XEDAPEN OROKORRAK

SEGURTASUN SAILA

2940

AGINDUA, 2024ko ekainaren 7koa, Jaurlaritzako lehenengo lehendakariorde eta Segurtasuneko sailburuarena, zeinaren bidez arautzen baita zibersegurtasun-arloko jarraitutasun-planak egitea autobabesarako euskal arauaren mende dauden zenbait jardueratarako.

Gaur egungo gizartea interkonektatuta dago, eta informazio-teknologien oso mende.

Garbi dago zibersegurtasun-mehatxuak benetakoak direla, eta horiei aurre egiteko hainbat estrategia eta araudi daude. Aurrerapen teknologikoak oso azkar gertatzen direnez, estrategia horiek etengabe ezarri behar dira.

Askotariko autoritateek dute arlo horretan jarduteko eskumena; beraz, zaila da gidalerroak elkarrekin garatzea. Eusko Jaurlaritza arlo horretan lanean ari da; besteak beste, Cyberzaintza-Euskal Zibersegurtasun Agentzia sortu du segurtasun publikoaren eremuan.

Zibersegurtasun-mehatxu bat dagoenean, lurraldeko funtsezko zerbitzuak arriskuan egon daitezke, eta horrek ondorio negatiboak izan ditzake biztanleengan.

Era berean, apirilaren 27ko 1/2017 Legegintzako Dekretuaren bidez onartutako Larrialdiak Kudeatzeko Legearen testu bateginaren 26. artikuluak aurreikusten duenez, Eusko Jaurlaritzak onartutako babes zibileko planetan exijitu ahal izango da jardueren jarraitutasun-planak prestatu eta ezarri behar direla azpiegitura kritiko eta baliabide nagusi batzuetarako, baldin eta funtsezkoak badira komunitaterako, haren egonkortasun ekonomiko eta sozialerako, eta arrisku larriak edo hondamendiak daudenean azkar leheneratu ahal izateko. Hori adierazten da Euskadiko Herri Babeseko Planean.

Era berean, Larrialdiak Kudeatzeko Legearen testu bategina onartzen duen apirilaren 27ko 1/2017 Legegintzako Dekretuak eta hura garatzeko araudiak autobabesa jorratzen dute prebentzio-neurri eta larrialdiei aurre egiteko euskal sistemarekin lotzeko katebegi gisa.

Larrialdiei aurre egiteko zenbait jarduera, zentro edo establezimenduren autobabes-betebeharrak arautzen dituen azaroaren 2ko 277/2010 Dekretuak –otsailaren 12ko 21/2019 Dekretuak aldatu zuen– autobabes-planak izan behar dituzten jarduerak eta plan horiek egiteko baldintzak jasotzen ditu.

Aurrekoa ikusita, komenigarria dirudi autobabes-planak nahitaez egin behar dituzten oinarrizko eta funtsezko sektoreetako jarduerek zibersegurtasunaren arloko jarraitutasun-planak ere egiteko mekanismoak ezartzea eta plan horiek dokumentu komun bakarrean biltzea.

Hori guztia kontuan izanik,

XEDATZEN DUT:

1. artikulua.– Xedea.

Agindu honen xedea da Euskal Autonomia Erkidegoarentzat lehentasunezkoak diren jarduera, zentro, establezimendu edo azpiegituretako zibersegurtasun-gertakariei aurre egiteko jarraitutasun informatikoko planak arautzea.

2. artikulua.– Aplikazio-eremua:

1.– Agindu honetan xedatutakoa aplikatuko zaie EAEko oinarrizko funtzio sozialak, osasuna, segurtasuna eta ongizate sozial eta ekonomikoa mantentzeko eta EAEko erakundeek nahiz haien administrazio publikoek eraginkortasunez jarduteko funtsezkoak diren sektoreetako jarduerei, baldin eta haien establezimenduren bat 277/2010 Dekretuaren mende badago (277/2010 Dekretua, azaroaren 2koa, Larrialdiei aurre egiteko zenbait jarduera, zentro edo establezimenduren autobabes-betebeharrak arautzen dituena, otsailaren 12ko 21/2019 Dekretuaren bidez aldatua).

2.– Artikulu honen aurreko paragrafoan aipatzen diren sektoreak agindu honen I. eranskinean daude kategorizatuta. Hala ere, segurtasun-arloan eskumena duen saileko titularraren agindu bidez, gerora eguneratu ahal izango dira, Europako Parlamentuaren eta Kontseiluaren 2022ko abenduaren 14ko 2022/2555 (EB) Zuzentarauaren transposizioaren arabera, edota zibersegurtasunaren arloan sektore horiekin zerikusia duen beste edozein araudiren arabera. 2022/2555 (EB) Zuzentaraua Europar Batasun osoan zibersegurtasun-maila eta bateratua bermatzeko neurriei buruzkoa da, 910/2014 (EB) Erregelamendua eta 2018/1972 (EB) Zuzentaraua aldatzen ditu eta 2016/1148 (EB) Zuzentaraua indargabetzen du (SRI 2 Zuzentaraua).

3.– Administrazio publiko eskudunek jarraitutasun-planak egiteko eta ezartzeko eskatu ahal izango diete agindu honen aplikazio-eremuan sartzen ez diren jardueren titularrei, arrisku edo kalteberatasun berezia badute.

4.– Era berean, artikulu honetako 2. eta 3. apartatuetan jasota ez dauden jarduera, zentro, establezimendu edo azpiegituren titularrek, beren borondatez, zibersegurtasuneko jarraitutasun-plan bat egin ahal izango dute, agindu honetan aurreikusitakoaren arabera; horrela, zibersegurtasunari dagokionez, planak nahitaez egin behar dituzten titularren erantzukizun berberak hartuko dituzte beren gain. Hala ere, edozein unetan eta beren borondatez, plana ez egitea eta ez kontrolatzea eskatu ahal izango dute, nahiz eta jarduerarekin jarraitu.

5.– Administrazioaren kontroletik salbuetsita daude Defentsa Ministerioaren, Espetxe Zuzendaritzaren, Segurtasun Indar eta Kidegoen eta Aduana Zaintzaren mendeko zentro, establezimendu edo instalazioak, bai eta organo judizialenak ere.

3. artikulua.– Aplikazio-irizpideak.

1.– Agindu honetan ezarritako zibersegurtasun-betebeharrak gutxieneko arau gisa edo zibersegurtasunaren arloko araudi espezifikoen arau osagarri gisa bete beharko dira.

2.– Agindu honetan aurreikusitako jarraitutasun-planak eta aplikagarria den beste araudi batek ezarritako prebentzio- eta autobabes-tresnak dokumentu bakar batean bateratu ahal izango dira, baldin eta bateratze horrekin saihestu badaiteke informazioa alferrik bikoiztea eta titularrak edo agintaritza eskudunak egindako lanak errepikatzea, betiere agindu honetako funtsezko baldintza guztiak betetzen badira.

4. artikulua.– Betebeharrak.

1.– Agindu honen 2. artikuluan aipatutako jardueren titularren betebeharrak honako hauek dira:

a) Zibersegurtasuneko jarraitutasun-plan bat egitea, zibersegurtasunaren arloan eskumena duen agintaritzak emandako jarraibideen arabera (planaren gutxieneko edukiak agindu honen II. eranskinean jasota daude).

b) Euskadiko Autobabes Erregistrora erregistro-datu hauek bidaltzea:

– Zibersegurtasuneko jarraitutasun-plana egiteko betebeharra.

– Zibersegurtasunaren arloko babeserako datu espezifikoak biltzen dituen fitxa, agindu honen III. eranskinean jasotakoa.

– Titularraren erantzukizunpeko adierazpena, zibersegurtasun-arloko arau guztiak betetzeari buruzkoa. Adierazpen hori eginda, babes zibileko eta larrialdietako agintaritza eskudunek ez dute plan horren edukia gainbegiratu, baliozkotu edo ikuskatuko.

c) Jarraipen-plana eraginkortasunez ezarri eta mantentzeko jarduketak egitea.

d) Jardueraren zibersegurtasun-arloko pertsona fisiko erantzuleak izendatzea, baldin eta titularrak ez badira.

e) Langileak informatzea eta prestatzea planaren edukiei buruz.

f) Jarraipen-planari aurre egiteko beharrezkoak diren baliabide material eta pertsonalak mantentzea.

g) Zibersegurtasun-arloko jarraitutasun-planean aurreikusita dauden neurriak aplikatzea.

h) Ariketak edo simulakroak egitea aldian-aldian.

i) Euskal Zibersegurtasun Agentziari IV. eranskinean jasotako zibersegurtasun-gorabeheren hasierako jakinarazpena egitea –eranskin horretan, zibersegurtasuneko jarraitutasun-planaren gutxieneko edukia zehazten da– Euskadiko Larrialdiak Koordinatzeko Zentroaren bidez (SOS Deiak-112). Horrek ez du eragotziko legeak eskatzen dituen bestelako jakinarazpenak egitea. Geroagoko jakinarazpenak zuzenean egingo zaizkio Euskal Zibersegurtasun Agentziari.

2.– Euskal Autonomia Erkidegoko larrialdien eta babes zibilaren arloko agintaritza eskudunak honako betebehar hauek ditu zibersegurtasuneko jarraitutasun-planei dagokienez:

a) Euskadiko Autobabes Planen Erregistroan atal berezi eta esklusibo bat gaitzea agindu honi lotutako jardueretarako, 2. artikuluaren arabera («Aplikazio-eremua»). Atal horretan, agindu honen III. eranskinean aipatutako zibersegurtasun-arloko babeserako datu espezifikoen fitxa erregistratu beharko da.

b) Agindu honi lotutako jarduerak egiteagatik zibersegurtasuneko jarraitutasun-plan bat gauzatzeko betebeharra dagoela egiaztatzea.

c) Euskal Zibersegurtasun Agentziara bidaltzea Euskadiko Larrialdiak Koordinatzeko Zentroaren bidez (SOS Deiak) jakinarazi diren zibersegurtasun-gorabeherak.

d) Euskadiko Autobabes Erregistroko datuak ongi balidatze aldera, soilik egiaztatuko da bete egiten dela azaroaren 2ko 277/2010 Dekretuaren 22. artikuluan eta 22 bis artikuluan ezarrita dagoena eta zibersegurtasun-arloko jarraitutasun-plana izatea derrigorrezkoa dela (277/2010 Dekretuak arautu zuen zer autobabes-betebehar eska dakizkiekeen zenbait jarduera, zentro edo establezimenduri, larrialdiei aurre egiteko; gerora, aldatu egin zen, otsailaren 12ko 21/2019 Dekretuaren bidez).

3.– Hauek dira Euskal Zibersegurtasun Agentziaren betebeharrak:

a) Zibersegurtasun-arloko jarraitutasun-plana gainbegiratzea eta ikuskatzea.

b) Zibersegurtasun-arloko babeserako datu espezifikoak biltzen dituen fitxa gainbegiratzea eta ikuskatzea.

XEDAPEN GEHIGARRIA

Agindu honen eranskinen edukia, I. eranskina izan ezik, aldatu ahal izango da Euskal Zibersegurtasun Agentziako titularraren ebazpen baten bidez. Ebazpen hori Euskal Herriko Agintaritzaren Aldizkarian argitaratuko da.

XEDAPEN IRAGANKORRA

Agindu honetan jasotako betebeharrak Euskal Herriko Agintaritzaren Aldizkarian argitaratu eta hurrengo egunetik aurrera bete beharko dituzte jarduera, zentro, establezimendu edo azpiegitura berri guztiek. Lehendik daudenei, berriz, gabealdi bat emango zaie, beren autobabeserako plana berrikusteko aldiaren parekoa.

AZKEN XEDAPENA

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

Vitoria-Gasteiz, 2024ko ekainaren 7a.

Jaurlaritzako lehenengo lehendakariorde eta Segurtasuneko sailburua,
JOSU IÑAKI ERKOREKA GERVASIO.

I. ERANSKINA

SEKTOREEN KATEGORIZAZIOA

Hauek dira Aginduaren 2.1 artikuluan aipatzen diren sektoreak:

a) Informazioaren eta komunikazioaren teknologiak.
b) Gobernua eta Administrazio Publikoa.
c) Energia.
d) Elikagaien katea.
e) Azpiegiturak eta garraiobideak eta logistika.
f) Finantzak.
g) Ura.
h) Eragile ekonomiko garrantzitsuak.
i) Osasuna.
j) Hiri- eta industria-hondakinak.
k) Industria-sektore arriskutsuak.
l) Ikerketa.

II. ERANSKINA

ZIBERSEGURTASUNAREN ARLOKO JARRAITUTASUN-PLANAREN GUTXIENEKO EDUKIA

1.– Plangintza eta kontrol operazionala: jardueraren berezko eskakizunak betetzeko beharrezkoak diren prozesuak planifikatu, ezarri eta kontrolatu behar dira, eta arriskuei eta aukerei heltzeko ekintzak ezarri.

2.– Negozioaren eraginaren azterketa eta arriskuen ebaluazioa: etendura baten merkataritza-inpaktua aztertzeko eta arriskuak ebaluatzeko prozesu bat ezarri eta mantendu behar da. Prozesu horretan, testuingurua zehaztu, irizpideak definitu eta etendura baten eragin potentziala ebaluatu behar dira.

3.– Negozioak jarraitutasuna izateko estrategiak eta irtenbideak: negozioak jarraitutasuna izateko estrategiak identifikatu eta hautatu behar dira, negozioaren eraginaren analisiaren eta arriskuen ebaluazioaren emaitzetan oinarrituta. Negozioak jarraitutasuna izateko estrategiek irtenbide bat edo bat baino gehiago izan ditzakete.

4.– Negozioak jarraitutasuna izateko planak eta prozedurak: alderdi interesdun garrantzitsuei ohartarazpen eta komunikazio egokiak egin ahal izateko egitura bat ezarri eta mantendu behar da, eta etendura bat gertatzen denean antolakundea administratzeko planak eta prozedurak eskaini behar dira. Negozioak jarraitutasuna izateko irtenbideak gauzatu behar direnean erabiliko dira planak eta prozedurak.

5.– Ariketa-programa: ariketen eta proben programa bat ezarri eta mantendu behar da, denborak aurrera egin ahala baliozkotu ahal izateko ea eraginkorrak diren negozioak jarraitutasuna izateko estrategia eta irtenbideak.

Euskal Zibersegurtasun Agentziak gida bat egingo du, zibersegurtasunaren arloko jarraitutasun-planaren dokumentuaren egituran oinarritua.

III. ERANSKINA

DATU ESPEZIFIKOEN FITXA

Zibersegurtasunaren arloko babeserako Datu Espezifikoen Fitxak eduki hau izango du gutxienez:

1.– Gorabehera eta alertetarako kontaktu-puntua.

1.1.– Antolakundeko zibersegurtasuneko gorabeherak eta alertak jakinarazteko arduradunaren kontaktu-puntua (izena, helbide elektronikoa eta telefonoa).

1.2.– Bigarren mailako kontaktua, kontaktu-puntu nagusia ez badago (izena, helbide elektronikoa eta telefonoa).

2.– Aplikatutako segurtasun-kontrolak. Honako hauek dituen adieraziko da:

2.1.– Informazioaren segurtasunari buruzko politika orokorra.

2.2.– Informazioaren segurtasunari buruzko politika espezifikoak.

2.2.1.– Eguneratzeak kudeatzeari buruzko politika espezifikoa.

2.2.2.– Pasahitzak kudeatzeari buruzko politika espezifikoa.

2.2.3.– Hornitzaileekiko harremanarekin lotutako informazioaren segurtasunari buruzko politika espezifikoa.

2.3.– Kalteberatasun teknikoen kudeaketa.

2.4.– Informazioaren eta lotutako beste aktibo batzuen inbentarioa: aktiboen identifikazioa.

2.5.– Babes- edo segurtasun-kopiak (backup).

2.6.– Programa maltzurren aurka babesteko mekanismoak. (antibirusa, EDR, etab.).

2.7.– Posta elektronikoa babesteko mekanismoak.

2.8.– Sarea segmentatzeko mekanismoak.

2.9.– Sarea kontrolatzeko mekanismoak (Firewall, IDS, IPS, NAC, etab.).

2.10.– Urrunetik sartzeko mekanismoak (VPN, urruneko mahaigaina, etab.).

2.11.– Aplikazioen segurtasun-mekanismoak (WAF, APIaren segurtasuna, etab.).

2.12.– Faktore anitzeko autentifikazio-mekanismoak.

2.13.– Segurtasun-auditoretza teknikoak.

2.13.1.– Segurtasuneko azken auditoria teknikoaren data.

2.14.– Antolakundeko langileen zibersegurtasunaren arloko kontzientziazioa.

2.14.1.– Langileak zibersegurtasunaren arloan kontzientziatzeko azken ekintzaren data.

2.15.– Zibersegurtasuneko gorabehera bat kudeatzeko ariketa edo simulazioa.

2.15.1.– Zibersegurtasuneko gorabehera bat kudeatzeko azken ariketaren edo simulazioaren data.

2.16.– Zibersegurtasuneko gorabeherei erantzuteko erreferentziazko hornitzaile bat.

IV. ERANSKINA

JAKINARAZI BEHARREKO ZIBERSEGURTASUNAREN ARLOKO GORABEHERA

Honela definitzen dira agindu honetan aipatzen diren jakinarazi beharreko zibersegurtasun-arloko gorabeherak:

1.– Zerbitzuetan nahasmendu nabarmenak eragin ditzaketen gorabeherak jakinaraziko dira. Horretarako, taxonomia honen barruan sailkatutakoak hartuko dira kontuan:

a) Eduki kaltegarria: sistemaren bat malwarez infektatzea.

b) Intrusioa: erasotzaile bat sartzearen ondorioz sistema bat arriskuan jartzea.

c) Erabilgarritasuna: zerbitzua emateari eragiten dion gorabehera bat.

d) Informazioa arriskuan jartzea: antolakundearen informazioa baimenik gabe eskuratzea eragiten duen gorabehera.

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

2.– Entitateak garaiz eta behar bezala bidaliko ditu beharrezkoak diren hasierako, bitarteko eta azken jakinarazpenak, jakinarazpenen denbora-leiho honen arabera:

a) Hasierako jakinarazpena gorabehera baten berri eman eta alerta pizteko komunikazio bat da.

b) Bitarteko jakinarazpena komunikatutako gorabeherari buruz une horretan eskuragarri dauden datuak eguneratzeko komunikazio bat da.

c) Azken jakinarazpena komunikatutako gorabeherari buruzko behin betiko datuak zabaltzeko eta berresteko azken komunikazioa da.

Hasierako jakinarazpena	Bitarteko jakinarazpena	Azken jakinarazpena
Berehalakoa.	24-48 ordu.	20 egun.

3.– Taulan «bitarteko jakinarazpena» eta «azken jakinarazpena» egiteko adierazitako denboren erreferentzia «hasierako jakinarazpena» bidaltzeko unea da. «Hasierako jakinarazpena» egiteko denbora-erreferentzia gorabeheraren berri izan den unea da.

4.– Entitateak, hasierako jakinarazpenean, une horretan gorabeherari buruz duen informazio guztia jakinaraziko du. Bitarteko jakinarazpenetan datu horiek eguneratu egingo dira, eta, ondoren, gorabeheraren azken jakinarazpena egin beharko da. Jakinarazpen guztietan, gutxienez, taula honetan jasotako informazio guztia emango da:

Zer jakinarazi	Deskribapena
Gaia	Gorabehera oro har deskribatzen duen esaldia. Eremu hau gorabeherari lotutako jakinarazpen guztiek heredatuko dute.
Jarduera-sektorea	Energia, garraioa, finantzak, etab.
Gorabeheraren data eta ordua	Ahalik eta zehaztasun handienarekin adierazi noiz gertatu den gorabehera.
Gorabehera detektatu den eguna eta ordua	Ahalik eta zehaztasun handienarekin adierazi noiz detektatu den gorabehera.
Jakinarazpen mota	Hasierakoa, bitartekoa edo azkena.
Jakinarazpenaren eguna eta ordua	Jakinarazpena noiz egiten den adierazi.
Deskribapena	Gertatutakoa zehatz-mehatz deskribatu.
Eragina izan duten baliabide teknologikoak	Gorabeherak eragin dien aktiboen kopuruari eta motari buruzko informazio teknikoa adierazi, IP helbideak, sistema eragileak, aplikazioak, bertsioak… barne.
Gorabeheraren jatorria	Gorabeheraren zergatia adierazi, jakina bada. Fitxategi susmagarri bat irekitzea, USB gailu bat konektatzea, web-orri maltzur batera sartzea, etab.
Taxonomia (sailkapena)	Sailkapen posiblea eta gorabehera mota, deskribatutako taxonomiaren arabera.
Ekintza-plana eta aurre egiteko neurriak	Ordura arte gorabeherarekin lotuta egindako jarduerak. Ezarritako ekintza-plana eta hartutako neurriak adierazi.
Eragina	Eragindakoa enpresa edo partikular bat den adierazi, eta eraginak zehaztu inpaktu-mailaren arabera.
Eragin ekonomiko zenbatetsia (jakinez gero)	Gorabeherarekin lotutako kostuak, zuzenekoak zein zeharkakoak.
Hedadura geografikoa (jakinez gero)	Tokikoa, autonomikoa, nazionala, nazioz gaindikoa, etab.
Ospearen gaineko kaltea (jakinez gero)	Operadorearen irudi korporatiboan duen eragina.
Erantsiak	Arazoaren kausa identifikatzen edo konpontzen laguntzeko zer eranskin gehitzen diren adierazi (pantaila-argazkiak, informazio-erregistroaren fitxategiak, mezu elektronikoak, etab.).
Eragindako erregulazioa	SEN/DBEO/Bestelakoak.

5.– Zibersegurtasuneko gorabehera baten jakinarazpenak ez du baztertzen edo ordezten beste organismo batzuei haien araudi espezifikoaren arabera egin behar zaien jakinarazpena.

6.– Era berean, Euskal Zibersegurtasun Agentziak zibersegurtasuneko gorabeherak prebenitzen, hautematen eta horiei erantzuten laguntzeko informazioa eman ahal izango du.