cyber zaintza
BASQUE CYBERSECURITY AGENCY

Zibersegurtasun-arloko jarraitutasun-planaren gida

2025eko azaroa

EUSKO JAURLARITZA
GOBIERNO VASCO

Aurkibidea

1 Dokumentuaren Kontrola

SINADUREN KONTROLA

	Izen-Abizena/Kargua	Data	Sinadura
Egilea:			

Oneslea:

BERTSIOEN KONTROLA

Bertsioa	Onarpen Data	Aldaketen kontrola
1.0	2025eko azaroa	Dokumentuaren 1. bertsioa

2 Sarrera

Hain interkonektatuka dagoen gizarte honetan, gero eta ohikoagoa da teknologia berriekiko eta informazio-sistemekiko mendekotasuna. Mendekotasun horrek, era berean, zibermehatxuen hazkunde handiagoa eragiten du, gorabehera txikietatik hasi eta informazioaren eskuragarritasuna, osotasuna eta konfidentzialtasuna arriskuan jartzen duten eraso sofistikatuetara arte.

Egoera honetan, ezinbestekoa da zibersegurtasunaren jarraipen-plan bat edukitzea, erresilientzia operatiboa bermatzeko. Modu horretan, funtsezko zerbitzuetan eta, horrenbestez, EAEko gizartean eta herritarrengan eragina izan dezaketen gorabeheren inpaktua murrizteko estrategia integral gisa jokatzen du plan horrek.

Botere publikoek bizitza eta segurtasuna babesteko konpromisoa dute; ez bakarrik larrialdietan erantzunez, baita horiei aurre hartuz ere. Gainera, funtsezkoa da herritarrek zibersegurtasunaren arriskuen berri izatea eta segurtasuna eskubide zein erantzukizun partekatua dela ulertzea.

Larrialdien eta Babes Zibilaren kudeaketari buruzko araudiak eta erregulazioak autobabes-planak izatera behartzen ditu sektore jakin batzuk, bereziki erakundeek ematen dituzten jarduerek larrialdiak eragin baditzakete edo izan baditzakete; beraz, ezinbestekoa da pertsonen bizitza eta segurtasuna babesteko planak izatea.

Horregatik, zibersegurtasunaren jarraipen-plan sendo bat ezartzeak erakundeek segurtasunaren eta arriskuen kudeaketaren aurrean duten konpromiso proaktiboa islatzen du. Horrek, gainera, aukera ematen du azkar eta koordinatuta erreakzionatzeko balizko eraso, eten edo akats teknologikoen aurrean. Halaber, aktibo kritikoak identifikatzea eta lehenestea, erantzukizunak argi esleitzea eta inplikatutako taldeen prestakuntza eraginkorra sustatzen ditu.

EAEn, Eusko Jaurlaritzak agindu bat garatu eta onartu du zibersegurtasunaren arloko jarraipen-planak egiteko beharra arautzeko, autobabeserako EAEko arauaren mendeko jarduera jakin batzuetarako.

Gida hau edozein erakunderi zibersegurtasunaren arloko jarraipen-plana modu argi, erraz eta eraginkorrean egiten, ezartzen eta mantentzen laguntzeko diseinatu da. Planaren funtsezko edukiak honako alderdi hauek jaso beharko ditu:

- Eragiketen plangintza eta kontrola.
- Eraginaren analisia eta arriskuen ebaluazioa.
- Negozioarekin jarraitzeko estrategiak.
- Larrialdietako prozedurak.
- Simulakroak eta ariketak.

3 Erreferentziazko araudia

Aplikatu beharreko erreferentziazko araudia honako hau da:

- Agindua, 2024ko ekainaren 7koa, lehenengo lehendakariorde eta Segurtasuneko sailburuarena, zeinaren bidez arautzen baita zibersegurtasunaren arloko jarraipen-planak egitea autobabeserako EAEko arauaren mendeko jarduera jakin batzuetarako.
- 1/2017 Legegintzako Dekretua, apirilaren 27koa, Larrialdiak Kudeatzeko Legearen testu bategina onartzen duena.
- 277/2010 Dekretua, azaroaren 2koa, zenbait jarduera, zentro edo establezimenduren autobabes-betebeharrak arautzen dituena, larrialdiei aurre egiteko.
- 21/2019 Dekretua, otsailaren 12koa, zeinaren bidez bigarrenez aldatzen baita zenbait jarduera, zentro edo establezimenduren autobabes-betebeharrak arautzen dituen dekretua, larrialdiei aurre egiteko.
- 2022/2555 (EB) Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2022ko abenduaren 14koa, Batasun osoan zibersegurtasun-maila komun handia bermatzeko neurriei buruzkoa, 910/2014 (EB) Erregelamendua eta 2018/1972 (EB) Zuzentaraua aldatzen dituena eta 2016/1148 (EB) Zuzentaraua indargabetzen duena (SRI 2 Zuzentaraua).

4 Helburua

Gidaren helburua da erreferentzia-esparru integral bat ezartzea, erakundeei zibersegurtasunaren arloko jarraipen-planak egiteko, ezartzeko eta eraginkortasunez mantentzeko beharrezkoak diren gutxieneko jarraibideak eta irizpideak identifikatzen, egituratzen eta aplikatzen laguntzeko. Horrela, zibersegurtasun-gorabeheren aurrean erresilientzia operatiboa eta indarrean dagoen araudia betetzen direla bermatuko da.

5 Irismena

Gida hau arau hauen aplikazio-eremuan sartzen diren jarduerak egiten dituzten erakunde guztiei zuzenduta dago:

- 277/2010 Dekretua, azaroaren 2koa, zenbait jarduera, zentro edo establezimenduren autobabes-betebeharrak arautzen dituena, larrialdiei aurre egiteko.
- Agindua, 2024ko ekainaren 7koa, lehenengo lehendakariorde eta Segurtasuneko sailburuarena, zeinaren bidez arautzen baita zibersegurtasunaren arloko jarraipen-planak egitea autobabeserako EAEko arauaren mendeko jarduera jakin batzuetarako.

6 Planaren edukia

2024ko ekainaren 7ko Aginduan ezarritakoaren arabera, zibersegurtasuneko jarraitutasun-plan baten gutxieneko edukia, II. eranskinean jasotakoa, honako hau da:

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

2. Negozioaren inpaktuaren azterketa eta arriskuen ebaluazioa: merkataritza-inpaktua aztertzeko eta etete-arriskuak ebaluatzeko prozesu bat ezarri eta mantendu behar da, testuingurua ezartzeko, irizpideak definitzeko eta eten batek izan dezakeen inpaktua ebaluatzeko.

3. Negozioaren jarraitutasunerako estrategiak eta irtenbideak: negozioaren jarraitutasun-estrategiak identifikatu eta hautatu behar dira, negozioaren inpaktuaren analisiaren eta arriskuen ebaluazioaren emaitzetan oinarrituta. Negozioarekin jarraitzeko estrategiek irtenbide bat edo gehiago izan ditzakete.

4. Negozioarekin jarraitzeko planak eta prozedurak: alderdi interesdun garrantzitsuei behar bezala ohartarazteko eta komunikatzeko aukera emango duen egitura bat ezarri eta mantendu behar da, eta etenaldi batean erakundea administratzeko planak eta prozedurak eman behar dira. Planak eta prozedurak negozioaren jarraitutasun-irtenbideak gauzatzeko erabiliko dira, beharrezkoa denean.

5. Ariketen programa: ariketen eta proben programa bat ezarri eta mantendu behar da, negozioaren jarraitutasunerako estrategien eta soluzioen eraginkortasuna denborarekin baliozkotzeko.

   Jarraian, zibersegurtasunaren arloko Jarraipen Planak izan behar duen egitura eta informazio xehatua jasotzen da, araudiak eskatutakoaren arabera:

6.1 Eragiketen plangintza eta kontrola

Lehen fase honetan, erakundeak bere eginkizunak betetzeko behar dituen jarduera eta negozio-prozesu guztiak identifikatu behar ditu, betiere autobabeserako euskal arauaren aplikazio-eremuaren barruan (277/2010 Dekretua). Identifikazio horiek egin ondoren, erakundeak zehaztu beharko du zer prozesu edo azpiprozesutan garatuko den Jarraipen Plana, eta, horrela, erantzun eraginkorra bermatuko du etenaldi posibleen aurrean.

6.2 Negozioan izandako inpaktuaren analisia eta arriskuen ebaluazioa

Prozesuen eta jardueren mapa identifikatuta, erakundeak negozioan edo BIAn (ingelesezko sigletan, Business Impact Analysis) duen eraginaren azterketa bat egin beharko du, gutxienez honako informazio hau duen jarduera edo prozesu bakoitzeko:

- Identifikatutako negozio-jarduera/-prozesu bakoitzaren eragiketarako beharrezkoak diren aktiboen inbentarioa:
  - Negozio-prozesuaren edo -jardueraren euskarri izango diren informazio-sistemen, aplikazioen eta plataformen zerrenda.

- Jarduerak egiteko bildu, prozesatu eta biltegiratu behar diren datuak eta informazioa, barneko zein kanpoko datuak barne.
- Eragiketarako beharrezkoak diren produktuak edo zerbitzuak hornitzen dituzten kanpo-hornitzaileak edo hirugarrenak.
- Barneko langileak, hau da, negozio-jarduera edo -prozesuan parte hartzen duten giza baliabideak.
- Eragiketa egiten den establezimendua (k).
- Eragiketarako beharrezkoak diren beste kokapen batzuk, hala nola bulegoak, solairuak, DPZak, etab.
- Beste IKT ekipamendu bat, hau da, informazio-sistemen kategorian zuzenean sartzen ez diren baina eragiketarako funtsezkoak diren ekipo teknologikoak, hala nola zerbitzariak, routerrak, switchak, gailu mugikorrak, IoT gailuak...

- Eten posible baten aurrean denbora kritikoak zehaztea. Zehazki, honako hauek identifikatu beharko dira:
  - Berreskuratze-denbora objektiboa (RTO, ingelesezko siglak). Erakunde batek prozesu, sistema edo zerbitzu bat berrezartzeko eman dezakeen gehieneko epe onargarria da, etenaldi baten ondoren, negozioan duen eragina onartezina izan aurretik.

    Bestela esanda, gorabehera gertatzen denetik zerbitzua guztiz edo partzialki berreskuratu arte igaro behar den denbora da.
  - Berreskurapeneko Puntu Objektiboa (RPO, ingelesezko siglak). Erakunde bat galtzeko prest dagoen gehieneko datu kopurua zehazten duena, denboran adierazita, etete edo hondamendi bat gertatuz gero. Erakundeak bere jardueretan eragin nabarmenik izan gabe jarduten jarrai dezan, datuak noiz arte berreskuratu behar diren adierazten du.
  - Etenaldirako Gehieneko Denbora Onargarria (MTPD, ingelesezko siglak). Prozesu bat etenda egon daitekeen gehieneko aldia da, erakundeari kalte konponezinik eragin gabe.

    RTOtik bereizten da; izan ere, MTPDk etenaldiak iraun dezakeen denbora osoa hartzen du kontuan, berreskuratze teknikoa ez ezik, negozioan izandako inpaktu-aldia eta erantzuteko gaitasun globala ere barnean hartuta.
  - Identifikatutako prozesu kritikoei eragin diezaieketen eta negozio-prozesu kritikoen konfidentzialtasuna, osotasuna eta erabilgarritasuna arriskuan jar dezaketen zibersegurtasuneko mehatxu eta ahulezia nagusiak identifikatzea.

    Identifikazio horren bidez, erakundeak erakundearen funtsezko aktiboak babesteko prebentzio- eta arintze-neurri egokiak hartu ahal izango ditu.

6.3 Negozioarekin jarraitzeko estrategiak eta irtenbideak

Negozio-jarduera eta -prozesu bakoitzaren inpaktuaren analisia eta arriskuen analisia egin ondoren, erakundeak behar diren jarraitutasun-estrategiak eta -irtenbideak identifikatu eta definitu beharko ditu, erantzun-denboren arabera kritikotzat jo diren prozesuek funtzionamendu normala eteten duen edozein gorabeheraren aurrean eraginkortasunez jarduten edo berreskuratzen jarraitu ahal izatea bermatzeko.

Estrategia eta soluzio horiek bat etorri behar dute azterketan ezarritako errekuperazio-denborekin. Horretarako, erakundeak prebentzio-ekintzak, eragiketa-kontingentziak eta berreskuratze-protokoloak barne har ditzaketen neurri batzuk ebaluatu eta hautatu beharko ditu, jarduera kritikoen eskuragarritasuna eta erresilientzia bermatzeko.

Soluzio horiek identifikatzeko, funtsezko alderdiak hartu behar dira kontuan, hala nola eskatutako azpiegitura teknikoa, giza euskarria, sistemen erredundantzia, kanpo-hornitzaileekiko akordioak eta akatsen aurrean jarduteko metodo alternatiboak. Era berean, garrantzitsua da estrategia horiek aukera ematea arrisku-egoera desberdinetara azkar egokitzeko eta ekonomikoki bideragarriak izateko, baliabideak optimizatzeko eta negozioan inpaktua minimizatzeko.

Azken batean, fase honen bidez, erakundeak eragiketa-jarraitutasuneko esparru integral bat ezartzen du. Esparru horrek bere aktiboak eta funtsezko prozesuak babesteaz gain, gorabeheren aurrean erantzuteko, egokitzeko eta berreskuratzeko gaitasuna indartzen du, eta, horrela, bezeroen, bazkideen eta gainerako alderdi interesdunen konfiantzari eusten dio.

6.4 Negozioarekin jarraitzeko planak eta prozedurak

Erakundeak prozesu bakoitzerako konponbideak edo estrategiak hautatu edo zehaztu ondoren, plan operatiboak eta berreskuratze-prozedura espezifikoak diseinatu eta egin beharko ditu, hautatutako estrategiei erantzuteko.

Plan horiek jarraibide, protokolo eta ekintzen multzo xehatua osatzen dute. Horien helburua da talde arduradunak gidatzea, gorabeheren edo etenaldien aurreko erantzuna aktibatzen den bitartean, negozioaren jarraitutasuna adostutako denboran berrezartzeko beharrezkoak diren jarduera operatiboak egiten direla bermatzeko.

Plan horiek argi eta zehatz definitu beharko dituzte jarraitu beharreko urratsak, zeregin bakoitzaren arduradunak eta jarduera bakoitza gauzatzeko behar diren baliabideak. Era berean, kontuan hartu behar dute zer baldintzatan aktibatu behar diren, barne- eta kanpo-komunikazioko mekanismoak, bai eta errekuperazioaren eraginkortasuna ebaluatzeko irizpideak ere.

6.5 Ariketen programa

Plan operatiboak eta berreskuratze-prozedura espezifikoak egin ondoren, erakundeak egiaztatu eta ziurtatu beharko du negozioaren jarraitutasun-plan eta -prozedura horiek eraginkorrak direla, ariketa- eta proba-programa bat ezarriz.

Ekitaldi-programa bermatzeko, erakundeak honako hauek egin beharko ditu:

- Proben helburuak eta irismena zehaztea, hau da, zer probatu nahi den eta egin beharreko proben irismena ezagutzea, egoerak definitzeko.

- Proben egutegia zehaztea, probak noiz egin behar diren planifikatuz. Horretarako, erakundeak egin beharreko proben egutegi saiakera eta eguneragarri bat ezarri beharko du, bai eta horien aldizkakotasuna ere.

- Proba bakoitzean egin beharreko jarduera eta zeregin guztiak aldez aurretik modu zehatz eta sekuentzialean dokumentatzea (checklists gisa), behar bezala garatzeko.

Planak eta prozedurak modu independentean proba daitezke, haien eraginkortasuna egiaztatzeko krisi-kudeaketako simulakro bat egin beharrik gabe. Negozioaren Jarraipen Planaren hasierako heldutasun-mailetan, komeni da jarraitutasun-alternatiba batzuk modu isolatuan probatzea, krisiak kudeatzeko simulakroetan sartu ahal izateko, heldutasun-maila egokia dutene

7 Eranskina

Proba-fitxaren adibideak:

Proba – titulua:	**Zentro alternatiboko aplikazioetan eta teknologian sartzeko ariketa aktiboa.**
Helburua:	Hondamendi teknologikoak berreskuratzeko planak modu aktiboan erabiltzea.
Eraginpeko eremuak:	Saila Azpiegiturak eta Saila Sistemak.
Probari eusteko eremuak:	Saila Telekomunikazioak.
Erreferentziako dokumentua:	Kontingentzia informatikoen plana.
Deskribapena:	
✓ Jarraitutasun teknologikoko prozesuen ezagutza-, ulermen- eta aplikazio-maila zehaztea. ✓ Jarraitutasuna bermatzeko behar diren baliabideen erabilgarritasuna zehaztea. ✓ Prozedurak eguneratuta dauden zehaztea. ✓ Prozesuan esku hartzen dutenen igurikimenen betetze-maila zehaztea.	
Froga-prozedura:	
Arduradunek krisi simulatuaren ondorioz kaltetuko den taldeko gainerako kideak bildu beharko dituzte, aldez aurretik asmo horren berri eman gabe. Bildu ondoren, arduradun bakoitzak simulatu beharreko krisi-egoera deskribatuko du, eta kide bakoitzak bere kargura izango dituen erantzukizunak gauzatu beharko ditu. Era berean, baliabide jakin bat erabiltzeko beharra hautematen den bakoitzean, baliabide hori erabilgarri dagoela egiaztatu beharko da.	
Probatu beharreko elementuak:	
☒ Prozedurak ☒ Gaikuntza ☐ Zentro alternatiborako sarbidea ☐ Negozio-prozesuak	☒ Telekomunikazioak ☒ Aplikazioak ☐ Giza baliabideak ☐ Komunikazioa	☐ Krisiaren kudeaketa ☐ Langileak lekuz aldatzea ☐ Normaltasunera itzultzea
Adierazleak:	✓ Teknologiaren jarraitutasuna berreskuratu arte igarotako denbora. ✓ Jarraitutasunerako behar diren baliabideen ehunekoa. ✓ Prozeduren ezagutzaren ehunekoa (ezagutza duten pertsonen kopurua/inplikatutako pertsonak). ✓ Prozeduretako errore kopurua (eguneratze-maila).	

EUSKO JAURLARITZA
GOBIERNO VASCO

cyber zaintza
BASQUE CYBERSECURITY AGENCY

Eskerrik asko!

www.ciberseguridad.eus