EUSKO JAURLARITZA GOBIERNO VASCO

SEGURTASUN SAILA
Babes Zibileko Sailburuordetza
Larrialdiei Aurre Egiteko eta
Meteorologiako Zuzendaritza

DEPARTAMENTO DE SEGURIDAD
Viceconsejería de Protección Civil
Dirección de Atención de Emergencias y
Meteorología

Euskadiko Babes Zibilerako Planaren – Larrialdiei Aurre Egiteko Bidea (LABI) – konfigurazio prozedura eskala handiko zibersegurtasun larrialdi baten aurrean.

Aldeko txostena jaso duena, Euskadiko Babes Zibileko Batzordearen 2025eko abenduaren 16ko ohiko bilkuran

Aurkeztua izan dena, Jaurlaritzaren Kontseiluan, 2026ko otsailaren 10ean

AURKIBIDEA

TESTUINGURUA ETA JUSTIFIKAZIOA

Mundu osoan zibersegurtasun-gorabeheren maiztasuna, konplexutasuna eta ondorioak era esponentzialean handitzeak arrisku-paradigma berria sortu du.
Estatuan zein nazioartean metatutako esperientziek, bereziki Estoniako (2007) eta, Ukrainako (2015-2017) oinarrizko zerbitzuen aurkako erasoek eta WannaCry ransomware zibereraso globalak (2017), agerian utzi dute horrelako mehatxuek sektoreko-gaitasunak gainditzen dituzten magnitudea lor dezaketela, eta, ondorioz, biztanleria arriskuan jar dezakeen eta dimentsio anitzeko erantzuna behar duen larrialdia eragin dezakeela, bai ikuspegi teknikotik, bai antolakuntzaren, politikaren, gizartearen eta babes zibilaren ikuspegitik.

Funtsezkoa da zibersegurtasun-gorabeherek gizarte aurreratuetan gero eta eragin handiagoa dutela onartzea, eta, beraz, babes zibilaren ikuspegitik lantzea. Horrek aukera ematen du, lehendik dauden autobabes-planak aldatu beharrik gabe, azken urteetan eskuratutako ezagutzak txertatzeko eta zibereraso batetik eratorritako eskala handiko gertakari baten aurrean, erantzun koordinatua emateko gaitasuna sendotuko duten prozedura espezifikoak izateko. Alde horretatik, Euskadiko Babes Zibileko Lurralde Plana – Larrialdiei Aurre Egiteko Bidea, (aurrerantzean LABI) – erreferentzia estrategikoa da antolamendu-esparru orokor gisa eta larritasun bereziko larrialdietarako plan zuzentzaile gisa, eta prozedura espezifikoak har ditzake, betiere izaera orokorra errespetatuz.

Testuinguru horretan, larritasun handiko zibersegurtasun-gorabeherek babes zibileko larrialditzat hartzeko moduko ezaugarriak dituzte: osasun-, energia-, logistika-, segurtasun-, finantza- edo komunikazio-sistemei aldi berean eragiteko aukera; kaltea hedatzeko abiadura; jatorria berehala esleitzeko zailtasuna; eta herritarrengan eta ordena publikoan izan dezakeen eragina. Beraz, beste arau-esparru espezifiko bat eratu beharrik gabe, egokia da egungo LABIk horrelako larrialdi baten aurrean erantzun koordinatua bermatzeko eskaintzen dituen ikaskuntzei eta aukerei buruz hausnartzea.

Izan ere, azken hamarkadetan indartu egin da larrialdien kudeaketaren ikuspegi integrala, "erresilientzia sistemikoaren" printzipioa txertatuz, bat etortzeko zenbait erakundek emandako jarraibideekin, hala nola, Zibersegurtasunerako Europar Batasuneko Agentziak (ENISA), Europoleko Ziberdelinkuentziaren Europako Zentroak (EC3), Kriptologia Zentro Nazionalak (CCN) edo Zibersegurtasuneko Institutu Nazionalak (INCIBE) emandakoekin. Europar Batasunaren 2020rako Zibersegurtasun Estrategiak eta Espainiako zibersegurtasun-esparruak esplizituki jasotzen dute larrialdi zibernetikoetan gobernantza indartzeko beharra, eta, horretarako, erakundeen arteko simulazio-ariketak eta lankidetza publiko-pribatuko protokoloak sustatzea.
Hala ere, zibersegurtasuneko mekanismo arrunten erantzuteko gaitasuna gainditzen duten eta inpaktu orokorrak eragiten dituzten egoeretan, LABIk erreferentzia-esparru bat eskaintzen du inplikatutako administrazio eta sektore guztiak koordinatzeko.

Gogoratu behar da LABIk erantzun-arkitektura bat ezartzen duela, zuzendaritza bakar eta koordinatu baten inguruan antolatua, euskal administrazio publiko guztien parte-hartzearekin eta tokiko eta estatuko gaitasunak integratzeko aukera ematen duena, beharrezkoa denean. Erakundeen arteko gobernantza-eredu horrek erakutsi du baliagarritasuna Covid-19aren pandemian, eta aukera eman zuen sektore anitzeko inpaktuak dituen osasun-larrialdi sistemikoa kudeatzeko. Pandemia baten eta zibersegurtasun-gorabehera baten ezaugarriak nabarmen desberdinak badira ere, biek dituzte premia edo behar berberak: koordinazioa, egoera aldakorretara azkar egokitzea, herritarrei modu eraginkorrean jakinaraztea eta erabakiak hartzeko euskarri tekniko espezializatuaren edukitzea.

Hala, LABIk zibersegurtasun-gorabeherak larrialdi-tipologia bereizi gisa berariaz jasotzen ez dituen arren, haien esparru malguak aukera ematen du, behar izanez gero, haiek eragindako salbuespenezko egoerak sartzeko.

Oraintsuko larrialdien kudeaketan (pandemia eta zero elektrizitatea, esaterako) lortutako esperientziak agerian utzi du garrantzitsua dela aholkularitza tekniko-zientifikoko egiturak, erakunde arteko koordinazio-foroak eta gizarte-komunikazioko mekanismo sinesgarri eta iraunkorrak izatea. Irakaskuntza horiek baliotsuak izan litezke zibersegurtasun-gorabehera larri baten aurrean ere, baldin eta oinarrizko zerbitzuei edo erakundeen ohiko funtzionamenduari eragiten badie.

Garrantzitsua da adieraztea, Euskadiren kasuan, Zibersegurtasunaren Euskal Estrategiak (2024-2029) eta Euskadiko Segurtasun Publikoaren Plan Orokorrak (2020-2025) esplizituki identifikatzen dutela zibererasoen ondoriozko arriskua hurrengo hamarkadako segurtasun-erronka nagusietako bat dela. Ikuspegi hori bat dator Babes Zibileko Sistema Nazionalaren 17/2015 Legearekin; izan ere, lege horrek aitortzen du beharrezkoa dela sortzen ari diren arriskuak integratzea eta zeharkako prebentzioaren kultura sustatzea. Era berean, 2024ko urritik indarrean dagoen (EB) 2022/2555 Zuzentarauak (NIS2) estatu kideek nazio-mailan gorabehera zibernetikoak kudeatzeko mekanismo egokiak izateko duten betebeharrean sakontzen du, eta azpimarratzen du beharrezkoak direla erantzuteko eta koordinazio estrategikorako planak.

Egungo sistemen interdependentzia teknologikoak berekin dakar zibersegurtasun-gorabehera larri batek domino efektuak izatea, eta sektore-eremua gainditzea, eta koordinazio-mekanismo sendoak beharko direla tokiko, autonomia-erkidegoko, estatuko eta nazioarteko mailetan.

Bestalde, arrisku zibernetikoei buruzko prestakuntza eta kontzientzia sozialaren kultura sustatu behar dela egiaztatu da, babes zibileko beste eremu batzuetan garatu denaren antzekoa. Esperientziak erakutsi du, beste larrialdi batzuetan bezala, aurrea hartzea, prestatzea, etengabeko prestakuntza eta simulazio-ariketak funtsezkoak direla inpaktua arintzeko eta erantzun-denborak murrizteko. Alde horretatik, LABIk antolamendu-aterki gisa jardun lezake, ezohiko larrialdiren bat gertatuz gero, eskura dauden gaitasunak modu ordenatu eta koordinatuan bideratzeko, hori guztia lege-konfigurazioa aldatu eta egitura berriak ezarri beharrik gabe.

Azken batean, zibersegurtasun-gorabeherei lotutako arriskuen hazkunde esponentzialaren aurrean, eta horrek ez du esan nahi LABI aldatu behar denik edo arau-figura berriak sortu behar direnik, komeni da hausnartzea nola aprobetxa daitekeen haren antolamendu-esparrua erreferentzi-oinarri gisa, larrialdi zibernetiko larriko egoeretan erakundeak koordinatzeko. Azken urteotan Euskadin eta Europan metatutako esperientziak erakusten duenez, mehatxuei erantzun eraginkorra emateko funtsezko zutabeak dira aurre hartze estrategikoa,

administrazioen arteko koordinazioa, aholkularitza teknikoa eta herritarrekiko komunikazio gardena. Mehatxuek, ikusezinak izan arren, ondorio ukigarriak, orokorrak eta iraunkorrak izan ditzakete.

1.SARRERA

1997ko ekainaren 24ko 153/1997 Dekretuaren bidez LABI deritzana onartu eta Euskadin larrialdiei aurre egiteko euskal sistemak dituen integrazio-bideak arautu ziren. (Akatsen zuzenketa, 1997ko abuztuaren 8ko EHAA, 148 zk.), (Akatsen zuzenketa, 1998ko urtarrilaren 21eko EHAA, 17 zk.) eta aldatua 2015eko urtarrilaren 13ko 1/2015 Dekretuaren bidez**,** zeinaren bidez onartzen baita berrazterketa berezi bat egitea «Larrialdiei Aurregiteko Bidea-Labi». Deritzan Euskadiko Babes Zibileko lurralde-planean (2015eko urtarrilaren 22ko EHAA, 14 zk.)

Euskal Autonomia Erkidegoko larrialdien kudeaketa antolatzeko oinarrizko tresna da**,** eta, zentzu horretan, Euskadiko plangintzak bete behar dituen irizpide orokorrak ezartzen ditu, bai eta antolaketa-marko orokor edo arrisku anitzeko esparrua ere, plangintza berezirik ez duten eta zuzendaritza edo koordinazio autonomikoa behar duten hondamendi-motako larrialdiei aurre egiteko.

Prozedura honen helburua da zehaztea, segurtasun publikoaren aurkako zibereraso edo zibersegurtasun-gorabehera baten aurrean, eta eskuratutako esperientziaren argitan, antolaketa-marko orokor horren puntu espezifikoak.

Jarraian, LABIren antolaketa-marko orokorraren xedapen orokorrak —beren osotasunean baliodunak—zibersegurtasun-gorabeherak eragindako larrialdi-egoera bati erantzuteko. nola egokitu daitezkeen azaltzen da.

Prozedura honi eranskin gisa gehitzen zaion Babes Zibilerako Planaren dokumentuaren testua eskuragarri dago honako webgunean**:** www.euskadi.eus/112**.**

LABIren idazpurua / atalburuak / atalak, zibersegurtasun-gorabeheraren ondoriozko larrialdi egoeran duten eginkizuna zehazten dutenak:

LABIko IDAZPURUA	Atalburuak / Atalak
Atariko idazpurua	2.- Eginkizunak
	3.- Lege-esparrua
IV. idazpurua. Zuzendaritza eta Koordinazio Arau Orokorrak	3.- Babes Zibileko Agintari Autonomikoak
	3.1.- Segurtasuneko sailburua
	3.2.- Lehendakaria

V. idazpurua. Euskal Autonomia Erkidegoko babes Zibilaren Antolaketa Orokorra	I.atalburua. EAE-KO BABES ZIBILEKO LURRALDE PLANAREN ZUZENDARITZA-EGITURA
	1.- Zuzendaria
	2.- Aholku batzordea
	3.- Informazio kabinetea
	II. atalburua. EKINTZA EGITURA
	Ekintza-taldeak
	2.4.- Eginkizunak eta osaketa
	2.4.1.- Esku-hartzeko taldea
	2.4.2.-Laguntza teknikoko taldea
	III. atalburua. OPERATIBITATEA
	2.EUSKADIKO BABES ZIBILEKO LURRALDE-PLANA AKTIBATZEA
	2.1. Kontzeptua
	2.2. Aplikazio-moduak, larrialdi-fasearen edo-egoeraren arabera
	IV. atalburua. BABES ETA KONPONKETA NEURRIAK
	1.-Babes-neurriak
	2.- Biztanleei informazioa ematea

2. ATARIKO IDAZPURUA

ATARIKO IDAZPURUA, LABIren EGINKIZUNAK atalean xedatutakoa, guztiz aplikagarria izanik, honako funtzio hauek zehazten dira, besteak beste, euskal autonomia erkidegoko biztanlerian eta/edo oinarrizko zerbitzuetan inpaktu handia duten zibersegurtasun-gorabeheren kasuan:

a) EGINKIZUNAK

- Erantzun malgua eta zibersegurtasuneko-gorabeheraren tamainari egokitua eskaintzea, gizartean eragin handia baitu, eta jarduera-ardatz guztiei modu integralean heltzea: euste teknikoa, berreskuratze operatiboa, babes juridikoa eta komunikazio instituzionala.

- Modu prebentiboan eta aurrea hartuta jardutea ahalbidetuko duen jarduera-esparru bat izatea, gorabeheraren ondorioak minimizatzeko eta oinarrizko zerbitzuen jarraitutasuna eta ehun sozioekonomikoaren erresilientzia bermatzeko.

- Sailen arteko eta erakundeen arteko parte-hartze eta koordinazio egokia bermatzea euskal administrazio guztien artean (LABI), bai eta-eraginpeko erakunde publiko eta pribatuekin edo oinarrizko azpiegituren arduradunekin ere.

- Indarrean dauden zibersegurtasuneko estrategiei euskarria ematea, informazio-sistemetako zibererasoen edo zibersegurtasun-gorabeheren ondoriozko larrialdi-egoeretan jarduketa teknikoak eta estrategikoak koordinatzea errazagoa izan dadin.
- Argi eta garbi definitzea jarduera-mailak (analisia eta diagnostikoa, neurrien proposamena, erabakiak hartzea) eta horietako bakoitzaren erantzukizunak, bai eta arrisku-egoeren aurrean antolatu behar diren erantzun-ildoak ezartzea ere.

- Antolamendu-egitura bat aurreikustea.

- Goragoko mailako plan eta prozedurekin erabateko koordinazioa ziurtatzea, autonomia-eremutik haragoko gorabeherei erantzuteko aktibatu ahal izateko.

b) LEGE-ESPARRUA

ATARIKO IDAZPURUAN, LABIren LEGE ESPARRUA atalean jasotako lege-erreferentziez gain, zibersegurtasunaren arloan aplikatzekoak diren xedapen hauek zerrendatzen dira:

Estatua

- 40/2015 Legea, urriaren 1ekoa, Sektore Publikoaren Araubide Juridikoarena.

- 12/2018. Errege Lege Dekretua, irailaren 7koa, Informazio Sare eta Sistemen. Segurtasunarena.

- 3/2018 Lege Organikoa, abenduaren 5ekoa, Datu Pertsonalak Babestekoa eta Eskubide Digitalak Bermatzekoa.

- 17/2015 Legea, uztailaren 9koa, Babes Zibileko Sistema Nazionalari buruzkoa.

- 6/2020 Legea, azaroaren 11koa, konfiantzazko zerbitzu elektronikoen zenbait alderdi arautzen dituena.

- (EB) 2022/2555 Zuzentaraua, Europar Batasun osoan zibersegurtasun-maila komun handia bermatzeko neurriei buruzkoa (NIS2 Zuzentaraua).

Euskadi

- 7/1981 Legea, ekainaren 30ekoa, Jaurlaritzari buruzkoa.

- 7/2023 Legea, ekainaren 29koa, Euskal Zibersegurtasun Agentzia sortzekoa.

3. ARRISKUEN ETA GERTAKARI GARRANTZITSUEN IDENTIFIKAZIOA

Zibersegurtasunaren eremuko arriskuak identifikatzeko, Euskal Autonomia Erkidegoko informazio-sistemei, azpiegiturei eta oinarrizko zerbitzuei eragin diezaieketen mehatxuen eta kalteberatasunen ebaluazio sistematikoa egin behar da.

Digitalizazio maila altua eta mendekotasun teknologiko handia duen testuinguruan, euskal gizartea, bere erakundeak eta enpresa-sarea ziberespazioan hainbat arriskuren menpe daude, eta horien artean nabarmentzen dira, besteak beste:

- Azpiegitura eta oinarrizko zerbitzuen aurkako erasoak (energia, ura, osasuna, garraioa, telekomunikazioak, etab.).
- Akats teknikoek, ahultasun posibleek eta/edo giza erroreek eragindako gertakariak.
- Teknologiaren bilakaerarekin lotutako mehatxu berriak, hala nola IoT gailuen erabilera masiboa, adimen artifizialaren hedapena edo sistema industrialen (ICS/SCADA) arteko interkonexioa.
- Zibereraso iraunkorrak eta oso sofistikatuak (APT).
- Ransomware eta estortsio digitala, zeinetan erasotzaileek datu garrantzitsuak enkriptatu eta haien askapenerako ordainketak eskatzen dituzten.
- Ekintza maltzurrak, hala nola sabotajeak, iruzur elektronikoak, informazio-lapurretak edo desinformazio-kanpainak.

Hala ere, arrisku edo gertakari horiek guztiak ez dute LABI aktibatzea ekarriko. Herritarren normaltasunean eragin handia duten zibersegurtasun-gertakariek soilik eragin dezakete LABI aktibatzea, prozedura honetan ezarritakoaren arabera, baldin eta oinarrizko azpiegiturei eragiten badiete, oinarrizko zerbitzuakl arriskuan jartzen badituzte edo babes zibileko larrialdi bat sortzen badute.

4. ZUZENDARITZA ETA KOORDINAZIOA ARAU OROKORRAK

Segurtasun Publikoa, Larrialdiak eta Babes Zibila arloko eskumena duen Sailaren titularrari dagokio LABIren zuzendaritza bakarra eta koordinazioa, baita larrialdi zibernetiko egoeretan ere, Lehendakariak eskumen horiek bere gain hartzea galarazi gabe, Larrialdien Kudeaketari buruzko Legearen testu bategina onartzen duen 2017ko apirilaren 27ko 1/2017 Legegintzako Dekretuan xedatutakoaren arabera.

Zuzendaritza hori LABI aktibatzeari lotuta egongo da, titularrak berak egindako eskaeraren bidez, Cyberzaintzaren eskaeraren bidez edo larrialdia ikusita, gertakari zibernetiko baten larritasunaren, hedaduraren edo eraginaren arabera, herritarren segurtasunari eragiten dioten zerbitzu eta azpiegitura funtsezkoak edo sistema publikoen funtzionamendu normala arriskuan jar dezakeenean.

Aktibazioa Cyberzaintzak egindako ebaluazio teknikoaren ondoren deklaratuko da, eta hark Larrialdien Arreta eta Babes Zibila arloko eskumena duen Sailaren titularrari jakinaraziko dio gertakariaren izaera, eta honek ebaluatuko du prozedura honetan ezarritako irizpideak betetzen diren ala ez zibersegurtasuneko larrialdia deklaratzeko.

Aurretik esandakoa galarazi gabe, LABIren IV. Idazpurua (ZUZENDARITZA ETA KOORDINAZIOA ARAU OROKORRAK) zibereraso baten ondoriozko larrialdiari aurre egiteko xedatutakoa honako kontu hauek hartuko ditu aintzat.

Ziberlarrialdiko egoeretan, eta prozedura honetan ezarritakoaren arabera, Eusko Jaurlaritzaren Zibersegurtasun Agentziak ere ebaluazio teknikoa egin beharko du, eta gertakariaren izaerari, eraginari eta larrialdiak izan dezakeen bilakaerari buruzko informazioa emango du. Testuinguru horretan, plana dagokion fasean eta egoeran aktibatu ahal izango da, eta, hala, beharrezko baliabide eta bitartekoen koordinazioa eta mobilizazioa bermatuko da.

Larrialdiak irauten duen bitartean, eta haren konplexutasun berezia, izaera sistemikoa edo erakundeen arteko eragina kontuan hartuta, Lehendakariak LABIren jardueren zuzendaritza bakarra eta koordinazio estrategikoa bere gain hartu ahal izango du, alarma egoera deklaratuz gero Estatuaren ordezkari gisa dagokion eskumenak galarazi gabe. Esleipen hori Larrialdien Kudeaketari buruzko Legearen 35. artikuluaren, Gobernuari buruzko 1981eko ekainaren 30eko 7/1981 Legearen 8. artikuluaren eta larrialdi egoerei aplikatu beharreko Estatuaren araudi espezifikoaren babesean gauzatuko da, hala nola Sektore Publikoaren Araubide Juridikoari buruzko 2015eko urriaren 1eko 40/2015 Legearen babesean

5. BABES ZIBILAREN ANTOLAKETA MARKO OROKORRA AUTONOMIA ERKIDEGOAN

LABIren V. Idazpuruan, EUSKAL AUTONOMIA ERKIDEGOKO BABES ZIBILAREN ANTOLAKETA OROKORRA, I. ATALBURUAN (ZUZENDARITZA-EGITURA)) ETA II. ATALBURUAN (EKINTZA-EGITURA) ezarritakoa errespetatuz, prozedura honetan ezarritakoaren arabera zibersegurtasun-gorabehera baten ondoriozko larriladi bati aurre egiteko.

Aipatutako kontsiderazioez gain, jarduteko eredu bat planteatzen da, bi jarduera-maila dituena. Lehenengoa, berez erabakitzekoa, zuzendariaren funtzioak zehaztuta eta euskal erakunde guztien eta Komunikazio Arloaren ordezkaritza izango duen Aholku Kontseilua. Bigarrena, teknikoa, Zibersegurtasuneko Batzorde Espezializatu baten inguruan antolatuko dena, eta mehatxua ebaluatzeaz, arriskuak aztertzeaz, eszenarioak aurreikusteaz eta Aholku Kontseiluari erantzun-neurrien proposamenak egiteaz arduratuko dena.

Aholku Kontseilua larrialdiaren kudeaketan zuzenean inplikatutako Eusko Jaurlaritzako departamentuen ordezkariek osatuko dute, eta, hala badagokio, beste erakunde publiko batzuetako ordezkariek ere bai (estatuko, autonomiako, tokiko mailakoak), gertaeren izaeraren eta hedaduraren arabera.

Batzorde Teknikoa Euskadiko Babes Zibileko Lurralde-Planaren zuzendariak izendatuko du, eta, besteak beste, Zibersegurtasunaren Euskal Agentziako teknikariak izango dira kide.

Prozedura honen esparruan, eta bereziki zibersegurtasuneko larrialdietarako, Batzorde Teknikoaren Koordinatzailearen figura aurreikusten da. Pertsona hori Planaren Zuzendaritzak izendatuko du, eta bere eginkizuna izango da Batzordearen lanak antolatzea, kideak koordinatzea eta Aholku Kontseiluari egindako txostenak eta proposamenak helaraztea.

Era berean, parte hartu ahal izango dute zibersegurtasunean, mehatxuen analisia, jarraitutasun operatiboan eta gorabehera konplexuei erantzuteko erakunde publiko zein pribatuetan aritzen diren adituek, zibersegurtasuneko gorabeheraren izaeraren eta ezaugarrien arabera.

a) ZUZENDARITZA EGITURA

i. ZUZENDARIA

Zibersegurtasuneko gertakarietatik eratorritako larrialdien kasuan, Planaren Zuzendariari dagokio, aurreikusitako funtzio orokorrez gain, honako erantzukizun espezifikoak bere gain hartzea:

- Aholku Kontseiluko kideak, Batzorde Teknikoaren Koordinatzailea eta hura osatuko duten adituak izendatzea.

- Batzorde Teknikoa osorik edo zati batean deitzea, ziberintzidentearen motaren eta larritasunaren arabera.

- Herritarrekin eta erakundeekin komunikazio argia, gardena eta koordinatua bermatzea, bai gertakariaren eraginari dagokionez, bai hartutako neurriei dagokienez.

- Komunikazio eta informazio arloa osatzea.

- Beste autonomía-erkidego batzuekin eta Estatuko organoekin koordinatzea, horretarako ezarritako organoen bidez, neurri koherente eta egokienak hartzeko helburuarekin.

- Zerbitzu eta azpiegitura funtsezkoen babesa bermatzeko erantzunaren artikulazioa ezartzea, mehatxuen zaintza, detekzio eta neutralizazioari, berreskurapen operatiboari eta oinarrizko zerbitzuen jarraitasunari dagokionez.

- Krisi larri eta luzearen aurrean, erabakiak hartzeko irizpide-hierarkia ezartzea, lehentasuna emanez biztanleriaren babesari, erakundeen jarraitasunari eta oinarrizko zerbitzuen funtzionamenduari, oreka bilatuz eta sortutako inpaktua baloratzeko.

- Zer informazio helaraziko den zehaztea: gardentasuna, adierazleak eta, kasuak, eremu kritikoen arabera.

- Ekonomiari eta enplegu-galerei eragindako kalteak arintzeko eta berreraikuntza sozioekonomikoa sustatzeko erantzunaren antolaketa ezartzea.

ii. AHOLKU-BATZORDEA

Aholku Batzordea larrialdiaren kudeaketan zuzenean inplikatutako Eusko Jaurlaritzako sailetako ordezkariek osatuko dute, bai eta, hala badagokio, autonomía-, foro- edo toki-eremuko beste erakunde publikoetako ordezkariek ere, gertakariaren izaera eta eraginaren arabera.

Oinarrizko osaerak honako hauek barne hartuko ditu, besteak beste:

- Lehendakaritza / Eusko Jaurlaritzako bozeramailetza.
- Segurtasun-alorrean eskumena duen saila.
- Ertzaintzaren Zuzendaritza.
- Larrialdiei eta Meteorologiari Arreta emateko Zuzendaritza.
- Cyberzaintzaren Zuzendaritza.
- Hiru foro-aldundietako ordezkariak.
- Euskadiko Udalen Elkartearen (EUDEL) ordezkaria.
- Lurralde historikoetako hiru hiriburuen ordezkaritza instituzionala.
- EAEko Gobernuaren Ordezkaritzako ordezkari bat.
- Gobernantza publiko eta digitalaren eskumena duen saila.
- Osasun-alorreko eskumenak duen saila, gertakariak osasun zerbitzuetan eragina badu.
- Ekonomia eta Ogasuna, Industria eta Energia, Osasuna, Hezkuntza eta Zientzia, eta beste sail batzuk, gertakariaren izaerak eragin ditzakeenak.

Planaren zuzendariak beste arduradun instituzional edo zuzendaritza-organo batzuk ere gehitu ahal izango ditu, gertakariaren bilakaeraren eta eraginaren arabera.

iii. INFORMAZIO-KABINETEA

Komunikazioak Babes Zibileko Planaren informazio-kabineteak gidatuko ditu. Larrialdia irauten duen bitartean informazioaren kanal ofiziala izango da, eta besteak beste, honako funtzio hauek izango ditu:

- Herritarrei eta erakundeei aldian-aldian gertakariaren bilakaeraren eta hartutako neurrien berri ematea.

- Informazio publikoaren gardentasuna, argitasuna eta irisgarritasuna bermatzea, eta desinformazioaren edo zurrumurruaen aurka egitea talde espezializatuekin lankidetzan.

- Autoprotekzio digitalari, oinarrizko segurtasunari eta praktika egokiei buruzko gomendioak zabaltzea enpresentzat, erakundeentzat eta herritarrentzat.

- Beharrezkotzat jotzen bada, informazioa eta zibersegurtasuneko alertak zabaltzeko teknologia eta aplikazio espezifikoen erabilera sustatzea.

b) EKINTZA EGITURA

LABIren II. Atalburuan larrialdiak kudeatzeko ekintza-egituraz ezarritakoari kalterik egin gabe, zibersegurtasuneko gertakari batek prozedura honetan definitutako larritasun-irizpideak betetzen baditu, erantzun teknikoa eta koordinazio instituzionala sendotuko dituzten antolaketa-elementu espezifikoak aurreikusten dira.

Horren harira, Aholku Batzordearen mendeko Batzorde Teknikoa eratuko da, Planaren zuzendariari laguntza tekniko eta espezializatua emateko organo nagusi gisa. Helburua da larrialdiari ikuspegi zeharkako eta sektore anitzekoa eskaintzea, ezagutza teknikoa, operatiboa eta instituzionala behar bezala integratuz. Batzordeak analisi, diagnostiko eta proposamenen nukleo gisa jarduten du, eta gertakariaren bilakaeraren ikuspegi orokorra eta denbora errealean ulertzea errazten du, baita egon daitezkeen arrisku-egoerak ulertzea ere.

Batzorde Teknikoak bere eginkizunen artean ditu larrialdiaren bilakaerari buruzko txosten teknikoak egitea, kontrastatutako datuetan eta adierazle garrantzitsuetan oinarrituta, eta Planaren Zuzendaritzari jarduera-proposamenak formulatzea. Proposamen horiek koordinazio interinstituzionalaren, bideragarritasun operatiboaren eta koherentzia estrategikoaren irizpideei erantzun beharko diete, eta ziberlarrialdiei aurre egiteko jarduketa-ardatzetan kokatuko dira: zerbitzu erabakigarrien jarraitutasun operatiboa, sistemen eta sareen segurtasuna, eta herritarrak eta kaltetutako erakundeen babesa.

Organo hau gaiaren arabera egituratuko da, gertakariaren izaerari eta eragin motari lotuta. Zibersegurtasunean, arrisku teknologikoen kudeaketan, oinarrizko azpiegituren babesean, datuen analisiaren eta jarraipen operatiboaren arloetan esperientzia duten teknikariek osatuko dute.

Era berean, administrazioko arlo giltzarrietako eremu arduradun operatiboek parte hartu ahal izango dute kide tekniko gisa, eta aditu-taldeen laguntza espezializatua izan dezakete, erantzun eraginkor eta koordinatua bermatzeko.

Antolaketa-diseinu hau malgua da eta zibesegurtasun-gertakariaren ezaugarrietara eta bilakaerara egokituko da. Planaren zuzendariak beharrezkoak diren beste kide batzuk izendatu ahal izango ditu eta, egokitzat jotzen duenean, kanpoko profesional eta adituei deialdia egingo die, haien ekarpena garrantzitsutzat hartzen bada.

6. OPERATIBITATEA

Prozedura honetan deskribatutako zerbitzu publikoetan eragina izan dezakeen zibersegurtasun-gorabehera bat detektatzen bada, zibersegurtasun Euskal Agentziak alerta tekniko preliminarra igorriko du, ezarritako arrisku-balorazio prozedurak aktibatuz. Alerta honek ez du automatikoki aktibatzen Euskadiko Larrialdiei Aurre Egiteko Plan Territoriala, baina abisu instituzional formalaren lehen maila da, eta hortik aurrera aztertuko da plana bere fase eta egoera operatiboetan aktibatzeko beharra.

LABIren V. idazpuruko (EUSKAL AUTONOMIA ERKIDEGOKO BABES ZIBILAREN ANTOLAKETA OROKORRA), III. Atalean (ATAZAK), ezarritakoa eragotzi gabe, eskala handiko zibersegurtasun-gertakari baten ondoriozko larrialdi bati aurre egiteko, jarraian azaltzen direnak ere hartuko dira kontuan.

EUSKADIKO BABES ZIBILEKO LURRALDE-PLANAREN AKTIBAZIOA

Euskadiko Babes Zibileko Lurralde-Plana aktibatzea gertakari teknikoaren analisiaren arabera egingo da, Euskal Zibersegurtasun Agentziak egindakoa, eta baldin eta oinarrizko zerbitzuen jarraipena larriki arriskuan egon daitekeela uste bada, Euskadiko lurraldean eraso deliberatu, akats sistemiko edo mehatxu baten ondorioz, sistema teknologiko garrantzitsuetan eragin nabarmena izanik.

Larrialdi-fase eta -egoeren araberako aplikazio-modalitateak, gertakariaren izaeraren, haren bilakaeraren eta kaltetutako lurralde-edo sektore- zehatzaren mende egongo dira, Euskadiko Babes Zibilerako Planaren testu nagusiko III. atalburuan, **ERAGINKORTASUNA** izenekoan, xedatutakoaren arabera. Elementu hauek baloratuko dira, besteak beste, oinarrizko zerbitzuetan (osasuna, energia, garraioa, komunikazioak, larrialdiak) funtzionaltasuna galtzea, oinarrizko azpiegituren integritatearentzako arriskua, eta gertakariaren inpaktu sozial edo instituzionala.

LABIren Zuzendaritza bakarra eta koordinazioa Lehendakariak bere gain hartzeak, testuinguru honetan, Euskadiko Babes Zibileko Planaren larrialdi-faseko 2. edo 3. egoera deklaratzea ekarriko du.

2. edo 3. egoerako, zibersegurtasun-gertakari baten aurrean Babes Zibileko Plana aktibatzeak, eta Lehendakariak Zizendaritza bere gain hartu duenean, eraginpeko erantzun-plan sektorialak edo espezifikoak integratzea ekarriko du. Erakunde eskudunak Aholku Batzordean ordezkatuta egongo dira, LABIn dagoeneko aurreikusitako baldintza eta eginkizunekin, eta ez da planean inolako aldaketarik egin beharko.

7.BABES ETA KONPONKETA NEURRIAK

LABIren V. Idazpuruan, **EUSKAL AUTONOMIA ERKIDEGOKO BABES ZIBILAREN ANTOLAKETA MARKO OROKORRA**, eta bere IV. kapituluan, **BABES ETA KONPONKETA NEURRIAK**, ezarritakoa eragotzi gabe, dokumentuan katalogatutako **zibersegurtasun-**

gorabehera baten ondoriozko larrialdi bati aurre egiteko, jarraian azaldutakoak diren ere hartuko dira kontuan.

a)KUDEAKETA ARLOAK

Ziberintzidentearen kudeaketarako arloak proposatzen dira, babes eta konponketa neurriak artikulatzeko:

- Informazio publikoaren komunikazio eta kudeaketa.
- Eraginaren analisia eta kaltetutako sistemen identifikazioa.
- Erantzun teknikoaren kudeaketa eta edukiera.
- Larrialdiaren ebazpena.
- Oinarrizko zerbitzuen berrezarpena.
- Zibersegurtasun instituzionala eta operatiboa.
- Erantzun antolatua erakundeen arteko koordinazioan.

Arlo horiek LABIn dagoeneko aurreikusita daudenen osagarri gisatzat hartzen dira eta kasuan kasuko gertakariaren izaerara eta irismenera egokitu beharko dira, Zibersegurtasun Euskal Agentziarekin koordinatuta.

b)BIZTANLEEI INFORMAZIO EMATEA

LABIren **BIZTANLEEI INFORMAZIO EMATEA** atalean ezarritakoa eragotzi gabe, zibersegurtasun-gorabehera baten ondoriozko larrialdiari aurre egiteko, jarraian azaltzen diren kontsiderazioak hartuko dira kontuan:
Herritarrei informazioa emango zaie, besteak beste, hauei gaiei buruz:

- Nola jokatu balizko afekzioen aurrean.
- Ziberhigiene eta oinarrizko autoprotekzio digitalerako aholkuak.
- Herritarrentzako arreta eta kontsulta kanalak.
- Zerbitzu publikoak etetearen ondorioz kaltetutako biztaleentzako behin-behineko eta alternatiboko irtenbideak eta alternatibak.
- Gertakariaren inpaktua murrizteko dibulgazio-materiala.

Era berean, **erantzun antolatua eta instituzionala azaltzen duen planaren gizarte-dibulgazioa** sustatuko da, erresilientzia-mekanismoak ulergarriago egiteko eta erantzukizun digitala bultzatzeko neurri garrantzitsu gisa. Horretarako:

- Informazioaren teknologiak (aplikazioa mugikorrak, jakinarazpen masiboak, alerta digital goiztiarrak) komunikazio eta alerta tresna gisa erabiltzea baloratuko da, egoki iritziz gero.

- Biztanleen profil digitalen aniztasunari erreparatuko zaio, eta mezuen ulermen-maila aztertuko da (adinaren, gaitasun digitalen, gizarte-zaurgarritasunaren arabera) edukiak modu eraginkor eta irisgarrian egokitzeko.