AGINDUA, SEGURTASUNEKO SAILBURUARENA, ZEINAREN BIDEZ ERABAKITZEN BAITA EUSKAL ZIBERSEGURTASUN AGENTZIAREN EGINKIZUNAK ETA ESKUMENAK GARATZEN DITUEN DEKRETU-PROIEKTUA ALDEZ AURRETIK ONARTZEA.

Segurtasuneko sailburuaren 2026ko ekainaren 9ko Aginduaren bidez, Euskal Zibersegurtasun Agentziaren eginkizunak eta eskumenak garatzen dituen dekretu-proiektua egiteko prozedura hastea erabaki zen.

Testua eta arau-inpaktuaren azterketaren memoria egin ondoren, bidezkoa da, Xedapen Orokorrak Egiteko Prozeduraren ekainaren 30eko 6/2022 Legearen 15. artikuluan ezarritakoaren arabera, aldez aurreko onarpena ematea, dagozkion entzunaldi- eta kontsulta-izapideak egin aurretik.

EBAZTEN DUT

LEHENENGOA.- Euskal Zibersegurtasun Agentziaren eginkizunak eta eskumenak garatzen dituen dekretu-proiektuaren testua aldez aurretik onartzea.

BIGARRENA.- Dekretu-proiektuaren prozedura izapidetzen jarraitzeko agintzea, hasteko aginduan eta ekainaren 30eko 6/2022 Legean ezarritako izapideekin bat etorriz.

Vitoria-Gasteiz, sinadura elektronikoaren eguna.

Bingen Zupiria Gorostidi
SEGURTASUNEKO SAILBURUA
SEGURTASUNEKO SAILBURUA

DEKRETU-PROIEKTUA, EUSKAL ZIBERSEGURTASUN AGENTZIAREN EGINKIZUNAK ETA ESKUMENAK GARATZEN DITUENA

ZIOEN AZALPENA

Sistemak eta zerbitzuak gero eta digitalizatuago daudenez, eta azpiegitura teknologikoak elkarren mende daudenez, zibersegurtasuna ezinbesteko elementu bihurtu da zerbitzu publikoen funtzionamendu egokia, funtsezko jardueren jarraitutasuna eta pertsonen, ondasunen eta interes publikoaren babesa bermatzeko. Beraz, ingurune digitalari lotutako arriskuen zeharkako izaerak jarduera publiko egituratua, koordinatua eta berariazko tresnak dituena eskatzen du, zibersegurtasun-gertakariak prebenitzeko, detektatzeko eta horiei eraginkortasunez erantzuteko.

Testuinguru horretan, 7/2023 Legeak, ekainaren 29koak, Euskal Zibersegurtasun Agentzia sortzekoak, Euskal Autonomia Erkidegoan zibersegurtasunaren arloko politikak planifikatu, koordinatu eta gauzatzeko erreferentziazko tresna publiko gisa egituratzen du Agentzia, eta eginkizun estrategiko, tekniko eta operatiboak esleitzen dizkio, informazio-sistemen eta zerbitzu publikoen eta funtsezko zerbitzuen babes-maila handia bermatzeko.

Martxoaren 19ko 34/2024 Dekretuak, Euskal Zibersegurtasun Agentziaren Estatutuak onartzen dituenak, haren antolamendua, egitura eta funtzionamendu-araubidea zehazten ditu, haren eskumenen irismena mugatuz, hargatik eragotzi gabe geroko arau-garapenaren bidez egin daitezkeen aldaketak. Era berean, urriaren 29ko 318/2024 Dekretuak Segurtasun Sailaren antolamendu-esparrua ezartzen du, Agentziaren jarduna biltzen duena.

Dekretu hau bat dator Euskal Sektore Publikoaren maiatzaren 12ko 3/2022 Legearen esparruan ezarritakoarekin, lege horren aplikazio-eremuan sartzen diren entitateak definitzen baititu, bai eta Administrazio Publikoen Administrazio Prozedura Erkidearen urriaren 1eko 39/2015 Legean ezarritakoarekin ere, zeinak administrazio-jarduna eta bitarteko elektronikoen bidezko izapidetzea arautzen baititu. Era berean, Segurtasunaren Eskema Nazionala arautzen duen maiatzaren 3ko 311/2022 Errege Dekretua aplikatu behar da, sektore publikoari aplikatu beharreko informazioaren segurtasunaren arloko gutxieneko printzipioak eta baldintzak ezartzen dituena.

Bestalde, ekainaren 24ko 153/1997 Dekretuak (LABI) araututako larrialdiei aurre egiteko eta babes zibileko euskal sistemak, eta autobabesaren arloko araudiak, bereziki azaroaren 2ko 277/2010 Dekretuak (otsailaren 12ko 21/2019 Dekretuak aldatu zuen), arrisku- eta larrialdi-egoerak kudeatzeko esparrua ezartzen dute. Eremu horretan, Lehen lehendakariorde eta Segurtasuneko sailburuaren 2024ko ekainaren 7ko Aginduak ezartzen du Autobabeserako Euskal Arauari lotutako jarduera jakin batzuetarako zibersegurtasunaren arloko jarraitutasun-planak egiteko betebeharra, jardueren jarraitutasunaren kudeaketan dimentsio digitala berariaz txertatuz.

Aurrekoari jarraiki, dekretu honen xedea da, alde batetik, Euskal Zibersegurtasun Agentziari ekainaren 29ko 7/2023 Legeak, hura sortzeari buruzkoak, esleitutako eginkizunak eta eskumenak garatzea eta zehaztea, esparru sistematiko bat emanez eremu estrategikoan, koordinazioan, ikuskaritza teknikoan, arriskuaren kudeaketan eta eragiketetan egiten dituen jarduerei; eta, bestetik, autobabeseko araudiaren esparruan eska daitezkeen zibersegurtasunaren arloko jarraitutasun-planak egiteko, bidaltzeko, gainbegiratzeko eta ikuskatzeko prozedura arautzea.

Horretarako, jarduteko oinarrizko araubide bat ezartzen du arauak, Agentziaren esku-hartzea modu koherentean antolatzeko aukera ematen duena, betiere administrazioen, organismoen eta erakundeen eskumen-eremuarekiko errespetua bermatuz, haiei baitagokie segurtasun-neurriak ezartzea eta kudeatzea dagozkien sistema eta zerbitzuetan.

Era berean, Dekretuak bere aplikazio-eremu subjektiboa mugatzen du. Horren barruan sartzen dira euskal sektore publikoa osatzen duten erakundeak, maiatzaren 12ko 3/2022 Legean aurreikusitako baldintzetan, bai eta Euskal Autonomia Erkidegoan zerbitzu publikoak edo funtsezko zerbitzuak kudeatzen dituzten erakundeak ere, eta, zibersegurtasunaren arloko jarraitutasun-planei dagokienez, autobabeseko araudiari lotutako jarduera, zentro, establezimendu eta instalazioen titularrak ere sartzen dira.

Era berean, arauak beharrezko koordinazio instituzionalerako mekanismoak artikulatzen ditu inplikatutako eragileen artean jarduera koherentea bermatzeko, larrialdiak kudeatzeko euskal sisteman integratzea barne, eta Agentziaren eginkizunak betetzeko beharrezkoa den informazioaren bilketa eta tratamendua arautzen du, konfidentzialtasunaren, datuen babesaren eta informazioaren segurtasunaren arloan behar diren bermeak gehituz.

Azken batean, Dekretu honen bidez, Euskal Zibersegurtasun Agentziaren eginkizunak eraginkortasunez garatzeko eta zibersegurtasuna planifikatzeko, arriskua kudeatzeko eta autobabeserako sistemetan integratzeko behar den esparru juridikoa ezartzen da, eta, horrela, Euskal Autonomia Erkidegoko zerbitzu publikoen eta funtsezko jardueren segurtasuna, jarraitutasuna eta erresilientzia indartzen laguntzen da.

Ondorioz, aplikatu beharreko ordenamendu juridikoan ezarritakoaren arabera, Segurtasuneko sailburuaren proposamenez, eta Jaurlaritzaren Kontseiluak [●] egindako bilkuran aztertu eta onartu ondoren, hauxe.

XEDATZEN DUT

I. TITULUA
XEDAPEN OROKORRAK

1. Artikulua. –Xedea.

Dekretu honen xedea da:

1.– Euskal Zibersegurtasun Agentziaren (aurrerantzean, Agentzia edo Cyberzaintza) eginkizunak eta eskumenak garatzea eta zehaztea, ekainaren 29ko 7/2023 Legean eta 34/2024 Dekretuak onartutako eta 15/2026 Dekretuak aldatutako estatutuetan aurreikusitakoa betez, bai eta horiek gauzatzeko oinarrizko jardun-araubidea eta funtsezko prozedurak ezartzea ere.

2.– Euskal autobabes-arauari lotutako jarduera jakin batzuetarako zibersegurtasunaren arloko jarraitutasun-planak egiteko, bidaltzeko, gainbegiratzeko eta ikuskatzeko prozedura arautzea, bitarteko elektronikoen bidez izapidetzea barne.

2. Artikulua. –Aplikazio-eremua.

1.– Dekretu honen aurreikuspenak euskal sektore publikoa osatzen duten administrazio, organismo eta entitateei aplikatuko zaizkie, Euskal Sektore Publikoari buruzko maiatzaren 12ko 3/2022 Legean aurreikusitako moduan.

2.– Halaber, dekretu honen aurreikuspenak aplikatuko zaizkie, enpresa-sareari zuzendutako alderdietan, Euskadin jarduera ekonomiko, enpresarial edo profesional bat garatzen duten enpresa, merkataritza-erakunde eta pertsona fisiko guztiei, beren kargura soldatapeko langileak dituzten edo ez kontuan hartu gabe. Jarduera horiek gauzatzean, arreta berezia eskainiko zaie Euskal Autonomia Erkidegoan funtsezko zerbitzuak kudeatzen dituzten erakundeei.

3.– Dekretu honetako aurreikuspenak herritarrei ere aplikatuko zaizkie, dekretuak berariaz aipatzen dituen alderdietan.

4.– Autobabeserako euskal arauari lotutako zenbait jardueratarako zibersegurtasunaren arloko jarraitutasun-planei buruzko eginkizunari dagokionez, xedapen hau aplikatuko zaie, soil-soilik, oinarrizko funtzio sozialak, osasuna, segurtasuna, gizartearen eta ekonomiaren ongizatea eta Euskadiko Erakundeen eta Administrazio Publikoen funtzionamendu eraginkorra mantentzeko beharrezkoak diren jarduera, zentro, establezimendu, gune, instalazio edo bulegoen titular diren pertsona fisiko edo juridikoei, betiere autobabesaren arloko betebeharrak betetzea eskatzen bazaie.

5.– Agentziak, bere eginkizunak behar bezala betetzeko, kasu bakoitzean egokien iritzitako zerbitzuak antolatuko ditu, eta horietako bakoitzerako zehaztuko du zerbitzu horiek euskal sektore publikoan, enpresa-sarean eta herritarrengan duten aplikagarritasuna.

II. TITULUA
FUNTZIOEN GARAPENA

3. Artikulua. –Zibersegurtasun-zerbitzuak emateko betebeharra.

Agentziak, bere eskumenen esparruan, eta une bakoitzean dituen baliabideen eskuragarritasuna kontuan hartuta, zibersegurtasun-zerbitzuak eman beharko dizkie bai euskal sektore publikoari, bai enpresa-sareari eta herritarrei, bere zerbitzu-katalogoan ezarritako baldintzetan.

I. KAPITULUA
FUNTZIO ESTRATEGIKOAK

4. Artikulua. –Jardueren koordinazioa.

1.– Agentziak koherentzia emango die euskal sektore publikoaren jarduerei, informazio garrantzitsua trukatzea erraztuko duen ikuspegi integral batetik. Horretarako, zibersegurtasunaren arloan garatzen dituen jarduerak kudeatu, koordinatu eta jarraipena egingo du, dauden beharrak identifikatuz eta behar horiei arreta egokia emateko bideratuz.

2.– Agentziak euskal sektore publikoa koordinatuko du administrazio, organismo eta entitateen zibersegurtasun-planak egin, garatu eta eguneratzean, zibersegurtasunaren arloko helburu komunak lortzeko ikuspegi koherentea, lerrokatua eta eraginkorra izan dadin.

5. Artikulua. –Euskadiko zibersegurtasun estrategia.

1.– Zibersegurtasunaren Euskal Estrategia Euskal Autonomia Erkidegoko zibersegurtasunaren arloko helburu estrategikoak eta jarduera-ildoak ezartzen dituen esparru-dokumentua da.

2.– Estrategiak lankidetza-prozesu bat izango du, eta prozesu horretan euskal sektore publikoaren eta enpresa-sarearen ordezkaritza ziurtatuko da.

3.– Estrategia Gobernu Kontseiluaren erabaki bidez onartuko da, segurtasunaren arloan eskumena duen saileko titularrak proposatuta.

4.– Indarraldia urte anitzekoa izango da, eta gutxienez bost urtean behin berrikusiko da eta teknologia-, antolamendu- edo arrisku-egoerak hala eskatzen duenean.

6. Artikulua. –Zibersegurtasun Estrategian parte hartzen duten organoak.

1.– Estrategiaren gobernantza-esparru bat egongo da, gutxienez, erakundeen arteko lankidetzarako bi organok osatua: bata, zuzendaritzakoa, lehentasunak ezartzeaz, ildo estrategikoak orientatzeaz eta jardueren koherentzia zaintzeaz arduratuko dena; eta bestea, teknikoa, zibersegurtasuneko jarduerak eta planak garatzeaz eta gauzatzeaz arduratuko dena.

2.– Estrategiak eragiten dien erakundeek gobernantza-organo horietan parte hartu beharko dute, hala eskatzen zaienean, beren eskumen-eremuaren, izaeraren edo dagozkion jardun-ildoetan duen zereginaren arabera. Horretarako, ordezkariak izendatu beharko dituzte, organo horiek esleituta dituzten jarraipen-, koordinazio- eta erabaki-eginkizunetan eraginkortasunez laguntzeko beharrezko gaitasun teknikoa eta funtzionala dutela bermatuz.

3.– Gobernantza-organoetan parte hartzeko, gutxienez:

a) Deitzen diren bilkuretara joatea eta horietan aktiboki parte hartzea.
b) Estrategiaren betetze-mailaren jarraipena eta ebaluazioa egiteko informazio garrantzitsua ematea.
c) Organo horietan hartutako erabakietatik eratorritako koordinazio-jardueretan laguntzea.

4.– Agentziak gidatuko du Euskadiko Zibersegurtasun Estrategia egiteko, berrikusteko eta haren jarraipena egiteko prozesua. Era berean, Estrategiaren gobernantza-ereduari laguntzeko organo gisa jardungo du, kudeaketa operatiboaren, hartutako akordioen jarraipenaren eta laguntza teknikoaren funtzioak bere gain hartuz. Horretarako, zehaztutako helburu estrategikoekin bat datorren parte-hartze eraginkorra bermatzeko beharrezkoak diren antolaketa-irizpideak, funtzionamendu-mekanismoak eta komunikazio-bideak ezarri ahal izango ditu.

7. Artikulua. –Zibersegurtasun eredua.

1.– Euskadiko Zibersegurtasun Eredua erreferentziazko tresna komuna da euskal sektore publikoan bitarteko elektronikoen erabilera segurua eta koherentea sustatzeko, eta zibersegurtasun sendo, koherente eta lerrokatua arian-arian ezartzeko irizpideak ezartzen ditu.

2.– Eredua tresna nagusia izango da Agentziak bultzatutako erreferentzia-esparru, jarraibide eta arau teknikoen multzoa artikulatzeko eta koherentzia emateko. Horretarako, Ereduak, gutxienez, honako elementu hauek jasoko ditu:

a) Zibersegurtasunaren arloko rolen eta erantzukizunen egitura formala, eredua artikulatu ahal izateko.
b) Garapen-maila progresiboen araberako bilakaeraren ikuspegia, zibersegurtasuneko kontrolen eta neurrien aplikazioa erakunde bakoitzaren testuingurura, baliabideetara, heldutasunera eta kritikotasunera egokitzeko.
c) Zibersegurtasuneko eremu funtzionalak; horietan modu koherentean bilduko dira kontrolak, irizpide teknikoak, jarraibideak eta arau teknikoak, eta errazago ulertu, aplikatu eta jarraituko dira.

3.– Agentziak Eredua prestatuko du, ezagupena sustatuko du eta arian-arian ezar dadin bultzatuko du, sustapen-, asistentzia- eta prestakuntza-ekintzak, laguntza-tresnak, gida praktikoak eta helburu horretarako baliagarri izan daitekeen beste edozein mekanismo garatuz.

4.– Agentziak euskal sektore publikoak Eredua betetzen duen ebaluatuko du, haren adopzio-mailaren jarraipena egingo du, hobetzeko beharrak identifikatuko ditu eta euskal sektore publiko osoaren segurtasuna eta erresilientzia indartzera bideratutako gomendioak emango ditu.

5.– Agentziak aldian behin berrikusiko du eredua, mehatxuen, teknologiaren eta aplikatu beharreko lege- eta araudi-esparruaren bilakaerara egokitzeko.

II. KAPITULUA
FUNTZIO OPERATIBOAK

8. Artikulua. –Zibersegurtasunaren arloko kontzientziazioa eta trebakuntza

1.– Agentziak zibersegurtasunaren arloko kontzientziazio- eta prestakuntza-jarduerak antolatu eta sustatuko ditu, euskal sektore publikoari, kolektibo profesionalei eta herritarrei zuzenduta, zibersegurtasunaren arloko jardunbide egokiak, erreferentziazko esperientziak eta ezagutza espezializatuak zabalduz, zibersegurtasunaren kultura, baliabide digitalen erabilera segurua eta lotutako arriskuen kudeaketa egokia indartzeko helburuarekin.

2.– Agentziak kasu bakoitzean egokienak diren bitarteko eta kanalen bidez zabalduko ditu landutako edukiak. Horretarako, jardunaldiak, tailerrak, dibulgazio-saioak eta ezagutza transferitzeko ekintzak antolatuko ditu, bai eta zibersegurtasuneko gaitasun teknikoak eta antolakuntzakoak hobetzera bideratutako ekimenak ere.

9. Artikulua. –Zibersegurtasun-gertakarien aurreko prestaketa

1.– Agentziak euskal sektore publikoaren eta enpresa-sarearen prestakuntza-maila ebaluatuko du, zibersegurtasun-gertakariei erantzuteko gaitasunei dagokienez.

2.– Agentziak simulakroak egingo ditu, euskal sektore publikoaren eta enpresa-sarearen zibersegurtasun-gertakariei erantzuteko gaitasuna trebatzen laguntzeko, hobetzeko alderdiak identifikatzeko helburuarekin.

10. Artikulua. – Zaintza digitala eta alerta goiztiarra

1.– Agentziak ziberinteligentzia-eredu espezifiko bat garatu eta eguneratuko du EAErako. Horren bidez, ingurune digitaleko zibersegurtasunarekin lotutako mehatxuen monitorizazio proaktiboa egingo du, Euskal Autonomia Erkidegoan eragina izan dezaketen arrisku eta jarduera gaiztoak identifikatu, aztertu eta aurreikusteko.

2.– Eredu horrek aukera emango du erakundeen arrisku-maila indibiduala zibersegurtasunaren ikuspegitik identifikatzeko, eta, era berean, ikuspegi orokorra emango du. Horri esker, Agentziak neurri globalak hartu ahal izango ditu Euskal Autonomia Erkidego osoaren babes-maila hobetzen laguntzeko.

3.– Mehatxu horietakoren bat identifikatzen bada, Agentziak alerta goiztiarreko eginkizunak beteko ditu erakundeetan, abisuak zabalduko ditu eta erantzunari laguntza teknikoa emango dio, informazio garrantzitsua, gomendioak eta orientabide teknikoak emanez, erakundeek arriskua arintzeko neurri egokiak hartu ahal izan ditzaten.

4.– Agentziak zibersegurtasun-alertak jakinarazteko kanalak eta prozedurak ezarriko ditu.

11. Artikulua. – Segurtasuneko auditoria teknologikoak

1.– Agentziak EAEko sektore publikoko azpiegitura teknologikoen, informazio-sistemen, aplikazioen, zerbitzu digitalen eta aktiboen kalteberatasun-maila aztertuko du, ustia daitezkeen ahuleziak identifikatzeko eta zibersegurtasun-arriskua murrizten laguntzeko. Era berean, auditoria teknologikoak egingo ditu, erakundeek eskatuta.

2.– Ahulezia kritikoak, aktiboki ustiatutako ahuleziak edo arrisku larria edo berehalakoa ekar dezaketen ahuleziak identifikatzen direnean, Agentziak ahalik eta azkarren jakinaraziko dio eragindako erakundeari, eta eskuragarri dagoen informazio teknikoa eta aplika daitezkeen euste-, arintze- edo zuzenketa-gomendioak emango dizkio.

12. Artikulua. – Zibersegurtasuneko Eragiketa Zentroa

1.– Agentziak segurtasun-eragiketen zentro bat (SOC) zabalduko du EAEko sektore publikoko azpiegitura teknologikoei eta informazio-sistemei eragiten dieten edo eragin diezaieketen segurtasun-gertaerak monitorizatzeko, aztertzeko eta kudeatzeko, batez ere aktibo kritikoak monitorizatzera bideratuta.

2.– Zibersegurtasuneko Eragiketa Zentroaren helburua hau izango da:

a) Segurtasun-gertaerak monitorizatzea.
b) Mehatxu, ahulezia eta portaera anomaloen identifikazio goiztiarra, korrelazioaren bidez eta monitorizatutako segurtasun-gertaerak aztertuz.
c) Zibersegurtasun-gertakariak detektatzea, erantzun koordinatua eta egokia emanez.
d) Gorabeherei eusteko, arintzeko eta berreskuratzeko laguntza teknikoa ematea, eragindako sistemen arduradunekin eta dagozkien erantzun-taldeekin koordinatuta.
e) Informazio tekniko garrantzitsua bildu eta aztertzea, erakundeen babes-gaitasunak hobetuko dituzten neurriak proposatzeko.

3.– Segurtasun Eragiketen Zentroak hala eskatzen duten erakundeen informazio- eta eragiketa-sistemetatik datozen gertaerak monitorizatuko ditu, dagozkien lankidetza-tresnen bidez.

4.– Segurtasun Eragiketen Zentroak zuzeneko gaitasuna duen kasuetan jardungo du, eta, gainerako kasuetan, detektatutako zibersegurtasuneko gertaerak eta balizko gertakariak identifikatu eta horien berri emango die kaltetutako erakundeei, beharrezko erantzun-jarduerak abiaraz ditzaten.

13. Artikulua. – Gorabeherei erantzuteko taldea

1.– Agentziak Euskal Autonomia Erkidegoan eskumena duen zibersegurtasun-gorabeherei erantzuteko taldearen (CSIRT) eginkizunak beteko ditu, eta CSIRTak eta haren jarduketa-eremuko erakunde baliokideak koordinatuko ditu.

2.– Agentziak gaitasun komun gisa jardungo du DFIR zerbitzua emango dien EAEko sektore publikoko entitateen zibersegurtasun-gorabeherei erantzuteko. Horrek barne hartuko ditu laguntza ematea, koordinatzea, eustea, artefaktuak aztertzea, desagerraraztea eta gorabeheren aurrean berreskuratzea, lerrokatzea eta eraginkortasun globala errazteko.

3.– Agentziak lankidetza-ereduak eta koordinazio-mekanismoak ezarri eta sustatuko ditu tokiko, autonomia-erkidegoko, estatuko eta nazioarteko beste CSIRT eta erantzun-talde batzuekin, informazio-trukea, zibersegurtasun-gorabeheren kudeaketa eraginkorra eta zibererasoen aurreko inpaktua eta berreskuratze-denbora murriztea errazteko, kontuan hartuta ziber-mehatxuen mugaz gaindiko izaera.

14. Artikulua. – Zibersegurtasun-gorabeheren analisia

1.– Agentziak teknologikoki ikertuko ditu EAEko sektore publikoari, enpresa-sareari edo herritarrei eragiten dieten edo eragin diezaieketen zibersegurtasun-gertakariak, bereziki EAEko sektore publikoarentzat bereziki garrantzitsuak direnak edo, haien izaeragatik, irismenagatik edo inpaktu potentzialagatik beharrezkotzat jotzen direnak.

2.– Agentziak txosten teknikoak egingo ditu ziber-mehatxuen prebentzioa, detekzioa eta erantzuna hobetzeko, eta gomendio teknikoak eta antolakuntzakoak egingo ditu, errepikatze-arriskua murrizteko eta sistemen erresilientzia indartzeko.

3.– Egindako ikerketen eta analisien emaitzak, nagusiki, Euskadiko Zibersegurtasun Eredua elikatzeko, EAEko sektore publiko osoari zuzendutako gomendioak, alertak eta prebentzio-

neurriak egiten laguntzeko eta bitarteko elektronikoen erabileran zibersegurtasun-maila ebaluatzen eta etengabe hobetzen laguntzeko erabiliko dira.

4.– Agentziak, bere eginkizun operatiboak betetzean, zibersegurtasunaren arloko laguntza tekniko espezializatua emango die agintaritza eskudunei, haiek hala eskatuz gero, legez kanpoko jokabideak prebenitzearekin eta ikertzearekin lotutako jarduketak behar bezala garatzeko, sistemen gaineko esku-hartze jarduketetan eta ebidentzia elektronikoak lortu, aztertu eta tratatzean laguntza teknikoa ematea barne.

III. KAPITULUA
AUDITORETZA ETA ARRISKU GOBERNANTZA FUNTZIOAK

15. Artikulua. – Auditoretza Teknikoko Organoa.

1.– Agentziak Auditoretza Teknikoko Organo (ATO) gisa jardungo du, eta euskal sektore publikoko informazio-sistemen auditoretza-eginkizunak beteko ditu, aplikatu beharreko araudian eta, bereziki, Segurtasunaren Eskema Nazionala (SEN) arautzen duen maiatzaren 3ko 311/2022 Errege Dekretuan aurreikusitakoaren arabera, sistemak, zerbitzuak eta prozesuak ezarritako segurtasun-betekizunetara zenbateraino egokitzen diren egiaztatzeko.

2.– SENen araberako auditoretzak aipatutako errege-dekretuan ezarritakoaren arabera egingo dira, bai eta SENen akreditazioaren arloko organo eskudunak emandako gida, jarraibide eta irizpide teknikoetan ezarritakoaren arabera ere. Horretarako, Agentziak behar diren prozedurak eta formatuak ezarriko ditu, bai auditoretza-prozesua garatzeko, bai emaitzak auditatutako erakundeei eta, hala dagokionean, egiaztapenaren arloan eskumena duen organoari jakinarazteko.

3.– Agentziak bermatuko du auditoretzak Segurtasun Eskema Nazionalaren arabera erabateko independentziaz, inpartzialtasunez eta konfidentzialtasunez egiten direla, Auditoretza Teknikoko Organoaren jarduera arautzen duten printzipioen eta horretarako ezarritako barne-prozeduren arabera.

4.– Sistemen ardura duten erakundeek edo organo eskudunek eskatuta egingo dira auditoretzak.

5.– Auditatutako erakundeek aktiboki lagundu beharko dute auditoretza-prozesua garatzen, auditoretza behar bezala egiteko beharrezkoak diren informaziorako, sistemetarako, instalazioetarako eta pertsonentzako sarbidea erraztuz, aplikatu beharreko araudian aurreikusitako baldintzetan.

6.– Auditoretza teknikoko jarduketak teknikoak izango dira, eta ez zehatzaileak, hargatik eragotzi gabe beste organo edo agintaritza batzuei kontrol, gainbegiratze edo zehapen-araubidearen arloan dagozkien eskumenak.

7.– Ikuskatutako sistemen ardura duten erakundeek ezarriko dituzte neurri zuzentzaileak.

16. Artikulua. – Ebaluazio teknikoak

1.– Agentziak aldizkako ebaluazio teknikoak egingo ditu euskal sektore publikoaren eremuan hedatutako zibersegurtasun-neurrien ezarpen-mailari, egokitasunari eta eraginkortasunari buruz, zibersegurtasunaren arloan hedatutako politika publikoen egoeraren eta haien denbora-bilakaeraren ikuspegi sendo eta objektiboa izateko.

2.– Ebaluazioek kontuan hartu ahal izango dituzte Euskadiko Zibersegurtasun Ereduaren ezarpen-maila, arrisku, heldutasun, erresilientzia eta erantzuteko gaitasunaren adierazle teknikoak edo zibersegurtasunaren arloan aplikatu beharreko araudia eta erregulazioa betetzea.

3.– Ebaluazio teknikoak aldian behin egingo dira, eta, gutxienez, bi urtean behin, Agentziak definitutako metodologia homogeneo baten arabera. Metodologia horrek aukera emango du emaitzak konparatzeko, joerak identifikatzeko eta hobekuntza-arloak hautemateko. Ebaluazio tekniko horiek inpaktu operatiboaren proportzionaltasun- eta minimizazio-irizpideak aplikatuz egingo dira, aztertutako sistemen eta zerbitzuen izaeraren, kritikotasunaren eta arrisku-mailaren arabera.

4.– Egindako ebaluazioen emaitza gisa, Agentziak ebaluazio-txosten teknikoak egingo ditu, agregatuak edo espezifikoak, dagokionaren arabera, eta txosten horietan jasoko dira egoeraren azterketa, ondorioak eta zibersegurtasun-gaitasunak hobetzera bideratutako gomendioak.

5.– Ebaluazio teknikoen emaitzak EAEko Zibersegurtasun Ereduaren eguneratzea bideratzeko erabiliko dira, EAEko Zibersegurtasun Estrategia egiteko informazio-iturri gisa, zibersegurtasunaren arloan lehentasunak eta indartze-jarduketak zehazten laguntzeko eta EAEko sektore publikoan bitarteko elektronikoen erabileran zibersegurtasun-maila etengabe hobetzen laguntzeko.

6.– Ebaluazio teknikoek izaera teknikoa izango dute, eta ez zehatzailea, eta ez dute ekarriko Agentziak bere gain hartzea aztertutako erakundeen informazio-sistemen kudeaketaren edo eragiketaren gaineko zuzeneko erantzukizunik, eta ez dituzte ordeztuko barne- edo kanpo-kontroleko beste organo batzuei dagozkien kontrolak.

17. Artikulua. – Arriskuaren kudeaketa

1.– Agentziak Euskal Autonomia Erkidegoan zerbitzu publikoak edo funtsezko zerbitzuak kudeatzen dituzten erakundeei buruzko informazio egokia bilduko du, informazioaren segurtasunaren egoerari dagokionez, dauden arriskuen, gaitasunen eta babes-mailen ikuspegi agregatua eta eguneratua izateko.

2.– Bildutako informazioa segurtasun-neurrien ezarpen-mailari, aktiboen eta funtsezko zerbitzuen identifikazioari edo mehatxuekiko esposizioari buruzkoa izan daiteke. Informazio hori zuzenean eskuratu ahal izango du Agentziak, bere eginkizunak betez, edo zeharka, erakundeek berek emandako datuen bidez.

3.– Bildutako informaziotik abiatuta, Agentziak zibersegurtasunaren arloko arrisku-azterketak eta -balorazioak egingo ditu, arrisku-agertoki garrantzitsuak, mendekotasun kritikoak eta indartzeko premiak identifikatzeko.

4.– Egindako analisietan oinarrituta, Agentziak neurri teknikoak, operatiboak, antolakuntzakoak edo koordinaziokoak proposatu ahal izango ditu arriskua murrizteko eta zerbitzu publikoen eta funtsezko zerbitzuen babesa indartzeko. Era berean, emaitzak erabiliko dira alderdi interesdunei beren eskumenen esparruan informazio garrantzitsua emateko eta zibersegurtasunaren arloko koordinazioa eta erabakiak hartzen laguntzeko.

18. Artikulua. – Zibersegurtasun-planetarako laguntza.

1.– Agentziak laguntza metodologikoa emango du zibersegurtasun-planetan jasotako helburuak, jarduketa-ildoak, lehentasunak eta neurriak definitzeko, Euskadiko Zibersegurtasun Ereduarekin lerrokatzea sustatuz, eta, horretarako, beharrezkotzat jotzen dituen material eta ekintza guztiak garatuz.

2.– Agentziak jarraipen- eta laguntza-mekanismoak ezarriko ditu zibersegurtasun-planak errazago gauzatzeko, zailtasun komunak identifikatuz eta, komeni denean, indartzeko edo doitzeko jarduketak proposatuz. Agentziak sinergiak ezarriko ditu baliabideak optimizatzeko eta jardueren eraginkortasuna indartzeko.

IV. KAPITULUA
ERAKUNDEEN ARTEKO KOORDINAZIOA ETA LANKIDETZA

19. Artikulua. – Administrazioen arteko lankidetza.

1.– Agentziak zibersegurtasunaren arloko koordinazio teknikoko mekanismoak bultzatuko ditu euskal sektore publikoa osatzen duten administrazioen artean, jarduketa koherente eta eraginkorra bermatzeko.

2.– Agentziak beharrezkoak diren lankidetza-akordioak eta hitzarmenak egin ahal izango ditu kasuan kasuko organo eskudunekin, bere zerbitzuak erakunde bakoitzaren barne-dinamikan txerta daitezen.

20. Artikulua. – Segurtasun Sailarekin koordinatzea.

1.– Agentziak hainbat koordinazio-mekanismo ezarriko ditu EAEko Administrazio Orokorreko Segurtasun Sailarekin:

a) Babes zibilaren eta larrialdien arloko eskumena duen zuzendaritzarekin, zibersegurtasun-gertakari batekin lotutako larrialdietan laguntza teknikoa emateko, bai eta Autobabes Planen Erregistroarekiko elkarreragingarritasuna lortzeko ere.

b) Larrialdiei aurre egiteko eta babes zibilerako euskal sistemarekin eta Ertzaintzarekin, behar den laguntza teknikoa emanez zibergorabeherekin lotutako larrialdietan.

c) LABIrekin, laguntza teknikoa emanez zibererasoen edo larrialdi-egoera eragin dezaketen zibersegurtasun-gorabeheren ondoriozko egoeretan.

d) Segurtasuna koordinatzeko eskumena duen zuzendaritzarekin, Euskadiko Azpiegitura Sentikorrak Babesteko Plana osatzen duten erakundeei zibersegurtasunaren arloan laguntzeko.

e) Hauteskunde-prozesuen arloko zuzendaritza eskudunarekin, hauteskunde-prozesuen zibersegurtasunarekin lotutako operatiboetan parte hartuz.

f) Zibersegurtasunaren koordinazioaren arloan eskumena duen Ertzaintzaren Burutzarekin, berrikuntzaren arloko jardueretarako eta ziberdelitua jazartzearekin lotutako neurrietarako.

g) Inteligentziaren arloan eskumena duen Ertzaintzaren bulegoarekin, ziberkriminalitatearen ikerketa-eremuetan.

h) Zibersegurtasun-osagaiarekin lotutako eginkizunak dituzten edo izan ditzaketen Ertzaintzako beste alor, burutza, atal eta unitate batzuekin, informazio-trukea, gertaeren balorazio teknikoa eta, beharrezkoa denean, jarduketa koordinatuak hartzea errazteko.

2.– Era berean, Agentzia Segurtasun Saileko gainerako zuzendaritzekin koordinatuko da, bai eta, hala badagokio, dagozkion sailburuordetzekin ere, beren eskumenen esparruan, zibersegurtasunaren eta gorabeheren kudeaketaren arloan jarduketa koherentea bermatzeko.

21. Artikulua. – Agintariekiko, organo judizialekiko eta polizia-kidegoekiko harremana.

Agentziak laguntza teknikoa emango du eta agintaritza eskudunekin, organo judizialekin eta polizia-kidegoekin behar den koordinazioa erraztuko du, zibersegurtasunari eta poliziaren informazio-sistemen babesari laguntzeko, informazio teknikoaren trukea, legez kontrakoak izan daitezkeen jardueren ikerketa eta beharrezkoak diren laguntza-neurriak sustatuz, betiere erakunde bakoitzaren eskumen-eremuak errespetatuz.

22. Artikulua. – Nazio Zentro Kriptologikoarekiko harremanak.

1.– Agentzia harremanetarako gune izango da Nazio Zentro Kriptologikoarekiko, bai Euskal Autonomia Erkidegoko Administrazio orokorreko erakunde bakoitzarekiko, bai haren mendeko edo hari atxikitako erakundeekiko, bereziki informazio-sistemetako segurtasun-aldagai nagusien egoerarekin lotutako informazio-betebeharrei dagokienez, bai eta informazio-sistemen segurtasunean eragin nabarmena duten gertakariak jakinaraztearekin lotutako guztiari dagokionez ere. Hori guztia subjektu aplikagarriek ezarritako betebeharrak betetzeari kalterik egin gabe egingo da.

2.– Horregatik, Euskal Autonomia Erkidegoko Administrazio orokorrak eta haren mendeko edo hari atxikitako erakundeek beren informazio-sistemetako segurtasun-aldagai nagusien egoeraren berri eman beharko diote Agentziari, bai eta informazio-sistema horien segurtasunean eragin nabarmena duten gorabeheren berri ere.

3.– Euskal sektore publikoa osatzen duten gainerako erakunde guztiek, zibersegurtasunaren kudeaketa eraginkorragoa izan dadin, Agentzia izendatu ahal izango dute Nazio Zentro Kriptologikoarekin harremanetan jartzeko puntu gisa, bai informazio-sistemetako segurtasun-aldagai nagusien egoerarekin lotutako informazio-betebeharrei dagokienez, bai ukitutako informazio-sistemen segurtasunean eragin nabarmena duten gertakariak jakinaraztearekin lotutakoei dagokienez, hargatik eragotzi gabe subjektu aplikagarriek ezarritako betebeharrak betetzea. Horretarako, hala erabakitzen denean, informatzeko betebeharraren borondatezko eskuordetze hori hala ezartzen duen akordio bat sinatuz formalizatu eta erregistratu beharko da.

23. Artikulua. – Kanpoko erakunde-harremanak.

1.– Agentziak lankidetza- eta elkarlan-harremanak ezarri eta mantendu ahal izango ditu zibersegurtasunaren arloan diharduten estatuko eta nazioarteko entitate eta organismoekin.

2.– Agentzia euskal sektore publikoaren solaskidea izango da zibersegurtasunaren arloko estatuko eta nazioarteko lankidetza-foro, -organismo eta -mekanismoen aurrean.

V. KAPITULUA
DATU-BILKETA

24. Artikulua. – Informazio-eskaerak.

1.– Agentziak bere eginkizunak behar bezala betetzeko beharrezkoa den informazioa eskatu ahal izango die 2. artikuluan bildutako subjektuei. Informazio-errekerimendu horiek behar bezala arrazoituta egon beharko dute, lortu nahi den helburuarekiko proportzionalak izan beharko dira, eta Agentziari esleitutako eginkizunak betetzeko behar-beharrezkoa den informaziora mugatu beharko dira.

2.– Eskatutako informazioa honako hauei buruzkoa izan ahalko da: zibersegurtasunaren arloko harreman-puntu espezifikoak, kudeatutako sistema, zerbitzu eta aktiboen ezaugarriak, zibersegurtasunaren egoera, segurtasun-neurriak ezartzea, arriskuen kudeaketa, zibersegurtasun-gertakariak gertatzea, Agentziak arriskuen edo mehatxuen jakinarazpena egin ondoren aplikatutako neurriak, hornidura-katea edo beste elementu tekniko garrantzitsu batzuk, kasu bakoitzean zehazten diren baldintzetan eta irismenarekin.

3.– Informazio-errekerimenduek ez dute zehapen-izaerarik izango, eta ez dute berez ekarriko Agentziak beste organo edo agintaritza batzuei dagozkien kontrol-, ikuskapen- edo gainbegiratze-eginkizunak bere gain hartzea, hargatik eragotzi gabe ordenamendu juridikoaren arabera aplikatzekoak diren lankidetza-betebeharrak.

4.– Agentziari emandako informazioa bere eginkizunak betetzeko baino ez da erabiliko, eta konfidentzialtasunez tratatuko da. Behar diren neurri teknikoak eta antolaketa-neurriak

hartuko dira informazio hori behar bezala babesteko, kontserbatzeko eta, hala badagokio, anonimizatzeko edo gehitzeko.

5.– Ezartzen diren epeetan eta moduan erantzungo zaie informazio-errekerimenduei, ahal dela bitarteko elektronikoen bidez, hargatik eragotzi gabe lankidetza-mekanismoak eta kanal espezifikoak antolatu ahal izatea haiek modu seguruan bidaltzea errazteko.

25. Artikulua. – Emandako informazioaren konfidentzialtasuna.

1.– Agentziak emandako zerbitzuetara sartzen diren erakundeek zerbitzu horien esparruan harengandik jasotzen duten informazioaren konfidentzialtasuna bermatu beharko dute, baldin eta informazio hori sentikorra bada edo informazio hori zabaltzeak arriskuan jar badezake ukitutako sistemen, zerbitzuen edo aktiboen edo ukitutako hirugarrenen segurtasuna.

2.– Agentziak emandako informazioa zein helburutarako eman den, helburu horietarako baino ez da erabiliko, eta ezin izango zaie hirugarrenei jakinarazi edo zabaldu Agentziaren berariazko baimenik gabe, aplikatu beharreko araudian aurreikusitako kasuetan izan ezik.

3.– Erakunde hartzaileek behar diren neurri teknikoak eta antolaketa-neurriak hartuko dituzte jasotako informazioa behar bezala babesteko, informazioaren segurtasunari buruz aplikatu beharreko araudiaren arabera.

4.– Artikulu honetan xedatutakoak ez ditu eragotziko ordenamendu juridikoaren arabera dagozkion lankidetza-, komunikazio- edo informazio-betebeharrak.

26. Artikulua. – Sekretu-betebeharra.

1.– Agentziaren zerbitzuko langileek eta Agentziari bere eginkizunak betetzen laguntzen dioten pertsonek edo erakundeek sekretua gorde beharko dute beren jardueraren ondorioz eskuratzen duten informazioari, datuei, dokumentuei, ezagutzei edo emaitzei dagokienez, edozein euskarri, formatu edo bitartekotan daudela ere.

2.– Sekretu-betebeharra, bereziki, honako hauei buruzko informaziora hedatuko da: informazio-sistemen segurtasuna, ahuleziak, mehatxuak, zibersegurtasun-gertakariak, ebidentzia teknikoak, konfigurazioak, babes-neurriak, jarraitutasun-planak, bai eta ukitutako sistemen eta zerbitzuen segurtasuna, konfidentzialtasuna edo funtzionamendu egokia arriskuan jar dezakeen beste edozein alderdi ere.

3.– Sekretu-betebeharrak indarrean jarraituko du zerbitzu-harremana, kontratuzkoa edo Agentziarekiko lankidetzakoa amaitu ondoren ere, hargatik eragotzi gabe ordenamendu juridikoaren arabera sekretua ez betetzeak ekar ditzakeen erantzukizunak.

VI. KAPITULUA
FUNTZIONAMENDU-ARAUBIDEA

27. Artikulua. – Agentziaren zerbitzuak eskuratzeko beharrezkoa den garapen-maila.

1.– Agentziak zehaztu ahal izango du zer zibersegurtasuneko garapen-maila eskatuko zaien erakundeei ematen duen zerbitzu bakoitza eskuratzeko, Euskadiko Zibersegurtasun Ereduan aurreikusitakoaren arabera.

2.– Artikulu honetan xedatutakoaren ondorioetarako, garapen-mailatzat hartuko da Euskadiko Zibersegurtasun Ereduan definitutako zibersegurtasuneko gaitasunen, neurrien eta kontrolen ezarpen-maila, horretarako ezartzen diren mekanismoen arabera ebaluatuta.

3.– Oro har, Agentziaren zerbitzuak eskuratzeko, erakunde interesdunek zibersegurtasuneko garapen-mailaren ebaluazio bat egin beharko dute gutxienez, autoebaluazio-prozesu baten bidez, Agentziak zehazten dituen baldintzetan.

4.– Agentziak garapen-maila batekin lotu ahal izango du zerbitzu bakoitza, eta betekizun bereiziak ezarri ahal izango ditu zerbitzuaren izaeraren, konplexutasun teknikoaren, inpaktu potentzialaren edo lotutako arriskuen arabera, EAEko Zibersegurtasun Ereduarekin bat etorriz.

5.– Garapen-mailaren ebaluazioak helburu hau izango du:

a) Agentziaren zerbitzuak egoki eta eraginkortasunez ematen laguntzea.
b) Euskadiko Zibersegurtasun Ereduaren aplikazio proportzionatua eta koherentea bermatzea.
c) Erakundeei orientazioa ematea, zibersegurtasun-gaitasunak pixkanaka hobetu ditzaten.

6.– Artikulu honetan xedatutakoa gorabehera, Agentziak gida-, laguntza- edo gaikuntza-zerbitzuak eman ahal izango ditu, erakundeei autoebaluazioa egiten edo beren garapen-maila hobetzen laguntzeko.

28. Artikulua. – Zibersegurtasun-gertakariak kudeatzeko eredua antolatzea.

1.– Zibersegurtasun-gertakariak kudeatzeari dagokionez, Agentziari dagokio III. Kapituluan ezarritakoa betetzea.

2.– Erakunde bakoitzari dagokio, kasu bakoitzean indarrean dagoen araudian ezarritakoa alde batera utzi gabe:

a) Ziber-erasoak eta zibersegurtasun-gertakariak kudeatzeko metodologia propioa definitzea.
b) Zibersegurtasuneko gertakariak eta zibererasoak kudeatzeko metodologia hori modu egokian antolatzeko behar diren irizpideak eta mekanismoak ezartzea.
c) Zibersegurtasuneko gertakariak eta zibererasoak behar bezala kudeatzeko behar diren baliabide materialak eta giza baliabideak mantentzea.
d) Pertsona bat edo batzuk izendatzea Agentziarekiko solaskide zibererasoak eta zibersegurtasun-gertakariak kudeatzeko, eta horretarako behar diren harremanetarako puntuak ezartzea.
e) Agentziatik jasotako zibersegurtasun-alerten jakinarazpenei arretaz erantzutea.
f) Zibersegurtasuneko gertakariak eta zibererasoak kudeatzea.
g) Izandako zibersegurtasun-gorabeheren eta zibererasoen berri ematea Agentziari, arretaz.
h) Zibersegurtasuneko gertakariak eta zibererasoak konpontzea.
i) Aldian behin ariketak edo simulakroak egitea, zibererasoak eta zibersegurtasun-gertakariak kudeatzeko metodologiaren eraginkortasuna egiaztatzeko.

3.– Erakunde bakoitzak formalki jakinaraziko dio Agentziari zibersegurtasun-gertakariak kudeatzeko solaskidearen edo solaskideen identifikazioa, eta Agentziari jakinaraziko dio solaskideen edo harremanetarako puntuen izendapenean izandako edozein aldaketa.

29. Artikulua. – Funtsezko sektoreentzako laguntza.

Agentziak berariazko euskarria emango die Euskal Autonomia Erkidegoko funtsezko sektoreei eta bereziki sentikorrak diren beste eremu batzuei, ematen dituzten zerbitzuen izaera kritikoa eta funtzionamenduari lotutako arriskuak kontuan hartuta, eta dekretu honetan aurreikusitako jarduketak eta zerbitzuak haien ezaugarri eta beharretara egokitu ahal izango ditu.

30. Artikulua. – Jarduketa teknikoak gauzatzeko zaintzak.

1.– Informazio-sistemetarako arriskutsuak izan daitezkeen Agentziaren jarduketa teknikoak planifikatuta, kontrolatuta eta modu proportzionalean egingo dira.

2.– Jarduketa horiek soil-soilik egingo dira erakunde arduradunaren gaikuntza, baimena edo berariazko eskaera duten sistema, aktibo edo inguruneetan, ezartzen diren baldintzetan, eta erakunde horri dagozkion eskumenak, erantzukizunak eta betebeharrak erabat errespetatuz.

3.– Agentzia ez da izango dekretu honetan aurreikusitakoaren arabera egindako informazio-sistemetarako arriskutsuak izan daitezkeen jarduketa teknikoen ondorioen erantzule, hargatik eragotzi gabe aplikatu beharreko esparru juridikoa edo hura gauzatzeko berariaz ezarritako baldintzak ez betetzeak ekar ditzakeen erantzukizunak.

4.– Nolanahi ere, Agentziak behar diren neurri teknikoak eta antolaketa-neurriak hartuko ditu egindako jarduketen inpaktua minimizatzeko eta tratatutako informazioaren konfidentzialtasuna, osotasuna eta eskuragarritasuna zaintzeko, bai eta egindako jarduketen dokumentazio eta trazabilitate egokia bermatzeko ere.

31. Artikulua. – Alderdien erantzukizuna.

Agentziak zerbitzuak emateak ez du esan nahi zuzeneko kudeaketa, administrazioa, eragiketa, mantentze-lanak eta erakundeen sistemen gaineko erantzukizuna bere gain hartuko dituenik. Bakoitzari dagokio bere eskumenen esparruan beharrezkoak diren segurtasun-neurriak ezartzea eta kudeatzea.

32. Artikulua. – Jardueren jarraipena.

Zerbitzuak emateko esparruan, Agentziak jardueren jarraipena egin ahal izango du, eta hartutako neurriei buruzko beharrezko informazioa eskatu ahal izango die erakundeei, eraginkorrak direla egiaztatzeko.

III. TITULUA
JARRAITUTASUN-PLANAK ZIBERSEGURTASUNAREN ARLOAN, AUTOBABESAREN ESPARRUAN

I. KAPITULUA
HELBURUA ETA BETEBEHARRAK

33. Artikulua. – Xedea.

Titulu honen xedea da Euskal Autonomia Erkidegoko lehentasunezko jarduera, zentro, establezimendu, espazio, instalazio edo bulego jakin batzuetan zibersegurtasun-arloko jarraitutasun-planak egiteko eta mantentzeko betebeharra arautzea, pertsonentzat, haien ondasunentzat eta ondare kolektiboarentzat arrisku-egoerak sor ditzaketen zibersegurtasuneko gertakari eta gorabeherei aurre egiteko tresna espezifiko gisa, halako moduz non horrelako egoerek modu bereziki larrian eragin diezaieketen.

34. Artikulua. – Aplikazio-eremua.

1.– Titulu honetan aurreikusitako betebeharrak sektore jakin batzuetako jarduerei, zentroei, establezimenduei, espazioei, instalazioei edo bulegoei aplikatuko zaizkie, baldin eta jarduera horiek egitea beharrezkoa bada herritarren oinarrizko gizarte-funtzioak, osasuna, segurtasuna, gizarte-ongizatea eta ongizate ekonomikoa mantentzeko, bai eta Euskadiko erakundeen eta haien administrazio publikoen funtzionamendu eraginkorrerako ere, baldin eta haien zentro, establezimendu edo azpiegituretakoren bat azaroaren 2ko 277/2010 Dekretuan xedatutakoaren mende badago. Dekretu hori otsailaren 12ko 21/2019 Dekretuak aldatu zuen, zeinaren bidez arautzen baitira zenbait jarduera, zentro edo establezimenduren autobabes-betebeharrak larrialdiei aurre egiteko.

2.– Aurreko apartatuan aipatzen diren sektoreak dekretu honen I. eranskinean zehazten dira; hala ere, eguneratu egin daitezke, xedapen hauen arabera:

a) Europako Parlamentuaren eta Kontseiluaren 2022ko abenduaren 14ko 2022/2555 (EB) Zuzentarauaren transposizioa. Zuzentarau hori Batasun osoan zibersegurtasun-maila erkide handia bermatzeko neurriei buruzkoa da, 910/2014 (EB) Erregelamendua eta 2018/1972 (EB) Zuzentaraua aldatzen ditu eta 2016/1148 (EB) Zuzentaraua (SRI 2 Zuzentaraua) indargabetzen du).
b) Zibersegurtasunaren arloan sektore horiekin zerikusia duen beste edozein erregulazio onartzea edo aldatzea.

3.– Agentziak zibersegurtasunaren arloko jarraitutasun-planak egitea eta ezartzea eskatu ahal izango die aurreko apartatuetan jasota ez dauden jarduera, zentro, establezimendu, espazio, instalazio edo bulegoen titularrei, arrisku, kalteberatasun edo inpaktu handiko inguruabarrak daudenean pertsonen segurtasunean, funtsezko zerbitzuetan edo interes publikoan.

4.– Aurreko apartatuetan sartuta ez dauden jarduera, zentro, establezimendu edo azpiegituren titularrek beren borondatez egin ahal izango dute zibersegurtasunaren arloko jarraitutasun-plan bat, dekretu honetan aurreikusitakoaren arabera.

35. Artikulua. – Aplikazio-irizpideak.

Kapitulu honetan aurreikusitako betebeharrak eska daitezkeen gutxienekoak izango dira, eta osagarri gisa aplikatuko dira aplikatzekoa den araudi sektorial espezifikoak arautzen ez dituen alderdietan.

36. Artikulua. – Betebeharrak.

1.– Titulu honi lotutako jarduera, zentro, establezimendu edo azpiegituren titularrek betebehar hauek izango dituzte:

a) Zibersegurtasunaren arloko jarraitutasun-plan bat egitea eta mantentzea, Agentziaren jarraibideen arabera. Plan horren gutxieneko edukia hurrengo kapituluan ezartzen da.
b) Euskadiko Autobabes Erregistroan inskribatzea kasu bakoitzari lotutako zibersegurtasuneko jarraitutasun-planen erreferentziak.
c) Zibersegurtasunaren arloko jarraitutasun-planen erregistroan inskribatzea, erregistro-datu gisa, honako hauek:
   - Lotutako autobabes-planei buruzko erreferentziak.
   - Zibersegurtasunaren arloko babeserako datu espezifikoak.
   - Zibersegurtasunaren arloko jarraitutasun-planari dagozkion metadatuak, dekretu honen II. eranskinean ezarritakoaren arabera.
   - Titularraren erantzukizunpeko adierazpena, zibersegurtasunaren arloko jarraitutasun-plana ezartzeari buruzkoa.
d) Zibersegurtasunaren arloko jarraitutasun-plana ezartzeko, mantentzeko eta haren eraginkortasuna etengabe hobetzeko beharrezkoak diren jarduketak garatzea.
e) Jardueraren zibersegurtasunaz arduratuko diren pertsona fisikoak izendatzea, titularraz bestelakoak direnean.
f) Bere zerbitzura dauden langileei zibersegurtasunaren arloko jarraitutasun-planaren edukiei buruzko informazioa eta prestakuntza ematea, dituzten erantzukizunen eta arriskuarekiko esposizio-mailaren arabera.
g) Zibersegurtasunaren arloko jarraitutasun-plana behar bezala aplikatzeko behar diren baliabide materialak eta giza baliabideak mantentzea.
h) Zibersegurtasunaren arloko jarraitutasun-planean aurreikusitako neurriak aplikatzea zibersegurtasuneko gertaerak edo gertakariak gertatzen direnean.
i) Aldian behin ariketak edo simulakroak egitea, planaren eraginkortasuna eta inplikatutako langileen prestakuntza-maila egiaztatzeko.
j) Agentziari jakinaraztea dekretu honen III. eranskinean definitutako zibersegurtasun-gertakariak, zuzenean Agentziari edo Euskadiko Larrialdiak Koordinatzeko Zentroaren bidez (SOS Deiak - 112), hargatik eragotzi gabe lege- edo arau-errekerimenduagatik egin beharreko beste edozein jakinarazpen. Ondorengo jakinarazpenak zuzenean egingo zaizkio Agentziari. Agentziari jakinarazi beharreko zibersegurtasun-gorabeheren

taxonomia, bai eta horretarako ezarritako kanalak ere, Agentziaren Zuzendaritza Nagusiaren ebazpen baten bidez zehaztuko dira, eta ebazpen hori Euskal Herriko Agintaritzaren Aldizkarian argitaratuko da.

2.– Larrialdien eta babes zibilaren arloko agintaritza eskudunari dagozkio zibersegurtasun-arloko jarraitutasun-planei buruzko betebehar hauek:

a) Euskadiko Autobabes Erregistroan atal espezifiko eta esklusibo bat gaitzea titulu honen mendeko jarduera, zentro, establezimendu, espazio, instalazio edo bulegoetarako. Bertan, Euskadiko Zibersegurtasun Arloko Jarraitutasun Planen Erregistroko sarreren erreferentzia erregistratu beharko da.
b) Agentziari titulu honen mendeko jarduera, zentro, establezimendu, espazio, instalazio edo bulegoen titularren sektorearen berri ematea.
c) Agentziari bidaltzea Euskadiko Larrialdiak Koordinatzeko Zentroaren (SOS Deiak - 112) bidez jasotako zibersegurtasun-gorabeheren jakinarazpenak.

3.– Agentziak betebehar hauek ditu:

a) Titulu honen mendeko jarduera, zentro, establezimendu, espazio, instalazio edo bulegoen titularrek zibersegurtasunaren arloko jarraitutasun-plan bat egiteko eta edukitzeko betebeharra dutela egiaztatzea.
b) Euskadiko Zibersegurtasunaren arloko Jarraitutasun Planen Erregistroan erregistratutako zibersegurtasunaren arloko babeserako datu espezifikoak gainbegiratzea eta ikuskatzea.
c) Titulu honen mendeko jarduera, zentro, establezimendu, espazio, instalazio edo bulegoen titularrek egindako Zibersegurtasunaren arloko Jarraitutasun Planaren metadatuak gainbegiratzea eta ikuskatzea.

II. KAPITULUA
ZIBERSEGURTASUNAREN ARLOKO JARRAITUTASUN-PLANAK

37. Artikulua. – Zibersegurtasunaren arloko jarraitutasun-plana.

1.– Zibersegurtasunaren arloko jarraitutasun-plana dokumentu bat da, zeinaren bidez definitzen baita nola jarraituko duen jarduera, zentro, establezimendu, espazio, instalazio edo bulego batek zibersegurtasun-gertakari batek eragindako eten esanguratsu baten aurrean, gertakari horrek jarduera geldiaraz ez dezan eta haren jarduera nagusiek aurrera jarraituko dutela ziurtatzeko.

2.– Jardueraren titularraren erantzukizuna da zibersegurtasunaren arloko jarraitutasun-plana egitea, ezartzea, mantentzea eta berrikustea.

38. Artikulua. – Egitura eta edukia.

1.– Zibersegurtasunaren arloko jarraitutasun-planak honako hauek jorratzen ditu: zibersegurtasun-arriskuen identifikazioa eta ebaluazioa, arrisku horiek prebenitzeko eta kontrolatzeko behar diren ekintzak eta neurriak, bai eta jarduera, zentroa, establezimendua, espazioa, instalazioa edo bulegoa geldiaraz dezakeen zibersegurtasun-gertakariaren bat gertatuz gero hartu beharreko babes-neurriak eta beste jarduketa batzuk ere.

2.– Zibersegurtasunaren arloko jarraitutasun-planaren gutxieneko edukiak honako hauek izango dira:

a) Eragiketen plangintza eta kontrola: jardueraren, zentroaren, establezimenduaren, espazioaren, instalazioaren edo mendekotasunaren berezko eskakizunak betetzeko beharrezkoak diren prozesuak planifikatu, inplementatu eta kontrolatu behar dira, eta zibersegurtasun-arriskuei eta -aukerei heltzeko ekintzak inplementatu.

b) Inpaktuaren analisia eta zibersegurtasun-arriskuen ebaluazioa: prozesu bat ezarri eta mantendu behar da eragiketa-inpaktua aztertzeko eta etete-arriskuak ebaluatzeko, zeinak testuingurua ezarriko baitu, irizpideak definituko baititu eta zibersegurtasun-gertakari batek eragindako etenaldi baten inpaktu potentziala ebaluatuko baitu.
c) Jarraitutasun-estrategiak eta -konponbideak: inpaktu-analisiaren eta zibersegurtasun-arriskuen ebaluazioaren emaitzetan oinarritutako eragiketa-jarraitutasuneko estrategiak identifikatu eta hautatu behar dira. Jarraitutasun-estrategiek irtenbide bat edo gehiago izan ditzakete.
d) Jarraitutasun-planak eta -prozedurak: alderdi interesdun garrantzitsuei behar bezala ohartaraztea eta komunikatzea ahalbidetzen duen egitura bat ezarri eta mantendu behar da, eta jarduketa-jarraibideak eman behar dira erakundea administratzeko zibersegurtasun-gertakari batek eragindako eragiketa-eten batean. Planak eta prozedurak jarraitutasun-irtenbideak gauzatzeko erabiliko dira, beharrezkoa denean.
e) Ariketen programa: ariketen eta proben programa bat ezarri eta mantendu behar da, jarraitutasun-estrategien eta -soluzioen eraginkortasuna denborarekin baliozkotzeko.

3.– Zibersegurtasunaren arloko jarraitutasun-planen garapena errazteko, Agentziak dokumentuaren egitura jasotzen duen gida bat argitaratu eta eguneratuko du.

39. Artikulua. – Plana ezartzeko irizpideak.

1.– Zibersegurtasunaren arloko jarraitutasun-plana ezartzeko, gutxienez, langileak prestatu eta gaituko dira, eta plana aplikatzeko behar diren bitartekoak eta baliabideak emango dira.

2.– Horretarako, zibersegurtasunaren arloko jarraitutasun-planak irizpide hauek hartuko ditu kontuan:

a) Aurretiazko informazioa: langileentzako informazio-mekanismoak ezarriko dira, bai zibersegurtasun-arriskuei buruz, bai zibersegurtasun-arloko jarraitutasun-planari berari buruz.
b) Jarraitutasun-planari esleitutako langileei prestakuntza teorikoa eta praktikoa ematea zibersegurtasunaren arloan, eta prestakuntza-jardueren programa egokia ezartzea.
c) Behar diren bitarteko eta baliabide ekonomikoak definitzea, hornitzea eta kudeatzea.

40. Artikulua. – Planaren eraginkortasunari eusteko irizpideak.

1.– Aldizkako prestakuntza-jardueren programa egoki bat ezarriko da jarraitutasun-planari esleitutako langileek zibersegurtasunaren arloan prestakuntza teorikoa eta praktikoa izango dutela ziurtatzeko, eta ezagutza horiek eskuratu direla egiaztatzeko sistemak edo moduak ezarriko dira.

2.– Beharrezko bitarteko eta baliabide material eta ekonomikoak mantentzeko programa bat egongo da.

3.– Zibersegurtasun-arloko jarraitutasun-planak ebaluatzeko eta, zibersegurtasun-gorabeheren kasuan, haien efikazia eta eraginkortasuna bermatzeko, probak, ariketak edo simulakroak egingo dira, planak berak ezartzen duen gutxieneko aldizkakotasunarekin, eta, nolanahi ere, gutxienez urtean behin, emaitzak ebaluatuz. Proba horien helburua izango da:

a) Zibersegurtasun-gertakari baten aurrean erantzuteko erakundearen eraginkortasuna.
b) Erantzun-erakundeari esleitutako langileen prestakuntza.
c) Langile guztien entrenamendua zibersegurtasun-gertakari bati erantzuteko.
d) Esleitutako bitarteko eta baliabideen nahikotasuna eta egokitasuna.
e) Jarduteko prozedurak egokiak izatea.

4.– Ariketek edo simulakroek berekin ekarriko dute zibersegurtasunaren arloko jarraitutasun-planean jasotako ekintzak guztiz edo partzialki aktibatzea. Ariketa, simulakro eta probetan, establezimenduaren barneko jarduketa-prozedurak erabiliko dira nagusiki.

5.– Zibersegurtasunaren arloko jarraitutasun-planaren eraginkortasunari eusteko jarduerei buruzko informazioa Agentziaren eskura gordeko da, bai eta egindako ebaluazio-txostenena ere.

41. Artikulua. – Planaren indarraldia eta hura eguneratzeko eta berrikusteko irizpideak.

Zibersegurtasunaren arloko jarraitutasun-planak indarraldi zehaztugabea izango du, behar bezala eguneratuta egongo da eta berrikusi egingo da, baldin eta jarduera edo azpiegiturak aldatzen badira hasierako idazketari dagokionez edo ariketa, simulakro edo proba bat egitearen ondorioen ondorioz, eta, gutxienez, hiru urtean behin.

III. KAPITULUA
ZIBERSEGURTASUNAREN ARLOKO JARRAITUTASUN-PLANEN ERREGISTROA

42. Artikulua. – Sorrera.

1.– Zibersegurtasunaren arloko jarraitutasun-planen erregistroa sortzen da plan horien datu garrantzitsuak inskribatzeko, bai eta betebeharpeko subjektuek dituzten beste zibersegurtasun-neurri batzuk inskribatzeko ere, Agentziari bere eskumenak baliatzeko behar duen informaziorako sarbidea errazteko, bai eta organo eskudunek erregistroaren administrazio-kontrola eta zibersegurtasunaren arloko gainbegiratze- eta ikuskapen-jarduketak egin ahal izateko ere.

2.– Erregistroa Euskal Zibersegurtasun Agentziari atxikitzen zaio, eta agentzia horrek kudeatuko du.

43. Artikulua. – Erregistroaren izaera, funtzioak eta egitura.

1.– Zibersegurtasunaren arloko jarraitutasun-plan bat edukitzeko betebeharra duten jarduera, zentro, establezimendu, espazio, instalazio edo bulegoen titularrek nahitaez inskribatu beharko dute erregistroan, dekretu honen eta aplikatu beharreko araudiaren arabera.

2.– Zibersegurtasunaren arloko jarraitutasun-planen erregistroa ez da publikoa izango. Jardueren, zentroen, establezimenduen, espazioen, instalazioen edo bulegoen titularrek soilik izango dute beren datuetarako sarbidea, beren erregistro-datuei dagokienez, bai eta Agentziak ere, dekretu honetan adierazitako baldintzetan.

3.– Erregistroak eginkizun hauek izango ditu:

a) Zibersegurtasun-arloko jarraitutasun-planei buruzko datuak inskribatzea eta erregistro-zenbaki bat esleitzea.
b) Erregistroko dokumentazioa elektronikoki artxibatzea, babestea eta zaintzea.
c) Zerbitzu publiko eskudunei Erregistroko datuetarako sarbide elektroniko segurua erraztea.
d) Titularrei erregistro-datuetarako sarbide elektroniko segurua ematea.
e) Erregistroko datuak aldian behin eguneratzeko eskatzea.

4.– Erregistroak hiru atal izango ditu:

a) Autobabes-planei buruzko erreferentzia-atala.
b) Zibersegurtasunaren arloko babeserako datu espezifikoen atala.
c) Zibersegurtasun-arloko jarraitutasun-planen atala.

5.– Erregistroa aplikazio-eremuan sartzen diren jardueraren titular, zentro, establezimendu, espazio, instalazio edo bulego bakoitzari dagozkion erregistro-orrien bidez antolatuko da.

44. Artikulua. – Autobabes-planei buruzko erreferentzia-atala.

Atal honetan, erreferentziazko datuak jasoko dira, zibersegurtasun-arloko jarraitutasun-planak dagozkien jarduera, zentro, establezimendu, espazio, instalazio edo egoitzekin

lotzeko, zeinetarako autobabes-plana garatu baita. Informazio hori azaroaren 2ko 277/2010 Dekretuak arautzen duen Autobabes Planen Erregistroan jasota dago (277/2010 Dekretua, azaroaren 2koa, zenbait jarduera, zentro edo establezimenduren autobabes-betebeharrak arautzen dituena, larrialdiei aurre egiteko).

45. Artikulua. – Zibersegurtasunaren arloko babeserako datu espezifikoen atala.

1.– Zibersegurtasun-babesari buruzko datu zehatzei eskainitako atal honek honako hauek barne hartuko ditu:

a) Zibergertakaririk gertatuz gero, titularrarekin harremanetan jartzeko datuak.

b) Titularrak dituen segurtasun- eta jarraitutasun-neurriak.

c) Informazio-sistemen ezaugarri nagusiak.

2.– Jardueraren, zentroaren, establezimenduaren, espazioaren, instalazioaren edo bulegoaren titular berak erabakitzen badu, bere aplikazio-eremuan, zibersegurtasuneko hainbat babes-neurri aplikatzea jarduera, zentro, establezimendu, espazio, instalazio edo bulegoetarako, erregistro-orri bat sortuko da kasu bakoitzerako, erregistro-orri bakoitzean lotuta gera daitezen dagokion autobabes-plana garatu den jarduera, zentro, establezimendu, espazio, instalazio edo bulego bakoitzaren zibersegurtasun-babeserako datu espezifikoak.

46. Artikulua. – Zibersegurtasun-arloko jarraitutasun-planen atala.

1.– Atal honetan, zibersegurtasunaren arloko jarraitutasun-planaren gutxieneko edukiak badaudela, ezarri direla, indarrean daudela eta mantentzen direla egiaztatzeko beharrezkoak diren metadatuak baino ez dira jasoko, eduki tekniko xehaturik jaso gabe. Berariaz, dekretu honen II. eranskinean zehaztutako informazioa jasoko da.

2.– Jardueraren, zentroaren, establezimenduaren, espazioaren, instalazioaren edo bulegoaren titular berak erabakitzen badu, bere aplikazio-eremuan, zibersegurtasunaren arloko jarraitutasun-plan ugari garatzea, erregistro-orri bat sortuko da kasu bakoitzerako, erregistro-orri bakoitzean lotuta gera daitezen dagokion autobabes-plana garatu den jarduera, zentro, establezimendu, espazio, instalazio edo bulego bakoitza.

3.– Planaren berrikuspen, eguneratze edo aldaketa garrantzitsuei buruzko komunikazioak ere inskribatuko dira.

47. Artikulua. – Erregistroaren antolaketa eta funtzionamendua.

Agentziak ezarriko ditu zibersegurtasunaren arloko jarraitutasun-planen erregistroaren funtzionamendurako beharrezkoak diren formulario normalizatuak, irizpide teknikoak eta prozedurak. Horiek guztiek bermatuko dute subjektu interesdunek sarbide telematikoa izatea, bai eta datuen konfidentzialtasuna, segurtasuna eta osotasuna ere.

48. Artikulua. – Izena emateko prozedura.

1.– Zibersegurtasunaren arloko jarraitutasun-plan bat izatera behartuta dauden jarduera, zentro, establezimendu, espazio, instalazio edo bulego bakoitzaren titularrek zibersegurtasunaren arloko jarraitutasun-planen erregistroan inskribatzeko eskatu beharko dute, eta inskriba daitezkeen datuak komunikatu beharko dituzte, dekretu honetan islatzen den nahitaezko dokumentazioarekin batera.

2.– Erregistro-prozedura euskarri elektronikoan baino ez da izapidetuko; horretarako, mekanismoak eta aplikazioak gaituko dira Eusko Jaurlaritzaren egoitza elektronikoaren barruan, eskabidea elektronikoki aurkeztu ahal izateko, behar den dokumentazioa onartutako formatuetan erantsita, interesduna identifikatu ondoren, ziurtapen-zerbitzuen emaileen konfiantzazko zerrendan dauden emaileek emandako sinadura elektronikoko ziurtagiri elektronikoetan oinarritutako sistemen bidez, bai eta gako itunduko sistemen bidez ere.

3.– Inskripzioak erregistroan jasotako datuen deklarazio-ondorioak baino ez ditu izango, eta ez du berez ematen behartuta dauden subjektuek deklaratutako datuen zehaztasunaren, gaurkotasunaren edo zuzentasunaren onarpen edo baliozkotze administratiborik.

49. Artikulua. – Inskribatutako titularren betebeharrak.

1.– Inskribatutako jardueren, zentroen, establezimenduen, espazioen, instalazioen edo bulegoen titularrek etengabe eguneratuta eduki behar dituzte erregistroan jasotako datuak. Horretarako, Agentziari jakinarazi beharko dizkiote gertatutako aldaketak, dagokion informazioa emanez, edo, bestela, telematikoki sartu ahal izango dira haien erregistro-datuetara, identifikazio elektronikoa egin ondoren, egiaztatzeko eta, hala badagokio, eguneratzeko.

2.– Jarduera, zentro, establezimendu, espazio, instalazio edo bulego batek arrisku edo kalteberatasun berezia badu, bere kabuz edo arrisku edo kalteberatasun bereziko inguruneetan egoteagatik, Agentziak, erregistroaz arduratzen den organo gisa, beharrezkotzat, egokitzat eta Erregistroaren xedeetarako proportzionatutzat jotzen den dokumentazio eta informazio gehigarria aurkezteko eskatu ahal izango die jardueraren titularrei, eta, beharrezkoa izanez gero, zibersegurtasunaren arloko jarraitutasun-planaren eduki osoa eskatu ahal izango du.

50. Artikulua. – Erregistroko inskripzioa ezereztea.

Zibersegurtasunaren arloko jarraitutasun-plana erregistroan inskribatu zaion zentroan, establezimenduan, espazioan, instalazioan edo bulegoan garatzen den jarduera amaitutakoan, titularrak idatzoharra ezerezteko eskatu beharko du gehienez ere hilabeteko epean, jarduera amaitzen denetik aurrera.

XEDAPEN GEHIGARRIAK

Lehenengo xedapen gehigarria. Agentziaren zerbitzu-katalogoa.

Agentziak bere Zerbitzuen Katalogoa garatu eta eguneratuko du, Agentziari esleitutako eginkizunak betetzean ematen diren zerbitzuak zehazteko eta antolatzeko tresna operatibo gisa.

Bigarren xedapen gehigarria. Zibersegurtasunaren arloko jarraitutasun-planen erregistroa sortzea.

Dekretu hau indarrean jarri eta hamabi hilabeteko epean, Euskadiko Zibersegurtasunaren arloko Jarraitutasun Planen Erregistroa sortuko du Agentziak.

XEDAPEN IRAGANKORRAK

Xedapen iragankorra. Egokitzeko epeak.

Euskal sektore publikoa osatzen duten entitateek gehienez ere hogeita lau hilabeteko epea izango dute, dekretu hau indarrean jartzen denetik aurrera, beren zibersegurtasuneko barne-esparrua Euskadiko Zibersegurtasun Eredura pixkanaka egokitzeko.

XEDAPEN INDARGABETZAILEA

Xedapen indargabetzaile bakarra.

Indargabetuta geratzen dira lehenengo lehendakariorde eta Segurtasuneko sailburuaren 2024ko ekainaren 7ko Agindua, zeinaren bidez arautzen baita zibersegurtasunaren arloko jarraitutasun-planak egitea EAEko autobabes-arauaren mendeko jarduera jakin batzuetarako, bai eta dekretu honetan xedatutakoaren aurkakoak diren maila bereko edo beheragoko xedapen guztiak ere.

AZKEN XEDAPENAK

Azken xedapena. Indarrean jartzea.

Dekretu hau Euskal Herriko Agintaritzaren Aldizkarian argitaratu eta hurrengo egunean jarriko da indarrean.

I. ERANSKINA SEKTOREEN KATEGORIZAZIOA

Dekretu honen 34. artikuluan aipatzen diren sektoreak honako hauek dira:

1. Energia
    a) Elektrizitatea
    b) Hirietako berokuntza- eta hozte-sistemak
    c) Petrolio gordina
    d) Gasa
    e) Hidrogenoa
2. Garraioa eta logistika
    a) Aireko garraioa
    b) Trenbideko garraioa
    c) Itsasoko eta ibaietako garraioa
    d) Errepideko garraioa
3. Finantzak, bankuak eta finantza-merkatuen azpiegiturak
4. Osasun-sektorea
5. Edateko ura
6. Hondakin-urak
7. Hiri- eta industria-hondakinak
8. Azpiegitura digitala
9. IKT zerbitzuen eta zerbitzu digitalen hornitzaileen kudeaketa
10. Administrazio publikoa
11. Espazioa
12. Posta- eta mezularitza-zerbitzuak
13. Substantzia eta nahaste kimikoak fabrikatzea, ekoiztea eta banatzea
14. Elikagaien ekoizpena, eraldaketa eta banaketa (elikadura-katea)
15. Fabrikazioa
    a) Osasun-produktuen fabrikazioa
    b) Produktu informatikoen, elektronikoen eta optikoen fabrikazioa
    c) Material elektrikoaren fabrikazioa
    d) Makineria eta ekipamenduen fabrikazioa
    e) Ibilgailu motordunen, atoien eta erdiatoien fabrikazioa
    f) Garraiorako beste material batzuen fabrikazioa
16. Ikerketa
17. Eragile ekonomiko garrantzitsuak

II. ERANSKINA ZIBERSEGURTASUNEKO BABESERAKO DATU ESPEZIFIKOAK

Zibersegurtasunaren arloko Jarraitutasun Planei dagozkien metadatuek informazio hau jaso beharko dute:

a) Planaren identifikazio orokorra:
- Jardueraren titularraren identifikazioa.
- Lotutako jarduerak, zentroak, establezimenduak, espazioak, instalazioak edo bulegoak identifikatzea.
- Jarduera-sektorea, I. eranskinaren arabera.
- Zibersegurtasunaren arloko Jarraitutasun Planaren arduraduna identifikatzea.
- Plana zein egunetan egin zen.
- Ezarpen efektiboaren data.
- Azken berrikuspenaren data.
- Aurreikusitako berrikuspen-maiztasuna.

b) Eragiketen plangintza eta kontrola:
- Zibersegurtasunaren arloko Jarraitutasun Planaren plangintza eta kontrol operazionala dagoela adieraztea.
- Planaren irismen orokorra estalitako zerbitzu, prozesu edo sistemei dagokienez.
- Jarraipenerako eta kontrolerako prozedura dokumentatuak egotea.
- Eragiketa-kontrolaren azken barne-egiaztapenaren data.

c) Negozioaren eraginaren azterketa eta arriskuen ebaluazioa:
- Inpaktu-azterketa baten existentziaren adierazpena.
- Zibersegurtasun-arriskuen ebaluazioa dagoela adieraztea.
- Azterketa eta ebaluazioa noiz egin den edo azken aldiz noiz eguneratu den.
- Erabilitako metodologiaren erreferentzia.
- Prozesu, zerbitzu edo sistema kritikoen identifikazio agregatua.

d) Negozioaren jarraitutasunerako estrategiak eta irtenbideak:
- Negozioaren jarraitutasun-estrategia definituen existentziaren adierazpena.
- Hartutako estrategien tipologia orokorra.
- Negozioaren eraginaren analisiaren emaitzekin bat datozen estrategien adierazpena.
- Estrategien onarpen-data edo azken eguneratze-data.

e) Negozioaren jarraitutasunerako planak eta prozedurak:
- Negozioarekin jarraitzeko planak eta prozedurak daudela dioen adierazpena.
- Komunikazio-plan bat izatea krisi-gorabeheren edo -egoeren aurrean.
- Plana aktibatzeko prozedurak egotea.
- Berreskuratzeko prozedurarik dagoen.
- Aktibazioaren eta koordinazioaren arduradunak identifikatzea.

f) Ariketen eta proben programa:
- Zibersegurtasunaren arloko jarraitutasun-planeko ariketen, simulakroen eta proben programa bat izatearen adierazpena.
- Ariketa, simulakro edo proben aurreikusitako aldizkakotasuna.
- Azken ariketaren, simulakroaren edo probaren data.
- Azken ariketaren, simulakroaren edo probaren tipologia.
- Plana berrikusteko adierazpena, ariketa, simulakro edo proba egin ondoren.

III. ERANSKINA JAKINARAZI BEHARREKO ZIBERSEGURTASUN-GERTAKARIAK

Dekretu honetan aipatzen diren jakinarazi beharreko zibersegurtasun-gertakariak horrela definituta daudela ulertu behar da:

1.– Zerbitzuetan ondorio nahasgarri nabarmenak izan ditzaketen gertakariak jakinaraziko dira, eta, ondorio horietarako, taxonomia honen barruan sailkatutakoak hartuko dira kontuan:

   a) Eduki kaltegarria: malware bidezko sistemaren baten infekzioa.

   b) Intrusioa: erasotzaileak sarbidea lortu duen sistema baten konpromisoa.

   c) Erabilgarritasuna: zerbitzua ematean eragina duen gertakaria.

   d) Informazioaren konpromisoa: organizazioaren informazioa baimenik gabe eskuratzea eragin duen gertakaria.

   e) Iruzurra: bitarteko elektronikoak erabiliz kalte ekonomikoa, materiala edo beste edozein eratakoa eragiten duen gertakaria.

2.– Erakundeak garaiz eta behar bezala bidaliko ditu eskatutako hasierako, bitarteko eta amaierako jakinarazpenak, honako denbora-leiho honen arabera:

   a) Hasierako jakinarazpena gertakari baten berri eman eta ohartarazteko komunikazio bat da.

   b) Tarteko jakinarazpena komunikatutako gertakariari buruz une horretan eskuragarri dauden datuak eguneratzeko komunikazio bat da.

   c) Azken jakinarazpena komunikatutako gertakariari buruzko behin betiko datuak zabaltzen eta berresten dituen azken komunikazioa da.

      i. Hasierako jakinarazpena: Berehalakoa.

      ii. Tarteko jakinarazpena: 24-48 ordu.

      iii. Azken jakinarazpena: 20 egun.

3.– Taulan «tarteko jakinarazpenerako» eta «azken jakinarazpenerako» adierazitako denborek «hasierako jakinarazpena» bidaltzen den unea dute erreferentziatzat. «Hasierako jakinarazpenaren» denbora-erreferentzia gertakariaren berri izandako unea da.

4.– Erakundeak, hasierako jakinarazpenean, gertakariari buruz une horretan ezagutzen duen informazio guztia jakinaraziko du. Datu horiek eguneratzen joango dira bitarteko jakinarazpenetan, eta, ondoren, nahitaezkoa izango da gertakariaren azken jakinarazpena egitea. Jakinarazpen guztietan, gutxienez, hemen adierazitako informazio guztia emango da:

   a) Gaia: gertakaria oro har deskribatzen duen esaldia. Eremu hau gertakariari lotutako jakinarazpen guztiek heredatuko dute.

   b) Jarduera-sektorea: energia, garraioa, finantzak, etab. (I. Eranskinaren arabera).

   c) Gertakariaren data eta ordua: ahalik eta zehatzen adierazi noiz gertatu den gertaera.

   d) Gertaera zein egunetan eta ordutan detektatu den: ahalik eta zehatzen adierazi noiz detektatu den gertaera.

   e) Jakinarazpen mota: hasierakoa, tartekoa edo amaierakoa.

   f) Jakinarazpenaren eguna eta ordua: adierazi noiz ari den jakinarazten.

   g) Deskribapena: Xehetasunez deskribatu gertatutakoa.

   h) Eragindako baliabide teknologikoak: gertakariak eragindako aktiboen kopuruari eta motari buruzko informazio teknikoa adieraztea, IP helbideak, sistema eragileak, aplikazioak, bertsioak,... barne.

i) Gertaeraren jatorria: adierazi gertakariaren arrazoia, ezaguna bada. Fitxategi susmagarri bat irekitzea, USB gailu bat konektatzea, web orri maltzur batera sartzea, etab.

j) Taxonomia (sailkapena): Sailkapena eta gertaera mota deskribatutako taxonomiaren arabera.

k) Ekintza-plana eta kontraneurriak: gertakariarekin lotuta orain arte egindako jarduerak. Adierazi jarraitutako ekintza-plana, ezarritako kontraneurriekin batera.

l) Eragina: Adierazi kaltetua enpresa bat edo partikular bat den, eta eraginak esleitutako inpaktu-mailaren arabera.

m) Zenbatetsitako eragin ekonomikoa (ezaguna bada): Gertakariari lotutako kostuak, zuzenak zein zeharkakoak.

n) Hedadura geografikoa (ezaguna bada): tokikoa, autonomikoa, nazionala, nazioz gaindikoa, etab.

o) Kalte erreputazionalak (ezagutzen badira): operadorearen irudi korporatiboari eragitea.

p) Erantsiak: arazoaren arrazoia ezagutzen edo konpontzen laguntzeko eransten diren dokumentuen zerrenda adierazi (pantaila-atzemateak, informazioa erregistratzeko fitxategiak, mezu elektronikoak, etab.).

q) Eragindako erregulazioa: SEN/DBEO/Bestelakoak.

5.– Zibersegurtasuneko gertakari bat jakinarazteak ez du baztertzen edo ordezten beste erakunde batzuei gertaera berengatik egin beharreko jakinarazpena, beren araudi espezifikoaren arabera.

6.– Halaber, Euskal Zibersegurtasun Agentziak zibersegurtasuneko gertakariak prebenitzen, hautematen eta erantzuten lagunduko duen informazioa eman ahal izango du.