cyber zaintza | BASQUE CYBERSECURITY AGENCY

Zibersegurtasunaren Euskal Estrategia

2024-2029

EUSKO JAURLARITZA
GOBIERNO VASCO

Aurkibidea

Laburpen exekutiboa 4
Zibersegurtasunaren testuinguru globala 8
Euskadiko egungo egoera 12
Zibersegurtasunaren erronkak Euskadin 16
Asmoa, printzipioak eta helburu estrategikoak 20
Jarduera-ildoak 24
Gobernantza-eredua 34
Jarraipena eta ebaluazioa 39

Laburpen exekutiboa

Laburpen exekutiboa

Euskadi gizarte modernoa eta zerbitzu aurreratuak dituen herrialdea da, aurrerapenarekin eta gizartearekin duen konpromisoa islatzen duena. Testuinguru horretan, eraldaketa digitalaren aldeko apustu irmoa egiten ari da, berrikuntza teknologikoa funtsezkoa dela onartuz, gero eta interkonektatuago dagoen ingurune global batean egoteko.

Teknologia berriak, hala nola Adimen Artifiziala (AI), gizartea errotik eraldatzen ari dira. Automatizazio industrialetik hasi eta laguntzaile birtualetaraino eta erabaki prediktiboak hartzeraino, AIk eraginkortasuna eta berrikuntza bultzatzen ditu.

Hala ere, eskura dauden teknologia eta tresnen bilakaera azkarrak erabilera-kasu berriak sortzen ditu eta, aldi berean, erakundeen esposizio-azalera handitzen du, zibergaizkileek beste eraso batzuk egiteko balia dezaketena.

Zibersegurtasuna gizarte osoari eragiten dion erronka den egoera horri aurre egiteko, zibersegurtasunaren kudeaketa globala inplementatu behar da, baita inplikatutako eragileek egindako jarduerak lerrokatzea ahalbidetuko duten koordinazio-mekanismoak eduki ere.

Testuinguru horretan onartu zen ekainaren 29ko 7/2023 Legea, **Zibersegurtasunaren Euskal Agentzia** sortzekoa. Agentzia, Cyberzaintza ere deitua, Eusko Jaurlaritzako Segurtasun Sailari atxikita dago, eta bere helburua da zibersegurtasuna sustatzea eta koordinatzea euskal sektore publikoan, sektore horren eskumeneko informazio-sistemen eta sare elektronikoen segurtasunaren eremuan, eta Euskal Autonomia Erkidegoaren, haren Administrazio publikoaren, herritarren eta haren enpresa-sarearen zibersegurtasunaren eta garapen digital seguruaren alorreko gaikuntza bultzatzea eta bultzatzea. Sortu ondoren, Agentziak Euskadiko zibersegurtasun-estrategia baten diseinua gidatu du, datozen urteetan alor horretako jardueren lerrokatzea sustatzeko helburuarekin. Prozesuan parte hartu dute Euskal Autonomia Erkidegoko Administrazio Publikoaren mailetako interesdun nagusiek, bai eta Zientzia, Teknologia eta Berrikuntzaren Euskal Sareko eragileek eta zibersegurtasunaren sektore pribatuko ordezkariek ere.

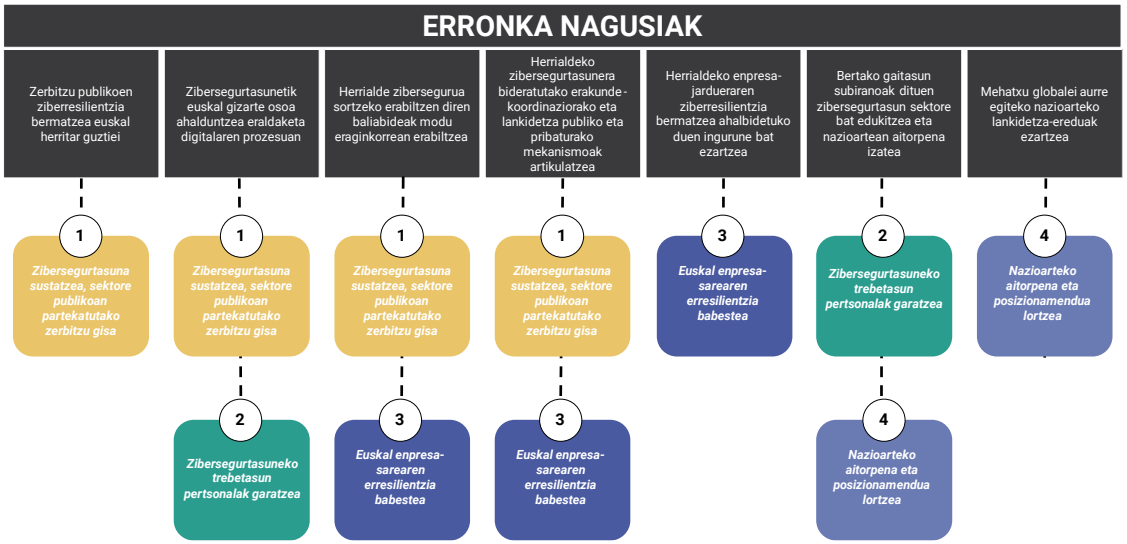
Dokumentu honek 2024-2029 aldirako **Zibersegurtasunaren Euskal Estrategia** garatzen du.

Estrategiaren **helburua** da Euskadi herrialde ziberresiliente bihurtzea, bere administrazio publikoa eta enpresa-sarea arrisku zibernetikoetatik babesteko gaitasunekin, eraldaketa digitalaren prozesuan gizartearen ahalduntzea sustatuz eta gaitasun horiek zibersegurtasun globala garatzeko ekarriz, nazioartean erreferentziazko lekua hartuz.

Zibersegurtasunaren estrategiak herrialdeak eremu horretan dituen erronkak identifikatzen ditu, eta helburu estrategiko batzuk planteatzen ditu. Helburu horiek lortzeko, zortzi jarduera-ildo zehazten ditu. Eta, era berean, lerro horietako bakoitzerako, kasu bakoitzean eskumena duen eragileak gidatu beharreko jarduera-multzo bat

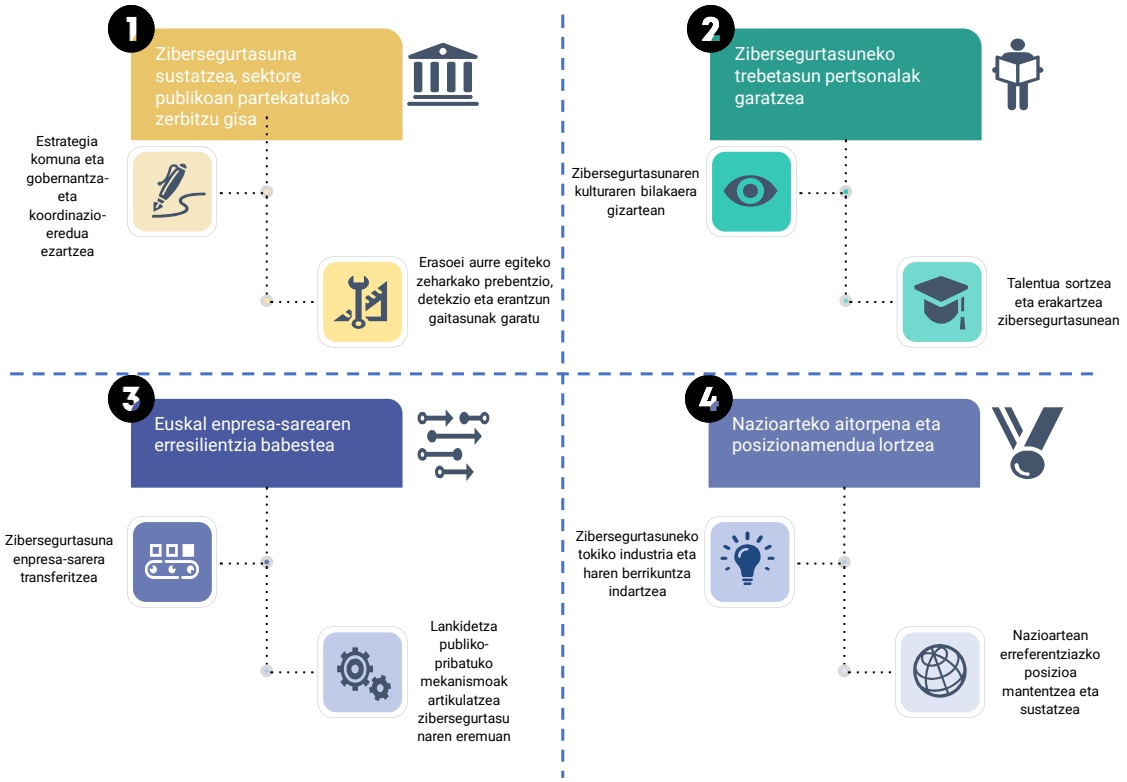
zehazten du, identifikatutako helburuak lortzeko. Jarduera horiek Euskadiko administrazio publiko guztiak, herritarrak, enpresa-sarea eta zibersegurtasunaren sektorea bera hartzen dituzte barne.

Irudi honetan, zibersegurtasunaren alorrean Euskadirentzat identifikatutako **zazpi erronkak eta lau helburu estrategikoak** agertzen dira:



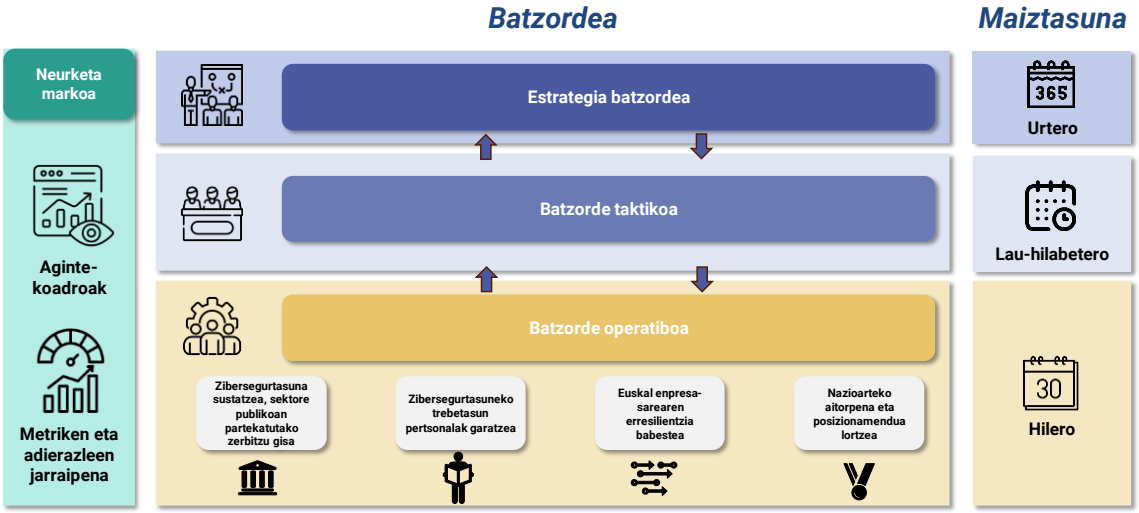
1. irudia: Zibersegurtasunaren Euskal Estrategiaren erronkak eta helburuak

Helburu horiek lortzeko, identifikatutako **zortzi jarduera-ildoak** azaltzen dira jarraian:



2. irudia: Zibersegurtasunaren Euskal Estrategiaren helburuak eta jarduera-ildoak

Euskadiko Zibersegurtasun Estrategiaren ezarpena bermatzeko, **Gobernantza-eredu** bat zehaztu da. Eredu horri esker, esku hartzen duten eragileen jarduna identifikatutako ekintza guztietan integratu ahal izango da, bai eta baliabideen inbertsioan behar bezalako hedapena, efizientzia eta erakundeen arteko eta alor publikoaren eta pribatuaren arteko koordinazioa bermatu ere.



3. irudia: Zibersegurtasunaren Euskal Estrategiaren gobernantza-eredua

Zibersegurtasunaren testuinguru globala

Zibersegurtasunaren testuinguru globala

Azken urteetan, aldaketa nabarmena gertatu da teknologiaren alorrean, eraldaketa digitalaren prozesuak eta Informazioaren eta Komunikazioaren Teknologien (IKT) etengabeko garapenak bultzatuta. Fenomeno horrek, enpresa-praktikak iraultzeaz gain, sortzen ari diren teknologiekiko mendekotasuna ere sortu du, egungo gizartean interkonexio digitaleko eredu berri bat sortzea sustatuz. Egoera horrek aurrerapen bat ekarri du fisikotik digitalera, progresibotik berehalakora, ukigarritik ukiezinera.

Hala eta guztiz ere, gero eta digitalizatuagoa eta interkonektatuagoa den ingurune bateranzko bilakaera horrek beste mehatxu eta erronka batzuk ere badakartza zibersegurtasunaren eremuan; izan ere, erakunde publikoen, enpresa pribatuen eta herritarren segurtasuna eta pribatutasuna arriskuan jartzen duten gertakarien aurreko prebentzioak, prestakuntzak eta erantzun eraginkorrak garrantzi berezia dute.

Paradigma digital berri honetan, teknologia disruptiboekiko mendekotasun handia eta hiperkonektibitatea nabarmentzen dira ziberkriminalitatearen gorakadaren arrazoi nagusi gisa, bereziki Administrazio Publikoari dagokionez, zibergaizkileentzat erakargarriena den helburutzat jotzen baita.

Testuinguru horretan, erronka horri aurre egiteko, Europar Batasunak (EB) aitortu du segurtasun-neurriak ezarri behar direla sistemak eta sareak babesteko, eta arreta berezia jarri behar dela eragile kritikoetan eta funtsezko zerbitzuetan.

Ildo horretan, EBk "Hamarkada Digitalerako EBren Zibersegurtasun Estrategia" izeneko zibersegurtasun-estrategia aurkeztu zuen 2020an. Estrategia horren jarduera-ildo nagusiak honako hauek dira: "funtsezko zerbitzuen eta konektatutako gailuen segurtasuna handitzea, zibereraso nagusiei erantzuteko gaitasun kolektiboak indartzea eta mundu-mailako bazkideekin lankidetzan aritzea, ziberespazio global, ireki, egonkor eta seguru batean nazioarteko segurtasuna eta egonkortasuna bermatzeko, giza eskubideak, oinarrizko askatasunak eta balio demokratikoak babestuz"[1].

Nazio mailan, Segurtasun Nazionaleko Kontseiluak 2021ean onartu zuen "Segurtasun Nazionaleko Estrategia (ESN) 2021. Bertan, munduko segurtasunaren egungo testuingurua deskribatzen da, eta eraldaketa globaleko lau dinamika identifikatzen dira: lehiaketa geopolitiko handiagoa; COVID-19aren ondorioek markatutako ingurune sozioekonomikoa; teknologiak eragindako eraldaketa-erritmoaren azelerazioa; eta, azkenik, trantsizio ekologikoaren prozesua. "[2]

Aurrekoaren ildotik, eremu honetan aplikatzekoa den araudia eta erregulazioa ere etengabe aldatu da, ingurune digital berri horri erantzuteko helburuarekin.

1 The EU's Cybersecurity Strategy for the Digital Decade. Data: 2020ko abendua.

2 Estrategia de Seguridad Nacional 2021. Data: 2021ko abendua.

Ildo horretan, aipatu behar dira EBn zibersegurtasunaren alorrean Europa mailan onartutako erreferentziako erregulazio nagusiak, hala nola:

- 2016/679 (EB) Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2016ko apirilaren 27koa, datu pertsonalen tratamenduari eta datu horien zirkulazio askeari dagokienez pertsona fisikoak babesteari buruzkoa, eta 95/46/EE Zuzentaraua (Datuak Babesteko Erregelamendu Orokorra) indargabetzen duena.
- 2019/881 (EB) Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2019ko apirilaren 17koa, ENISAri (Zibersegurtasunerako Europar Batasuneko Agentzia) eta informazioaren eta komunikazioaren teknologien zibersegurtasunaren ziurtapenari buruzkoa eta 526/2013 (EB) Erregelamendua indargabetzen duena («Zibersegurtasunari buruzko Erregelamendua»).
- 2022/2555 (EB) Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2022ko abenduaren 14koa, Batasun osoan zibersegurtasun-maila erkide handia bermatzeko neurriei buruzkoa, 910/2014 (EB) Erregelamendua eta 2018/1972 (EB) Zuzentaraua aldatzen dituena eta 2016/1148 (EB) Zuzentaraua (NIS 2 Zuzentaraua) indargabetzen duena.
- 2022/2557 (EB) Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2022ko abenduaren 14koa, erakunde kritikoen erresilientziari buruzkoa eta Kontseiluaren 2008/114/EE Zuzentaraua indargabetzen duena.
- Ziberresilientziari buruzko Europako Legearen proposamena (Cyber Resilience Act - CRA), produktu edo softwarea osagai digitalarekin erosten edo erabiltzen duten kontsumitzaile eta enpresak babestea helburu duena, produktu horietarako nahitaezko zibersegurtasun-baldintzak ezarriz.
- Adimen Artifizialari buruzko Europako Legearen proposamena, EBko merkatu bakar osoan IA seguru eta fidagarri baten garapena eta onarpena sustatzea helburu duena.

Bestalde, segurtasun-alorreko erreferentziazko erregulazio nagusiak, estatu mailan, honako hauek dira:

- 3/2018 Lege Organikoa, abenduaren 5ekoa, Datu Pertsonalak Babestekoa eta eskubide digitalak bermatzekoa.
- 43/2021 Errege Dekretua, urtarrilaren 26koa, Informazio Sare eta Sistemen Segurtasunari buruzko irailaren 7ko 12/2018 Errege Lege Dekretua garatzen duena.
- 8/2011 Legea, apirilaren 28koa, azpiegitura kritikoak babesteko neurriak ezartzen dituena.
- 704/2011 Errege Dekretua, maiatzaren 20koa, azpiegitura kritikoak babesteko erregelamendua onartzen duena.
- 311/2022 Errege Dekretua, maiatzaren 3koa, Segurtasun Eskema Nazionala arautzen duena.

Ondorio gisa, egungo gizartea aldaketa globaleko prozesu batean murgilduta dago, teknologia berriak sartzearen ondorioz. Horrek eragina du sortzen ari diren erronka eta mehatxuei helduko dien espazio global eta zibersegurua osatzeko moduan.

Testuinguru horretan, gobernuek eta erakundeek zibersegurtasun-estrategiak definitzera eta ezartzera bideratu behar dituzte beren ahaleginak, esparru horretako erregulazio nagusiekin lerrokatuta, bai nazioartean, bai estatuan, sareen, sistemen eta azpiegituren erabilera segurua bermatzeko, arreta berezia eskainiz operadore kritikoei eta funtsezko zerbitzuei, mundu modernoaren funtsezko sektoreei euskarri ematen baitiete.

Euskadiko egungo egoera

Euskadiko egungo egoera

Gero eta ingurune digitalizatuagoan, datuen eta sistemen babesa bermatzea funtsezkoa da, batez ere teknologia aurreratuak erabiltzen dituzten erakundeentzat. Ezinbestekoa da ekintza proaktiboak hartzea informazioaren osotasuna, erabilgarritasuna eta konfidentzialtasuna zaintzeko eta, horrela, eraso zibernetikoak saihesteko.

Funtsezko sektoreak herrialde baten funtzionamendurako eta garapenerako berebiziko garrantzia dutenak dira. Testuinguru horretan, sektore publikoaren eta pribatuaren arteko lankidetza funtsezkoa da erronka zibernetiko berriei aurre egiteko eta Euskadiko funtsezko sektoreetan zibersegurtasuna bermatzeko.

Teknologia berrien etengabeko bilakaera horren aurrean, ezinbestekoa da, halaber, Euskadiko administrazio publikoak etengabe egokitzea ingurune aldakor eta gero eta konplexuago batera, gizarteari zerbitzuak modu eraginkor eta seguruan emateko.

Testuinguru horretan, Euskadik zibersegurtasunean espezializatutako enpresen kontzentrazio nabarmena du, milioi bat biztanleko konpainien kopurua nabarmen gaindituz, estatuko zein Europako beste ekonomia batzuekin alderatuta. Ildo beretik, zibersegurtasunaren alorreko jarduera ekintzailea nabarmentzen da Euskadin, estatu mailan handienetakoen artean, eta nabarmena da beren teknologia propioa garatzen duten startupen presentzia.

Era berean, esparru publikotik hainbat nazioartekotzeko-tresna eta zibersegurtasuneko laguntza-programa antolatu dira, Euskadiko enpresa-sarearen lehiakortasuna hobetzea helburu dutenak.

Bestalde, Euskadiko sektore publikoak zibersegurtasuneko gaitasun ugari ditu, zerbitzuen eraginkortasuna, irisgarritasuna eta segurtasuna hobetzeko.

Gaitasun horiek, batez ere, jarduera operatiboetan oinarritzen dira, eta ahalmen gehigarri batzuk dituzte araudiak eta prozesuak sustatzeko, aholkatzeko eta formulatzeko. Hala ere, indartu egin behar dira bai prebentzioaren, detekzioaren eta gorabeheren aurreko erantzunaren eremua, bai zibersegurtasunaren estrategiaren, gobernantzaren eta kudeaketa koordinatuaren eremua. Gaitasun horiek ez indartzeak arrisku nabarmenak ekar ditzake, hala nola gaitasunak zatikatzea edo ikuspegi nazionalarekin eta nazioartekoarekin bat ez etortzea.

Testuinguru horretan sortu da Euskadiko Zibersegurtasun Agentzia, Cyberzaintza, zeinaren helburua baita Euskal Sektore Publikoaren zibersegurtasuna sustatzea eta koordinatzea, sektore horren eskumeneko informazio-sistemen eta sare elektronikoen segurtasunaren esparruan, eta Euskal Autonomia Erkidegoaren, haren Administrazio Publikoaren, herritarren eta haren enpresa-sarearen zibersegurtasunaren eta garapen digital seguruaren alorreko gaikuntza bultzatzea eta bultzatzea. Erakunde hori funtsezko elementua da ahaleginak zentralizatzeko eta zibermehatxuen aurrean erantzuna optimizatzeko, eta, horrela, inplikatutako eragile guztien ekintza bateratu eta eraginkorra bermatzen da.

Hurrengo irudian, Euskadin zibersegurtasunaren alorrean jarduten duten erakunde publiko nagusiak agertzen dira.

4. irudia: Ziberseguritasunaren alorrean jarduten duten erakunde nagusiak

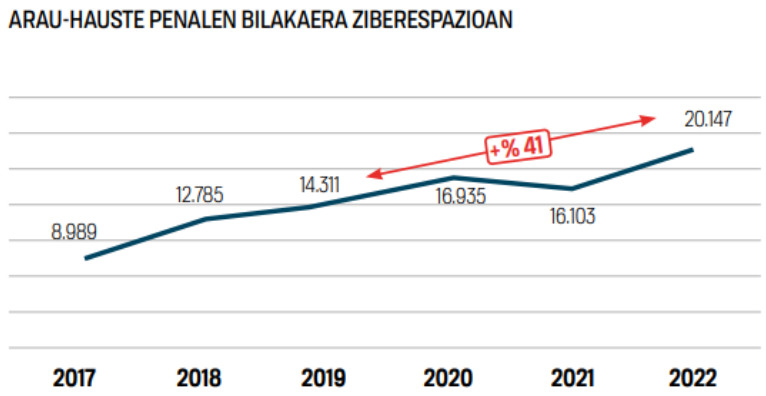
Esparru horretan, nabarmentzekoa da, halaber, Euskadiko Segurtasun Publikorako Informazio Teknologien eta Komunitateen Plan Estrategikoa (PETICSEG 2021-2024). Ekimen honek aukera ematen du Euskadiko segurtasun publikoaren esparruan informazioaren eta komunikazioen teknologiak (IKT) garatzeko eta ezartzeko jarraibideak eta helburuak ezartzeko.

Halaber, Euskadik Euskadiko Segurtasun Publikoaren Plan Orokorra du (2025), eta plan horrek herritarren segurtasunarekin lotutako arriskuen, ekintzen eta baliabideen azterketa eta proiekzio orokorrak biltzen ditu. Zibersegurtasunari, azpiegitura kritikoei eta sentikorrei dagokienez, planak aktibo digitalak eta funtsezko azpiegiturak babesten ditu mehatxu zibernetikoen eta beste arrisku batzuen aurka.

Aurretik azaldutakoan oinarrituta, ondoriozta daiteke, urteetan zehar, Euskadik zibersegurtasunaren aldeko apustu irmoa egin duela, eraldaketa digitalaren goraldian

dagoen gizarte batek aurrean dituen erronkei erantzuna emanez, euskal gizartearentzako gune fidagarri eta ziberseguru gisa kokatzen saiatuz.

Testuinguru horretan, ziberdelituen hazkundeak goranzko joera erakusten du Euskadin. Hori ez da gertaera isolatu bat, eta joera global bat islatzen du. Hurrengo grafikoan, argitaratutako Euskal Poliziaren azken Delinkuentzia Memoriaren datuak agertzen dira:



5. irudia: Ziberdelituen bilakaera Euskadin

Era berean, 2023ko lehen seihilekoan goranzko joera horri eutsi zitzaion, aurreko urteko aldi beraren aldean %31ko igoerarekin. Gaur egun, Euskadin salatzen diren lau delituetatik bat teknologia berrien bidez egiten da.

Zifrek adierazten duten bezala, arriskuak gero eta handiagoak dira gizartea digitalizatzen den heinean. Erasoen sofistikazioak eta teknologiaren bilakaerak nabarmen handitu dute dauden mehatxuen kopurua. Finantza-iruzurretatik ransomware-erasoetaraino, erakunde publikoek zein enpresek segurtasun-neurri berriak indartu eta garatu behar dituzte, haien informazioa eta azpiegiturak babesteko.

Zibersegurtasunaren erronkak Euskadin

Zibersegurtasunaren erronkak Euskadin

Euskadiko zibersegurtasunaren alorreko funtsezko eragile nagusiek parte hartu duten azterketa sakona egin eta zibersegurtasunaren ekosistemaren nazioarteko iturriak kontsultatu ondoren, zibersegurtasunaren alorreko erronka estrategikoak identifikatu dira. Erronka horiek erakusten dute nola eragin diezaieketen Euskadiri, eta, ondorioz, baita haren gizarteari eta enpresa-sareari ere, mehatxu globalek, eta abiapuntua dira 2024-2029 zibersegurtasun-estrategiaren bidez heldu beharreko helburu estrategikoak ezartzeko.

Identifikatutako erronka nagusiak, datozen bost urteetan erantzuna eman nahi zaienak, jarraian jasotzen dira.

ZERBITZU PUBLIKOEN ZIBERRESILIENTZIA BERMATZEA EUSKAL HERRITAR GUZTIEI

Euskadiko sektore publikoaren eraldaketa digitala abian da. Herritarrek kalitatezko zerbitzu publikoak dituzten herrialde batean, segurtasun juridiko eta fisikoko testuinguruan, gero eta digitalagoak diren zerbitzu horien ziberresilientzia bermatzea behar bezala heldu beharreko erronka da.

Zerbitzuen erresilientzia eta informazioaren babesa euskal gizarte osoarentzat bermatu behar da, Administrazio Publikoarekiko harremanean konfiantza sortuz. Gainera, erresilientzia hori herritar guztiei bermatu behar zaie, alde batera utzita zein lurralde historikotan bizi diren, zein administraziorekin duten harremana eta zein ezaugarri eta zirkunstantzia pertsonal dituzten.

Badira erronka horri aurre egiteko kontuan hartu behar diren alderdi batzuk, hala nola ingurune batzuen zaharkitze teknologikoa edo beste batzuen malgutasun maila.

ZIBERSEGURTASUNETIK EUSKAL GIZARTE OSOA AHALDUNTZEA ERALDAKETA DIGITALAREN PROZESUAN

Zibersegurtasuna ez da eremu erabat teknologikoa, zerbitzuak eta informazioa hainbat aplikazio-eremutatik babestu behar dira. Neurriak ez dira soilik babesean oinarritzen, arriskuak kudeatzeko, arazoak detektatzeko, gorabeherei erantzuteko eta horiek berreskuratzeko neurriak ere badaude. Funtsezkoa da gizarteari kontzientziazio- eta trebakuntza-maila bat ematea, arriskuez jabetu eta erabaki informatuak hartu ahal izateko. Horrek aukera ematen die herritarrei beren babeserako eragile aktibo bihurtzeko, eta funtsezkoa da eraldaketa digitalaren abantailez baliatu ahal izateko.

Gizartean dagoen eten digitala eta hura osatzen duten kolektiboen berezitasunak direla eta, erronka horri ikuspegi global batetik heldu behar zaio. Beraz, kontuan hartu behar dira Euskadin egon daitezkeen berezitasun guztiak, bai ikuspegi pertsonaletik, bai ikuspegi sozial eta profesionaletik, besteak beste.

HERRIALDE ZIBERSEGURUA SORTZEKO ERABILTZEN DIREN BALIABIDEAK MODU ERAGINKORREAN ERABILTZEA

Euskadiko Administrazio Publikoak bere beharretara egokitutako zerbitzuak eskaintzen dizkio gizarteari, hiru jarduera-mailatan banatutako antolamenduarekin; maila horietako bakoitzak egitura eta gaitasun desberdinak ditu. Testuinguru horretan, gizarteari eskainitako zerbitzu publikoak optimizatu ahal izateko, baliabideen eraginkortasuna funtsezko alderdia da, baita zerbitzu digitalen kasuan ere.

Zibersegurtasuna mehatxu globala da, eta babes-erronka asimetrikoa da. Horrela, eremu honetan ere, baliabideen erabileran eraginkorragoa izatea funtsezko faktorea izango da arriskuak modu eraginkorragoan kudeatzea ahalbidetuko duten neurri gehiago hedatu ahal izateko.

HERRIALDEKO ZIBERSEGURTASUNERA BIDERATUTAKO ERAKUNDE-KOORDINAZIORAKO ETA LANKIDETZA PUBLIKO ETA PRIBATURAKO MEKANISMOAK ARTIKULATZEA

Euskadiren ziberresilientzia lortzeko, erakundeen arteko koordinazio-maila erabat zehaztua eta trebatua izan behar da, behar den kasuetan erantzun bakarra identifikatu ahal izateko.

Horrez gain, funtsezkoa da lankidetza publiko-pribatuko mekanismoak antolatzea, ziberresilientzia hori herrialde osora eramateko eta arrakasta izateko aukerak handitzeko. Lankidetza publiko-pribatua Euskadiren nortasunaren ezaugarrietako bat denez, erronka horri aurre egiteko, egindako saioetan identifikatu diren indarretan oinarritu behar da.

HERRIALDEKO ENPRESA-JARDUERAREN ZIBERRESILIENTZIA BERMATZEA AHALBIDETUKO DUEN INGURUNE BAT EZARTZEA

Segurtasuna, kontzeptu orokor gisa, enpresa-sareak bere jarduera garatzeko orduan gehien baloratzen duen alderdietako bat da. Testuinguru horretan, Euskadin dagoen segurtasun publikoaren mailaren ondorioz, nazioartean erreferentzia diren enpresak herrialdean jaio eta garatzen dira.

Testuinguru global batean, non enpresa-eremuan eraldaketa digitala gero eta azkarragoa eta beharrezkoagoa den, enpresa-sareak bere jarduerak eta emaitzak babestu behar ditu zibernetikaren esparruan ere. Enpresen babesa enpresa-sareak lehen eskutik aurre egin beharreko alderdia bada ere, Euskadik erronka bat du: herrialdeko enpresa-jardueraren ziberresilientzia bermatzeko egoerarik onena emango duten beharrezko neurriak hartzea.

BERTAKO GAITASUN SUBIRANOAK DITUEN ZIBERSEGURTAUN SEKTORE BAT EDUKITZEA ETA NAZIOARTEAN AITORPENA IZATEA

Zibersegurtasuna erronka globala da, eta halakotzat hartu behar da. Herrialde eta eskualde askotan garatutako gaitasunak daude. Euskadik, gaur egun, posizionamendu eta begirune ona du, eta bere zibersegurtasun-sektorea gai izan da nazioarteko proiekzioa duten irtenbideak eta gaitasunak sortzeko. Hala ere, aspalditik, enpresa-inguruneak egindako eragiketa batzuen ondorioz, Euskadin jaiotako eragile garrantzitsuek beste herrialde edo eskualde batzuetara eraman dituzte erabakiguneak.

Gainera, babesaren alorrean erabiltzen diren tresna nagusiak hirugarren herrialdeetako enpresen mende daude. Hala ere, Euskadik sektore sendoa du, eragile ugari ditu eta berrikuntza-maila nabarmena du. Horrek aukera eman behar du erronka horri posizio baikorretik aurre egiteko. Era berean, nazioarteko presentzia handia duen tokiko enpresa-sarea funtsezko aliatua izan daiteke.

MEHATXU GLOBALEI AURRE EGITEKO NAZIOARTEKO LANKIDETZA-EREDUAK EZARTZEA

Ziberkrimena bezalako mehatxu globalen aurrean, gero eta eragin handiagoa baitute Euskadin ere, ezinezkoa da gure herrian oinarritutako defentsa bilatzea. Mehatxu horiei ahalik eta hobekien aurre egiteko, nazioarteko lankidetza-ereduak ezarri behar dira, ahal denean mehatxuei aurrea hartzeko eta, hala ez denean, modurik onenean erantzuteko. Testuinguru horretan, herrialde guztiek dute mehatxu komun baten eragina eta interesdunen kopurua oso handia da, eta lankidetza-ereduek behar bezala funtzionatzea erronka handia da. Euskadik, herrialde txikia izanik, bai azalerari dagokionez, bai biztanleriari dagokionez, garrantzia hartzen lagunduko dion ikuspegi batetik konpondu behar du erronka hori.

Abiapuntua ona da; izan ere, gaur egun, Euskadi nazioarteko hainbat forotan ordezkatuta dago, eta garrantzi berezia du Estatuan eta Europan. Oro har, lankidetza-posizio batetik edo lidergo-posizio batetik, balioa sortzen duen eskualdetzat hartzen da. Egoera hori aprobetxatu behar da erronkari aurre egiteko orduan.

Asmoa, printzipioak eta helburu estrategikoak

Asmoa, printzipioak eta helburu estrategikoak

Gizarteen eta haien ehun ekonomikoaren garapenaren gakoetako bat gizarteek hartzen duten zibersegurtasun-maila da. Herritarren segurtasun-maila apartekoa izanik, Euskadik zibersegurtasun-arriskuetatik babestu behar du bere burua, eta gizartea ahaldundu behar du eraldaketa digital seguru bat egiteko, etorkizunean behar bezala garatu ahal izateko.

Testuinguru horretan, helburu estrategikoak eraikitzeko oinarri gisa, Euskadiko Zibersegurtasun Estrategia arautzen duten helburuak eta printzipioak formulatu dira.

ASMOA

Zibersegurtasunaren Euskal Estrategiaren helburu nagusia Euskadi herrialde ziberresiliente bihurtzea da, bere Administrazio Publikoa eta enpresa-sarea IKTen esparruko arrisku eta mehatxuetatik babesteko gaitasunekin, eraldaketa digitalaren prozesuan gizartearen ahalduntzea sustatuz eta gaitasun horiek emanez zibersegurtasun globala garatzeko, nazioartean erreferentziazko lekua hartuz.

PRINTZIPIOAK

Euskadiko Zibersegurtasun Estrategia funtsezko sei printzipiotan oinarritzen da, eta horiek funtsezkoak dira estrategia eraginkor bat diseinatu eta gauzatzeko.

Funtsezko printzipioak

6. irudia: Zibersegurtasunaren Euskal Estrategiaren printzipioak

- **Erresilientzia:** Aldaketa teknologikoetara egokitzen gara eta mehatxu berrien aurrean erreakzionatzen dugu, funtsezko zerbitzuen jarraitutasuna eta eraginkortasuna ziurtatuz eta informazio sentikorra babestuz.
- **Lankidetza:** Zibersegurtasunaren alorreko ezagutzak, estrategiak eta jardunbide egokiak eraginkortasunez trukatzeko laguntzen dugu. Helburua da

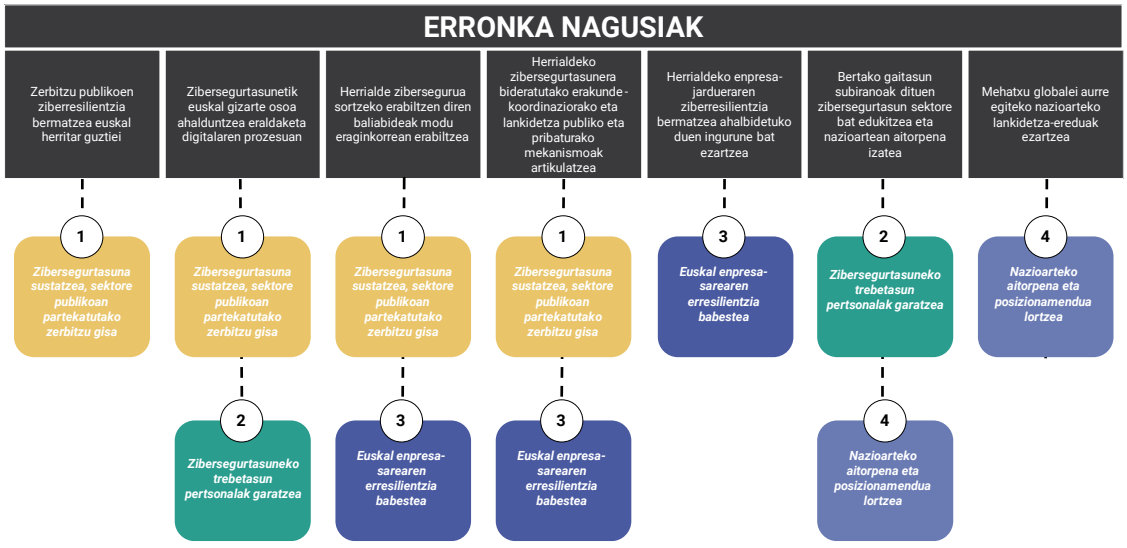
zibermehatxuen aurrean erantzun kolektiboa emateko gaitasuna hobetuko duen fronte bateratu bat finkatzea, horrela gure segurtasun digitalaren maila handituz.

- **Eraginkortasuna:** Prozedurak eta zeharkako konponbideak inplementatzen ditugu, identifikatutako sinergiak aprobetxatuz, eskura ditugun baliabideak eta zibersegurtasuneko gaitasunak optimizatzeko.
- **Hurbiltasuna:** Lotura sendoak sortzen ditugu, herritar guztiekiko komunikazioa errazteko, gure lanean hurbiltasuna sustatuz. Segurtasun digitalaren kultura guztiontzako irisgarria eta ulergarria sustatzen dugu, zibersegurtasuneko ekimenetan gizartearen parte-hartzea eta konpromisoa erraztuz.
- **Lidergoa:** Segurtasun digitalaren alorreko ekintzak bultzatzen eta gidatzen ditugu, erabaki proaktiboak hartuz eta helburu estrategiko argiak zehaztuz, helburu komunak lortzera bultzatuz eta motibatuz.
- **Berrikuntza eta etengabeko hobekuntza:** Erronka berriei heltzeko eta prozesuak optimizatzeko aukera emango diguten azken teknologia eta joerak hartzea sustatzen dugu.

HELBURUAK

Egoera horren aurrean, Euskadik lau helburu estrategiko nagusi lortu behar ditu 2024-2029 aldian.

Helburu estrategiko horietako bakoitza erronka bati edo gehiagori lotuta dago, honako irudi honetan erakusten den bezala:



7. irudia: Zibersegurtasunaren Euskal Estrategiaren helburuak

- **Zibersegurtasuna sustatzea, sektore publikoan partekatutako zerbitzu gisa:** Euskadiko Administrazio Publikoek, Eusko Jaurlaritza buru dutela, beharrezkoak diren lankidetza-ahalmen eta -mekanismoak hedatu behar dituzte, bai barnekoak, bai beste eragile batzuekikoak, herritarrei, enpresa-sareari eta euskal gizarte osoari zibersegurtasun-maila egokia bermatzeko, behar bezala gara daitezen eta beren eskubideak babes ditzaten.

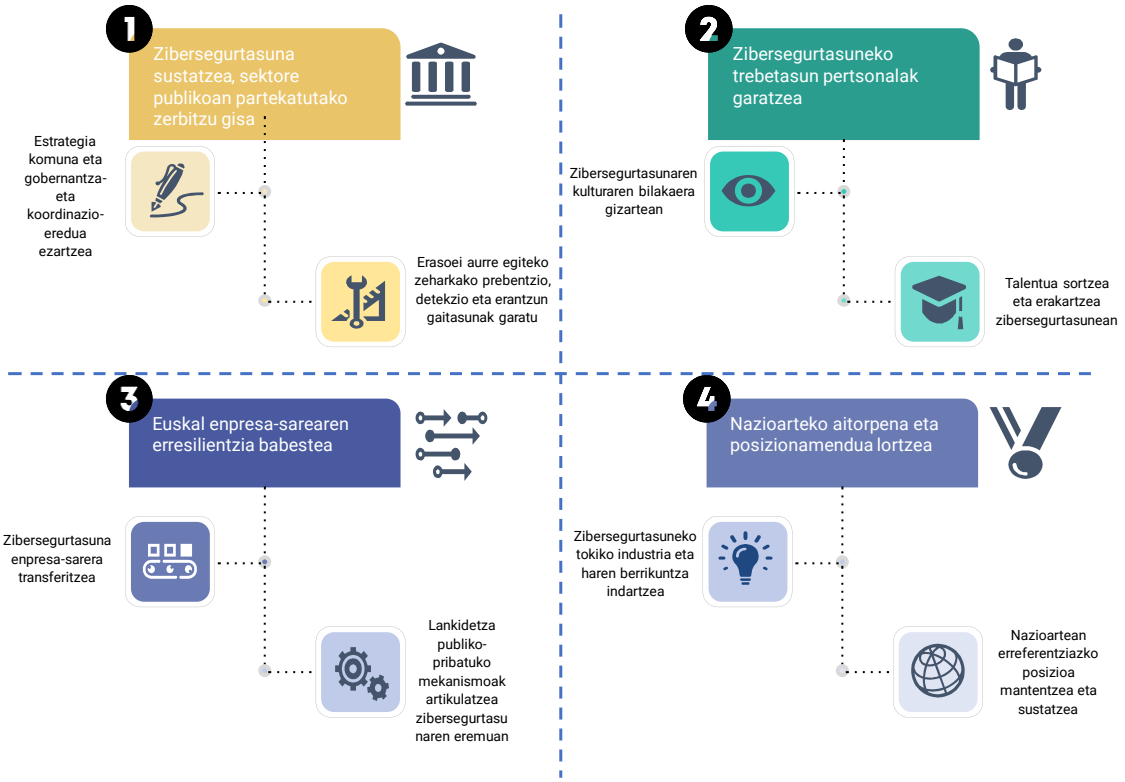
- **Zibersegurtasuneko trebetasun pertsonalak garatzea:** Pertsonak funtsezko alderdiak dira gizartea eraldaketa digitalean ahalduntzea lortzeko. Testuinguru horretan, estrategiak aukera eman behar die pertsonei trebetasun eta kultura nahikoak emateko, gero eta handiagoa den arrisku-ingurune batean askatasunez moldatzeko eta gure herrialdean beharrezko ezagutza sortzeko.
- **Euskal enpresa-sarearen erresilientzia babestea:** Zibersegurtasun-estrategiaren bidez, herrialdeko enpresa-sareak babes-maila handiena izatea bultzatu behar da, arrisku-egoera konplexuen aurrean erresiliente izan dadin. Alor publikoaren eta pribatuaren arteko lankidetzak eta enpresa-sare osorako dauden gaitasunak eskura jartzeak, enpresa traktoreetatik abiatuta, eremu horretako jarduera markatu behar dute.
- **Nazioarteko aitorpena eta posizionamendua lortzea:** Nazioarteko zibersegurtasuneko ekosistemaren barruan eragile garrantzitsua eta fidagarria izateak lankidetza-mekanismo hobeak artikulatzea ahalbidetzen du, ingurune konplexu eta asimetriko batean. Herrialdeari zibersegurtasun-ahalmen subiranoak ematea, puntako segurtasun-industria baten bidez, eta nazioartean giltzarri diren organismoetako kide izateak babes osoagoa zabaltzea ahalbidetuko du.

Jarduera-ildoak

Jarduera-ildoak

Jarraian, Estrategian identifikatutako erronka nagusiak ebazteko aukera emango duten jarduera-ildoak deskribatzen dira.

Ildo horretatik, jarduera-ildo bakoitza 2024-2029 aldirako ezarritako helburuak lortzeko helburua duten zenbait jarduera nagusik osatzen dute.



8. irudia: Zibersegurtasunaren Euskal Estrategiaren jarduera-ildoak

1. JARDUERA-ILDOA

Estrategia komuna eta gobernantza- eta koordinazio-eredua ezartzea

Sektore publikoak zibersegurtasunaren alorrean egiten duen jarduera bateratzea herrialde-ikuspegiarekin. Ikuspegi horretan, gizarte osoak segurtasun-maila berarekin jasoko ditu zerbitzu publikoak, edozein administrazio publikorekin jarduten duela ere.

Jarduera nagusiak:

- Zibersegurtasunaren alorrean Euskadiko sektore publikoaren lerrokatzea indartzeko eta koordinatzeko estrategia komuna hedatzea.
- Zibersegurtasunaren eremuan, Euskadiko administrazio publiko guztientzat beharrezkoak diren zerbitzuak modelatzea ahalbidetuko duen gobernantza-eredu bat hedatzea.
- Zibersegurtasunaren alorreko rolak eta erantzukizunak garatzea Euskadiko sektore publikoaren barruan, baterako jarduketa-eredu bat ezartzea ahalbidetzeko.
- Segurtasun-politiken, arau teknikoen eta babes-neurrien erreferentzia-eredu bat garatzea, dauden zibersegurtasun-araudiak osatzeko eta Euskadiko administrazio publiko guztien premia partikularrekin bat egiteko, haien hedapena errazteko.
- Berrikuspen-eredu bat sortzea, zerbitzu publikoek jasaten dituzten arrisku zibernetikoak identifikatu, ebaluatu eta kudeatzeko.
- Teknologiak ezartzeko esparru bat ezartzea, zeharkako gaitasunetan eta tresna komunetan oinarritua, eta adopzio berrietarako irizpide bateratuak emanez, hainbat alderdi kontuan hartuta, hala nola alderdi linguistikoak.
- Euskadiko administrazio publiko guztietan zibersegurtasunaren betetze-mailaren eta egoeraren aldizkako ebaluazioa.
- Lankidetza aktiboko mekanismoak sortzea, segurtasun integralaren eremuan, eta prozesu bateratu eta homogeneoak, hala eskatzen duten jarduketetarako.
- Euskadiko segurtasun publikoko planarekin bat egiteko plan bat sustatzea.

2. JARDUERA-ILDOA

Erasoei aurre egiteko zeharkako prebentzio, detekzio eta erantzun gaitasunak garatu

Zibersegurtasunaren alorreko arriskuei eta mehatxuei aurre egiteko beharrezko gaitasunak ematea Euskadiko sektore publikoari, ikuspegi holistiko eta eraginkor batetik.

Jarduera nagusiak:

- Cyberzaintzako CERTen gaitasunak indartu, zerbitzuak zabalduz eta zibererasoen prebentzio eta detekzio zein Euskadiko sektore publikoa babestera bideratu, eta, horrela, herrialdearen erresilientzia babestuz.
- Euskadiko sektore publikoan gertatutako zibererasoak kudeatzeko eta horiei erantzun koordinatua emateko beharrezkoak diren gaitasunak garatzea.
- Krisiak kudeatzeko prozedura ezartzea herrialde-mailan, Euskadiko eragile guztiak kontuan hartuta.
- Administrazio publiko guztientzat zaintza digitaleko eta alerta goiztiarreko eredu bat garatzea, Euskadira egokitutako arrisku-/herrialde-mapa bat garatzea barne.
- Kolektibo sentikorrei zuzendutako ekimen estrategikoei laguntzeko neurriak ezartzea, modu fokalizatuan eta horien arduradunekin koordinatuta.
- Zibererasoak ikertzeko gaitasunak handitzea, gizarte osoa babesteko eta Euskadiko polizia integralaren delitu zibernetikoak jazartzeko.
- Zibererasoei eta zibermehatxuei buruzko informazioa partekatzeko eredu bat garatzea.
- Zibersegurtasun-krisiak kudeatzeko eredu bat hedatzea eta entrenatzea, Euskadiko larrialdi-planarekin koordinatuta.
- Euskadiko zerbitzu publikoen eta funtsezko zerbitzuen erresilientzia-plan bat definitzea, haien babesa lehenesteko eta egokitzeko.
- Euskadiko administrazio publikoei laguntzeko zerbitzu bat abian jartzea, zibersegurtasuneko proiektu bereziak gauzatzeko eta hirugarrenak kudeatzeko.

3. JARDUERA-ILDOA

Zibersegurtasunaren kulturaren bilakaera gizartean

Herritarren artean zibersegurtasunaren alorreko sentsibilizazioa eta kontzientziazioa sustatzea, herrialdeko zibersegurtasunaren kultura hobetzeko.

Jarduera nagusiak:

- Zibersegurtasuna adin goiztiarretik landuko duten hezkuntza-programak sustatzea, Euskadin zibersegurtasunaren kultura garatzea ahalbidetuko dutenak, herritarrak eraldaketa digitalean ahalduntzera bideratuta.
- Zibersegurtasunari helduko dioten kontzientziazio-kanpainak garatzea, jardunbide seguruak eta jokabide arriskutsuen ondorioak nabarmenduz. Publiko zabalarengana iristeko komunikazio-kanal irisgarriak erabiltzea.
- Zibersegurtasunaren inguruko kontzientziazio-programa bat sortzea Ertzaintzako kideentzat eta Euskadiko polizia-kidegoentzat, Polizia eta Larrialdietako Euskal Akademiaren prestakuntzaren barruan sartzeko.
- Zibersegurtasunaren inguruko kontzientziazio- eta sentsibilizazio-programa bat sortzea langile publikoentzat eta politikarientzat.
- Euskadin dauden herritarren profilak egokitutako sentsibilizazio- eta kontzientziazio-programak diseinatzea.
- Gizarteak zibersegurtasunaren babesean parte-hartze aktiboa izan dezan sustatzea, gertakarien salaketa sustatuz eta etika digitala sustatuz. Erantzukizun partekatuko kultura bat sortzeak zibersegurtasuna indartzen du gizarteko maila guztietan.

4. JARDUERA-ILDOA

Talentua sortzea eta erakartzea zibersegurtasunean

Profesionalen artean talentua eta zibersegurtasuneko gaitasunak indartzea, hura erakarriz, garapen-planak eginez eta zibersegurtasunaren eremuko profilak birbideratuz.

Jarduera nagusiak:

- Beste eskualde eta kultura batzuetatik datozen eta zibersegurtasunean talentua erakartzea erraztuko duten mekanismoak hedatzea, gure gizartean integratzea indartuz.
- Hezkuntza-erakundeen eta enpresen arteko lankidetza estuko eredu bat abiaraztea, mentoretza-programak eta baterako proiektuak erraztuz, ikasleek beren ezagutzak benetako enpresa-inguruneetan aplikatzeko aukera izan dezaten.
- Profilak zibersegurtasunera bideratzeko eredu bat ezartzea, gaitasun teknikoaren, ziurtagirien, esperientzia praktikoaren eta arautu gabeko prestakuntzaren bidez. ITko profesionalentzako edo zibersegurtasunera aldatu nahi duten erlazionatutako eremuentzako berrentrenamendu-programak erraztea
- Prestakuntza espezializatuko eredu bat garatzea zibersegurtasuneko eremu guztietan, unibertsitateekin eta lanbide-heziketako zentroekin batera.
- Zibersegurtasunaren alorreko bokazioa bultzatzea, bai gaian interesa duten profilei dagokienez, bai ordezkaritza txikiagoa duten kolektiboei dagokienez, ekimen espezifikoen bidez.

5. JARDUERA-ILDOA

Zibersegurtasuna enpresa-sarera transferitzea

Herrialdeko enpresa-sareari zibersegurtasun-gaitasunak ematea ahalbidetuko dioten mekanismoak ezartzea, aurre egin behar dieten arriskuei eta mehatxuei aurre egiteko.

Jarduera nagusiak:

- Programa bat hedatzea, erakundeei aukera emango diena beren jardueraren barruan zibersegurtasuneko tokiko gaitasunak txertatzeko, eta tokiko teknologiak eta produktuak enpresen bidez nazioartekotzearen alde egiteko.
- Enpresa-sarearen heldutasuna eta lehia-posizioa identifikatzea ahalbidetuko duten behatoki sektorialak abian jartzea, bezeroentzako zibersegurtasunaren balioaren ikuspegitik.
- EAEko enpresa-ehunean zibersegurtasun-gaitasunak txertatzeko laguntza- eta aholkularitza-lerro bat ezartzea, Euskadiko zibersegurtasun-sektorearekin lehian sartu gabe.
- Sektoreko eragile garrantzitsuen arteko lankidetza sustatuko duten lantaldeak sortzea.
- Udaletan lagundutako harreman-sare bat hedatzea, zibersegurtasuna Euskadiko enpresa-sare osora iristeko.

6. JARDUERA-ILDOA

Lankidetza publiko-pribatuko mekanismoak artikulatzea zibersegurtasunaren eremuan

Erakunde publikoen eta ekosistema pribatuaren arteko lankidetza-mekanismoak sustatzea, erresilientzia indartzeko eta erasoek herrialdeko gizartean eta ehun ekonomikoan duten eragina murrizteko.

Jarduera nagusiak:

- Lankidetza publiko-pribatuaren mekanismoen aldeko apustua egitea, Euskadiko enpresa-sarearen eta funtsezko zerbitzuen erresilientzia bermatzeko, programa espezifikoen bidez eta BZP gisa existitzen diren programen laguntza eta osagarriaren bidez.
- Ekimen publiko-pribatuak eta zibersegurtasuneko kontsulta-organoak sustatzea.
- Sektore publikoaren eta pribatuaren artean gardentasuna eta konfiantza sustatzea, zibersegurtasunaren ekosistemari buruzko informazioa partekatzean eta erronkei aurre egiteko elkarrekin lan egitean.
- Zibermehatxuei eta ahultasunei buruzko informazioa partekatzeko komunikazio-kanalak ezartzea.
- Koordinazio-protokoloak eta -mekanismoak definitzea, erakunde publikoen eta pribatuen arteko lankidetza errazteko.

7. JARDUERA-ILDOA

Zibersegurtasuneko tokiko industria eta horren berrikuntza indartzea

Zibersegurtasunaren enpresa-sektorea indartzea, haren subiranotasuna sustatzea eta haren nazioartekotzea bultzatzea.

Jarduera nagusiak:

- Enpresa berritzaileak hazteko tresnak sortzea, enpresa horien iraunkortasuna eta euskal enpresa gisa finkatutako hazkundea ahalbidetzeko.
- Negozio-aukerak identifikatzea, ideia berritzaileak garatzea eta tokiko enpresa berriak sortzea ahalbidetuko duen behatoki bat identifikatzea eta abian jartzea, beharrezko baliabideak, esperientzia eta kontaktuak eskainiz.
- Tokiko zerbitzu eta hornitzaile homologatuen katalogo bat garatzea, kontratazio-prozesuetan erakunde potentzialak identifikatzeko prozesua errazteko.
- Industriarekin lankidetzan aritzeko programak definitzea, eragileen eta tokiko enpresen arteko lankidetza ahalbidetzeko, ikerketa aplikatua sustatzeko eta zibersegurtasuneko irtenbide berriak garatzeko, merkaturako transferentzia teknologikoa erraztuz.

8. JARDUERA-ILDOA

Nazioartean erreferentziazko posizioa mantentzea eta sustatzea

Euskadik zibersegurtasunaren alorrean estatuan eta nazioartean duen posizio nabarmena aktiboki sendotzea eta sustatzea.

Jarduera nagusiak:

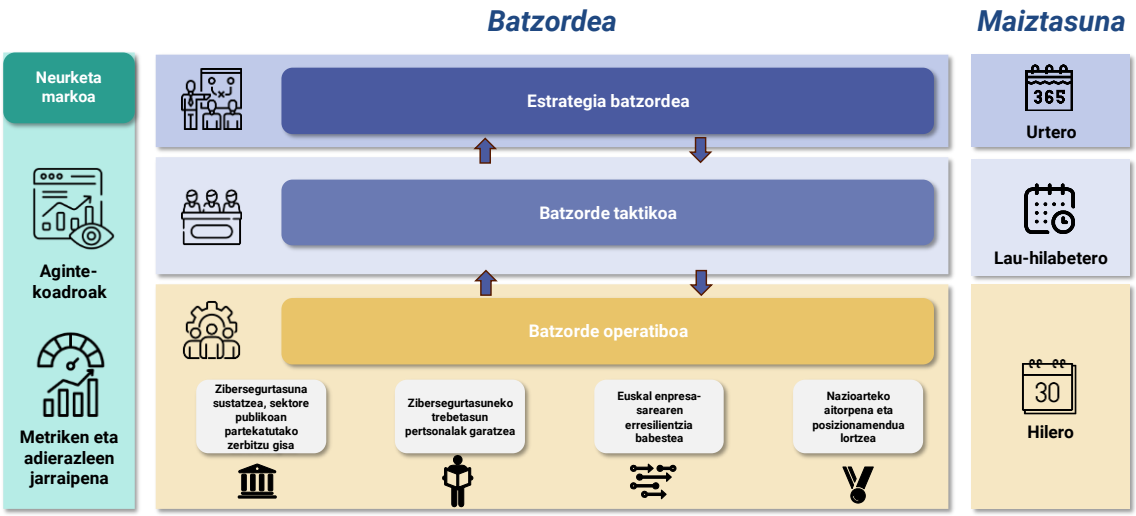
- Euskal erakundeek zibersegurtasunaren alorrean garrantzitsuak diren nazioarteko foro, hitzaldi eta ekitaldietan parte hartzea ahalbidetuko duten beharrezko mekanismoak definitzea eta ezartzea, Euskadin tokiko gaitasunak eta zerbitzuak zabaltzeko.
- Zibersegurtasuneko nazioarteko eta estatuko foro eta elkarte nagusietan Cyberzaintza sartzea, lankidetzarako eta balioa sortzeko erreferentziazko eragile gisa.
- Erakunde liderrak identifikatzea, baliabideetarako, ezagutza-iturri berrietarako eta ikusgarritasun handiagoko merkatuetarako sarbidea erraztuko duten aliantza estrategikoak ezartzeko.
- Euskal zibersegurtasunaren sektoreari laguntzea, nazioarteko posizionamendu- eta hazkunde-lanetan.
- Euskadin garatutako aurrerapenak eta gaitasunak ikusarazteko eta nazioarteko gizartearen esku jartzeko mekanismoak ezartzea.
- Estatuan, Europan eta nazioartean Euskadirekin zerikusia duten erreferenteen sare bat sortzea, Euskadiren aitorpena eta posizionamendua bultzatzeko.

Gobernantza-eredua

Gobernantza-eredua

Zibersegurtasunaren Euskal Estrategiaren ezarpen arrakastatsuak gobernantza-eredu sendo eta ondo egituratu bat eskatzen du, definitutako jardun-ildoetan inplikatutako eragile guztiak barne hartzen dituena.

Horretarako, hiru mailatan oinarritutako eta estrategiaren jarraipena egitea ahalbidetuko duen neurketa-esparru batek lagundutako erreakzio-batzorde eta mekanismoen eredu bat ezarri da.



9. irudia: Zibersegurtasunaren Euskal Estrategiaren gobernantza-eredua

Estrategian definitutako adierazleen egoera monitorizatzeko eta zaintzeko eginkizunak betetzeko, jarraipen- eta koordinazio-organo bat izendatuko da.

Jarraian, batzorde bakoitzaren lehendakaritzak, zein pertsonak osatu behar duten, eginkizunak, aldizkakotasuna eta jardun-eremua zehazten dira.

Estrategia batzordea
Lehendakaritza
⚷ Segurtasun Saileko burua, sailburu gisa.
Kideak
⚷ Euskadiko Zibersegurtasun Agentziaren Zuzendaritza Nagusia, Batzorde Taktikoarekiko lotura gisa ere jardunez. ⚷ Batzorde Estrategikoko buruak zehaztuko ditu Batzorde Estrategikoaren gainerako osaera eta antolaketa-arauak.
Funtzioak
• Batzorde Estrategikoaren lehendakaritzaren eginkizuna izango da Estrategia Neurtzeko Eredua onartzea, eta horren jarraipena Batzorde Estrategikoari aurkeztuko dio, hura biltzen denean. • Estrategiaren helburuen betetze-mailaren jarraipena. • Erabaki estrategikoak hartzea. • Adierazle garrantzitsuen azterketa orokorra. • Arriskuak gainbegiratzea. • Eskalatutako problemak ebaztea.
Maiztasuna
❖ Urtero.
Jarduera-eremuak
✓ Zeharkakoa.

Batzorde taktikoa
Lehendakaritza
⚷ Euskadiko Zibersegurtasun Agentziaren Zuzendaritza Nagusia.
Kideak
⚷ Euskadiko Zibersegurtasun Agentziaren Estrategia Zuzendaritza, Batzorde Operatiboekiko lotura gisa ere jardunez. ⚷ Batzorde Taktikoko buruak zehaztuko ditu Batzorde Taktikoaren gainerako osaera eta antolaketa-arauak.
Funtzioak
• Estrategiaren hedapenean egindako aurrerapena monitorizatzea ahalbidetuko duen neurketa-ereduaren proposamena. • Estrategiaren helburuen betetze-maila neurtzea. • Aurrekontuen analisia eta kudeaketa. • Jarduera-ildoen jarraipena eta koordinazioa. • Egindako jardueren eta mugarrien analisia. • Jarduera berrien plangintza. • Erabaki taktikoak hartzea. • Adierazleak definitzea eta gainbegiratzea. • Arriskuen kudeaketa. • Problemak ebaztea.
Maiztasuna
❖ Lau – hilabetero.
Jarduera-eremuak
✓ Zeharkakoa.

Batzorde operatiboa
Lehendakaritza
⚷ Euskadiko Zibersegurtasun Agentziaren Estrategia Zuzendaritza duen pertsona edo hark eskuordetzea aukeratzen duen pertsona, batzorde bat baino gehiago egon baitaitezke. Horretarako, kontuan hartuko da banakako batzorde bakoitzak zein jarduera-eremutara zuzentzen duen.
Kideak
⚷ Euskadiko Zibersegurtasun Agentziaren Estrategia Zuzendaritza duen pertsonak zehaztuko ditu batzordeen osaera eta antolaketa-arauak.
Funtzioak
• Estrategia neurtzeko eredua ezartzea eta mantentzea. • Aurrekontuak gauzatzea. • Lotutako jardueren eta zereginen jarraipen zehatza. • Lan-metodologiak eta ekintza operatiboak definitzea. • Egindako atazen analisia. • Zeregin berriak planifikatzea. • Erabaki operatiboak hartzea. • Adierazleak neurtu eta mantentzea. • Arriskuak eta arazoak eskalatzea.
Maiztasuna
❖ Hilero.
Jarduera-eremuak
✓ Zibersegurtasuna sustatzea, sektore publikoan partekatutako zerbitzu gisa. ✓ Zibersegurtasuneko trebetasun pertsonalak garatzea. ✓ Euskal enpresa-sarearen erresilientzia babestea. ✓ Nazioarteko aitorpena eta posizionamendua lortzea.

Jarraipena eta ebaluazioa

Jarraipena eta ebaluazioa

Euskadiko Zibersegurtasun Estrategiaren hedapenean egindako aurrerapenaren jarraipen eraginkorra eta zehatza ziurtatzeko, funtsezkoa da jarraipen-eredu eraginkorra izatea. Eredu horri esker, aurrerapena ebaluatu, desbideratzeak identifikatu eta neurri zuzentzaileak hartu ahal izango dira, ezarritako helburuak lortzen direla bermatzeko.

Neurketa-ereduak metrikak, adierazleak eta aginte-taula bat izan beharko ditu, estrategiaren ezarpenean izandako aurrerapena eraginkortasunez ebaluatzeko eta gainbegiratzeko.

Batzorde taktikoaren ardura izango da estrategiaren hedapenean izandako aurrerapena neurtzeko aukera emango duen eredu bat proposatzea.

Batzorde estrategikoaren lehendakaritzaren eginkizuna izango da Neurketa-eredua onartzea, eta horren jarraipena Batzorde Estrategikoari aurkeztuko dio, hura biltzen denean.

EUSKO JAURLARITZA
GOBIERNO VASCO