzuen katalogoa

2.1.

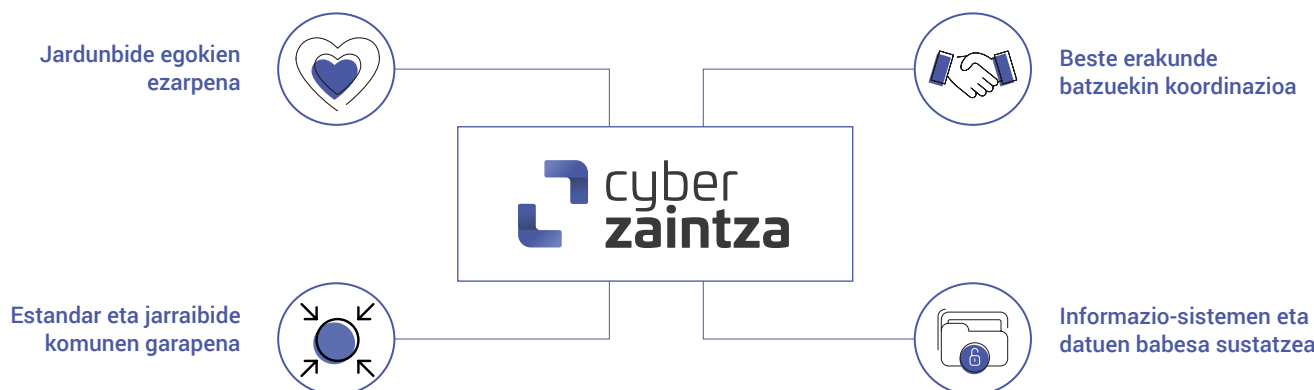
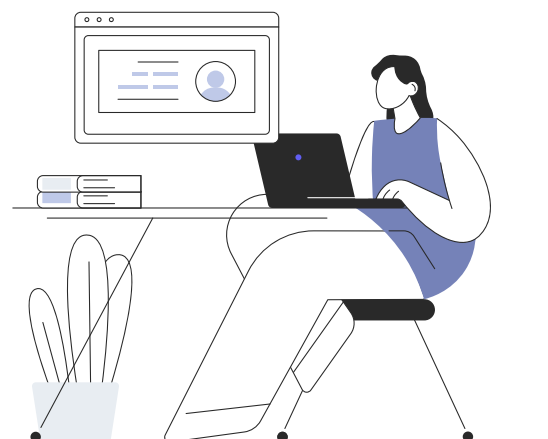
Katalogoko zerbitzuen oinarria eta funtsa

Katalogo honetan jasotako zerbitzuak Cyberzaintzaren eskumen-, estrategia- eta operatibotasun-esparruan oinarritzen dira, eta Euskadiko zibersegurtasunaren eremuan duten misioa eta eginkizunak gauzatzeko tresna nagusia dira.

Lehenik eta behin, zerbitzu horiek Cyberzaintzaren izaeran eta funtzioetan oinarritzen dira, Euskal Autonomia Erkidegoko sektore publikoko erakunde publiko gisa, berezko nortasun juridikoarekin eta Segurtasun Sailari atxikita. **Zibersegurtasunaren Euskal Agentzia sortzeko** ekainaren 29ko 7/2023 Legean ezarritakoaren arabera, Cyberzaintzak zibersegurtasunaren arloko sustapen, koordinazio eta laguntza funtzioak ditu esleituta, bai eta euskal sektore publikoaren, enpresa sarearen eta herritarren eremuan gaikuntza eta garapen digital segurua bultzatzea ere. Zerbitzuen katalogoa, beraz, eginkizun horien adierazpen operatiboa da, eta modu ordenatu, garden eta koherentean emateko aukera ematen du.

Bigarrenik, katalogoko zerbitzuak zuzenean bat datoz **Zibersegurtasunaren Euskal Estrategiarekin** (2024 - 2029). Estrategia horrek Herrialdeak arlo horretan dituen erronka nagusiak identifikatzen ditu, eta helburu estrategikoak eta jarduteko ildoak zehazten ditu, denboran modu koordinatuan eta iraunkorrean gauzatzea eskatzen dutenak. Katalogoan sartutako zerbitzuen bidez, Cyberzaintzak helburu horiek lortzen laguntzen du, zibermehatxuen aurrean gobernantza-, prebentzio-, detekzio- eta erantzun-ekintzak gidatuz eta lagunduz, eta inplikaturako eragileen arteko lankidetzaz erraztuz.

Halaber, katalogoak Cyberzaintzaren balio-proposamena du oinarri, **Euskadin zibersegurtasuna indartzeko, ikuspegi integral eta kolaboratibo baten bidez**. Eskaintzen diren zerbitzuek jardunbide egokiak hartzea, estandar eta jarraibide komunak garatzea, beste erakunde batzuekin koordinatzea eta informazio-sistemak eta datuak babestea sustatzen dute, eta euskal sektore publikoak eta haren inguruak zibersegurtasunean duen heldutasun-maila orokorra handitzen laguntzen dute.



Azkenik, zerbitzuen katalogoa **erreferentziatzeko tresna dinamikoa** da, erakunde erabiltzaileei aukera ematen diena eskura dituzten zerbitzuak eta horien irismena eta emateko baldintzak modu argi eta egituratuan ezagutzeko, eta zerbitzuen eskaintza pixkanaka Euskadiko ekosistema digitalaren mehatxuen, arau-esparruaren eta beharren bilakaerara egokitzeko.

2.2.

Zerbitzuen eskaintzaren segmentazioa

Cyberzaintzaren zerbitzuen eskaintza segmentazio objektibo eta bertikal baten arabera egituratzen da, Euskadin dauden zibersegurtasun beharrei modu espezifikoan eta proportzionatua erantzuteko.

Segmentazio horrek aukera ematen du zerbitzuak testuinguru, heldutasun maila eta ingurune bakoitzaren arau-esparrura egokitzeko, zerbitzu eraginkorragoa eta eremu bakoitzaren berezko arrisku eta betebeharrekin bat datorrena bermatuz.

Illo horretan, katalogoko zerbitzuak honako publiko objektibo eta bertikaletan antolatzen dira:



Sektore publikoa

Euskal sektore publikora bideratua, eta bertikal espezifikoak barne hartuta, hala nola administrazio publikoa, segurtasuna, osasuna eta hezkuntza.



Enpresak

Enpresa-sareari zuzendua, arreta berezia jarritz enpresa estrategikoei, autobabesaren arloan betebeharrak espezifikoak dituzten enpresei eta beste enpresa batzuei.



Herritarrak

Hainbat kolektibori egokitutako zerbitzuekin, bereziki: adingabeak, helduak eta gizarte-bazterketa jasateko arriskuan dauden taldeak.

Bertikal bidezko antolaketa horrek erakunde edo kolektibo mota bakoitzerako **zerbitzu egokienak identifikatzea errazten du**, eta Cyberzaintzari bere jarduera lehenesteko eta espezializatzeko aukera ematen dio, ingurune bakoitzaren ezaugarrien eta beharren arabera.

2.3.

Zerbitzuen jarduera-eremuak

Cyberzaintzaren zerbitzuak zibersegurtasunaren zikloan duten jardun-eremuaren arabera sailkatzen dira, xede duten publikoa edo publiko bertikala edozein dela ere, nazioartean onartutako jardunbide egokiekin eta estandarrekin lerrotatutako ikuspegi integral bati jarraituz.

Honako hauek dira jarduera-eremuak:



Prebentzioa

Zibersegurtasun gertakarien probabilitatea murriztera bideratutako zerbitzuak, aurrea hartuz, kontzientziatuz, babes neurriak hartuz eta gaitasunak indartuz.



Detekzioa

Zibersegurtasuneko gertakariak edo mehatxuak garaiz identifikatzeko zerbitzuak barne hartzen ditu, erantzun bizkorragoa eta eraginkorragoa ahalbidetzen duten tresnak, sistemak eta mekanismoak erabiliz.



Erantzuna

Gertakariak detektatu ondoren haiek kudeatzeko behar diren zerbitzuak biltzen ditu, haien eragina geldiarazteko, suspertzen laguntzeko eta eragindako erakundeentzako ondorioak minimizatzeko.



Gobernantza

Zibersegurtasuna modu koherente, koordinatu eta iraunkorrean kudeatzeko aukera emango duten esparru, jarraibide, estandar eta antolaketa-egiturak ezartzera bideratutako zerbitzuak biltzen dituena.

Eremu horiek, eskaintako zerbitzu motak mugatzeaz gain, esku hartzeko esparru egituratu bat osatzen dute, zibersegurtasunaren dimentsioei modu integrarean heltzeko eta katalogoak **Zibersegurtasunaren Euskal Estrategiarekin** eta aplikatu beharreko arau-esparruarekin duen koherentzia bermatzeko.

2. 4.

CyberOrratz

CyberOrratz Cyberzaintzak garatutako erreferentzia esparrua da, edozein erakunderen zibersegurtasuna egituratzeko, ebaluatzeko eta indartzeko berariaz diseinaturik. Kontrolatan eta ezarpen-mailetan oinarritutako metodologiari esker, aukera ematen du lehentasun argiak ezartzeko, heldutasun-maila neurtzeko eta etengabeko hobekuntza-jarduerak planifikatzeko funtsezko arloetan, hala nola arriskuen kudeaketan, araudia betetzean, audiotretzan eta sistemen eta informazioaren babes integratzean. Eredu horrek euskal sektore publikoarentzat gomendatutako estandarrak, jarraibideak eta arau teknikoak bultzatzeko aginduari erantzuten dio, entitateei oinarri sendoa bermatuz beren segurtasun-jarrerara sendotzeko.

CyberOrratzen egitura zibersegurtasun domeinuetan egituratzen da, eta horietako bakoitzak ere duen zehar ezartzen diren kontrolak eta neurriak biltzen ditu. Eredu horiek honako hauek hartzen dituzte:

Zibersegurtasunaren gobernua

Aktiboen eta azpiegituren babesa

Gertakariei erantzutea

Aktiboen identifikazioa eta sailkapena

Monitorizazioa, detekzioa eta alerta

Suspertzea eta erresilientzia

Katalogoko zerbitzu bakoitza zuzenean lotzen da domeinu horietako kontrolekin, jardunbide onenekin lerrokatutako eta erakunde bakoitzaren benetako beharretara egokitutako eskaintza bermatuz.

Oinarri horren gainean, ereduak sei kontrol-maila progresibo ezartzen ditu:



Egitura horrek zibersegurtasunaren ezarpen ordenatu eta pertsonalizatua ahalbidetzen du, erakunde bakoitzaren heldutasun-mailara egokituz eta katalogoko zerbitzuak etengabeko hobekuntza-zikloan integratzea erraztuz. Zerbitzu bakoitza ereduaren kontrol espezifiko batekin lotzen denez, erantzun eraginkorra eta neurrikoa bermatzen da behar bakoitzerako.

2. 5.

Katalogoa mantentzea

Cyberzaintzako **zerbitzuen katalogoa etengabe eguneratzen da**, Agentziaren helburu estrategikoetara eta erakunde erabiltzaileen beharretara egokitzen dela bermatzeko.

Cyberzaintzako Zuzendaritza Batzordeak Katalogoaren bilakaera bultzatzen eta bideratzen du, erakundearen helburu estrategikoak eta erakunde erabiltzaileetan hautemandako beharrak zerbitzuak definitzera eta lehenestera eramanez, eta zerbitzu eta jarduerak-ildo berriak identifikatzen parte hartuz, horien arduradunekin koordinatuta.

Zerbitzuen Katalogoaren kudeaketa eta gainbegiratzea modu koordinatuan egiten da erakundearen barruan, barne hartutako zerbitzuen koherentzia, kalitatea eta egokitasuna zainduz, eta, bereziki:

- Katalogoan definitutako zerbitzuen egokitasuna ebaluatuz, haien erabilgarritasunari, irismen funtzionalari eta kalitate-baldintzei dagokienez.
- Zerbitzuen, Cyberzaintzaren barne-prozesuen, horiei eusten dieten azpiegituren eta xede diren erakundeen ikuspegi orokorra mantenduz.
- Katalogoaren jarraipena eginez, zerbitzuak emateko erreferentziazko tresna gisa.

Zuzendaritza Batzordeak, gutxienez urtean behin, zerbitzuen katalogoaren edukia berrikusten du, hala badagokio, arau-testuinguruaren, testuinguru estrategikoaren eta operatiboaren bilakaerara eta antzemandako behar berrietara egokitzeko.

03.

Erakundeen eskubideak eta betebeharrak

3.1.

Erakundearen eskubideak

Katalogo honetako zerbitzuren bat erabiltzen duen edozein erakundek gutxienez honako eskubide hauek ditu eskuratuta:

- Honako hauek lortzeko behar diren baliabideak edukitzea eta eskura izatea:
 - Zerbitzuen Katalogoan sartzea, Cyberzaintzak eskaintzen dizkion zerbitzuak ezagutzeko,
 - Zerbitzu bakoitzaren ezaugarri orokorrak kontsultatzea, haren helburua, irismena eta kolektiboa ezagutzeko,
 - Zerbitzua erabiltzeko baldintza aplikagarrietan sartzea, eta
 - Cyberzaintzarekin eskatutako zerbitzuei buruz ezarritako akordioen berezko ezaugarriak ezagutzea.
- Jasotzen dituen zerbitzuei buruzko erreklamazioak egin ahal izango ditu.
- Jasotzen dituen zerbitzuetan dauden aukerak baliatu ahal izango ditu bere beharretara egokitzeko, zerbitzuaren berezko ezaugarrietan ezarritakoaren arabera, eta, horretarako, bide eta prozedura formalizatuak erabili ahal izango ditu.
- Harremanetarako pertsonak eta horietara sartzeko bideak izango ditu, zerbitzuari buruzko alderdiak jorratzeko.
- Cyberzaintzari ematen dion informazioaren tratamendu konfidentziala jasotzea, informazio hori emandako zerbitzuen helbururako soilik erabiliko dela eta aplikatzekoa den araudiaren arabera babestuta egongo dela bermatuz.
- Cyberzaintzak egindako jarduerak premiaren, proportzionaltasunaren eta eragin minimoaren irizpideetara egokitzeko eskatzea, jardunbide egokien estandarrekin bat etorriz.

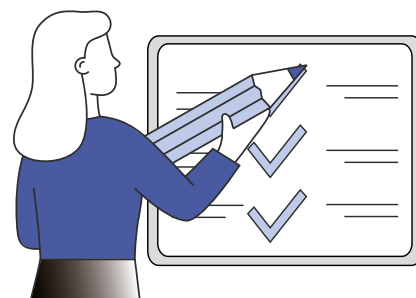


3.2.

Erakundearen betebeharrak

Katalogo honetako zerbitzuren bat erabiltzen duen edozein erakunde erabiltzailek honako betebeharrak hauek ditu gutxienez:

- Jasotzen dituen zerbitzuen ezaugarriak eta Cyberzaintzak bere gain hartutako kalitate konpromisoak ezagutzea, eta batera ezarritako erabilera baldintzak eta akordioak betetzea.
- Zerbitzuak eta lotutako informazioa arduraz erabiltzea, aplikatzekoa den araudiaren arabera, lortutako informazioaren erabilera zerbitzuen helburura mugatuz eta berariaz baztertuz irabazi-asmoko, legez kanpoko edo baimenik gabeko merkataritza-erabilerak, eta beharrezkoa ez denean informazio hori suntsitzeko konpromisoa hartuz.
- Informazioa eskatzeko, komunikazioak kudeatzeko edo zerbitzuak emateko baldintzetan aldaketak eskatzeko ezarritako sarbide kanalak eta prozedurak erabiltzea, bai eta Cyberzaintzak bidalitako jakinarazpenak jaso izanaren adierazpena ematea eta arduraz kudeatzea ere.
- Zerbitzuak behar bezala eman ahal izateko behar den informazioa ematea eta eguneratuta edukitzea, katalogoan eta ezarritako akordioetan aurreikusitakoaren arabera.
- Zerbitzuak osatzen dituzten baliabide teknologikoen erabilerrari eta datu pertsonalen tratamenduari buruz indarrean dagoen legeria betetzea.



- Cyberzaintzari jakinaraztea, jakin bezain laster, erakundearen, erabiltzaileen edo beste erakunde batzuen informazioaren eskuragarritasunari, osotasunari edo konfidentzialtasunari eragin diezaieketen zibersegurtasun eta zibermehatxuetako gertakariak, Segurtasun Eskema Nazionalaren (ENS) CCN - CCN-STIC 817 gidan jasotako gertakariak barne.
- Zerbitzuak ematean eskuratzen duen informazioaren konfidentzialtasuna mantentzea, aplikatu beharreko araudiaren arabera.
- Cyberzaintzari baimena ematea zerbitzuak behar bezala emateko beharrezkoak diren balidazioak egiteko. Balidazio horien artean egon daitezke, besteak beste, ahultasunak aurkitzea eta baliozkotzea, kredentzialak baliozkotzea edo azaldutako informazioa egiaztatzea. Jarduera horiek jardunbide egokien estandarren arabera egingo dira, eta edozein inpaktu potentzial minimizatuz.
- Cyberzaintzari baimena ematea emandako informazioa zerbitzuak ematen parte hartzen duten hirugarrenekin edo Euskadiko beste erakunde batzuekin partekatzeko, babes-neurriak hartzeko beharrezkoa denean.

3.3.

Gorabeheren jakinarazpena

Kontrakoa xedatzen ez bada, zibersegurtasuneko gertakari bati buruz Cyberzaintzara bidali behar den jakinarazpen edo komunikazio oro idatziz egin beharko da, eta helbide elektronikora bidali:



incidencias@cyberzaintza.eus

3.4.

Zerbitzuaren kalitatea eta konpromisoak

Cyberzaintzak, katalogo honetan jasotako zerbitzuen prestazioaren esparruan, konpromiso eta betebeharrak hartzen ditu bere gain:

- Zerbitzuak ematea katalogo honetan ezarritako baldintzetan eta kasu bakoitzean dagozkion eginkizunen arabera.
- Zerbitzuak modu profesionalan, arduratsuan eta puntualean emateko dauden arazoizko bitartekoak eta ahaleginak aplikatzea, aplikatzekoak diren ohiko kalitate-estandarren arabera.
- Erakunde erabiltzaileekin komunikazio eta koordinazio egokia izatea zerbitzuak emateari dagokionez, ezarritako kanalen bidez.
- Zerbitzuak ematearen ondorioz eskuratzen den informazioaren tratamendu konfidentziala bermatzea, aplikatzekoa den araudiarekin bat etorritik eta haien helburuarekin, hargatik eragotzi gabe segurtasun- eta prebentzio-arrazoiengatik informazio jakin bat beste erakunde edo organismo batzuekin modu mugatu eta kontrolatua partekatzea, hori ezinbestekoa denean hirugarrenak zibermehatxuetatik babesteko, betiere «need to know» printzipioa aplikatuta.
- Cyberzaintzak, bere eginkizunak betetz, ez du bere gain hartzen informazio-sistemen eta erakunde erabiltzaileen segurtasun-sistemen zuzeneko kudeaketa, eragiketa eta erantzukizuna, eta erakunde horiei dagokie segurtasun-neurriak ezartzea, kudeatzea eta mantentzea, bakoitzaren eskumenen esparruan.



04.

Zerbitzu-lerroak

Kudeaketa errazteko, katalogoko zerbitzuak **hamar kategoria nagusitan edo zerbitzu-lerrotan antolatu dira**, eta antzeko ezaugarriak eta helburu komun bat dituzten jarduerak biltzen dituzte. Ikuspegi egituratu horrek zerbitzuak eraginkorrako eta koherenteago administratzea ahalbidetzen du, jarduera bakoitza Cyberzaintzaren helburu estrategikoekin bat datorrela ziurtatuz.

4.1. Auditoretza

4.2. Kontzientziazioa

4.3. Koordinazio estrategikoa

4.4. Arriskuaren gobernua

4.5. Mehatxuen inteligentzia

4.6. Euskadiko segurtasun eredua

4.7. Segurtasun-eragiketak (SOC)

4.8. Gertakariei erantzutea (CSIRT)

4.9. Erasoko segurtasuna

4.10. Ezagutzaren transferentzia

4.1. Auditoretza

Auditoretzako ekintza-ildoak **ebaluazio objektibo eta independentera bideratuta dago**, informazioaren segurtasunaren eta zibersegurtasunaren arloko arauen, antolamenduen eta teknikaren betetze-mailaren arabera.

Auditoretza lerroaren barruan, honako zerbitzu hauek sartzen dira:



Segurtasunaren ebaluazioa

Segurtasuna ebaluatzeko zerbitzuaren helburua da erakundeek segurtasun-araudi nagusiak eta aplikatu beharreko erreferentzia-esparruak betetzen dituztela berrikustea eta ziurtatzea. Prozesu horren barruan sartzen da ezarritako kontrolen implementazio egokiaren ebaluazioa, aldiari behingo ebaluazioen bidez, hobekuntza-arlo posibleak identifikatzea helburu dutenak.

OAT (Auditoretza Teknikoko Organoa)

Auditoretza Teknikoko Organoaren zerbitzua arduratzen da auditoretzak egiteaz Segurtasun Eskema Nazionalaren arabera (311/2022 Errege Dekretua, maiatzaren 3koa, Segurtasun Eskema Nazionala arautzen duena) euskal administrazio publikoarentzat, eta, Kriptologia Zentro Nazionalak emandako aitortpenaren arabera, dagozkion adostasun-ziurtagiriak eman eta kudeatzen ditu.

Zibersegurtasunaren arloko jarraipen-planak gainbegiratzeko

Zibersegurtasun arloko jarraitutasun planak gainbegiratzeko zerbitzua arduratzen da autobabes planen arloan betebeharrak dituzten erakundeek jarraipena egiteaz, eta horiei Lehen Lehendakariorde eta Segurtasun sailburuaren 2024ko ekainaren 7ko AGINDUA aplikatzen zaie. Agindu horren bidez, autobabeseko euskal arauaren mendeko jarduerak batzuetarako zibersegurtasun arloko jarraipen planak egitea arautzen da, eta erakunde horiek zibersegurtasun arloko jarraipen planei buruz behar den informazioa erregistratzen eta eguneratuta mantentzen dute.

4. 2.

Kontzientziazioa

Kontzientziazio-lerroaren helburu nagusia **zibersegurtasunaren kultura sendoa sustatzea** da, bai eta pertsonen eta erakundeek **egungo ingurunean dauden arrisku digitalei buruz duten ezagutza- eta konpresio-maila handitzea** ere. Gainera, teknologiaren erabileran jokabide seguruak eta arduratsuak sustatu nahi ditu.

Lerro honek Cyberzaintzak eskainitako hainbat zerbitzu biltzen ditu, hainbat publiko objektibo eta bertikalen behar espezifikoak aurre egiteko diseinatuak. Zerbitzu horien artean daude:



Phishing kanpaina

Phishing kanpainen zerbitzuak phishing erasoak egiten ditu, erakunde batek mehatxu horiek detektatzeko eta horiei erantzuteko duen gaitasuna ebaluatzeko eta indartzeko berariaz diseinatuak. Kanpaina horien emaitzek informazio baliotsua ematen dute dauden ahuleziei buruz, eta kontzientziatzeko eta etengabe hobetzeko estrategiak garatzen laguntzen dute.

Kontzientziazioa

Kontzientziazio zerbitzua herritarren eta Euskadiko erakundearen artean zibersegurtasunaren ezagutza eta kultura indartzeko hezkuntza jardunaldiak antolatzean datza. Helburua da egungo munduan dauden arrisku digitalen kontzientzia handitzea eta parte-hartzaileei Internet eta teknologia berriak modu seguruago eta arduratsuagoan erabiltzeko beharrezko trebetasunak ematea.

4. 3.

Koordinazio estrategikoa

Koordinazio estrategikoko lerroaren helburu nagusia da **dauden zibersegurtasuneko baliabideak zeharkako ikuspegi batetik koordinatzea**, haien eraginkortasuna optimizatu eta hobetzeko.

Koordinazio estrategikoaren ildoaren barruan, Cyberzaintzak honako zerbitzu hauek ditu:

Euskadiko
Zibersegurtasun
Estrategiaren
hedapena

Euskal Autonomia Erkidegoko zibersegurtasun estrategia hedatzeko zerbitzuaren helburua da Estrategiaren prestaketa, ezarpena eta jarraipena gidatzea eta laguntzea, estrategia behar bezala gauzatzea bultzatuz. Horretarako, Cyberzaintzak aktiboki parte hartzen du definitutako gobernu organoetan, eta laguntza teknikoa ematen du koordinazio operatiboaren eta beharrezko laguntza teknikoaren bidez, bai eta Estrategiaren aurrerapen maila etengabe ebaluatuz eta gainbegiratzuz ere. Estrategiaren inplementazioan laguntza eta euskarria behar duten erakundeei ematen zaie zerbitzua, zibersegurtasun ekimenak zehaztutako esparru estrategikoarekin lerrokatzea erraztuz eta ezarritako helburuak lortzen lagunduz.

Zerbitzuak
kudeatzeko bulegoa

Zerbitzuak kudeatzeko bulegoaren zerbitzua erakunde erabiltzaileekiko harremanetarako kanal bakarra eta zentralizatua da, Cyberzaintzari lotutako eskaerak kudeatzeko, eta laguntza eta arreta integrala ematen du, zibersegurtasunaren arloan dituzten premia espezifikoekin koordinatuta eta lerrokatuta.

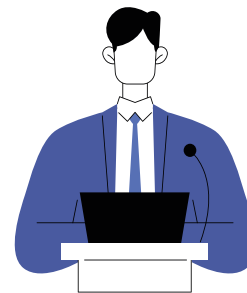
Zerbitzu honen bidez, jasotako eskaeren kudeaketa, koordinazioa eta jarraipena egiten da, publiko objektibo eta bertikalen eskakizunak identifikatuz eta aztertuz, eta barnean arlo arduradunetara bideratuz, arreta eraginkorra izan dezaten. Era berean, bulegoak ekimenak zeharkako ikuspegi batetik garatzea bultzatzen du, jarduerak gauzatzean koherentzia bermatuz eta arloaren artean informazio garrantzitsua trukatzeko erraztuz, ezarritako prozeduren arabera.

4. 4.

Arriskuaren gobernua

Arriskuaren gobernu-zerbitzuen lerroaren helburu nagusiak dira Euskal Autonomia Erkidegoko **zibersegurtasunarekin lotutako teknologia- eta antolamendu-arriskuak identifikatzea eta ebaluatzea**, eta arrisku horiek kudeatzeko eta arintzeko jarduerak garatzea, arriskua kudeatzeko esparru bat garatuz eta hedatuz, erakundeek arrisku-mailaren ikuspegi argia eta zeharkakoa izan dezaten, zibersegurtasunaren arloko problematika uler dezaten eta erabaki informatuak har ditzaten, eta babes-neurri egokiak ezar ditzaten, babes hori sustatzen duten berariazko ekimenak garatuz.

Arriskuaren gobernu-lerroaren barruan, Cyberzaintzak honako zerbitzu hauek ditu:

Arriskuaren
ebaluazioa

Arriskua ebaluatzeko zerbitzua Cyberzaintzaren arriskua kudeatzeko frameworkean oinarritzen da, eta Euskal Autonomia Erkidego osoko zibersegurtasun-arriskuen ikuspegi integrala eta zeharkakoa eskaintzen du. Esparru horren bidez, normalizatu behar diren arrisku espezifikoak identifikatzen dira, eta arrisku garrantzitsu guztiak behar bezala aintzat hartzen eta ebaluatzen direla ziurtatzen da. Zerbitzu honen eginkizun nagusia arrisku teknologikoak eta antolakuntzakoak aztertzea da, horien eraginaren eta probabilitatearen arabera lehenetsiz, eta arrisku horiek alderdi interesdunei benetan jakinaraziz. Gainera, neurketa etengabe eguneratzen eta hobetzen duen sistema dinamiko gisa inplementatzen da, mehatxuen ingurunean izandako aldaketak eta zibersegurtasuneko praktika onenak islatzeko.

Arriskuaren
kudeaketa

Arriskua kudeatzeko zerbitzuak barne hartzen du erakunde bakoitzaren arrisku-maila kontuan hartzea, etengabe eta haren ezaugarri bereziak eta jarduten duten ingurunea kontuan hartuta, eta hura tratatzeko behar diren segurtasun-neurriak zehaztea, hura arintzeko aukera, etengabeko monitorizazioa eta salbuespenen kudeaketa kontuan hartuta. Era berean, arrisku horiek tratatzeko beharrezkoak diren ekintzak definitzea eta lehenestea eta ekintza horiek koordinatzeko proiektu espezifikoak planifikatzea aurreikusten du.

Harmonizazio
bulegoa

Harmonizazio-bulegoaren zerbitzuak arriskuak kudeatzeko mekanismoak aplikatzeko jardunbide egokiak esparruak garatzea eta horiek aplikatzeko gidak egitea biltzen ditu, bai eta erakundeek horiek aplikatzeko jarraibideak prestatzea ere. Halaber, garatutako material guztiak interpretatzen laguntzen du, eta Cyberzaintzaren gainerako zerbitzuak hartzen laguntzen du.

Proiektu berezien
kudeaketa

Proiektu bereziak kudeatzeko zerbitzuak euskarria eskaintzen du Euskadiko sektore publikoaren barruko zibersegurtasunarekin lotutako ekimen espezifikoek kudeaketan. Halaber, laguntza ematen du proiektu horiei lotutako arriskuak kudeatzeko, eta laguntza teknikoa zibersegurtasun-zerbitzuak kontratatzeko.

4. 5.

Mehatxuen inteligentzia

Mehatxuen inteligentzia-zerbitzuaren helburu nagusia da **erakundeei zibersegurtasunaren arloko balizko mehatxuei buruzko informazio garrantzitsua eta prozesagarria ematea**. Horrek erasoei aurrea hartzea, erabaki informatuak hartzea eta babesa indartzea errazten die.

Illo horrek Cyberzaintzaren hainbat zerbitzu biltzen ditu, jarduera maltzurrei eta mehatxuei buruzko informazioa bildu, aztertu eta partekatzeko. Zerbitzu horien artean sartzen dira:



Alerta goiztiarra

Alerta goiztiarreko zerbitzua zaintza digitalean eta etengabeko monitorizazioan oinarritzen da. Adimen aurreratuko eredu bat erabiliz, hainbat iturritako datuak aztertzen dira zibersegurtasun arloko balizko arriskuak eta gertakariak identifikatzeko. Balizko mehatxu bat hautematean, alerta goiztiarrak ematen dira, kaltetuak ez izateko eta eraginkortasunez erantzuteko gomendio espezifikoekin batera.

Zibermehatxuei
buruzko informazioa
trukatzea

Zibermehatxuei buruzko informazioa trukatzeko zerbitzuak hainbat erakunde eta entitateren arteko lankidetzaren bidez, zibermehatxuei buruzko datuak modu arin eta eraginkorrean partekatzeko. Plataforma espezializatuak erabiliz, erasotzaileek erabiltzen dituzten konpromiso-adierazleak, taktikak, teknikak eta prozedurak buruzko informazioa bildu eta banatzen da. Informazio-truke horrek aukera ematen die erakundeei hautemateko eta erantzuteko gaitasuna hobetzeko.

4. 6.

Euskadiko segurtasun eredua

Euskadiko segurtasun ereduen zerbitzu-lerroaren helburu nagusia **zibersegurtasuneko esparru integral bat ezartzea** da, zibermehatxuen aurrean ingurune digital seguru eta erresilientea bermatzeko oinarri gisa.

Euskadiko segurtasun ereduen lerroaren barruan, Cyberzaintzak honako zerbitzu hauek ditu:



Euskadiko segurtasun ereduaren hedapenean laguntzea eta jarraipena egitea

CyberOrratzen hedapenean laguntzeko zerbitzuak, Euskadiko zibersegurtasun ereduak, laguntza espezializatua eskaintzen die erakunde erabiltzaileei, eredua pixkanaka ezartzen laguntzeko. CyberOrratz zibersegurtasuneko erreferentzia-esparru komuna da, Cyberzaintzak landu eta sustatua, eta segurtasun politikak, arau teknikoak eta babes neurriak integratzen dituen printzipio, kontrol eta irizpide teknikoaren multzo egituratu gisa ulertzen da, indarrean dagoen araudiarekin eta Euskadiko administrazio publikoen behar espezifikoekin lerrokatuta. Zerbitzu horren bidez, Agentziak ereduen hedapena, ezagutza eta ezarpena bultzatzen ditu, laguntza, laguntza tekniko, prestakuntza-ekintzak, gida praktikoa eta laguntza-tresnak eskainiz, euskal sektore publikoan zibersegurtasuna modu koherente, homogeneo eta lerrokatuan ezartzea errazteko, betiere erakunde bakoitzaren eskumenak errespetatuz.

4. 7.

Segurtasun-eragiketak (SOC)

SOCen zerbitzu lerroaren helburu nagusia da erakundeen **azpiegitura teknologikoak babestea**, etengabeko monitorizazioaren bidez, eta horrek zibersegurtasun arloko balizko gertakarien aurrean erantzuteko denbora murrizten du.

SOC lerroaren barruan, Cyberzaintzak honako zerbitzu hauek ditu:



SOC

Segurtasun eragiketen zentroaren (SOC) zerbitzua erakundeen barruan gertatzen diren barne gertaerak monitorizatzeko da, jardura susmagarriak denbora errealean detektatzeko eta aztertzeko. Zerbitzu horri esker, erakundeek modu arin eta eraginkorrean erantzun dezakete zibersegurtasun arloko gertakari potentzialen aurrean.

Threat hunting

Threat hunting zerbitzua ingurune korporatiboen barruko mehatxuen identifikazio proaktiboan oinarritzen da. Helburua mehatxu ezezagunak detektatzea eta arintzea da, eta, horrela, mehatxu horien eragina prebenitzea, gauzatu ahal izan baino lehen.

4. 8.

Gertakariei erantzutea (CSIRT)

Segurtasun Informatikoko Gertakariei Erantzuteko Taldearen (CSIRT) zerbitzu-lerroaren helburu nagusia **erakundeei segurtasun-gertakariak kudeatzen laguntzea** da. Ikuspegi integral batekin, hainbat erakunderi eragiten dieten gertakarien aurreko erantzuna koordinatu nahi da, eta informazio erabakigarria partekatu, gainerakoak babesteko.

Lerro honek Cyberzaintzak eskainitako hainbat zerbitzu biltzen ditu, gertakariei emandako erantzunaren hainbat alderdiri heltzeko diseinatuak. Zerbitzu horien artean daude:

**Aholkularitza**

Aholkularitza-zerbitzuak gomendio orokorrak ematen ditu segurtasun informatikoko gorabeheraren bat izanez gero nola jokatu jakiteko. Era berean, beharrezkoa denean, Cyberzaintzako gertakariei erantzuteko talde tekniko espezializatuak beharrezko ekintzak implementatzen ditu gertakaria ez hedatzeko eta komunitateari mehatxuaz ohartarazteko.

Koordinazioa

Zibersegurtasun arloko gertakariak koordinatzeko zerbitzua aktibatu egiten da gertakari horiek Cyberzaintzaren helburu diren publikoetan eragin anitza eta esanguratsua dutenean. Helburua aholkularitza tekniko espezializatua ematea eta prebentzio-neurriak hartzea da, gertakariak beste erakunde batzuei eragin ez diezaien. Zerbitzu honek erantzun azkarra eta koordinatua bermatzen du, gertakariaren irismena eta ondorioak minimizatuz, tartean dauden alde guztiak beren ekintzetan informatuta eta lerrokatuta daudela bermatuz.

DFIR

Auzitegiko Analisi Digitala eta Gertakarien Erantzuna Zerbitzuaren (DFIR) helburua da segurtasun gertakari baten aurrean ebidentzia digitalak urrunetik eskuratzea eta aztertzea, gertakaria konpontzen laguntzeko.

Krisien kudeaketa

Krisiak kudeatzeko zerbitzua Euskadiko sektore publiko osorako plan integral bat koordinatzeaz arduratzen da, eta ziurtatzen du erakunde guztiak prest egongo direla segurtasun-gertakari kritiko baten ondoriozko krisia modu eraginkorrean kudeatzeko.

Takedown

Takedown zerbitzua Internetetik eduki maltzurra edo baimenik gabea kentzeko egiten diren ekintzei dagokie.

**Zibersegurtasun
arloko gertakariei
erantzuteko
prestakuntza**

Zibersegurtasun arloko gertakariei erantzuteko prestaketa zerbitzuak erakundeei prebentzio prozesuak eta gaitasunak ezartzen laguntzen die, haien heldutasuna ebaluatzen du eta hobekuntzak proposatzen ditu gertakarien aurreko erantzuna optimizatzeko.

4. 9.

Erasoko segurtasuna

Erasoko segurtasuna lerroaren helburu nagusia da **erakundeen sistemetan mehatxuak eta ahultasunak identifikatzea erasotzaile batek egin aurretik**, eta, horrela, balizko zibererasoen aurrean defentsarako gaitasuna indartzea.

Erasoko segurtasuna lerroaren barruan, Cyberzaintzak honako zerbitzu hauek ditu:

Auditorerza
teknikoa

Auditorerza teknikoko zerbitzuak, besteak beste, penetrazio-probak (pentesting), aplikazioen auditorerzak, Wi-Fi sareak eta konfigurazioak biltzen ditu. Helburua babes-maila ebaluatzea eta hobetu daitezkeen alderdiak identifikatzea da.

EASM

Eraso eta Arintze Azaleraren Ebaluazio Zerbitzuak (EASM) erakundeen esposizio-azalera aztertzen du, arrisku teknologikoaren maila zehazteko. Ebaluazio horretatik abiatuta, gomendio espezifikoak proposatzen dira, identifikatutako arriskuak arintzeko. Gainera, zerbitzua ez da soilik berehalako babesean oinarritzen, epe luzera erresilientzia handitzea ere bilatzen du.

Red team

Red team zerbitzuaren helburua erakunde baten aurkako benetako erasoaren simulazioak egitea da. Zerbitzu honek sistemen eta defentsen ahuleziak identifikatzen eta zuzentzen laguntzen du, bai eta babes-ekipoen eraginkortasuna ebaluatzen ere.

4. 10.

Ezagutzaren transferentzia

Ezagutza transferitzeko zerbitzuen lerroaren helburu nagusia da **zibersegurtasuneko trebetasunen espezializazioa eta garapena sustatzea** hainbat publikoren artean, baita operatiboak eta arrakasta kasuak Cyberzaintzako publikoetara esportatzea ere. Gainera, heldutasun-maila handiagoa duten erakundeetatik heldutasun-maila txikiagoa dutenetara esportatu nahi dira jarduteko moduak, dokumentazioa, klausulak, etab. Horrela, ezagutzak eta praktikak trukatzea sustatzen da, zibersegurtasunaren estandar orokorra handitzeko.



Entrenamendua

Entrenamendu-zerbitzua hondamendien aurrean simulakroak eta errekupeazio-probak egiteko eta koordinatzeko tekniketan zentratzen da. Horrek barne hartzen ditu ziberariketa indibidualak zein kolektiboak, erakundeak krisiak eraginkortasunez kudeatzeko prestatzen dituztenak.

Prestakuntza

Prestakuntza-zerbitzua Agentziaren helburu diren publikoak zibersegurtasunean espezializatzen laguntzeko diseinatuta dago. Gaikuntzak ezarritako kanalak erabiliz edo metodo alternatiboan bidez egin daitezke, ohiko baliabideekin landu ezin diren gai espezifikoak helduz zaienean.

05.

Zerbitzu-fitxak

Jarduera-eremua hobeto mugatzeko, erakunde erabiltzaile bati eskainitako zerbitzu bakoitzeko deskribapen-fitxa bat sartu da, zerbitzu horien ezaugarri diren oinarrizko alderdiak jasotzeko.

5.1. Auditoretza

- 5.1.1. Segurtasunaren ebaluazioa
- 5.1.2. OAT - Auditoretza Teknikoko Organoa
- 5.1.3. Jarraitutasun-planak gainbegiratzea

5.2. Kontzientziakzioa

- 5.2.1. Kontzientziakzioa
- 5.2.2. Phishing kanpainak

5.3. Koordinazio estrategikoa

- 5.3.1. Euskadiko Zibersegurtasun Estrategiaren hedapena
- 5.3.2. Zerbitzuak kudeatzeko bulegoa

5.4. Arriskuaren gobernuak

- 5.4.1. Arriskuaren ebaluazioa
- 5.4.2. Arriskuaren kudeaketa
- 5.4.3. Harmonizazio bulegoa
- 5.4.4. Proiektu berezien kudeaketa

5.5. Mehatxuen inteligentzia

- 5.5.1. Alerta goiztiarra
- 5.5.2. Ziber mehatxuei buruzko informazioa trukatzea

5.6. Euskadiko segurtasun eredua

- 5.6.1. Euskadiko segurtasun ereduaren hedapenean laguntzea eta jarraipena egitea

5.7. Segurtasun-eragiketak (SOC)

- 5.7.1. SOC
- 5.7.2. Threat hunting

5.8. Gertakariei erantzutea (CSIRT)

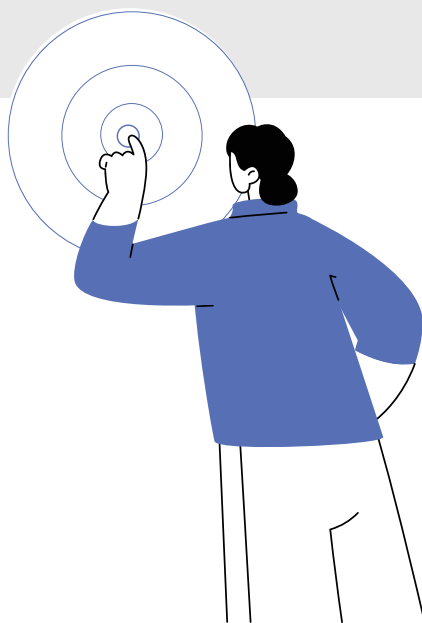
- 5.8.1. Aholkularitza
- 5.8.2. Koordinazioa
- 5.8.3. DFIR
- 5.8.4. Krisien kudeaketa
- 5.8.5. Takedown
- 5.8.6. Zibersegurtasun arloko gertakariei erantzuteko prestakuntza

5.9. Erasoko segurtasuna

- 5.9.1. Auditoretza teknikoa
- 5.9.2. EASM
- 5.9.3. Red team

5.10. Ezagutzaren transferentzia

- 5.10.1. Prestakuntza
- 5.10.2. Entrenamendua



5.1. Auditoretza

5.1.1.
Segurtasunaren ebaluazioaZerbitzu-lerroa
AuditoretzaHarremanetarako guneak
evaluacion@cyberzaintza.eus

Segurtasuna Ebaluatzeko Zerbitzuaren helburua da erakundeek **segurtasun araudi nagusiak eta aplikatu beharreko erreferentzia esparruak betetzen dituztela berrikustea eta ziurtatzea**. Prozesu horren barruan sartzen da ezarritako kontrolen inplementazio zuzenaren ebaluazioa, hobetzeko arlo posibleak identifikatu nahi dituzten aldizkako ebaluazioen bidez.

**Publiko hartzailea**

- ✓ Euskal sektore publikoa
- ✓ Enpresa estrategikoak
- ✓ Autobabeserako betebeharra duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak

**Helburua**

Erakundeak zibersegurtasunaren arloan duen egokitasun-mailaren ikuspegi objektiboa izatea ahalbidetzen du, **erabakiak hartzea eta hobetzeko jarduerak lehenestea** erraztuz.

**Ezaugarriak**

- Segurtasun-araudien betetze-maila eta aplikatu beharreko erreferentzia-esparruak ebaluatzea.
- Informazio egituratua lortzea, ikuskatutako prozesuen arduradunekin egindako bileren bidez.
- Ezarritako segurtasun-kontrolak in situ edo urrunetik ebaluatzea. Ebaluatu beharreko zerbitzuaren izaeragatik edo aplikatu beharreko araudiaren arabera.
- Ezarritako kontrolak behar bezala inplementatu direla egiaztatzea.
- Adostutako ekintza zuzentzaileen proposamena eta jarraipena.

**Zerbitzuaren aukerak****CyberOrratz ebaluazioa.**

Aztertutako zerbitzuak, prozesuak eta **CyberOrratz sistemak segurtasun-eredura** zenbateraino egokitzen diren identifikatzea eta ebaluatzea, emaitzen txostena eginda eta dagozkien betetze-mailak zehaztuta.

Arauen ebaluazioa.

Aztertutako zerbitzuak, prozesuak eta sistemak adostutako **zibersegurtasun esparrura** zenbateraino egokitzen diren identifikatzea eta ebaluatzea, emaitzen txostenarekin batera.

**Zerbitzua eskatzeko prozedura**

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearren.

**Zerbitzuak CyberOrratzi egiten dion ekarpena**

Zerbitzuaren aplikazio egokia ziurtatzea helburu duen ereduaren alderdirako gomendatutako **ezarpen-maila**:

1

2

3

4

5



Lantzen duen ereduaren alderdia:

Kontrola**G3.4****Auditoretza eta
betetze programa**

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.

5.1.2. OAT - Auditoretza Teknikoko Organoa



Zerbitzu-lerroa
Auditoretza

Harremanetarako guneak
oat@cyberzaintza.eus

Auditoretza Teknikoko Organoaren zerbitzua arduratzen da auditoretzak egiteaz, Segurtasun Eskema Nazionalaren arabera (311/2022 Errege Dekretua, maiatzaren 3koa, Segurtasun Eskema Nazionala arautzen duena), Euskal Administrazio Publikoarentzat, eta, Zentro Kriptologiko Nazionalak emandako aitortpenaren arabera, dagozkion **adostasun ziurtagiriak** eman eta kudeatzen ditu.



Publiko hartzailea

- ✓ Euskal sektore publikoa
- ✗ Enpresa estrategikoak
- ✗ Autobabeserako betebeharrak duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak



Helburua

Erakundeak Segurtasunaren Eskema Nazionala betetzeko berme objektibo eta independentea lortzen du, eta segurtasun juridikoa eta bere zibersegurtasun-mailarekiko konfiantza ematen ditu kontrol-organoen eta alderdi interesdunen aurrean.



Ezaugarriak

- Ikuskatu eta, hala badagokio, ziurtatu beharreko irismena zehaztea.
- Sistemen kategoria edo SENekiko adostasuna ebaluatzen irizpidetza hartu beharreko Betetze Espezifiko Profila zehaztea.
- Adostasun-auditoretza planifikatzea.
- Auditoretzaren fase asinkronoa garatzea eta dokumentuetan jasotako segurtasun-neurrien aurretiazko ebaluazioa egitea.
- Auditoretzaren fase sinkronoa garatzea, urrutetik edo in situ, adostutako plangintzaren arabera, eta segurtasun neurriak ebaluatzea.
- Auditoretza-txostena entregatzea.
- Hala badagokio, gauzatutako Ekintza Zuzentzaileen Plana ebaluatzea.
- Hala badagokio, ziurtagiria emateko erabakia.
- Hala badagokio, ezohiko auditoretza garatzea.



Zerbitzuaren aukerak

PCEn arabera ENS auditoretza.

PCEn arabera ENS auditoretza: **Auditoretza** ENSren arabera garatzea (eta dagokion ziurtagiria ematea, hala badagokio), **bezeroak hautatutako Betetze Profil Espezifiko** baten arabera.

ENS auditoretza, kategoriaren arabera.

Auditoretza ENSren arabera garatzea (eta dagokion ziurtagiria ematea, hala badagokio), **auditatutako sistemen kategoriaren arabera** (oinarrizkoa, ertaina edo handia, dagokionaren arabera).



Zerbitzua eskatzeko prozedura

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearen.



Zerbitzuak CyberOrratzi egiten dion ekarpena

Zerbitzuaren aplikazio egokia ziurtatzea helburu duen ereduaren alderdirako gomendatutako **ezarpen-maila**:

1 2 3 4 5



Lantzen duen ereduaren alderdia:

Kontrola

G3.4

Auditoretza eta betetze programa

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.

5.1.3. Jarraitutasun-planak gainbegiratzea



Zerbitzu-lerroa
Auditoretza

Harremanetarako guneak
jarraipena@cyberzaintza.eus

Zibersegurtasun arloko jarraitutasun planak gainbegiratzeko zerbitzua arduratzen da autobabes planen arloan betebeharrak dituzten erakundeek **jarraipena** egiteaz, eta horiei Lehen Lehendakariorde eta Segurtasun sailburuaren 2024ko ekainaren 7ko AGINDUA aplikatzen zaie. Agindu horren bidez, autobabeseko euskal arauaren mendeko jarduera batzuetarako zibersegurtasun arloko jarraipen planak egitea arautzen da, eta erakunde horiek **zibersegurtasun arloko jarraipen planei** buruz behar den informazioa **erregistratzen eta eguneratuta** mantentzen dute.



Publiko hartzailea

- ☐ Euskal sektore publikoa
- ☐ Enpresa estrategikoak
- ☒ Autobabeserako betebeharra duten enpresak
- ☐ Beste enpresak
- ☐ Herritarrak



Helburua

Aukera ematen dio erakundeari zibersegurtasun-alorreko jarraipen-planetan dituen betebeharrak etengabe betetzen direla bermatzeko, eta eskatutako informazioa modu sistematikoan erregistratuta eta gainbegiratuta dagoela ziurtatzeko.



Ezaugarriak

- Zibersegurtasunaren arloko jarraipen-planei buruzko informazioa erregistratzeko betebeharraren jarraipena egitea.
- Arlo horretan erregistratutako informazioaren ebaluazioa.
- Erregistratutako informazioan egindako aldaketak eta eguneratzeak gainbegiratzea.



Zerbitzuaren aukerak

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.



Zerbitzua eskatzeko prozedura

Zibersegurtasun arloko informazioa izapidetzeko, erakundeak jardueraren datuak Autobabes Erregistroan eman ondoren, Zibersegurtasun arloko babeserako datu espezifikoek fitxa inprimakia bete behar du.

Ondoren, Zibersegurtasunaren Euskal Agentziara – Cyberzaintzara bidali behar da, Erregistro Elektronikoko Orokorren bidez.

Informazio gehiago nahi izanez gero, “Zibersegurtasunaren arloko Jarraitutasun Plan bat egiteko laguntza-gida” kontsulta daiteke.

Zibersegurtasunaren arloko jarraipen-planei buruzko informazio gehiago FAQ hauetan.

5.2. Kontzientziazioa

5.2.1.
KontzientziazioaZerbitzu-lerroa
KontzientziazioaHarremanetarako guneak
csirt@cyberzaintza.eus

Kontzientziazio Zerbitzua herritarren eta Euskadiko erakundearen artean zibersegurtasunaren ezagutza eta kultura indartzeko **hezkuntza-jardunaldiak** antolatzen datza. Helburua da egungo munduan dauden **arriku digitalen kontzientzia handitzea** eta parte-hartzaileei Internet eta teknologia berriak modu seguruagoan erabiltzeko beharrezko trebetasunak ematea.

Zerbitzu hori kolektibo partikularrei zuzendutako ekimen espezifikoekin osatzen da, hala nola zibersegurtasuneko profesionalei, adinekoei edo adingabeiei zuzendutakoekin. Ekimen horien artean daude, besteak beste, **material espezifikoak egitea**, jolas-jarduerak antolatzea edo kanpaina espezializatuak diseinatzea.

**Publiko hartzailea**

- ✓ Euskal sektore publikoa
- ✓ Enpresa estrategikoak
- ✓ Autobabeserako betebeharrak duten enpresak
- ✓ Beste enpresak
- ✓ Herritarrak

**Ezaugarriak**

- Kontzientziazioko hezkuntza-jarduerak eta -jardunaldiak antolatzea, herritarren eta Euskadiko erakundearen artean zibersegurtasunaren kultura indartzeko.
- Interneten eta teknologia berrien erabileran jardunbide egokiak sustatzeko prestakuntza-edukiak diseinatzea, lantzea eta zabaltzea.
- Kolektibo jakin batzuei egokitutako ekimen espezifikoak garatzea, hala nola zibersegurtasuneko profesionalei, adinekoei edo adingabeiei.
- Dibulgazio-jarduerak, jolas-jarduerak edo kanpaina espezializatuak antolatzea, xede diren publikoen ezaugarrietara eta beharretara egokituta.
- Kontzientziazio edukiak eta mezuek aldiaren behin eguneratzea, arriku digitalen bilakaeraren eta sortzen ari diren joeren arabera.

**Helburua**

Pertsona edo erakunde erabiltzaileak zibersegurtasunaren duen kontzientzia maila indartzen du, teknologia digitalak modu seguruagoan eta arduratsuegi erabiltzeko **praktika onak** eta oinarritzko irizpideak bereganatuz eta arriku digitalekiko esposizioa murriztuz.

**Zerbitzuaren aukerak****Materialen garapena.**

Zibersegurtasunaren arloan **kontzientziazioko materialak** diseinatzea eta lantzea.

Kontzientziazio saioak ematea.

Zerbitzuaren xede diren publikoentzako **kontzientziazio-jardunaldiak** eta **-saioak** antolatzea.

**Zerbitzua eskatzeko prozedura**

Kontzientziazio-materialak, kanpainak eta dibulgazio-ekintzak publikoaren eskura jartzen dira, Agentziaren webgunearen eta sare sozialen bidez.

Zerbitzuaren gainerako elementuei atxiki edo horietan parte hartu ahal izateko, ezinbestekoa izango da haiek izendatutako harremanetarako puntuaren bitartez eskatu eta kudeatzea, bai eta eskatzaileak solaskide bat zehaztea ere, zerbitzua benetan emateko aukera berma dezan.

**Zerbitzuak CyberOrratzi egiten dion ekarpena**

Ezarpn-maila guztietarako gomendatzen da.



Lantzen duen ereduaren alderdia:

Kontrola**G1.6****Oinarritzko kontzientziazioa eta prestakuntza**

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.



5.2.2. Phishing kanpainak

Zerbitzu-lerroa
Kontzientziazioa

Harremanetarako guneak
csirt@cyberzaintza.eus

Phishing kanpainen zerbitzuak phishing erasoak egiten ditu, mehatxu horiek detektatzeko eta horiei erantzuteko **erakunde baten gaitasuna ebaluatzeko eta indartzeko berariaz diseinatuak**. Kanpaina horien emaitzek informazio baliotsua ematen dute dauden ahuleziei buruz, eta gaitzeko eta **etengabe hobetzeko estrategiak** garatzen laguntzen dute.



Publiko hartzailea

- ✓ Euskal sektore publikoa
- ✗ Enpresa estrategikoak
- ✗ Autobabeserako betebeharra duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak



Helburua

Erakunde erabiltzaileari aukera ematen dio **phishing-erasoen aurrean duen esposizio-maila erreala** ezagutzeko, ahuleziak eta arrisku-portaerak identifikatuz eta **kontzientziazioa sendotzeko** eta erakundearen detekzio- eta erantzun-gaitasuna hobetzeko oinarri objektibo bat izanez.



Ezaugarriak

- Phishing-kanpainak diseinatzeko eta gauzatzen espezializatutako teknikariak ematen dute zerbitzua.
- Zerbitzua eskaripean ematea, erakunde eskatzaileak zehaztutako helburuen eta irismenaren arabera.
- Phishing-kanpainak zenbait zailtasun- eta errealismo-mailarekin konfiguratzea, erakundearen zibersegurtasun-heldutasunera egokituta.
- Kanpainan lortutako emaitzak aztertzea, eta ahuleziak eta jokabide arriskutsuak identifikatzea.
- Emaizten txostenak egitea, phishing-erasoak detektatzeko eta haiei erantzuteko gaitasuna ebaluatzeko eta hobekuntza-ekintzak definitzen laguntzeko.



Zerbitzuaren aukerak

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.



Zerbitzua eskatzeko prozedura

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearren.



Zerbitzuak CyberOrratzi egiten dion ekarpena

Zerbitzuaren aplikazio egokia ziurtatzea helburu duen ereduaren alderdirako gomendatutako **ezarpen-maila**:

1

2

3

4

5



Lantzen duen ereduaren alderdia:

Kontrola

G3.5

Phishing etikoa

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.

5.3. Koordinazio estrategikoa

5.3.1.

Euskadiko Zibersegurtasun Estrategiaren hedapena



Zerbitzu-lerroa
Koordinazio estrategikoa

Harremanetarako guneak
estrategia@cyberzaintza.eus

Euskadiko Zibersegurtasun Estrategia Hedatzeko zerbitzua da Estrategia lantzen, ezartzen eta haren jarraipena egiten laguntzea eta haren buru izatea, haren gauzatze egokia bultzatuz.

Horretarako, Cyberzaintzak **aktiboki parte hartzen du zehaztutako gobernu-organoetan**, koordinazio operatiboaren eta beharrezko laguntza teknikoaren bidez laguntza teknikoa emanez, bai eta Estrategiaren aurrerapen-maila etengabe ebaluatuz eta gainbegiratuz ere.

Zerbitzua ematen zaie Estrategia inplementatzeko laguntza eta euskarria behar duten erakundeei, beren zibersegurtasun-ekimenak **definitutako esparru estrategikoarekin lerrokatzea** erraztuz eta ezarritako helburuak lortzen lagunduz.

**Publiko hartzailea**

- ✓ Euskal sektore publikoa
- ✓ Enpresa estrategikoak
- ✓ Autobabeserako betebeharra duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak

**Helburua**

Laguntza espezializatua lortzeko aukera ematen die erakundeei, beren zibersegurtasun-ekimenak Euskadiko Zibersegurtasun Estrategiarekin lerrokatzeko, eta, horrela, helburu estrategiko komunekin koherente eta bat datorren ezarpena lortzen laguntzeko.

**Ezaugarriak**

- Euskadiko Zibersegurtasun Estrategia egiten, berrikusten eta jarraitzen aitzindaria izatea.
- Estrategia eskualde-eremuan behar bezala inplementatzea bultzatzea.
- Estrategiari lotutako gobernu-organoetan aktiboki parte hartzea.
- Laguntza teknikoa ematea koordinazio operatiboaren eta akordioen jarraipenaren bidez.
- Estrategiaren aurrerapen-maila etengabe ebaluatzea eta gainbegiratzea.
- Ekimenak zehaztutako helburu estrategikoekin lerrokatzea bultzatzea.

**Zerbitzuaren aukerak**

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.

**Zerbitzua eskatzeko prozedura**

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearen.

5.3.2. Zerbitzuak kudeatzeko bulegoa



Zerbitzu-lerroa
Koordinazio estrategikoa

Harremanetarako guneak
zerbitzuak@cyberzaintza.eus

Zerbitzuak kudeatzeko bulegoaren zerbitzua da **erakunde erabiltzaileekiko harremanetarako kanal bakarra eta zentralizatua**, Cyberzaintzari lotutako eskaerak kudeatzeko, eta laguntza eta arreta integrala, koordinatua eta zibersegurtasunaren arloan dituzten behar espezifikoekin bat datorrena eskaintzen ditu.

Zerbitzu honen bidez, jasotako **eskaeren kudeaketa, koordinazioa eta jarraipena** egiten da, helburu diren publikoen eta sektoreen eskakizunak identifikatuz eta aztertuz, eta barne-mailan arlo arduradunetara bideratzen dira, arreta eraginkorra izan dezaten.

Halaber, Bulegoak zeharkako ikuspegi batetik bultzatzen du ekimenen garapena, **jarduerak gauzatzean koherentzia bermatuz** eta arlo desberdinen artean informazio garrantzitsua trukatzeko erraztuz, ezarritako prozeduren arabera.



Publiko hartzailea

- ✓ Euskal sektore publikoa
- ✓ Enpresa estrategikoak
- ✗ Autobabeserako betebeharrak duten enpresak
- ✗ Beste enpresak
- ✗ Herritarak



Helburua

Erakunde erabiltzaileari erreferentziako eta laguntzako **kanal bakarra** ematen dio, bere eskaeren kudeaketa sinplifikatu eta ordenatzeko aukera ematen diona, zibersegurtasunaren arloan dituen **premiekin** koordinatutako eta lerrokatutako arreta ziurtatuz.



Ezaugarriak

- Cyberzaintzaren erakunde erabiltzaileekiko harremanetarako kanal bakar eta zentralizatua.
- Eskuragarri dauden zibersegurtasun zerbitzuetarako sarbide ordenatu eta egituratua ematea.
- Jasotako eskaeren kudeaketa, koordinazioa eta jarraipen integrala.
- Xede diren publikoen eta sektoreen beharrak identifikatzea eta aztertzea.
- Eskaerak arlo arduradunetara bideratzea, arreta eraginkorra emateko.
- Jardueren koherentzia bermatzea eta arloen arteko informazio-trukea sustatzea.



Zerbitzuaren aukerak

Identifikazioa.

Zibersegurtasunaren arloko **beharrak identifikatzea**.

Identifikazioa + Euskarria.

Euskadin zibersegurtasunaren arloan dauden beharrak identifikatzea eta **implementazioan laguntzea**.



Zerbitzua eskatzeko prozedura

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearren.

5.4. Arriskuaren gobernua

5.4.1.
Arriskuaren ebaluazioa

Zerbitzu-lerroa
Arriskuaren gobernua

Harremanetarako guneak
riesgos@cyberzaintza.eus

Arriskua ebaluatzeko zerbitzua **Cybertzaintzaren arriskua kudeatzeko frameworkean oinarritzen** da, eta Euskal Autonomia Erkidego osoko zibersegurtasun-arriskuen ikuspegi integrala eta zeharkakoa eskaintzen du. Esparru horren bidez, normalizatu beharreko **arrisku espezifikoak identifikatzen** dira, eta arrisku garrantzitsu guztiak behar bezala kontuan hartzen eta ebaluatzen direla ziurtatzen da. Zerbitzu honen funtzio nagusia da arrisku teknologikoak eta antolakuntzakoak aztertzea, haien **eraginaren eta probabilitatearen arabera lehenetsiz**, eta alderdi interesdunei arrisku horien berri emanez. Gainera, neurketa etengabe eguneratu eta hobetzen duen **sistema dinamiko** gisa inplementatzen da, mehatxuen inguruko aldaketak eta zibersegurtasuneko jardunbiderik onenak islatzeko.

**Publiko hartzailea**

- ✓ Euskal sektore publikoa
- ✓ Enpresa estrategikoak
- ✗ Autobabeserako betebeharra duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak

**Ezaugarriak**

- Cyberzaintzaren arriskuak kudeatzeko framework-a argitaratzea eta eguneratzea
- Cyberzaintzaren arriskuak kudeatzeko framework-a aplikatzeko tresnak, liburutegiak eta katalogoak argitaratzea.
- Hartzailearen zibersegurtasun arriskuak identifikatzea eta katalogatzea.
- Identifikatutako zibersegurtasun arriskuak aztertzea.
- Zibersegurtasun arriskuen analisiak normalizatzea eta homogeneizatzea.
- Zibersegurtasun arriskuen analisisen emaitzak ebaluatzea.
- Arriskuen ebaluazioen emaitzak aztertzea eta lehenestea.
- Zibersegurtasun arriskuen ebaluazioaren eta lehenespenaren emaitzak jakinaraztea.

**Helburua**

Erakundeak bere zibersegurtasun-arriskuen ikuspegi objektiboa, homogeneoa eta lehenetsia lortzen du, eta, horri esker, bere esposizio-maila ulertzen du, arriskuak modu sendoa konparatzen ditu eta erabakiak hartzeko oinarri komun eta eguneratu bat du.

**Zerbitzuaren aukerak****Euskarri metodologikoa.**

Zerbitzuaren erabiltzaileek Cyberzaintzaren arriskua kudeatzeko **framework-a modu eraginkorrean** aplikatu ahal izateko beharrezkoak diren **tresnak eta mekanismoak gaitzea**.

Arriskuaren analisisa.

Arriskua ebaluatzeko jarduerak gauzatzea, arriskuak identifikatu eta katalogatzetik hasi eta emaitzak aztertu eta lehenetsi arte, eta **dagokion jakinarazpena** egitea.

**Zerbitzua eskatzeko prozedura**

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearren.

**Zerbitzuak CyberOrratzi egiten dion ekarpena**

Ezarpen-maila guztietarako gomendatzen da.



Lantzen duen ereduaren alderdia:

Kontrola G2.9 Arriskuak kudeatzeko metodologia

Kontrola G4.1 Arriskuaren kudeaketa kuantitatiboa

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.



5. 4. 2. Arriskuaren kudeaketa

Zerbitzu-lerroa
Arriskuaren gobernua

Harremanetarako guneak
riesgos@cyberzaintza.eus

Arriskua kudeatzeko zerbitzuaren barruan sartzen da **erakunde bakoitzaren arrisku-maila kontuan hartzea**, modu jarraituan eta haren ezaugarri partikularrak eta jarduten duten ingurunea kontuan hartuta, eta horiek **tratatzeko beharrezkoak diren segurtasun-neurriak zehaztea**, horiek arintzeko aukera, etengabeko monitorizazioa eta salbuespenen kudeaketa kontuan hartuta. Era berean, arrisku horiek tratatzeko beharrezkoak diren **ekintzak definitzea eta lehenestea** eta ekintza horiek koordinatzeko proiektu espezifikoak planifikatzea aurreikusten du. Arriskuen jarraipen eta kudeaketa prozesu osoa **Cyberzaintzaren arriskua kudeatzeko frameworkaren arabera** egiten da, metodologia sendo eta eraginkorra bermatuz.



Publiko hartzailea

- ✓ Euskal sektore publikoa
- ✓ Enpresa estrategikoa
- ✗ Autobabeserako betebeharrak duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak



Helburua

Erakundeak akonpainamendu aditua lortzen du bere **arrisku-maila erabaki eragingarri** bihurtzeko, segurtasun-neurriak lehenesteko eta etengabeko jarraipena egiteko bere esposizioa modu jarraituan murrizteko.



Ezaugarriak

- Erakundearen arrisku-mailak ebaluatzea, haien ezaugarriak eta testuingurua kontuan hartuta.
- Arriskua kudeatzeko estrategiak zehaztea, kontuan hartzen den kasuistika bakoitzerako.
- Zehazten diren arriskua kudeatzeko estrategiei lotutako arriskua tratatzeko ekintzak definitzea eta lehenestea.
- Arriskuak arintzeko jarduerak antolatzea, hala erabakitzen den kasuetan.
- Arriskuen bilakaeraren jarraipena, kudeaketa osoan zehar.
- Segurtasuneko salbuespenak kudeatzea, horien analisia, tratamendua eta jarraipena barne, Cyberzaintzaren arriskuak kudeatzeko frameworkean ezarritako irizpideen arabera.
- Arriskua arintzeko ekintzak koordinatzeko proiektu espezifikoak diseinatzea eta planifikatzea.
- Arriskuen egoeraren eta horiei lotutako estrategia eta ekintzen etengabeko jarraipena egitea, Cyberzaintzaren arriskua kudeatzeko frameworkaren arabera.



Zerbitzuaren aukerak

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.



Zerbitzua eskatzeko prozedura

Zerbitzuan parte hartzeko edo esleitzeko, **nahitaezkoa** izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearen.



Zerbitzuak CyberOrratzi egiten dion ekarpena

Zerbitzuaren aplikazio egokia ziurtatzea helburu duen ereduaren alderdirako gomendatutako **ezarpen-maila**:

1

2

3

4

5



Lantzen duen ereduaren alderdia:

Kontrola

G4.1

Arriskuaren kudeaketa kuantitatiboa

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.

5. 4. 3. Harmonizazio bulegoa



Zerbitzu-lerroa
Arriskuaren gobernu

Harremanetarako guneak
observatorio@cyberzaintza.eus

Harmonizazio Bulegoaren zerbitzuak barnean hartzen ditu **arriskuak kudeatzeko mekanismoak** aplikatzeko jardunbide egokien esparruen garapena eta **mekanismo horiek aplikatzeko giden prestaketa**, bai eta erakundeek aplikatu beharreko jarraibideen prestakuntza ere. Halaber, garatutako material guztiak interpretatzeko laguntza ematen du, eta Cyberzaintzako gainerako zerbitzuak hartzeko laguntza.



Publiko hartzailea

- ✓ Euskal sektore publikoa
- ✓ Enpresa estrategikoak
- ✓ Autobabeserako betebeharrak duten enpresak
- ✓ Beste enpresak
- ✗ Herritarrak



Ezaugarriak

- Segurtasun-neurriak aplikatzeko jardunbide egokien esparruak prestatzea eta argitaratzea.
- Cyberzaintzako arriskuak kudeatzeko frameworka aplikatzeko gidak eta eskuliburuak egitea eta argitaratzea.
- Segurtasun-neurri espezifikoak aplikatzeko gidak eta eskuliburuak egitea eta argitaratzea.
- Erakundearen segurtasun-neurriak ezartzeko eta artikulatzeko laguntza-materialak prestatzea eta argitaratzea.
- Erakundeei laguntzea argitaratutako markoak, gidak, eskuliburuak eta laguntza-materialak interpretatzen.
- Enpresei laguntzea Cyberzaintzaren zerbitzuak behar bezala erabiltzen eta aplikatzen



Zerbitzua eskatzeko prozedura

Zerbitzu horren bidez sortzen diren eduki guztiak (markoak, gidak, eskuliburuak eta askotariko laguntza-materiala) publikoaren eskura jartzen dira, Agentziaren webgunearen eta sare sozialen bidez.

Zerbitzuaren gainerako elementuei atxiki edo horietan parte hartu ahal izateko, ezinbestekoa izango da haiek izendatutako harremanetarako puntuaren bitartez eskatu eta kudeatzea, bai eta eskatzaileak solaskide bat zehaztea ere, zerbitzua benetan emateko aukera berma dezan.



Zerbitzuak CyberOrratzi egiten dion ekarpena

Ezarpen-maila guztietarako gomendatzen da.



Helburua

Erakundeari aukera ematen dio arriskuaren kudeaketan segurtasunez aurrera egiteko, erreferentzia argi, homogeneo eta kontrastatuak edukiz, inprobisazioa murrizteko, segurtasun neurrien ezarpena bizkortzeko eta zibersegurtasun arloko jarduerak guztien koherentzia eta eraginkortasuna hobetzeko.



Zerbitzuaren aukerak

Materialak prestatzea.

Material espezifikoak garatzea, erakundeek planteatutako behar espezifikoek eskatuta.

Asistentzia.

Garatutako materialak interpretatzen eta/edo Cyberzaintzaren zerbitzuak integratzen laguntzeko eskaerei erantzutea

Lantzen duen ereduaren alderdia:

Kontrola	G1.2	Informazioaren Segurtasun Politika
Kontrola	G6.1	Jardunbide egokien aplikazioa

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.



5. 4. 4. Proiektu berezien kudeaketa

Zerbitzu-lerroa
Arriskuaren gobernua

Harremanetarako guneak
observatorio@cyberzaintza.eus

Proiektu bereziak kudeatzeko **zerbitzuak zibersegurtasunarekin lotutako ekimen espezifikoak kudeatzeko laguntza** eskaintzen die zerbitzua zuzentzen zaien hartzaileei. Halaber, proiektu horiei lotutako arriskuak kudeatzeko laguntza ematen du, eta zibersegurtasun-zerbitzuak kontratatzeke laguntza teknikoa.



Publiko hartzailea

- ✓ Euskal sektore publikoa
- ✓ Enpresa estrategikoak
- ✓ Autobabeserako betebeharra duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak



Ezaugarriak

- Informazio-sistemen ereduzko proiektuetan zibersegurtasuneko eskakizunak eta eskakizunak zehaztea, baita zibersegurtasuneko ereduzko proiektuetan eskakizun eta eskakizun funtzionalak ere.
- Aholkularitza tekniko espezializatua zibersegurtasuneko zerbitzuak eta/edo proiektuak kontratatzeke prozesuetan, beharrak eta eskakizunak definitzen laguntzetik proposamenak ebaluatzen laguntzeraino.
- Garatutako proiektuei aplika dakizkiekeen zibersegurtasuneko eskakizunak eta eskakizunak egiaztatzeke eta baliozkotzeke prozesuetan laguntzea.
- Zibersegurtasunaren arloan bereziki konplexuak diren ekimen berezien eta proiektu berezien kudeaketarako euskarria.



Helburua

Erakundeak laguntza aditua lortzen du zibersegurtasuneko **proiektu konplexuei** bermeekin ekiteko, baldintzen definizio egokia eta arriskuak kudeaketa eraginkorra ziurtatuz, eta horrek ziurgabetasunak murriztea eta segurtasun handiagoz aurrera egitea ahalbidetzen dio.



Zerbitzuaren aukerak

Errekerimendu-fasea.

Proiektuaren eskakizunak zehazteke faserako laguntza.

Kontratazio-fasea.

Proiekturako zibersegurtasun arloko zerbitzuak eta/edo proiektuak kontratatzeke faserako laguntza.

Proiektu bereziak.

Zibersegurtasunaren arloko proiektu berezietan eta **ekimen berezietan laguntzea**.



Zerbitzua eskatzeko prozedura

Zerbitzuan parte hartzeke edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateke aukera bermatzearren.

5.5. Mehatxuen inteligentzia

5.5.1.

Alerta goiztiarra



Zerbitzu-lerroa
Mehatxuen inteligentzia

Harremanetarako guneak
csirt@cyberzaintza.eus

Alerta goiztiarreko zerbitzua **zaintza digitalean eta etengabeko monitorizazioan** oinarritzen da. **Adimen-eredu aurreratu** bat erabiliz, hainbat iturritako datuak aztertzen dira, zibersegurtasun-arrisku eta -gorabehera potentzialak identifikatzeko. Balizko mehatxu bat detektatzean, **alerta goiztiarrak ematen** dira, eta, horiekin batera, gomendio espezifikoak ere bai, kaltea saihesteko eta eraginkortasunez erantzuteko.

**Publiko hartzailea**

- ✓ Euskal sektore publikoa
- ✓ Enpresa estrategikoak
- ✓ Autobabeserako betebeharra duten enpresak
- ✓ Beste enpresak
- ✓ Herritarrak

**Helburua**

Pertsonak edo erakundeak mehatxu garrantzitsuei buruzko informazio aurreratu eta testuingurua jasotzen du, baita gomendio operatiboak ere, gertakariak prebenitzeko, arriskuarekiko esposizioa murrizteko eta zibersegurtasunaren arloan erantzuteko gaitasuna indartzeko.

**Ezaugarriak**

- Zibersegurtasun mehatxuak goiz detektatzeko garrantzitsuak diren informazio-iturriak etengabe monitorizatzea.
- Hainbat iturritatik datozen datuak aztertzea, anomaliak identifikatzera bideratutako inteligentzia-ereduen bidez.
- Zibersegurtasun mehatxu posibleak goiz detektatzea, monitorizatutako informazioarekin lotutako analisian oinarrituta.
- Alerta goiztiarrak ematea, identifikatutako mehatxuak prebenitzeko eta horiei erantzuteko berariazko gomendioekin batera.
- Azterketa-ereduak eguneratzea eta etengabe hobetzea, mehatxuen ingurunearen bilakaeraren arabera.

**Zerbitzuaren aukerak**

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.

**Zerbitzua eskatzeko prozedura**

Etengabe eguneratzen da zibermehatxurik berrienei buruzko dokumentazioa, eta publikoaren eskura jartzen dira Agentziaren webgunearen eta sare sozialen bidez.

Zerbitzuaren gainerako aukeretan atxikitzeko edo parte hartzeko, ezinbestekoa izango da izendatutako harreman-puntuaren bidez eskatzea eta kudeatzea, bai eta zerbitzua benetan emateko aukera bermatuko duen solaskide bat zehaztea ere.

**Zerbitzuak CyberOrratzi egiten dion ekarpena**

Ezarpn-maila guztietarako gomendatzen da.



Lantzen duen ereduaren alderdia:

Kontrola**D2.5****Alerta goiztiarra**

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.



5.5.2.

Ziber mehatxuei buruzko informazioa trukatzeari

Zerbitzu-lerroa
Mehatxuen inteligentzia

Harremanetarako guneak
csirt@cyberzaintza.eus

Zibermehatxuei buruzko informazioa trukatzeko zerbitzuak erakundeen eta erakundeen arteko lankidetzari errazten du, zibermehatxuei buruzko datuak arin eta eraginkortasunez partekatzeko. **Plataforma espezializatuak** erabiliz, erasotzaileak erabiltzen dituzten **konpromiso-adierazleak, taktikak, teknikak eta prozedurak** buruzko informazioa bildu eta banatzen da. Informazio-truke horri esker, erakundeek hobetu egin dezakete hautemateko eta erantzuteko gaitasuna.

**Publiko hartzailea**

- ✓ Euskal sektore publikoa
- ✓ Enpresa estrategikoak
- ✗ Autobabeserako betebeharrak duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak

**Helburua**

Erakundeak zibermehatxuei buruzko adimena eskuratzen du, eta, horri esker, zibersegurtasun arloko gertakarien detekzioa eta erantzuna berehala hobetu, benetako eraso ereduak aurreikusi eta babesa indartu dezake, beste erakunde batzuekin lankidetzari aktiboa eginez.

**Ezaugarriak**

- Hainbat erakunde eta lankidetzari iturrik zibermehatxuei buruz emandako informazioa biltzea.
- Zibermehatxuei buruzko informazioa modu arin eta egituratuak trukatzeari parte hartzen duten erakundeen artean.
- Eragile maltzurak erabiltzen dituzten konpromiso-adierazleak, taktikak, teknikak eta prozedurak partekatzeari.
- Trukatutako informazioa banatzea, erakundearen detekzio- eta erantzun-gaitasuna hobetzen laguntzeko.
- Plataforma espezializatuak erabiltzea, informazio-truke segurua eta eraginkorra bermatzeko.

**Zerbitzuaren aukerak****Informazio estandarri trukatzeari.**

Mehatxuei buruzko informazioa trukatzeko zerbitzuan parte hartzea, komunitateak partekatutako informaziorako sarbidearekin eta kontsultarako aukerarekin.

Informazio aurreratuaren trukea.

Mehatxuei buruzko informazioa trukatzeko zerbitzuan aktiboki parte hartzea, informazio propioa ematea eta lehenetsitako eta testuinguruan kokatutako informazioa jasotzea barne.

**Zerbitzua eskatzeko prozedura**

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzeari zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearren.

**Zerbitzuak CyberOrratzi egiten dion ekarpena**

Zerbitzuaren aplikazio egokia ziurtatzeari helburu duen ereduaren alderdirako gomendatutako **ezarpen-maila**:

1

2

3

4

5

Lantzen duen ereduaren alderdia:

Kontrola**D5.1****Threat Intelligence**

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.

5.6. Euskadiko segurtasun eredua

5. 6. 1.

Euskadiko segurtasun ereduaren hedapenean laguntzea eta jarraipena egitea



Zerbitzu-lerroa
Euskadiko segurtasun eredua

Harremanetarako guneak
zerbitzuak@cyberzaintza.eus

CyberOrratz hedatzeko laguntza-zerbitzuak, Euskadiko zibersegurtasun ereduak, **laguntza espezializatua** eskaintzen die erakunde erabiltzaileei, **eredua pixkanaka ezartzen laguntzeko**.

CyberOrratz zibersegurtasunaren arloko **erreferentziatzko esparru komuna** da, Cyberzaintzak egin eta sustatzen duena, eta **printzipio, kontrol eta irizpide tekniko**en multzo egituratu gisa ulertzen da, segurtasun-politikak, arau teknikoak eta babes-neurriak integratzen dituen, indarrean dagoen araudiarekin eta Euskadiko administrazio publikoaren behar espezifikoekin lerrokatuta.

Zerbitzu horren bidez, Agentziak eredua hedatzea, ezagutzea eta onartzea bultzatzen du, eta, horretarako, **laguntza, laguntza teknikoak, prestakuntza-ekintzak, gida praktikoak eta laguntza-tresnak** ematen ditu, euskal sektore publikoan zibersegurtasunaren ezarpen koherentea, homogeneoa eta lerrokatua errazteko, betiere administrazio bakoitzaren eskumenak errespetatuz.



Publiko hartzailea

- ✓ Euskal sektore publikoa
- ✓ Enpresa estrategikoak
- ✓ Autobabeserako betebeharra duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak



Helburua

Erakundeak bere segmentuaren barruan duen **segurtasun mailaren ikusgarritasun objektiboa** irabazten du, eta bide orri argi bat du pixkanaka hobetzeko. Horri esker, **ebidentzietan oinarritutako erabakiak** har ditzake, eta zibersegurtasuneko jarduerak eta inbertsioak eraginkortasunez lehenetsi.



Ezaugarriak

- Zibersegurtasuneko printzipio, kontrol eta irizpide teknikoetan oinarritutako erreferentziatzko esparru komun bat hornitzea, indarrean dagoen zibersegurtasun araudiarekin eta euskal sektore publikoaren behar eta berezitasunekin bat datorrena.
- Euskadiko zibersegurtasun eredua pixkanaka ezartzeko laguntza espezializatua ematea.
- Erakunde erabiltzaileei zuzendutako laguntza, laguntza tekniko eta prestakuntzako ekintzak bultzatzea.
- Ereduzko materialak, gidak eta erreferentziatzko dokumentazioa egitea eta eskuragarri jartzea, eredua modu homogeneoan ezartzea errazteko.
- Ereduen ezarpen-mailaren etengabeko ebaluazioa eta jarraipena, hobekuntza-arloak identifikatuta.
- Zibersegurtasun koherente, homogeneo eta lerrokatua sustatzea administrazio publikoaren artean.



Zerbitzuaren aukerak

Oinarritzko laguntza.

Euskadiko segurtasun eredua ezartzen laguntzea, **ereduzko materialak emanez eta eredu hori ezartzeari buruzko orientazio orokorra emanez**.

Laguntza aurreratua.

Euskadiko segurtasun eredua ezartzeko laguntza, **etengabeko laguntza, ezarpen mailaren jarraipena eta hobetzeko gomendioak barne**.

Laguntza integrala.

Euskadiko segurtasun eredua ezartzeko laguntza osoa, **etengabeko laguntza, jarraipena, aldizkako ebaluazioa eta ereduaren etengabeko hobekuntzan laguntzea barne**.



Zerbitzua eskatzeko prozedura

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearren.

5.7. Segurtasun-eragiketak (SOC)

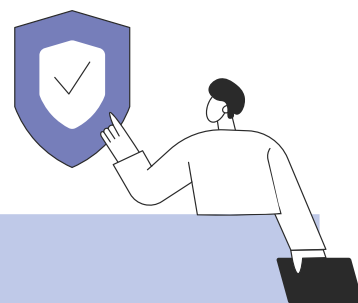
5.7.1.
SOC

Zerbitzu-lerroa

Segurtasun-eragiketak (SOC)

Harremanetarako guneak

csirt@cyberzaintza.eus



Segurtasun Eragiketen Zentroaren zerbitzuak (SOC) erakundeen barruan gertatzen diren barne-gertaerak monitorizatzen ditu, jarduera susmagarriak denbora errealean **detektatzeko eta aztertzeko**. Zerbitzu horri esker, erakundeek modu arin eta eraginkorrean erantzun dezakete zibersegurtasun-gorabeheren aurrean.



Publiko hartzailea

- ✓ Euskal sektore publikoa
- ✗ Enpresa estrategikoak
- ✗ Autobabeserako betebeharrak duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak



Ezaugarriak

- Erakundearen sistemetan sortutako segurtasun ekitaldien etengabeko monitorizazioa.
- Zibersegurtasun arloko jardura susmagarriak eta balizko gertakariak detektatzea eta denbora errealean aztertzea.
- Segurtasun-ekitaldien korrelazioa eta analisia, portaera anomaloak identifikatzeko.
- Hautemandako segurtasun-gertakariak kritikotasunaren arabera sailkatzea eta lehenestea.
- Erakundeei alertak eta informazio garrantzitsua jakinaraztea, gertakarien aurrean erantzun arina eta eraginkorra emateko.



Helburua

Erakundeari bere ingurune digitalaren etengabeko zaintza eta denbora errealeko analisia lortzeko aukera ematen dio, eta horrek aukera ematen dio jardura susmagarriak goiz detektatzeko, gorabeheren aurrean erantzuteko denbora murrizteko eta zibersegurtasun-mehatzuen aurrean erreakzionatzeko eta erresilientzia operatiboa izateko gaitasuna nabarmen hobetzeko.



Zerbitzuaren aukerak

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.



Zerbitzua eskatzeko prozedura

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearren.



Zerbitzuak CyberOrratzi egiten dion ekarpena

Zerbitzuaren aplikazio egokia ziurtatzea helburu duen ereduaren alderdirako gomendatutako **ezarpen-maila**:



Lantzen duen ereduaren alderdia:

Kontrola

D3.4

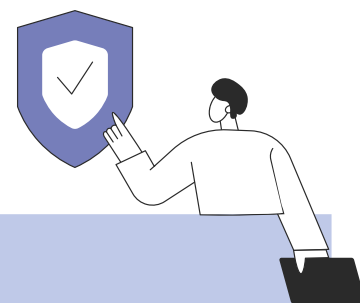
SOC perimetral

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.

5.7.2. Threat hunting

Zerbitzu-lerroa
Segurtasun-eragiketak (SOC)

Harremanetarako guneak
csirt@cyberzaintza.eus



Threat hunting zerbitzua ingurune korporatiboetan **mehatxuak modu proaktiboan identifikatzean** oinarritzen da. Haren helburua **mehatxu ezezagunak detektatzea eta arintzea** da, gauzatu aurretik haien eragina prebenituz.



Publiko hartzailea

- ✓ Euskal sektore publikoa
- ✗ Enpresa estrategikoak
- ✗ Autobabeserako betebeharrak duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak



Helburua

Erakundeari aukera ematen dio babes-maila handitzeko, **mehatxu aurreratuak eta ikusezinak proaktiboki identifikatuz**, gertakari kritikoen arriskua murriztuz eta defentsarako gaitasuna indartuz, analisi espezializatuei eta adituen gomendioei esker.



Ezaugarriak

- Zibersegurtasun-mehatxuen bilaketa proaktiboa erakundearen inguruneetan, aurrez definitutako alerten mende soilik egon gabe.
- Segurtasun-datuen eta -gertaeren analisi aurreratuak, portaera anomaloak eta mehatxu ezezagunak identifikatzeko.
- Bilaketa-hipotesiak garatzea, aktore maltzurrek erabiltzen dituzten teknika, taktika eta prozeduretan oinarrituta.
- Hunting-prozesuetan detektatutako balizko mehatxuak identifikatzea eta baliozkotzea.
- Lortutako aurkikuntzen berri ematea, identifikatutako mehatxuak arintzeko eta prebenitzeko gomendioak barne.



Zerbitzuaren aukerak

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.



Zerbitzua eskatzeko prozedura

Zerbitzuan parte hartzeko edo esleitzeko, **nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearren.**



Zerbitzuak CyberOrratzi egiten dion ekarpena

Zerbitzuaren aplikazio egokia ziurtatzea helburu duen ereduaren alderdirako gomendatutako **ezarpen-maila**:

1

2

3

4

5



Lantzen duen ereduaren alderdia:

Kontrola

D5.3

Threat hunting

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.

5.8. Gertakariei erantzutea (CSIRT)

5.8.1.
Aholkularitza

Zerbitzu-lerroa
Gertakariei erantzutea (CSIRT)

Harremanetarako guneak
incidencias@cyberzaintza.eus

Aholkularitza-zerbitzuak gomendio orokorrak ematen ditu segurtasun informatikoko gorabeheraren bat izanez gero nola jokatu jakiteko. Halaber, beharrezkoa denean, Cyberzaintzaren gertakariei erantzuteko talde tekniko espezializatuak beharrezko ekintzak inplementatzen ditu gertakariaren hedapena saihesteko eta komunitateari mehatxuaren berri emateko.



Publiko hartzailea

- ✓ Euskal sektore publikoa
- ✓ Enpresa estrategikoak
- ✓ Autobabeserako betebeharra duten enpresak
- ✓ Beste enpresak
- ✓ Herritarrak



Helburua

Pertsonak edo erakundeak zibersegurtasun-gertakariaren hasierako kudeaketarako orientabidea jasotzen du, haren inpaktua murrizteko eta haren hedapena saihesteko aukera ematen duten euste-, erantzun- eta prebentzio-gomendio argiekin.



Ezaugarriak

- Erakundeei aholkularitza ematea segurtasun informatikoko gertakariaren aurrean jarduteko metodologietan, eusteko eta erantzuteko gomendio orokorrak emanez.
- Jakinarazitako gertakariaren hasierako azterketa, egin beharreko ekintzak behar bezala bideratzeko.
- Laguntza tekniko espezializatua, gertakaria ez hedatzeko eta haren inpaktua murrizteko, gertakariaren izaerak hala eskatzen duenean.
- Kudeatutako gertakariaren ondoriozko segurtasun-gomendioak ematea, etorkizunean antzeko egoerak prebenitzeko.
- Komunitateari mehatxu garrantzitsuen berri ematea, gertakariak eragin handiagoa izan dezakeenean.



Zerbitzuaren aukerak

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.



Zerbitzua eskatzeko prozedura

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearren.



Zerbitzuak CyberOrratzi egiten dion ekarpina

Ezarpn-maila guztietarako gomendatzen da.



Lantzen duen ereduaren alderdia:

Kontrola

R2.4

CSIRT

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.

5. 8. 2. Koordinazioa



Zerbitzu-lerroa
Gertakariei erantzutea (CSIRT)

Harremanetarako guneak
incidencias@cyberzaintza.eus

Zibersegurtasun-gorabeherak koordinatzeko zerbitzua **aktibatu** egiten da gorabehera horiek Cyberzaintzaren helburu diren publikoetan **eragin ugari eta esanguratsua** dutenean. **Aholkularitza tekniko espezializatua ematea eta prebentzio-neurriak hartzea** du helburu, gorabeherak beste erakunde batzuei eragin ez diezaien. Zerbitzu horrek erantzun azkarra eta koordinatua bermatzen du, **gorabeheraren irismena eta ondorioak minimizatuz** eta alde guztiak informatuta eta beren ekintzetan lerrokatuta daudela bermatuz.



Publiko hartzailea

- ✓ Euskal sektore publikoa
- ✓ Enpresa estrategikoak
- ✗ Autobabeserako betebeharra duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak



Helburua

Inpaktu handiko gertakarien aurrean erantzun koordinatua eta aditua ematen dio erakundeari, eta aukera ematen dio azkar jarduteko, gertakariaren hedapena geldiarazteko, haren ondorioak murrizteko eta ekosistema osoa babesteko, inplikaturako eragileen arteko komunikazio argi baten eta lerrokatze eraginkor baten bidez.



Ezaugarriak

- Zibersegurtasun arloko gertakarien aurrean zerbitzua aktibatzea, Cyberzaintzaren helburu diren publikoetan eragin anizkuna eta esanguratsua izanik.
- Inplikaturako erakundeen eta eragileen arteko erantzunaren koordinazioa, jarduketara azkarra eta eraginkorra bermatzeko.
- Aholkularitza tekniko espezializatua, gertakaria kudeatzen den bitartean erabakiak hartzen laguntzeko.
- Gertakaria beste erakunde batzuetara ez hedatzeko prebentzio-neurriak definitzea eta sustatzea.
- Inplikaturako aldean arteko komunikazio egituratua eta jarraitua, informazio garrantzitsua behar bezala partekatuko dela bermatuz.
- Gertakariaren bilakaeraren jarraipena, egonkortzen den arte, koordinazio eta gainbegiratze ikuspegitik.



Zerbitzuaren aukerak

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.



Zerbitzua eskatzeko prozedura

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearren.



Zerbitzuak CyberOrratzi egiten dion ekarpena

Zerbitzuaren aplikazio egokia ziurtatzea helburu duen ereduaren alderdirako gomendatutako **ezarpen-maila**:

1

2

3

4

5



Lantzen duen ereduaren alderdia:

Kontrola

R4.2

Zibergertakarien
kudeaketa integratua

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundeen testuinguruan behar bezala aplikatzen dela ziurtatzen du.

5.8.3.
DFIR

Zerbitzu-lerroa
Gertakariei erantzutea (CSIRT)

Harremanetarako guneak
incidencias@cyberzaintza.eus

Auzitegiko Analisi Digitalaren eta Gertakariei Erantzuteko Zerbitzuaren (DFIR) helburua da **segurtasun gertakari baten aurrean ebidentzia digitalak urrunetik eskuratzea** eta aztertzea, gertakaria konpontzen laguntzeko.

**Publiko hartzailea**

- ✓ Euskal sektore publikoa
- ✗ Enpresa estrategikoak
- ✗ Autobabeserako betebeharrak duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak

**Ezaugarriak**

- Segurtasun informatikoko gertakariekin lotutako ebidentzia digitalak eskuratzea.
- Eskuratutako ebidentzia digitalen auzitegi-azterketa, gertakariaren jatorria, irismena eta kausak identifikatzeko.
- Erakundeei laguntza tekniko espezializatua ematea gertakaria konpontzeko.
- Laguntza teknikoak errekuperazioan.
- Gertakaria konpontzen eta neurri zuzentzaileak hartzen lagunduko duten ondorio teknikoak lantzea.

**Helburua**

Horri esker, erakundeak laguntza espezializatua izango du segurtasun-gertakari bat sakon aztertzeko, haren jatorria, irismena eta kausak identifikatzeko, eta gertakari hori bermeekin konpontzeko, eta etorkizuneko babesa indartuko duten neurri zuzentzaileak lehengoratzeko eta ezartzea eraztuko du.

**Zerbitzuaren aukerak**

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.

**Zerbitzua eskatzeko prozedura**

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearren.

**Zerbitzuak CyberOrratzi egiten dion ekarpena**

Zerbitzuaren aplikazio egokia ziurtatzea helburu duen ereduaren alderdirako gomendatutako **ezarpen-maila**:



Lantzen duen ereduaren alderdia:

Kontrola**R3.3****DFIR**

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.

5. 8. 4. Krisien kudeaketa



Zerbitzu-lerroa
Gertakariei erantzutea (CSIRT)

Harremanetarako guneak
incidencias@cyberzaintza.eus

Krisiak kudeatzeko zerbitzua arduratzen da Euskadiko sektore publiko osorako plan integral bat koordinatzeaz, eta segurtatzen du erakunde guztiak prest daudela segurtasun-gorabehera kritiko batetik eratorritako krisi bat eraginkortasunez kudeatzeko.

Halaber, krisiaren kudeaketan estrategikoak diren erakundeei **etengabeko laguntza** eskaintzen die, eta krisi hori eragin duen gertakariaren ondorioei aurre egiteko eta ondorio horiek arintzeko beharrezko laguntza dutela ziurtatzen du.



Publiko hartzailea

- ☒ Euskal sektore publikoa
- ☒ Enpresa estrategikoak
- ☒ Autobabeserako betebeharra duten enpresak
- ☒ Beste enpresak
- ☒ Herritarrak



Helburua

Erakundeari zibersegurtasuneko krisi bat eraginkortasunez kudeatzeko koordinazioa eta laguntza estrategikoa ematen dio, krisi horren eragina minimizatuz eta sektore publiko osoan erantzun lerrokatua ziurtatuz.



Ezaugarriak

- Zibersegurtasunaren arloko krisiak kudeatzeko plan integral bat definitzea eta koordinatzea Euskadiko sektore publiko osorako.
- Erakunde publikoei laguntza ematea, segurtasun-gertakari kritikoaren ondoriozko krisien aurrean prestatzeko.
- Krisiaren kudeaketan inplikaturako eragileen koordinazio estrategikoa, jarduketa lerrokatua eta koherentea ziurtatuz.
- Krisiaren kudeaketan erakunde estrategikoei laguntza jarraitua ematea, erabakiak hartzea eta gertakariaren ondorioak arintzea erraztuz.
- Krisiaren bilakaeraren jarraipena, ikuspegi estrategikotik, egonkortzeraino.



Zerbitzuaren aukerak

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.



Zerbitzua eskatzeko prozedura

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendaturako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearen.



Zerbitzuak CyberOrratzi egiten dion ekarpena

Zerbitzuaren aplikazio egokia ziurtatzea helburu duen ereduaren alderdirako gomendaturako **ezarpen-maila**:

1

2

3

4

5



Lantzen duen ereduaren alderdia:

Kontrola

C4.1

Krisiaren jarraipen-
eta kudeaketa-plana

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.

5.8.5. Takedown



Zerbitzu-lerroa
Gertakariei erantzutea (CSIRT)

Harremanetarako guneak
csirt@cyberzaintza.eus

Takedown zerbitzua Interneteko **eduki maltzurra** edo **baimenik gabekoa** kentzeko egiten diren ekintzei dagokie.



Publiko hartzailea

- ✓ Euskal sektore publikoa
- ✓ Enpresa estrategikoak
- ✓ Autobabeserako betebeharra duten enpresak
- ✓ Beste enpresak
- ✓ Herritarrak



Helburua

Pertsonari edo erakundeari aukera ematen dio **Internetetik eduki maltzurak ezabatzeko** eskatzeko, haien eragina murriztuz eta erakundearen eta herritarren babesa indartuz.



Ezaugarriak

- Erakundeentzat edo herritarrentzat arriskutsuak izan daitezkeen eduki maltzurak edo baimendu gabekak identifikatzea.
- Atzemandako edukiaren aurretiazko azterketa, erretiratze-ekintzen bideragarritasuna zehazteko.
- Eduki maltzurak edo baimenik gabekoak kentzeko eskaerak kudeatzea zerbitzuen hornitzaileen, plataformen edo erakunde arduradunen aurrean.
- Erretiratze-ekintzen jarraipena, ebatzi edo itxi arte.
- Takedownen ekintzen egoerari eta emaitzei buruzko komunikazioa alderdi interesdunei.



Zerbitzuaren aukerak

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.



Zerbitzua eskatzeko prozedura

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearren.



Zerbitzuak CyberOrratzi egiten dion ekarpena

Ezarpn-maila guztietarako gomendatzen da.



Lantzen duen ereduaren alderdia:

Kontrola

R2.4

CSIRT

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.

5. 8. 6. Zibersegurtasun arloko gertakariei erantzuteko prestakuntza



Zerbitzu-lerroa
Gertakariei erantzutea (CSIRT)

Harremanetarako guneak
csirt@cyberzaintza.eus

Zibersegurtasun-gorabeherei erantzuteko prestakuntza-zerbitzua prebentzio-fasean oinarritzen da, eta helburua du **erakundeei laguntzea segurtasun-gorabeherei eraginkortasunez eta modu koordinatuan erantzuteko behar diren prozesuak, prozedurak eta gaitasunak zehazten**. Halaber, erakundearen heldutasun-maila ebaluatzen da, hobetu beharreko arloak identifikatzeko eta horiei erantzuteko gaitasuna indartzeko.



Publiko hartzailea

- ✓ Euskal sektore publikoa
- ✗ Enpresa estrategikoak
- ✗ Autobabeserako betebeharra duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak



Helburua

Aukera ematen dio erakundeari zibersegurtasun-gorabeherei aurre egiteko prestakuntza indartzeko, eta argi eta garbi zehaztutako prozesuak, prozedurak eta rolak ditu, eraginkortasunez eta modu koordinatuan erantzuteko.



Ezaugarriak

- Erakundeak zibersegurtasun gertakariei erantzuteko duen heldutasun maila ebaluatzea, gaitasun arrakalak eta hobetzeko arloak identifikatuz.
- Gertakariei erantzuteko planak diseinatzea eta garatzea, rolak, erantzukizunak, jarduteko prozedurak eta koordinazio-mekanismoak definituta.
- Zibersegurtasuneko gertakarien aurrean erantzun arin eta sendoa emateko prozedura operatiboak eta jarduteko gidak definitzea.
- Planak eta prozedurak aplikatu beharreko araudi- eta arau-esparruekin lerrotzea, bai eta zibersegurtasunaren arloko jardunbide onekin ere.



Zerbitzuaren aukerak

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.



Zerbitzua eskatzeko prozedura

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearren.



Zerbitzuak CyberOrratzi egiten dion ekarpena

Ezarpen-maila guztietarako gomendatzen da.



Lantzen duen ereduaren alderdia:

Kontrola

G2.3

Gertakarien kudeatzailea

Kontrola

R2.1

Zibergertakariei erantzuteko prozedura

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.

5.9. Erasoko segurtasuna

5.9.1.
Auditoria tekniko

Zerbitzu-lerroa
Erasoko segurtasuna

Harremanetarako guneak
csirt@cyberzaintza.eus

Ikuskaritza teknikoko zerbitzuak **hainbat proba-mota** hartzen ditu, hala nola sartze-probak (pentesting), aplikazioen ikuskapenak, Wi-Fi sareak eta konfigurazioak, besteak beste. **Helburua da babes-maila ebaluatzea eta hobetu daitezkeen alderdiak identifikatzea.**

**Publiko hartzailea**

- ✓ Euskal sektore publikoa
- ✗ Enpresa estrategikoak
- ✗ Autobabeserako betebeharra duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak

**Ezaugarriak**

- Sistemen, aplikazioen eta komunikazioen segurtasun-mailaren ebaluazio teknikoak, proba kontrolatuak eginez.
- Ahultasun teknikoak, konfigurazio ahuleziak eta eraso sektore posibleak identifikatzea.
- Hainbat aktiboren gaineko segurtasun-probak gauzatzea, hala nola aplikazioen, hari gabeko sareen eta sistemen konfigurazioen gainekoak.
- Erakundearen testuinguruan identifikatutako ahultasunek izan dezaketen eragina aztertzea.
- Auditoritzaren emaitzekin txosten teknikoak egitea, babes-maila hobetzera bideratutako gomendioak barne.

**Helburua**

Erakundeak bere **segurtasun-mailaren ebaluazio tekniko objektiboa** lortzen du, eta ahuleziak eta konfigurazio-ahuleziak identifikatzen ditu proba kontrolatuen bidez. Horri esker, gerta daitezkeen erasoei aurrea hartzen die eta aktibo digitalen babesa indartzen du.

**Zerbitzuaren aukerak**

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.

**Zerbitzua eskatzeko prozedura**

Zerbitzuan parte hartzeko edo esleitzeko, **nahitaezkoa** izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearen.

**Zerbitzuak CyberOrratzi egiten dion ekarpena**

Zerbitzuaren aplikazio egokia ziurtatzea helburu duen ereduaren alderdirako gomendatutako **ezarpen-maila**:

1

2

3

4

5



Lantzen duen ereduaren alderdia:

Kontrola

D3.3

Kanpoko pentesting-a

Kontrola

D4.3

Barneko pentesting-a

Kontrola

D5.2

Iturburu-kodearen auditoriazak

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.

5.9.2.
EASM

Zerbitzu-lerroa
Erasoko segurtasuna

Harremanetarako guneak
csirt@cyberzaintza.eus

Eraso eta Arintze Azaleraren Ebaluazio Zerbitzua (EASM) **erakundeen esposizio-azalera aztertzean datza, haien arrisku teknologikoaren maila zehazteko** helburuarekin. Ebaluazio horretatik abiatuta, **gomendio espezifikoak proposatzen dira**, identifikatutako arriskuak arintzeko. Gainera, zerbitzua ez da soilik berehalako babesean bideratzen, **epe luzerako erresilientzia handitzea ere bilatzen du.**

**Publiko hartzailea**

- ✓ Euskal sektore publikoa
- ✗ Enpresa estrategikoak
- ✗ Autobabeserako betebeharrak duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak

**Helburua**

Interneten duen esposizioaren ikuspegi argia lortzeko aukera ematen dio erakundeari, kanpotik ikus daitezkeen arriskuak identifikatuz eta lehenetsiz, **eraso-azalera murrizteko eta epe luzerako erresilientzia teknologikoa indartzeko.**

**Ezaugarriak**

- Erakundearen eraso-eremua osatzen duten Interneteko aktiboak identifikatzea eta aztertzea.
- Identifikatutako esposizio-azalerei lotutako arrisku teknologikoaren ebaluazioa.
- Konfigurazio ez-seguruak, zerbitzu arriskutsuak eta kanpotik ikus daitezkeen ahuleziak detektatzea.
- Identifikatutako arriskuei lehentasuna ematea, duten larritasunaren eta izan dezaketen eraginaren arabera.
- Hautemandako arriskuak arintzera bideratutako gomendio espezifikoak egitea.
- Erakundearen epe luzeko erresilientzia hobetzen laguntzea, haren eraso-azalera murriztuz.

**Zerbitzuaren aukerak**

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.

**Zerbitzua eskatzeko prozedura**

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearren.

**Zerbitzuak CyberOrratzi egiten dion ekarpena**

Zerbitzuaren aplikazio egokia ziurtatzea helburu duen ereduaren alderdirako gomendatutako **ezarpen-maila**:

1

2

3

4

5



Lantzen duen ereduaren alderdia:

Kontrola

D3.3

Pentesting

Kontrola

I3.3

Ahultasunak identifikatzea

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.

5.9.3. Red team



Zerbitzu-lerroa
Erasoko segurtasuna

Harremanetarako guneak
csirt@cyberzaintza.eus

Red team zerbitzuaren helburua da erakunde baten **aurkako benetako eraso**en simulazioak egitea. Zerbitzu horrek sistemen eta defentsen ahultasunak identifikatzea eta zuzentzea errazten du, baita **babes-ekipoen eraginkortasuna ebaluatzea** ere.



Publiko hartzailea

- ✓ Euskal sektore publikoa
- ✗ Enpresa estrategikoak
- ✗ Autobabeserako betebeharrak duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak



Ezaugarriak

- Erakundearen aurkako eraso errealeko simulazioa, kontrolatutako eszenatokitik aktore maltzurren portaera erreplikatzeko.
- Eraso aurreratuei aurre egiteko antolakundearen defentsa tekniko, antolakuntzazko eta prozedurazkoen eraginkortasunaren ebaluazioa.
- Detekzio- eta erantzun-sistemen, -prozesuen eta -gaitasunen ahuleziak identifikatzea.
- Babes-ekipamenduen prestakuntza- eta erreakzio-mailaren azterketa simulatutako egoeren aurrean.
- Simulazioen emaitzekin txostenak egitea, defentsa-gaitasunak hobetzeko gomendioak barne.



Helburua

Benetako eraso baten aurrean nola eutsiko liokeen egiaztatzeko aukera ematen dio erakundeari, bere defentsen eta ekipoen eraginkortasunaren ikuspegi argia lortuz, eta, horri esker, arrisku kritikoak murriztu, erabakiak hobeto hartu eta gertakari bat gertatu baino lehen erantzuteko gaitasuna sendotuz.



Zerbitzuaren aukerak

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.



Zerbitzua eskatzeko prozedura

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearren.



Zerbitzuak CyberOrratzi egiten dion ekarpena

Zerbitzuaren aplikazio egokia ziurtatzea helburu duen ereduaren alderdirako gomendatutako **ezarpen-maila**:

1

2

3

4

5



Lantzen duen ereduaren alderdia:

Kontrola

D6.1

Red Team

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.

5.10. Ezagutzaren transferentzia

5.10.1.
Prestakuntza

Zerbitzu-lerroa

Ezagutzaren transferentzia

Harremanetarako guneak

csirt@cyberzaintza.eus

Prestakuntza zerbitzua agentziaren helburu diren publikoak **zibersegurtasunean espezializatzen** laguntzeko diseinatuta dago. **Gaikuntzak ezarritako kanalak erabiliz edo metodo alternatiboen bidez** egin daitezke, ohiko baliabideekin landu ezin diren gai espezifikoak heltzen zaienean.

**Publiko hartzailea**

- ✓ Euskal sektore publikoa
- ✓ Enpresa estrategikoak
- ✗ Autobabeserako betebeharrak duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak

**Helburua**

Entitateari aukera ematen dio bere langileei zibersegurtasunaren arloko irizpidea eta ikuspegia emateko, funtsezko taldeek beren erantzukizunarekin bat datozen **ezagutzak** dituztela ziurtatuz, eta horrek antolaketa arriskua murrizten du eta erakundearen babes globala indartzen du.

**Ezaugarriak**

- Zibersegurtasunean espezializatutako trebakuntza-saioak, xede-publikoaren ezagutza-mailara, rolerak eta behar espezifikoetara egokitutako edukiak dituztenak.
- Parte-hartzaileei prestakuntza egiteko behar diren materialak eta prestakuntzako edukiak eskaintzea.
- Prestakuntza-edukiak etengabe eguneratzea, eta praktika onenekin, mehatxuen bilakaerarekin, indarrean dagoen araudiarekin eta zibersegurtasunaren arloko erreferentziatzko estandarrekin bat datozela bermatzea.

**Zerbitzuaren aukerak**

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.

**Zerbitzua eskatzeko prozedura**

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearren.

**Zerbitzuak CyberOrratzi egiten dion ekarpena**

Ezarpen-maila guztietarako gomendatzen da.

1

2

3

4

5



Lantzen duen ereduaren alderdia:

Kontrola**G1.6****Kontzientziazioa eta oinarritzko prestakuntza**

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.

5.10.2. Entrenamendua



Zerbitzu-lerroa
Ezagutzaren transferentzia

Harremanetarako guneak
csirt@cyberzaintza.eus

Entrenamendu zerbitzuak hondamendiren bat gertatzen denean **simulazioak eta errekupeazio probak** egiteko eta **koordinatzeko teknikak** ditu ardatz. Horrek barne hartzen ditu ziberariketa indibidualak zein kolektiboak, erakundeak krisiak eraginkortasunez kudeatzeko prestatzen dituztenak.



Publiko hartzailea

- ✓ Euskal sektore publikoa
- ✓ Enpresa estrategikoak
- ✗ Autobabeserako betebeharra duten enpresak
- ✗ Beste enpresak
- ✗ Herritarrak



Helburua

Entitateari aukera ematen dio krisiak kudeatzeko benetako gaitasuna probatzeko eta indartzeko, bere taldeek egoera kritikoan aurrean modu koordinatuan eta eraginkorrean jarduten dutela ziurtatuz, funtsezko hobekuntzak identifikatuz eta benetako egoera bat gertatu aurretik jarraitutasuna eta erresilientzia operatiboa indartuz.



Ezaugarriak

- Simulazio-eraketak eta hondamendien aurreko errekupeazio-probak koordinatzea, bai banakakoak, bai taldekakoak.
- Simulazio-eraketak eta hondamendien aurreko errekupeazio-probak egitea, erakundeek krisi-egoerei erantzuteko duten gaitasuna ebaluatzeak.
- Krisi-egoerei erantzuteko prozeduretan eta gaitasunetan aplika daitezkeen hobekuntzak identifikatzeko eta kudeatzeko laguntza, egindako eraketen emaitzetatik abiatuta.



Zerbitzuaren aukerak

N/A. Zerbitzu honek ez du zerbitzu-tipologiarik.



Zerbitzua eskatzeko prozedura

Zerbitzuan parte hartzeko edo esleitzeko, nahitaezkoa izango da harremanetarako izendatutako gunearen bidez eskatu eta kudeatzea zerbitzu hori, eta eskatzaileak solaskide bat zehaztea, zerbitzua benetan emateko aukera bermatzearren.



Zerbitzuak CyberOrratzi egiten dion ekarpena

Ezarpn-maila guztietarako gomendatzen da.



Lantzen duen ereduaren alderdia:

Kontrola

R2.1

Zibergertakariei erantzuteko prozedura

Zerbitzu horrek kontrol hori ezartzeko eta indartzeko behar den euskarri metodologikoa ematen du, eta erakundearen testuinguruan behar bezala aplikatzen dela ziurtatzen du.



Sarean ere, auzolana.
Por ti hacemos red.

Informazio orokorra:

945 236 636

info@cyberzaintza.eus



www.zibersegurtasun.euskadi.eus

EUSKO JAURLARITZA



GOBIERNO VASCO