



Cyberzaintzaren Plan Estrategikoa 2025 - 2028

Aurkibidea

1	Sarrera	4
1.1	Dokumentuaren helburua	4
1.2	Testuingurua	4
1.2.1	Cyberzaintzari buruz	4
1.2.2	Zibersegurtasunaren Euskal Estrategia	4
2	Printzipioak.....	6
2.1	Egitekoa	6
2.2	Balio-proposamena	6
2.3	Jarduketa-eremuak	6
2.4	Hartzaileak	7
2.5	Kanalak	7
3	Ekintza-plana	8
3.1	Ekintza-ildoak	8
3.2	Hedatze-plana	9
3.2.1	Zerbitzuak	9
3.2.2	Gaur egungo egoera	13
3.2.3	Ibilbide-orria	49
3.2.4	Zerbitzuak emateko eredua	52
4	Gobernantza-eredua	53
4.1	Administrazio Kontseilua	53
4.2	Zuzendaritza Batzordea	53
4.3	Arloak	54
5	Jarraipena eta ebaluazioa	55
5.1	Jarraipen-sistema	55
5.2	Jarraipena egiteko mekanismoak	55
5.2.1	Arloko bilerak	55
5.2.2	Zuzendaritza Batzordearen bilerak	55
5.2.3	Administrazio Kontseiluaren bilerak	55
5.3	Ebaluazio-tresnak	55
5.3.1	Monografikoa	56
5.3.2	Aginte-taula	56

5.3.3	Adierazleen katalogoa	56
I. eranskina - Cyberzaintzaren 2025-2028 aldirako Plan Estrategikoaren	adierazleen katalogoa	57
II. eranskina – Jauraritzaren kudeaketa-adierazleak (2025)		63

1 Sarrera

1.1 Dokumentuaren helburua

Dokumentu honetan, Cyberzaintzaren 2025-2028 aldirako Plan Estrategikoa jasotzen da. Mugarri garrantzitsua da hau, Euskal Zibersegurtasunaren Agentzia sortzen duen Legea (7/2023 Legea, ekainaren 29koa) onetsi eta gero ondutako lehenengo plana delako.

Agentziaren datozen lau urteetako jarduerak eta helburuak gidatuko dituen esparru egituratu bat ezartzea da Plan Estrategikoaren helburua, eta hori, agentziaren jarduna 7/2023 Legean ezarritako eginkizunekin eta Zibersegurtasunaren Euskal Estrategiarekin (eskualdeko zibersegurtasun-arloko lehentasunak eta helburuak zehazten ditu) bat etorriko dela bermatuta.

1.2 Testuingurua

1.2.1 Cyberzaintzari buruz

Cyberzaintza (Euskal Zibersegurtasunaren Agentzia) Euskal Autonomia Erkidegoko sektore publikoko zuzenbide pribatuko ente publikoa da; nortasun juridiko propioa du, eta Segurtasun Sailari atxikita dago.

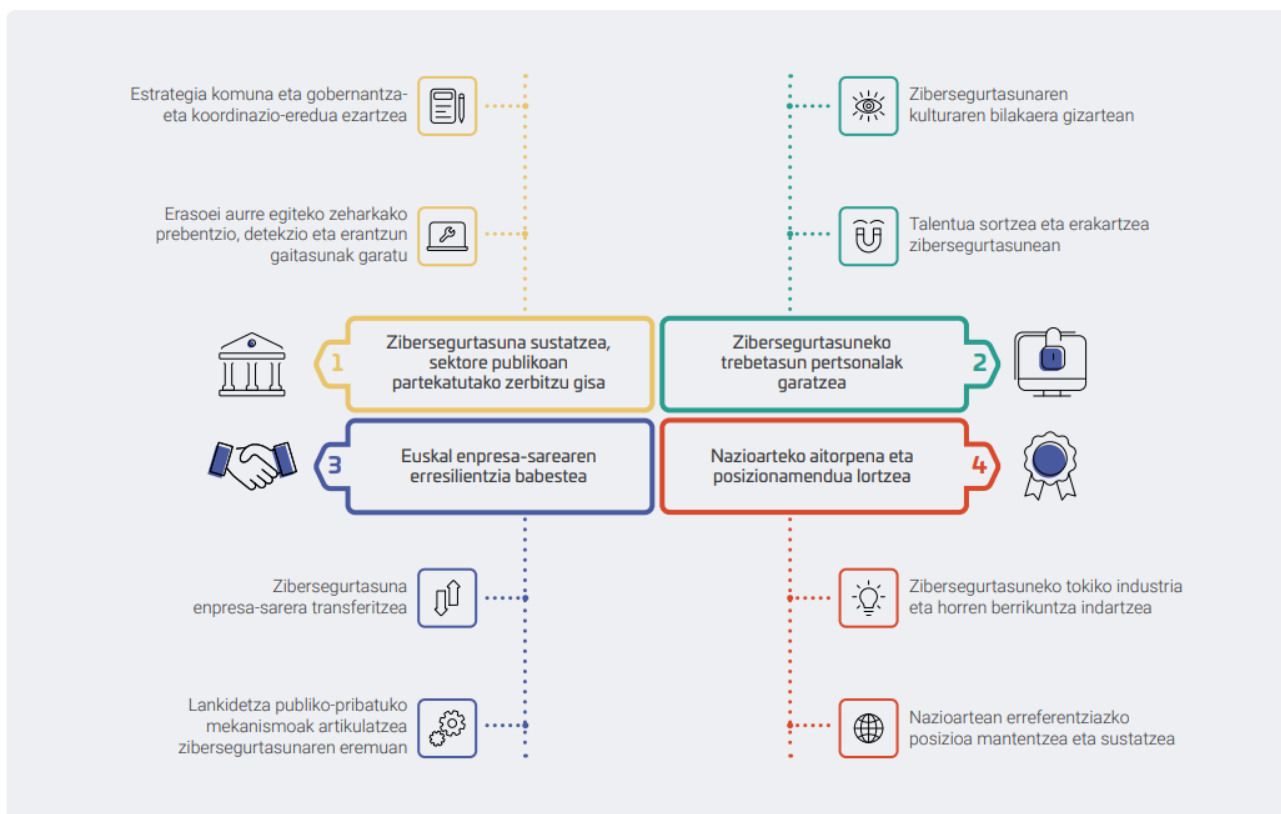
Euskal Autonomia Erkidegoko sektore publikoan zibersegurtasuna sustatzea eta koordinatzea da Cyberzaintzaren xedea, sektore horren eskumeneko informazio-sistemen eta sare elektronikoen segurtasunaren esparruan; halaber, Euskal Autonomia Erkidegoa, bertako Administrazio Publikoa, herritarrak eta enpresa-sarea zibersegurtasunean eta garapen digital seguruan treba daitezen babestu eta bultzatzea du xede.

[Euskal Zibersegurtasunaren Agentzia sortzen duen Legeak \(7/2023, ekainaren 29koa\)](#) 2. artikuluan ezartzen ditu agentziari dagokion eginkizunak, xede hori betetzeko.

1.2.2 Zibersegurtasunaren Euskal Estrategia

Zibersegurtasunaren Euskal Estrategiak (2024-2029), herrialdeak eremu horretan dituen erronkei heltzen die, eta lau helburu estrategiko ezartzen. Era berean, helburuok lortzeko zortzi jarduera-ildo zehazten dira, eta bakoitzak zenbait ekintza espezifiko biltzen ditu, eskudun agenteek bideratu beharko dituztenak. Estrategia honetan jasotzen diren jarduerak ez dituzte EAEko administrazio publikoak bakarrik inplikatzeko, baita herritar guztiak, enpresa-sarea eta zibersegurtasunaren sektore osoa ere.

EAE herrialde ziberresilientea bihurtzea da estrategiaren xedea, bere Administrazio Publikoa eta enpresa-sarea arrisku zibernetikoetatik babesteko gai izan dadin. Horretarako, gizartea eraldaketa digitaleko prozesuan ahalduntzea sustatzen du, eta zibersegurtasun orokorra garatzeko gaitasunak ematen, nazioartean erreferentzia izateko.



Zibersegurtasunaren Euskal Estrategiaren helburuak eta jarduerak

Cyberzaintzaren 2025-2028 aldirako Plan Estrategikoa bat dator, guztiz, Zibersegurtasunaren 2024-2029 aldirako Euskal Estrategiarekin, eta proposatutako ekintzek eta neurriek, Cyberzaintzaren misioa indartzeaz gainera, herrialdearen estrategian ezarritako helburuekin eta jarduketak-ildoekin bat egitea ziurtatzen du.

2 Printzipioak

2.1 Egitekoa

Agentziaren egitekoa da zibersegurtasuna sustatzea eta koordinatzea Euskal Sektore Publikoaren maiatzaren 12ko 3/2022 Legeak mugatutako euskal sektore publikoan, sektore horren eskumeneko informazio-sistemen segurtasunaren eta sare elektronikoen segurtasunaren esparruan; eta Euskal Autonomia Erkidegoa, bertako Administrazio publikoa, herritarrak eta enpresa-sarea zibersegurtasunean eta garapen digital seguruan treba daitezen babestea eta bultzatzea.

2.2 Balio-proposamena

Cyberzaintzak bere balio-proposamena aurkezten du, bere egitekoa bete eta Zibersegurtasunaren Euskal Estrategiarekin bat etortzeko. EAEn zibersegurtasuna indartzeko neurriak eta ekintzak sustatzea da proposamenaren helburua, eta, horri begira, lankidetzak, kontzientziazioa eta informatika-sistemen eta datu sentikorren babesa bultzatzen ditu.

- EAEko zibersegurtasuna sustatzen dugu.
- Beste batzuekin koordinatzen dugu zibersegurtasuna, EAEren barruan eta kanpoan.
- Zibersegurtasunaren Euskal Estrategiarekin eta aplikatzekoa den lege-esparruarekin bat gatoz.
- Estandarrak eta jarraibideak ematen ditugu.
- Gobernantza-, prebentzio-, detekzio- eta erantzun-zerbitzuak ematen ditugu.
- EAEko sektore publikoa, enpresa-sarea eta herritarrak ditugu xede.

2.3 Jarduketa-eremuak

Cyberzaintzaren jarduera lau jarduketa-eremutan sailkatzen da. Jarduketa-eremuok, esku hartzeko eremuak zehazteaz gain, zibersegurtasunaren askotariko alderdiak modu integralean jorratzeko esparru egituratu bat ezartzen dute, bat etorrita nazioartean aintzatetsitako jardunbide egokien estandarrekin.

Hona hemen lau jarduketa-eremuak:

- **Prebentzioa:** segurtasun-gertakari posibleak gertatu aurretik saihestera bideratutako zerbitzu guztiak sartzen dira hemen.
- **Detekzioa:** segurtasun-gertakariak goiz identifikatzea, sistemak eta erremintak erabilia. Detekzio goiztiarrak aukera ematen du edozein mehatxuri azkarrago eta eraginkortasunez erantzuteko.
- **Erantzuna:** segurtasun-gertakaria detektatu ondoren behar diren zerbitzuak biltzen ditu.
- **Gobernantza:** zibersegurtasuna modu integralean kudeatzeko behar diren jarraibideak eta egiturak ezartzen ditu.

2.4 Hartzaileak

Cyberzaintzak askotariko publikoa du xede, hau da, EAEko sektore publikoa, enpresa-sarea eta herritarrak. Zerbitzuen eskaintza hainbat bertikaletan segmentatuta dago, sektore bakoitzaren premia espezifikoak asebetetzeko. Ingurune bakoitzeko zibersegurtasun-premiak berariaz jorratzea eta zerbitzuak premia partikular horietara egokitzea da segmentazio horren funtsezko helburua.

Hona hemen orain arte zehaztutako bertikal nagusiak:

Hartzaileak	Bertikala
Sektore publikoa	Sektore publikoa – Administrazioa Segurtasuna Osasuna Hezkuntza
Enpresak	Enpresa estrategikoak Autobabes-arloan betebeharrak dauzkaten enpresak Beste enpresa batzuk
Herritarrak	Adingabeak Helduak

2.5 Kanalak

Cyberzaintzak zuzenean ematen die zerbitzu bertikalei, edo, bestela, hainbat kanal erabiltzen ditu zerbitzuak antolakunde hartzailerara iristea ziurtatzeko. Prozesua honako premisa hauei jarraikiz gauzatzen da:

- Sektore publikorako zerbitzuak Cyberzaintzak ematen ditu zuzenean, salbuespen hauekin:
 - Ezagutzen transferentzia **Polizia eta Larrialdietako Euskal Akademiarekin, Administrazio Publikoaren Euskal Institutuarekin eta arlo horretan lan egiten duten beste entitate edo egitasmo publiko batzuekin** egindako akordioen bidez kudeatzen da.
 - 20.000 biztanle baino gutxiagoko udalerriei zerbitzu emateko, Cyberzaintza dagokion **foru-aldundiarekin** koordinatzen da.
- Enpresei, berriz, Cyberzaintzak zuzenean ematen die zerbitzu; hala ere, aldi baterako akordioak egin daitezke arlo horretan lan egiten duten **klusterrekin, enpresa elkarteekin eta bestelako entitate edo egitasmo publikoekin**.
- Herritarrei, azkenik, Cyberzaintzak norabide bakarrean eskaintzen die zerbitzua, baita ekintza espezifikoek bitartez ere, zeinak hauen bidez bidera baitaitezke: **Hezkuntza Saila, Ertzaintza, Lanbide, KZ Gunea, Tknika** eta **irabazi-asmorik gabeko elkarteak** eta **entitateak**.

3 Ekintza-plana

3.1 Ekintza-ildoak

Ezarritako printzipioei jarraikiz, Cyberzaintzaren egitekoa eta eginkizunak betetzeko hamaika ekintza-ildo zehaztu dira. Ekintza-ildo bat zibersegurtasunaren eremuan helburu jakin bat lortzera bideratutako jarduera espezifikoaren multzo bat da. Hona hemen ekintza-ildoaren deskribapen laburra:

- **Auditoretza**

Auditoretzaren ekintza-ildoaren helburu nagusia da zibersegurtasuneko funtsezko araudiak betetzen direla ebaluatzea eta ziurtatzea, bai eta ebaluazioari jarraipena egiten laguntzea ere.

- **Kontzientziazioa**

Kontzientziazioaren ekintza-ildoaren helburu nagusia da zibersegurtasunaren kultura sendo bat sustatzea eta, era berean, gizabanakoek nahiz antolakundeek egungo ingurune digitalen arrisku digitalen buruzko ezagutza- eta ulermen-maila handiagoak izatea. Gainera, teknologiaren erabileran jokabide seguruak eta arduratsuak sustatu nahi ditu.

- **Aholkularitza**

Aholkularitzaren ekintza-ildoaren helburu nagusia da zibersegurtasunaren arloko problematika hobeto ulertaraztea eta proiektu espezifikoaren kudeaketan laguntzea.

- **Koordinazio estrategikoa**

Koordinazio estrategikoaren ildoaren helburu nagusia da zibersegurtasun-baliabideak zeharkako ikuspegi batetik koordinatzea, horien efizientzia optimizatu eta hobetzeko.

- **Arriskuaren kudeaketa**

Arriskuaren kudeaketaren ekintza-ildoaren helburu nagusia da zibersegurtasunarekin lotutako arrisku teknologikoak eta antolamenduko arriskuak identifikatzea, ebaluatzea eta arintzea. Ikuspegi integral horrek aukera ematen die antolakundeei beren arrisku-mailaren ikuspegi argia eta zeharkakoa lortzeko, eta, hala, erabaki informatuak hartzea eta babes-neurri egokiak ezartzea errazten da.

- **Mehatxuen alorreko inteligentzia**

Mehatxuen alorreko inteligentziaren ekintza-ildoak helburu du antolakundeei zibersegurtasunaren eremuko balizko mehatxuei buruzko informazio garrantzitsua eta prozesagarria ematea. Horrek erraztu egiten die erasoei aurrea hartzea, erabaki informatuak hartzea eta babesa indartzea.

- **EAEko segurtasun-eredua**

EAEko segurtasun-ereduaren ekintza-ildoaren helburu nagusia da zibersegurtasuneko esparru integral bat ezartzea, horren bidez bermatzeko ingurune digitala segurua eta zibermehatxuekiko erresilientea izatea. Eremu digitalerako eredu hori bat etorriko da EAEko Segurtasun Publikoko Plan Orokorrearekin, eta, beraz, lurraldeko erronkei erantzuneko dien segurtasun-eredu integral eta zabalago baten zati izango da.

- **Segurtasun-arloko operazioak (SOC)**

Segurtasun-arloko operazioen ekintza-ildoaren helburu nagusia da antolakundeen azpiegitura teknologikoak etengabeko monitorizazioaren bidez babestea, horrek murriztu egiten baitu zibersegurtasun-gertakarien aurrean erantzuteko denbora.

- **Gertakariei erantzutea (CSIRT)**

Segurtasun Informatikoko Gertakariei Erantzuteko Taldearen (CSIRT) ekintza-ildoaren helburu nagusia da antolakundeei laguntzea segurtasun-gertakariak kudeatzen. Ikuspegi integral batetik, hainbat entitateri eragiten dieten gertakarien aurrean eman beharreko erantzuna koordinatu nahi da, eta informazio erabakigarria partekatu, gainerakoak babesteko.

- **Segurtasun ofentsiboa**

Segurtasun ofentsiboaren ekintza-ildoaren helburu nagusia da antolakundeen sistemetan mehatxuak eta ahultasunak identifikatzea, erasotzaile batek halakoak hauteman aurretik, eta, horrela, balizko zibererasoen aurrean defendatzeko gaitasuna indartzea.

- **Ezagutzaren transferentzia**

Ezagutzaren transferentziaren ekintza-ildoaren helburu nagusia da zibersegurtasuneko espezializazioa eta trebetasunen garapena sustatzea, bai eta Cyberzaintzaren erabiltzaileetara jardunbideak eta arrakasta-kasuak esportatzea ere. Gainera, heldutasun-maila handiagoa duten entitateetatik heldutasun-maila txikiagoa dutenetara jarduteko moduak, dokumentazioa, klausulak, etab., esportatu nahi dira. Hala, ezagutzak eta praktikak trukatzea sustatzen da, zibersegurtasunaren estandar orokorra igotzeko.

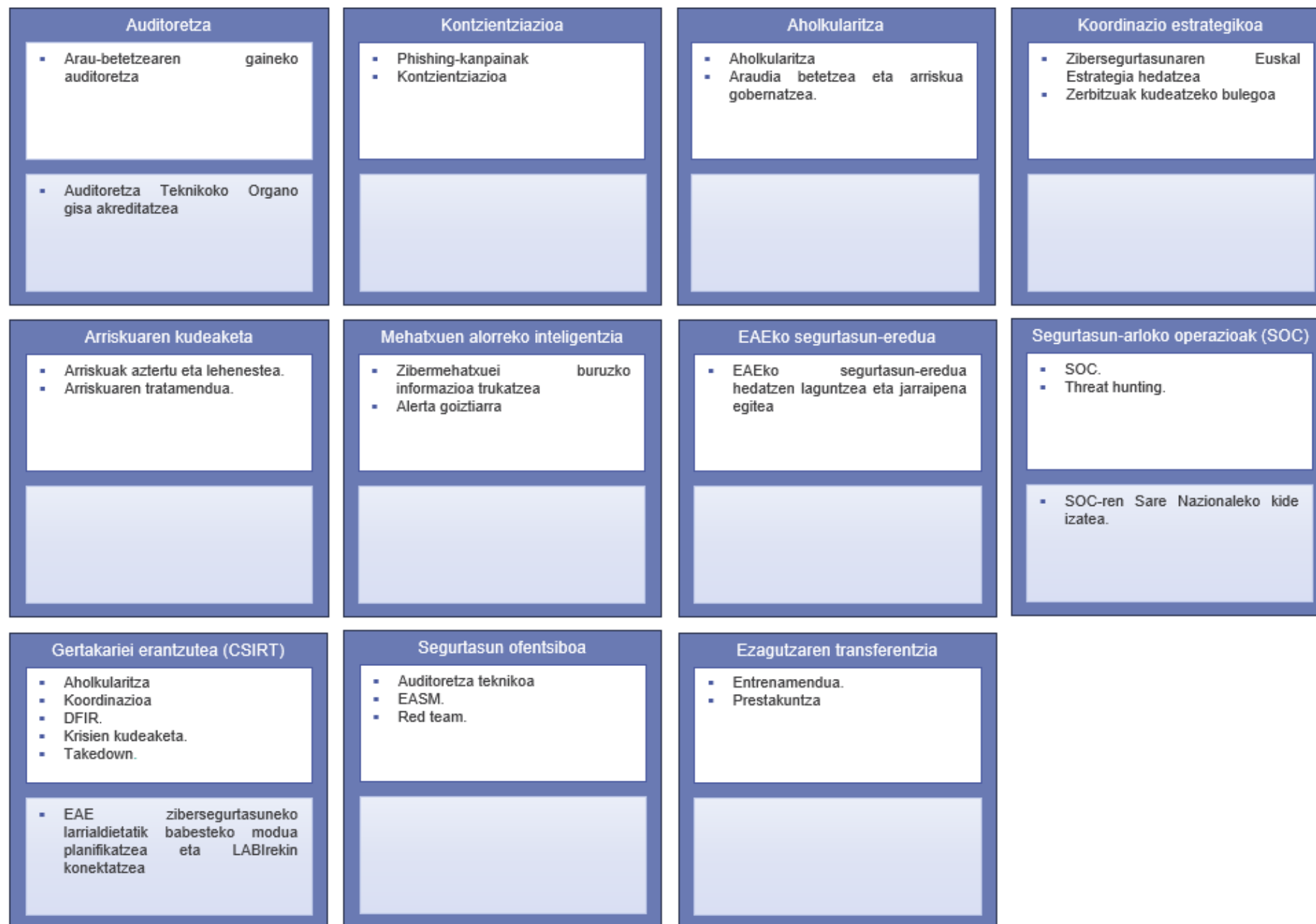
3.2 Hedatze-plana

3.2.1 Zerbitzuak

Ekintza-ildoak, batez ere, zerbitzu gisa ezarriko dira. Ekintza-ildo bakoitza bat dator zerbitzu-ildo batekin, non antzeko ezaugarriak eta helburu komun bat dauzkaten banakako zerbitzu ugari biltzen baitira. Horrela, jardunean koherentzia estrategikoz jokatzeko bermatzen da.

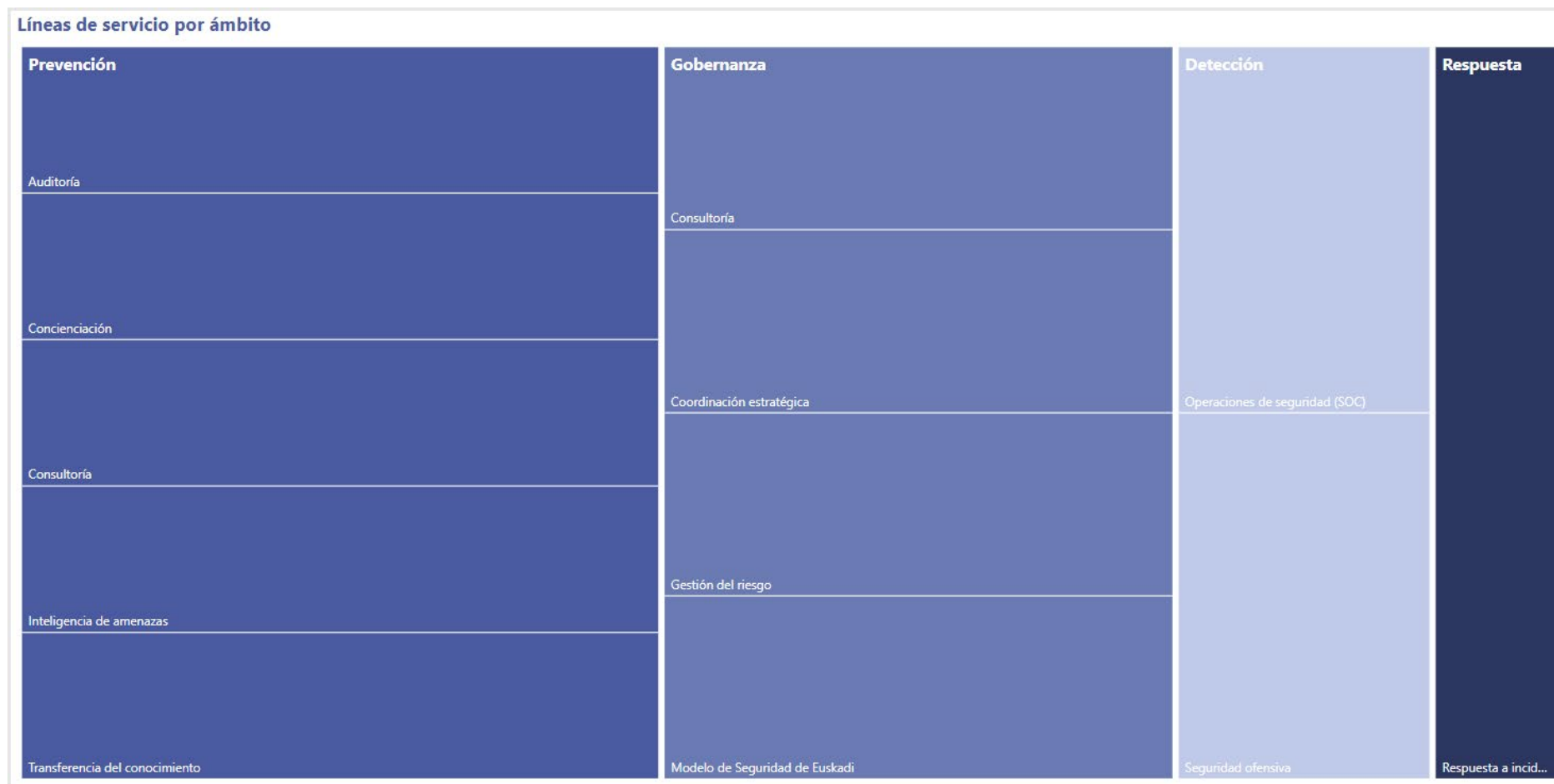
Zerbitzuen estalduratik at leudekeen jardueretan, ekintza-ildoak egitasmo osagarrien bidez zabalduko dira.

Taula honetan, zerbitzuak (ildoaren arabera) eta orain arte identifikatutako egitasmo osagarriak laburbiltzen dira:



3.2.1.1 Zerbitzu-ildoak, eremuaren arabera

Grafiko honetan, zerbitzu-ildoak jarduketa-eremuen arabera nola antolatzen diren ikusten da:



3.2.1.2 Barne-zerbitzuak

Jarduera hauek guztiak garatzeko, Cyberzaintzaren jarduna ahalbidetuko duten eta funtzionamendu ona ziurtatuko duten zenbait barne-zerbitzu behar dira. Barne-zerbitzuek barruan hartzen dituzte proposatutako ekintzak benetan ezartzeko ezinbestekoak diren euskarri-arloak. Hona hemen barne-zerbitzuak:

Administrazioa eta Zerbitzuak

- Alderdi ekonomikoak eta langileen kontuak kudeatzea, araudi juridiko aplikagarria betetzen dela ziurtatzea eta agentziaren funtzionamendu osoari laguntzeko zerbitzu orokorrak ematea du helburu.

Zibersegurtasuneko I+G+B berrikuntza-proiektuak garatzen laguntzea

- Zerbitzuaren helburua da Europako partzuergoetan parte hartzea sustatzea, soluzio berritzaileak goiz har daitezen sustatzea eta administrazio publikoak babesteko erabilera-kasuak identifikatzea.

Cyberzaintzaren arau-betetzea

- Euskal Zibersegurtasunaren Agentzian aplikatzekoa den araudia betetzea da zerbitzuaren helburua.

Cyberzaintzaren Plan Estrategikoa garatu eta hedatzea

- Cyberzaintzaren Plan Estrategikoa garatu eta betearaztea da zerbitzuaren helburua, koherentzia estrategiko eraginkorra ziurtatzeko xedez. Hor barruan sartzen da zehaztutako estrategia ezartzeko ekintza-plan bat egitea eta plan horren ezarpena ebaluatu eta etengabe monitorizatzea.

Segurtasun korporatiboa

- Zerbitzuaren helburua da antolakundearen azpiegitura eraginkortasunez administratzen dela bermatzea, agentziaren aktibo fisiko eta digitalak babestea eta informazioaren osotasuna eta konfidentziasuna ziurtatuko dituzten segurtasun informatikoko kontrolak ezartzea da.

Komunikazio-zerbitzua

- Cyberzaintzaren eta hartzaileen arteko elkarerraginari bide ematea da zerbitzuaren helburua, informazio garrantzitsua argi eta irisgarri helaraztea ziurtatzeaz batera. Hor barruan sartzen da politikei, programei eta zerbitzuei buruzko informazioa ematea eta, aldi berean, irudi instituzional ona edukitzea, barne- eta kanpo-komunikazioa kudeatzea, komunitatearen kezkei erantzutea eta organismoaren eta gizartearen arteko konfiantza indartzea.

3.2.2 Gaur egungo egoera

Zerbitzuen katalogoak banakako 24 zerbitzu jasotzen ditu, 11 zerbitzu-ildotan antolatuta. Xede-publiko bakoitzari zer zerbitzu eskainiko zaizkion zehaztu da. Eskaintza taula honetan dago:

Línea del servicio	Ciudadanía	Empresas	Sector Público
Auditoría		✖	✖
Concienciación	✔	✖	✖
Consultoría		✖	✖
Coordinación estratégica		✖	✖
Gestión del riesgo		✖	✖
Inteligencia de amenazas	✔	✔	✔
Modelo de Seguridad de Euskadi		✖	✖
Operaciones de seguridad (SOC)			✖
Respuesta a incidentes (CSIRT)	✔	✔	✔
Seguridad ofensiva		✖	✖
Transferencia del conocimiento		✖	✖

Las líneas de servicio con un rombo rojo no están activas, mientras que las marcadas con un círculo verde sí lo están.

Erronbo gorria duten zerbitzu-ildoak ez daude erabilgarri; borobil berdea dutenak, ordea, bai. Gaur egun, zehaztutako zerbitzuen % 28,37 aktibatu dira. Balio hori kalkulatzeko, bertikalen arabera segmentatutako zerbitzu-eskaintza hartu dugu kontuan.

Zerbitzu bakoitzari buruzko informazio xehea jaso dugu hemen: dagokion ildo, zerbitzuaren deskribapena, zerbitzua ematen zaien bertikalen xehetasunak eta zerbitzuaren jarduketa-eremua.

Auditoretza

Línea del servicio	Empresas	Sector Público
Auditoría		
Auditoría al cumplimiento normativo		

Ficha de servicio

Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Auditoría

Servicios

Auditoría al cumplimiento normativo

Ámbito

Prevención

Línea del servicio

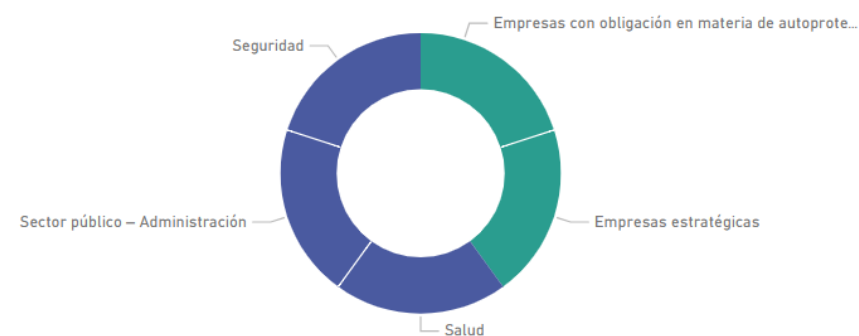
Auditoría

Verticales

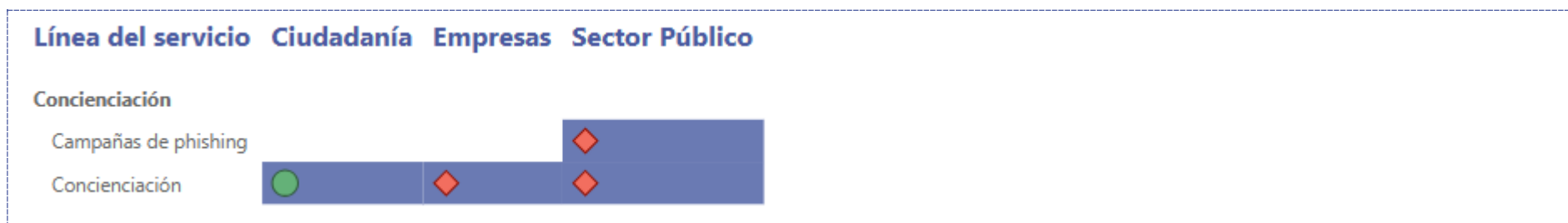
● Empresas ● Sector Público

Descripción del servicio

El servicio de auditoría de cumplimiento normativo se orienta a revisar y asegurar que las organizaciones cumplan con las principales normativas de seguridad y marcos de referencia aplicables. Este proceso incluye la evaluación de la implementación correcta de los controles establecidos, a través de evaluaciones periódicas que buscan identificar posibles áreas de mejora. Si se detectan incumplimientos, se proponen soluciones adecuadas para corregirlos. Además, el servicio ofrece seguimiento y apoyo continuo para facilitar el cumplimiento de las normas de seguridad aplicables. Este servicio también abarca el soporte en la elaboración de los planes de continuidad en materia de ciberseguridad para ciertas actividades sujetas a la norma vasca de autoprotección, asegurando que dichos planes cumplan con los requisitos mínimos establecidos.



Kontzientziazioa



Ficha de servicio

Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Concienciación

Servicios

Campañas de phishing

Concienciación

Ámbito

Prevención

Línea del servicio

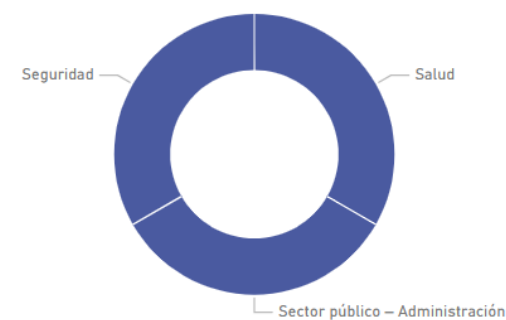
Concienciación

Verticales

● Sector Público

Descripción del servicio

El servicio de campañas de phishing realiza ataques de phishing específicamente diseñados para evaluar y fortalecer la capacidad de una organización para detectar y responder ante estas amenazas. Los resultados de estas campañas proporcionan información valiosa sobre las debilidades existentes, facilitando el desarrollo de estrategias de capacitación y mejora continua.



Ficha de servicio

Información detallada de los servicios

Filtro por línea del servicio

Concienciación

Servicios

Campañas de phishing

Concienciación

Ámbito

Prevención

Línea del servicio

Concienciación

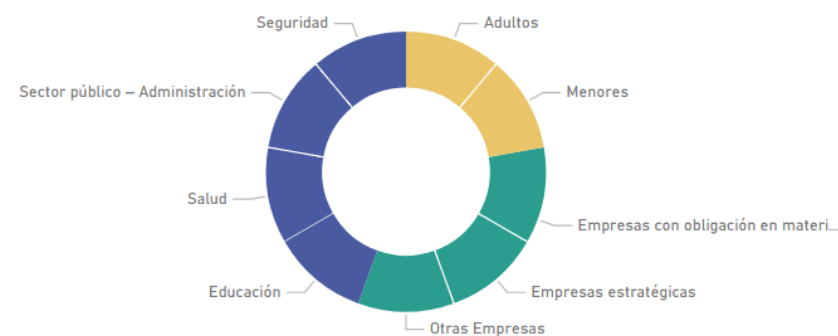
Descripción del servicio

El servicio de concienciación consiste en la organización de jornadas educativas para reforzar el conocimiento y la cultura de ciberseguridad entre los ciudadanos y las organizaciones de Euskadi. Su propósito es aumentar la conciencia sobre los diversos riesgos digitales presentes en el mundo actual y proporcionar a las personas participantes las habilidades necesarias para utilizar internet y las nuevas tecnologías de manera más segura y responsable.

Este servicio se complementa con iniciativas específicas dirigidas a colectivos particulares, como profesionales de la ciberseguridad, personas mayores o menores de edad. Estas iniciativas incluyen la elaboración de materiales específicos, la organización de actividades recreativas o el diseño de campañas especializadas, entre otras.

Verticales

● Ciudadanía ● Empresas ● Sector Público



Aholkularitza

Línea del servicio	Empresas	Sector Público
Consultoría		
Consultoría		
Gestión de proyectos especiales		

Ficha de servicio

Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Consultoría

Servicios

Consultoría
Gestión de proyectos especiales

Ámbito

Prevención

Línea del servicio

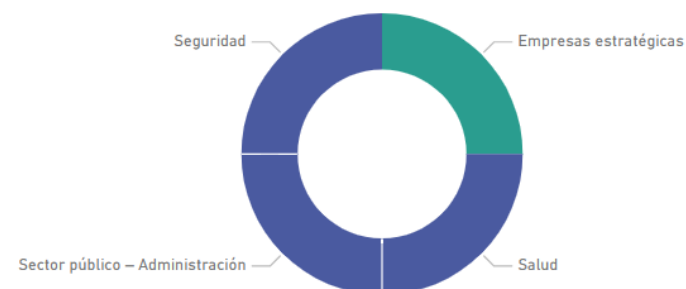
Consultoría

Verticales

● Empresas ● Sector Público

Descripción del servicio

El servicio de consultoría incluye el acompañamiento para diseñar planes de ciberseguridad y su seguimiento. Asimismo, ofrece asistencia en la identificación de necesidades específicas en el ámbito de la ciberseguridad y brinda apoyo en la elaboración de los planes formativos para los clientes.



Ficha de servicio

Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Consultoría

Servicios

Consultoría

Gestión de proyectos especiales

Ámbito

Gobernanza

Línea del servicio

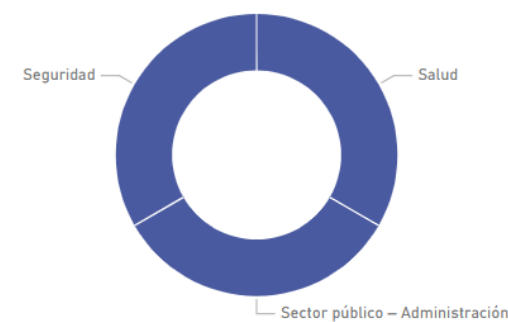
Consultoría

Verticales

● Sector Público

Descripción del servicio

El servicio de gestión de proyectos especiales ofrece soporte en la gestión de iniciativas específicas relacionadas con la ciberseguridad dentro del sector público en Euskadi. Asimismo, proporciona ayuda en la gestión de los riesgos vinculados a dichos proyectos y asesora en la contratación de servicios de Ciberseguridad.



Koordinazio estrategikoa

Línea del servicio	Empresas Sector Público	
Coordinación estratégica		
Despliegue de la Estrategia de Ciberseguridad de Euskadi		
Oficina de gestión de servicios		

Ficha de servicio

Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Coordinación estratégica

Servicios

Despliegue de la Estrategia de Ciberseguridad de Euskadi

Oficina de gestión de servicios

Ámbito

Gobernanza

Línea del servicio

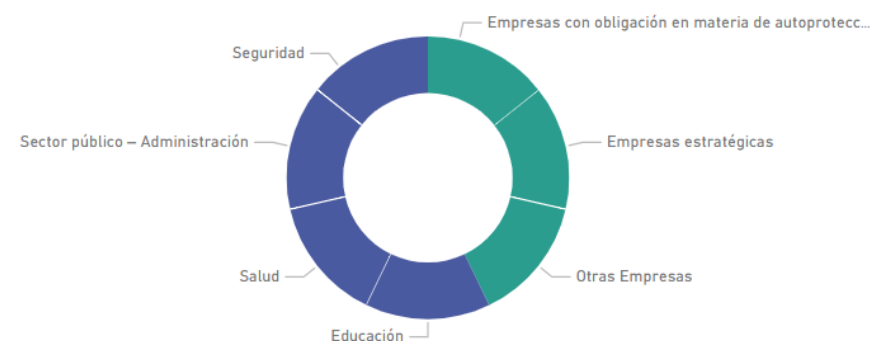
Coordinación estratégica

Verticales

● Empresas ● Sector Público

Descripción del servicio

Desde el servicio de despliegue de la Estrategia de Ciberseguridad de Euskadi se participa activamente en los órganos de gobierno definidos en la Estrategia de Ciberseguridad de Euskadi 2024-2029, con el fin de promover su implementación. Este servicio se ocupa de evaluar y supervisar el progreso de la estrategia, impulsando que las acciones planificadas se lleven a cabo de manera efectiva y de que los objetivos de ciberseguridad para la región se alcancen.



Ficha de servicio

Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Coordinación estratégica

Servicios

Despliegue de la Estrategia de Ciberseguridad de Euskadi

Oficina de gestión de servicios

Ámbito

Gobernanza

Línea del servicio

Coordinación estratégica

Verticales

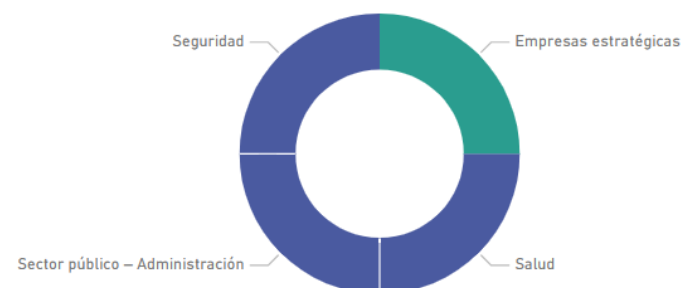
● Empresas ● Sector Público

Descripción del servicio

El servicio de oficina de gestión de servicios se encarga de la activación, gestión y seguimiento de la demanda de Cyberzaintza. Este servicio identifica las necesidades específicas de los públicos objetivo y las traslada internamente para ser gestionadas con las áreas correspondientes.

Además, establece el modelo de gobernanza para coordinar las actuaciones del sector público de Euskadi en materia de ciberseguridad, definiendo los roles y responsabilidades necesarios para su implementación. Y supervisa el nivel de despliegue de las acciones programadas y de los modelos establecidos, utilizando indicadores específicos a través del personal técnico delegado.

Asimismo, apoya el desarrollo de las iniciativas de la agencia ofreciendo una perspectiva integral que permite proporcionar información relevante a otras áreas de la Agencia.



Arriskuaren kudeaketa

Línea del servicio	Empresas	Sector Público
Gestión del riesgo		
Analítica y priorización del riesgo		
Tratamiento del riesgo		

Ficha de servicio

Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Gestión del riesgo

Servicios

Analítica y priorización del riesgo

Tratamiento del riesgo

Ámbito

Gobernanza

Línea del servicio

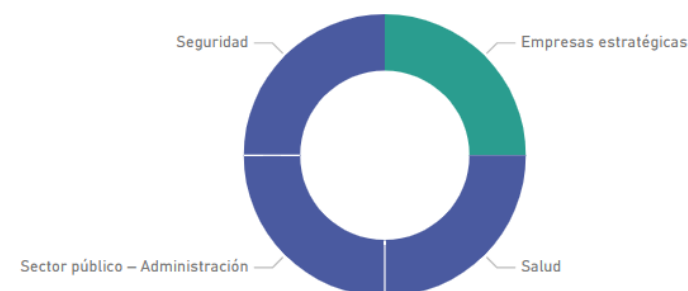
Gestión del riesgo

Verticales

● Empresas ● Sector Público

Descripción del servicio

El servicio de analítica y priorización del riesgo se basa en el framework de gestión del riesgo de Cyberzaintza, ofreciendo una visión integral y transversal de los riesgos de ciberseguridad en toda la Comunidad Autónoma del País Vasco. A través de este marco, se identifican los riesgos específicos que deben ser normalizados, asegurando una consideración y gestión adecuadas de todos los riesgos relevantes. La función predominante de este servicio consiste en evaluar tanto los riesgos tecnológicos como organizativos, priorizándolos según su impacto y probabilidad, y comunicando efectivamente dichos riesgos a las partes interesadas. Además, se implementa como un sistema dinámico que actualiza y mejora continuamente la medición para reflejar los cambios en el entorno de amenazas y las mejores prácticas en ciberseguridad.



Ficha de servicio

Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Gestión del riesgo

Servicios

Analítica y priorización del riesgo

Tratamiento del riesgo

Ámbito

Gobernanza

Línea del servicio

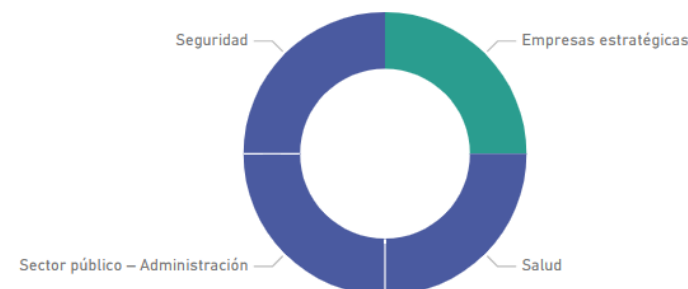
Gestión del riesgo

Verticales

● Empresas ● Sector Público

Descripción del servicio

El servicio de tratamiento del riesgo comprende una evaluación exhaustiva del nivel de riesgo de cada cliente, teniendo en cuenta sus características particulares y el entorno en el que operan. Los riesgos identificados se gestionan a lo largo de su ciclo de vida, desde la identificación y evaluación inicial hasta la implementación de medidas de mitigación y el monitoreo continuo, incluyendo la gestión de excepciones de seguridad. Se definen y priorizan las acciones necesarias para mitigar los riesgos más críticos y, además, se identifican y planifican proyectos específicos para coordinar estas acciones de mitigación. Todo el proceso de seguimiento y gestión de riesgos se lleva a cabo de acuerdo con el framework de gestión del riesgo de Cyberzaintza, garantizando una metodología consistente y efectiva.



Mehatxuen alorreko inteligentzia

Línea del servicio	Ciudadanía	Empresas	Sector Público
Inteligencia de amenazas			
Alerta temprana			
Intercambio de información sobre ciberamenazas			

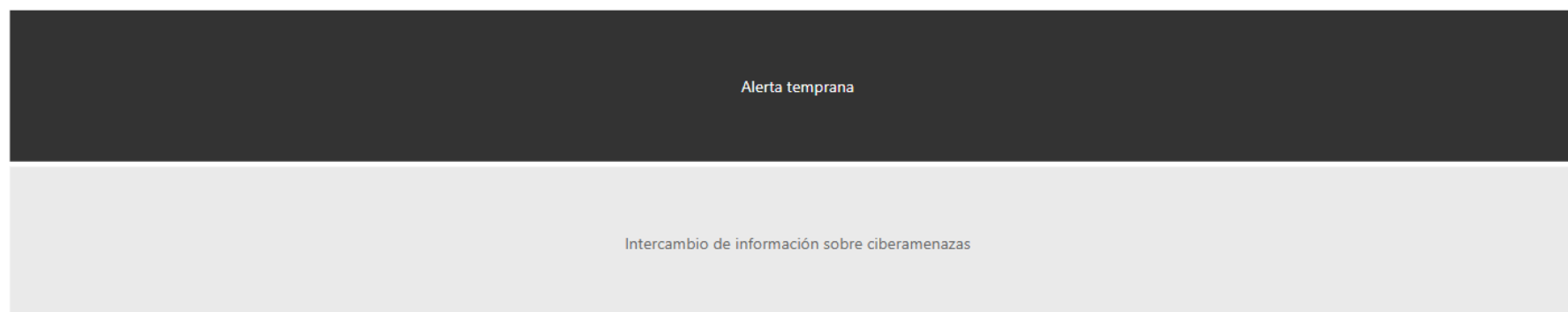
Ficha de servicio

Información detallada de los servicios

Filtro por línea del servicio

Inteligencia de amenazas

Servicios



Ámbito

Prevención

Línea del servicio

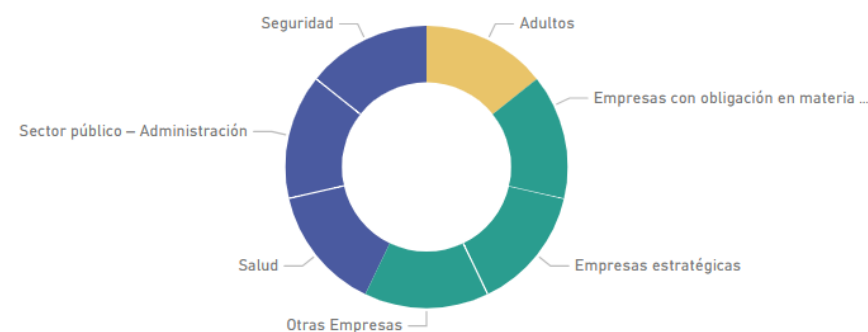
Inteligencia de amenazas

Verticales

● Ciudadanía ● Empresas ● Sector Público

Descripción del servicio

El servicio de vigilancia digital y alerta temprana se centra en la monitorización continua. Utilizando un modelo de inteligencia avanzado, se analizan datos de diversas fuentes para identificar patrones sospechosos y actividades anómalas. Al detectar una posible amenaza, se emiten alertas tempranas acompañadas de recomendaciones específicas para prevenir verse afectado y responder de manera efectiva.



Ficha de servicio

Información detallada de los servicios

Filtro por línea del servicio

Inteligencia de amenazas

Servicios

Alerta temprana

Intercambio de información sobre ciberamenazas

Ámbito

Prevención

Línea del servicio

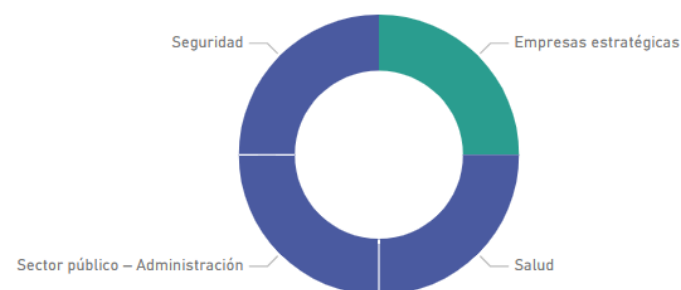
Inteligencia de amenazas

Verticales

● Empresas ● Sector Público

Descripción del servicio

El servicio de intercambio de información sobre ciberamenazas facilita la colaboración entre diferentes organizaciones y entidades para compartir datos sobre ciberamenazas de manera ágil y efectiva. Utilizando plataformas especializadas, se recopila y distribuye información sobre indicadores de compromiso, tácticas, técnicas y procedimientos utilizados por los atacantes. Este intercambio de información permite a las organizaciones mejorar su capacidad de detección y respuesta.



EAEko segurtasun-eredua

Línea del servicio	Empresas Sector Públi	
Modelo de Seguridad de Euskadi		
Acompañamiento y seguimiento en el despliegue del Modelo de Seguridad de Euskadi		

Ficha de servicio

Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Modelo de Seguridad de Euskadi

Servicios

Acompañamiento y seguimiento en el despliegue del Modelo de Seguridad de Euskadi

Ámbito

Gobernanza

Línea del servicio

Modelo de Seguridad de Euskadi

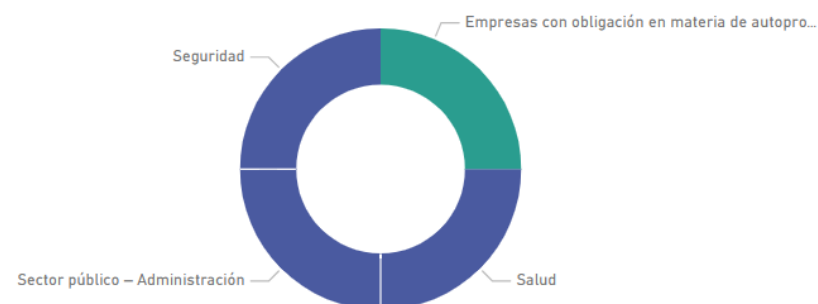
Verticales

● Empresas ● Sector Público

Descripción del servicio

El servicio de acompañamiento y seguimiento en el despliegue del Modelo de Seguridad de Euskadi se basa en el marco de referencia en ciberseguridad establecido por Cyberzaintza. Este marco incluye elementos clave, tales como políticas de seguridad, normas técnicas y medidas de protección, necesarios para establecer una base sólida de seguridad. Además, se complementa con las normativas de ciberseguridad existentes y se alinea con las necesidades específicas de las administraciones públicas de Euskadi, facilitando así su implementación.

Se proporciona asistencia a las organizaciones durante la implantación del modelo, asegurando que todas las entidades puedan adoptar las mejores prácticas en ciberseguridad. También se desarrollan materiales tipo para estructurar el modelo, los cuales se distribuyen para fomentar su adopción. Además, se lleva a cabo una evaluación y monitoreo continuo del modelo para garantizar su eficacia y promover mejoras constantes.



Segurtasun-arloko operazioak (SOC)

Línea del servicio	Sector Público
Operaciones de seguridad (SOC)	
SOC	
Threat hunting	

Ficha de servicio

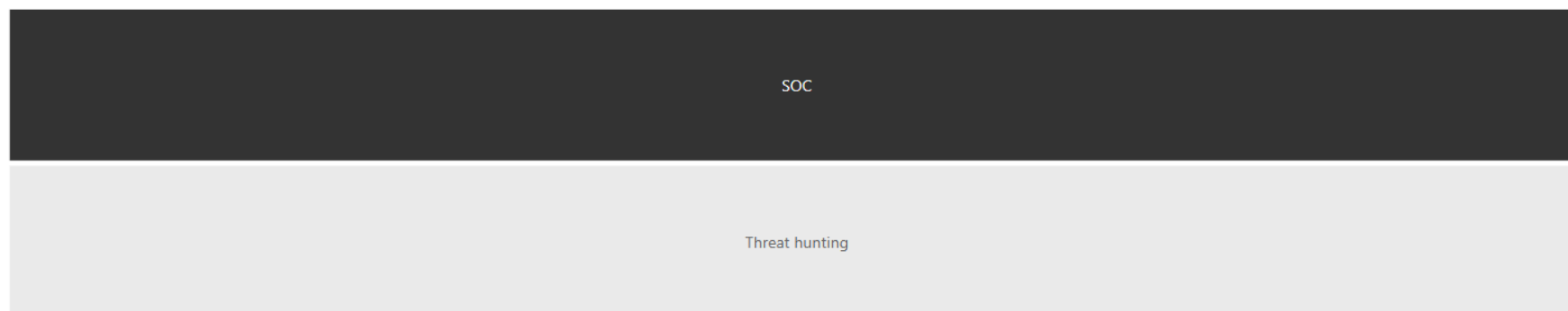
Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Operaciones de seguridad (SOC)

Servicios



Ámbito

Detección

Línea del servicio

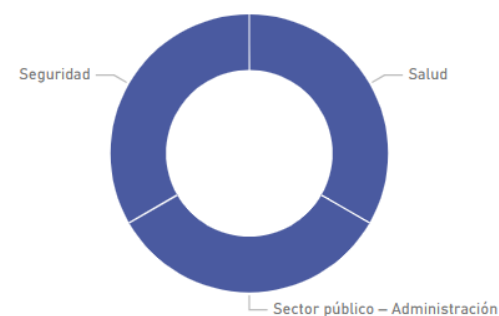
Operaciones de seguridad (SOC)

Verticales

● Sector Público

Descripción del servicio

El servicio de Centro de Operaciones de Seguridad (SOC) está destinado a la monitorización de eventos los internos que ocurren dentro de las organizaciones con el fin de detectar y analizar actividades sospechosas en tiempo real. Este servicio permite a las organizaciones responder de manera ágil y eficaz ante potenciales incidentes de ciberseguridad.



Ficha de servicio

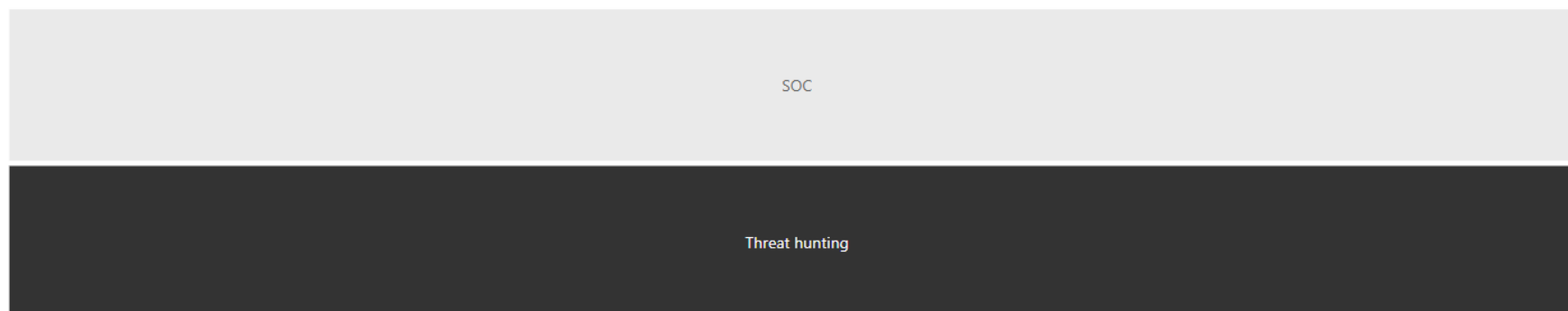
Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Operaciones de seguridad (SOC)

Servicios



Ámbito

Detección

Línea del servicio

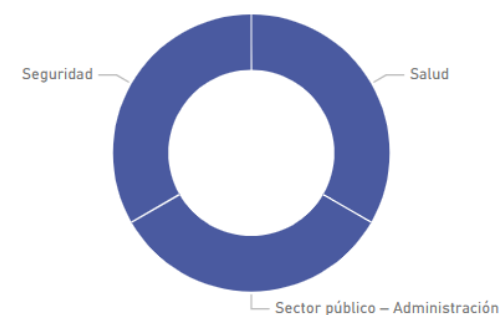
Operaciones de seguridad (SOC)

Verticales

● Sector Público

Descripción del servicio

El servicio de threat hunting se centra en la identificación proactiva de amenazas dentro de los entornos corporativos. Su objetivo es detectar y mitigar amenazas desconocidas, previniendo así su impacto antes de que puedan materializarse.



Gertakariei erantzutea (CSIRT)

Línea del servicio	Ciudadanía	Empresas	Sector Público
Respuesta a incidentes (CSIRT)			
Asesoramiento	●	●	●
Coordinación		◆	◆
DFIR			◆
Gestión de crisis			◆
Takedown	●	●	●

Ficha de servicio

Información detallada de los servicios

Filtro por línea del servicio

Respuesta a incidentes (CSIRT)

Servicios

Asesoramiento	Gestión de crisis
Coordinación	Takedown
DFIR	

Ámbito

Respuesta

Línea del servicio

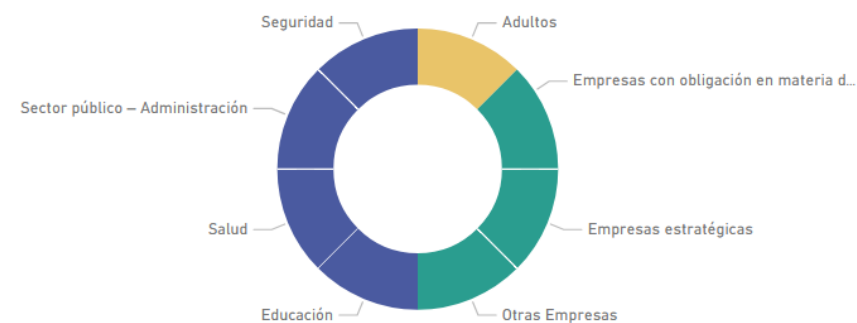
Respuesta a incidentes (CSIRT)

Descripción del servicio

El servicio de asesoramiento proporciona recomendaciones generales sobre cómo actuar si se ha experimentado un incidente de seguridad informática. Asimismo, cuando es necesario, el equipo técnico especializado en respuesta a incidentes de Cyberzaintza implementa las acciones necesarias para evitar la propagación del incidente y alertar a la comunidad sobre la amenaza.

Verticales

● Ciudadanía ● Empresas ● Sector Público



Ficha de servicio

Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Respuesta a incidentes (CSIRT)

Servicios

Asesoramiento	Gestión de crisis
Coordinación	Takedown
DFIR	

Ámbito

Respuesta

Línea del servicio

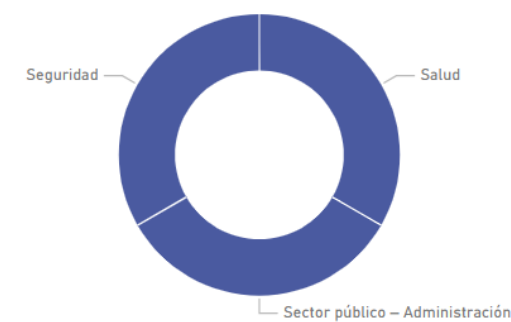
Respuesta a incidentes (CSIRT)

Descripción del servicio

El servicio de gestión de crisis se encarga de coordinar un plan integral para todo el sector público en Euskadi, asegurando que todas las instituciones estén preparadas para gestionar una crisis derivada de un incidente de seguridad crítico de manera eficaz.

Verticales

● Sector Público



Ficha de servicio

Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Respuesta a incidentes (CSIRT)

Servicios

Asesoramiento	Gestión de crisis
Coordinación	Takedown
DFIR	

Ámbito

Respuesta

Línea del servicio

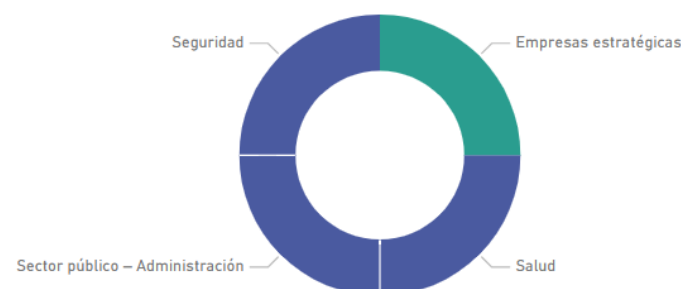
Respuesta a incidentes (CSIRT)

Descripción del servicio

El servicio de coordinación de incidentes de ciberseguridad se activa cuando estos tienen un impacto múltiple y significativo en los diferentes públicos objetivo de Cyberzaintza. Su propósito es proporcionar asesoramiento técnico especializado y tomar medidas preventivas para evitar que el incidente afecte a otras entidades. Este servicio asegura una respuesta rápida y coordinada, minimizando el alcance y las consecuencias del incidente, y garantizando que todas las partes involucradas estén informadas y alineadas en sus acciones.

Verticales

● Empresas ● Sector Público



Ficha de servicio

Información detallada de los servicios

Filtro por línea del servicio

Respuesta a incidentes (CSIRT)

Servicios

Asesoramiento	Gestión de crisis
Coordinación	Takedown
DFIR	

Ámbito

Respuesta

Línea del servicio

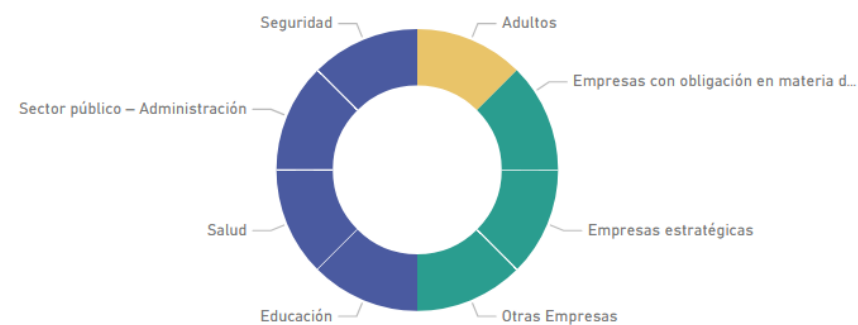
Respuesta a incidentes (CSIRT)

Descripción del servicio

El servicio de Takedown se refiere a las acciones que se realizan para retirar contenido malicioso o no autorizado de internet.

Verticales

● Ciudadanía ● Empresas ● Sector Público



Ficha de servicio

Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Respuesta a incidentes (CSIRT)

Servicios

Asesoramiento	Gestión de crisis
Coordinación	Takedown
DFIR	

Ámbito

Respuesta

Línea del servicio

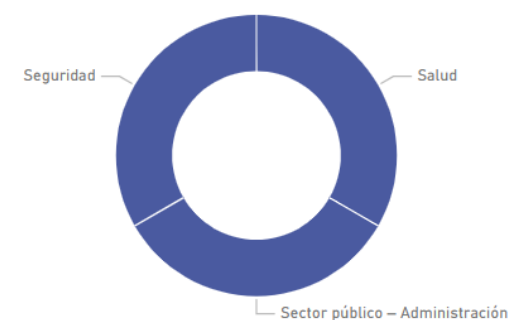
Respuesta a incidentes (CSIRT)

Verticales

● Sector Público

Descripción del servicio

El servicio de Análisis Forense Digital y Respuesta a Incidentes (DFIR) consiste en la adquisición y el análisis de evidencias digitales ante un incidente de seguridad, con el propósito de dar apoyo en la resolución del incidente.



Segurtasun ofentsiboa

Línea del servicio	Empresas	Sector Público
Seguridad ofensiva		
Auditoría técnica		◆
EASM	◆	◆
Red team		◆

Ficha de servicio

Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Seguridad ofensiva

Servicios



Ámbito

Detección

Línea del servicio

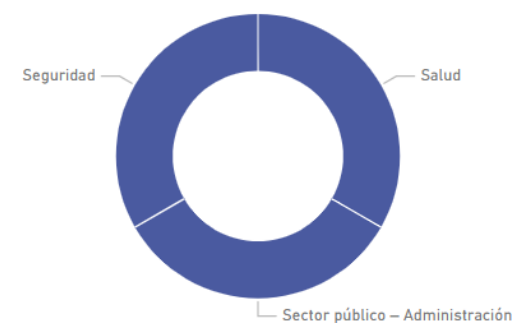
Seguridad ofensiva

Verticales

● Sector Público

Descripción del servicio

El servicio de auditoría técnica abarca pruebas de penetración (pentesting), auditorías de aplicaciones, redes Wi-Fi y configuraciones, entre otros aspectos. Su objetivo es evaluar el nivel de protección e identificar potenciales aspectos de mejora.



Ficha de servicio

Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Seguridad ofensiva

Servicios

Auditoría técnica	Red team
EASM	

Ámbito

Detección

Línea del servicio

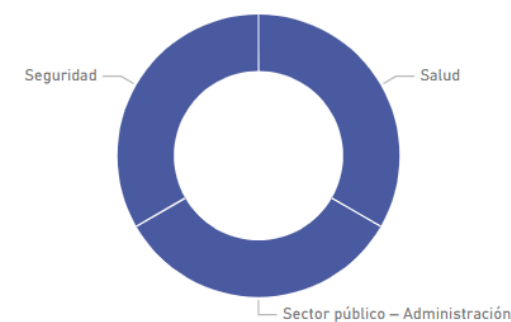
Seguridad ofensiva

Verticales

● Sector Público

Descripción del servicio

El servicio de red team se enfoca en realizar simulaciones de ataques reales contra una organización. Este servicio facilita la identificación y corrección de vulnerabilidades en los sistemas y defensas, así como la evaluación de la efectividad de los equipos de protección.



Ficha de servicio

Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Seguridad ofensiva

Servicios

Auditoría técnica	Red team
EASM	

Ámbito

Detección

Línea del servicio

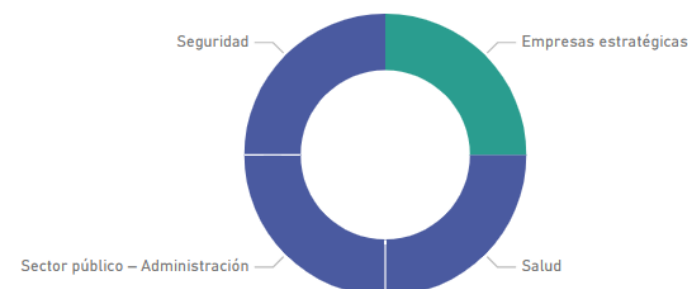
Seguridad ofensiva

Descripción del servicio

El servicio de Evaluación de la Superficie de Ataque y Mitigación (EASM) consiste en analizar la superficie de exposición de las organizaciones, con el objetivo de determinar su nivel de riesgo tecnológico. A partir de esta evaluación, se proponen recomendaciones específicas que permitan mitigar los riesgos identificados. Además, el servicio no solo se enfoca en la protección inmediata, sino que también busca aumentar la resiliencia a largo plazo.

Verticales

● Empresas ● Sector Público



Ezagutzaren transferentzia

Línea del servicio	Empresas	Sector Público
Transferencia del conocimiento		
Entrenamiento		
Formación		

Ficha de servicio

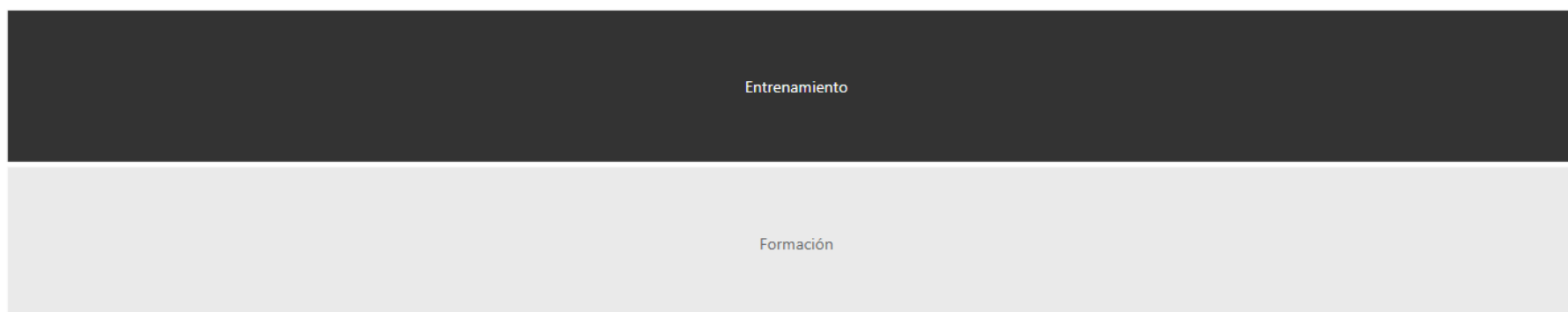
Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Transferencia del conocimiento

Servicios



Ámbito

Prevención

Línea del servicio

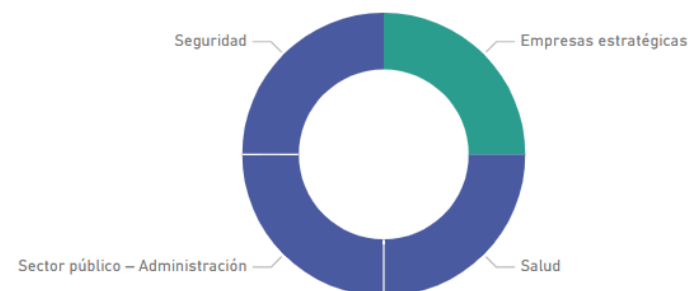
Transferencia del conocimiento

Verticales

● Empresas ● Sector Público

Descripción del servicio

El servicio de entrenamiento se centra en técnicas de operación y de coordinación de ejercicios de simulacros y pruebas de recuperación ante catástrofes. Esto incluye ciberejercicios tanto individuales como colectivos, que preparan a las organizaciones para gestionar crisis de manera eficaz.



Ficha de servicio

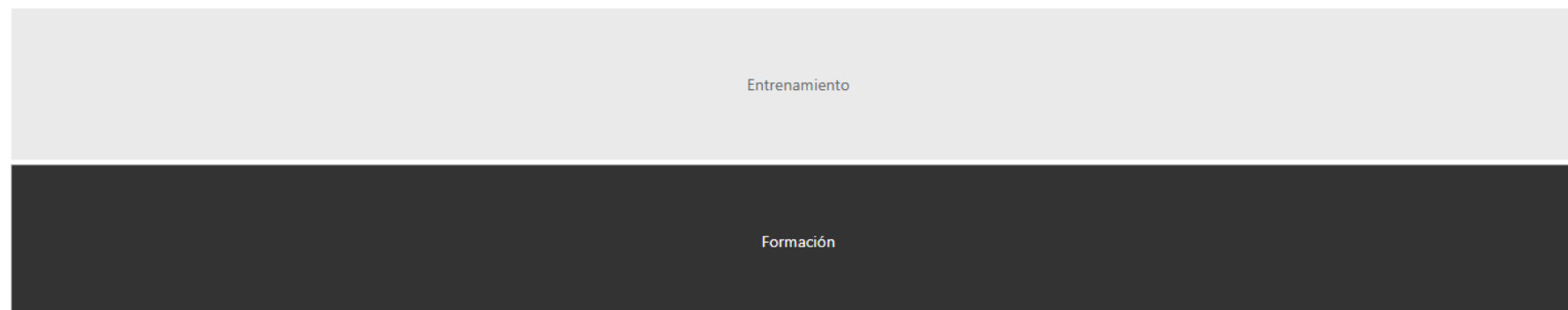
Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Transferencia del conocimiento

Servicios



Ámbito

Prevención

Línea del servicio

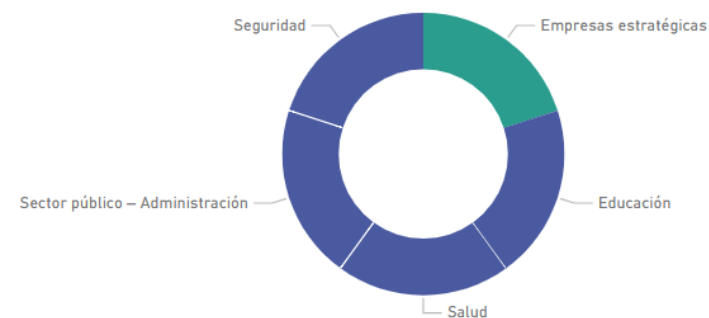
Transferencia del conocimiento

Verticales

● Empresas ● Sector Público

Descripción del servicio

El servicio de formación está diseñado para contribuir a la especialización en ciberseguridad de los distintos públicos objetivos de la Agencia. Las capacitaciones pueden llevarse a cabo utilizando los canales establecidos o mediante métodos alternativos cuando se aborden temas específicos que no puedan ser tratados con los medios convencionales.

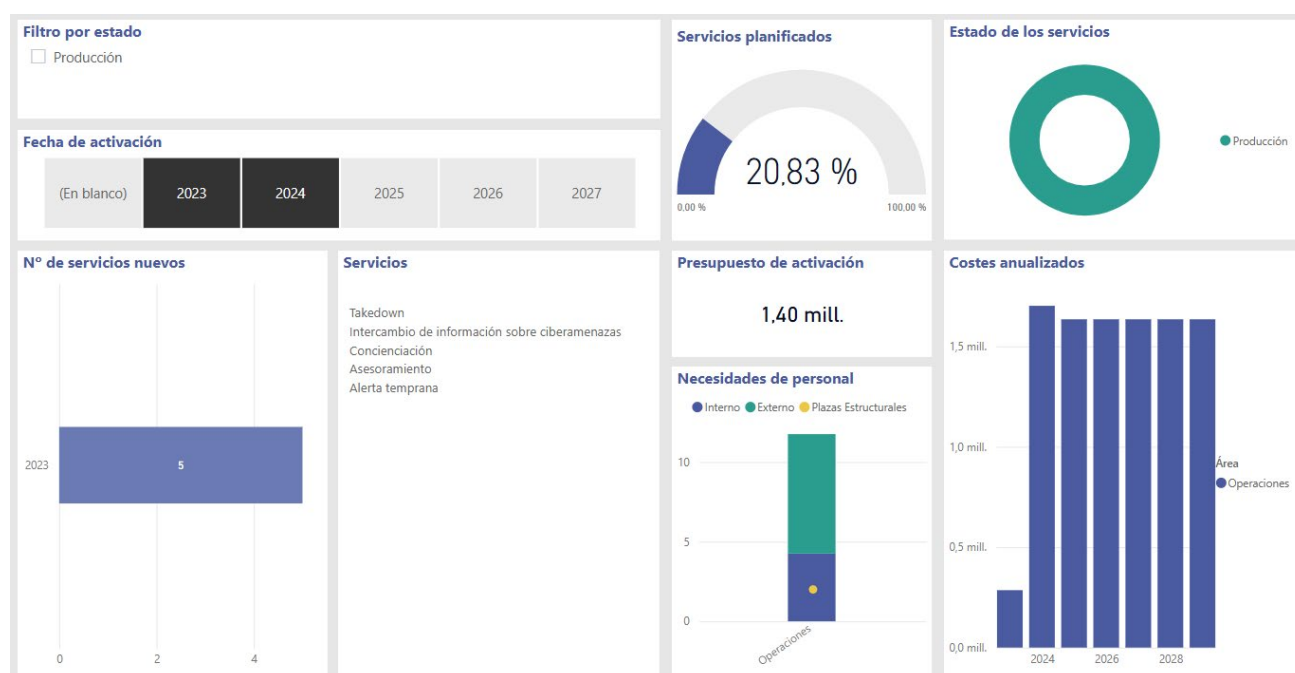


3.2.3 Ibilbide-orria

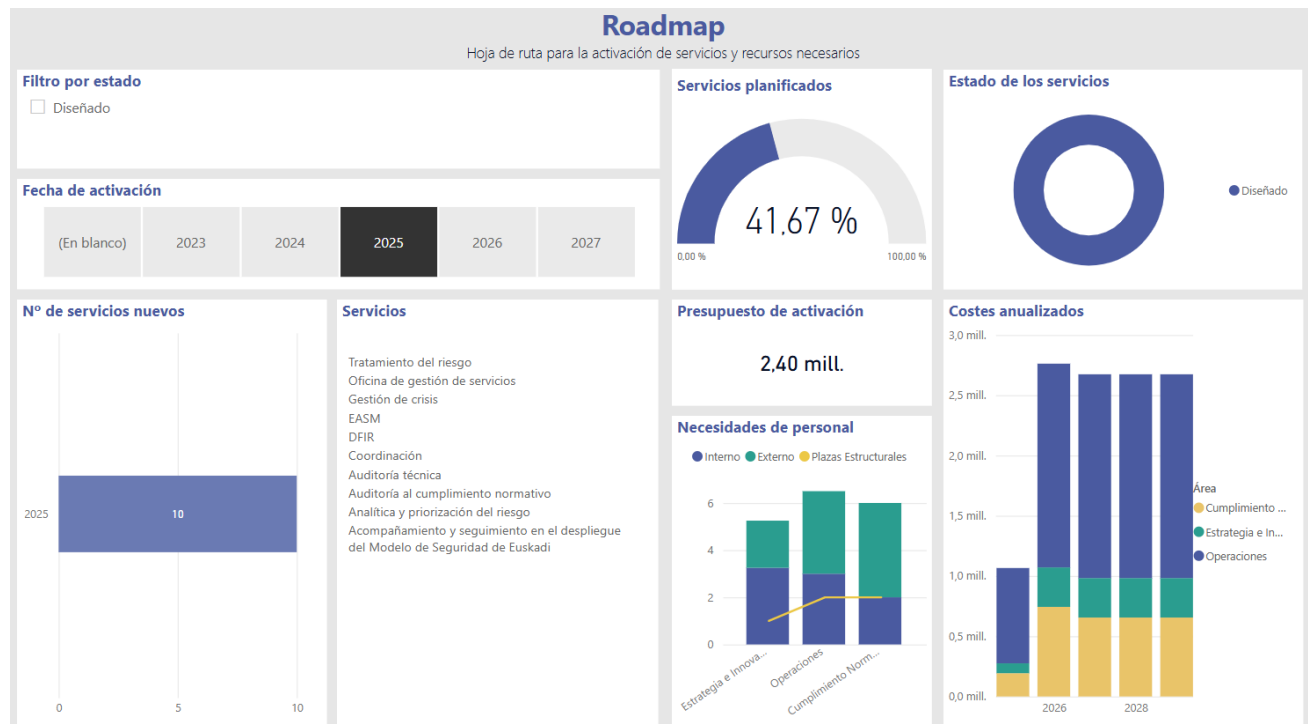
Jarraian, zerbitzuak aktibatzeko ibilbide-orria xehatzen da, zerbitzu planifikatuen zerrenda eta zerbitzuak ezartzeko beharko diren baliabideen zenbatespena barne hartuta. Langile-premiak nahiz aurrekontu-premiak zenbatetsi dira, martxan jartzeko kostua eta zerbitzuaren urteko mantentze-lanen kostua aintzat hartuta.

Hasierako egoera

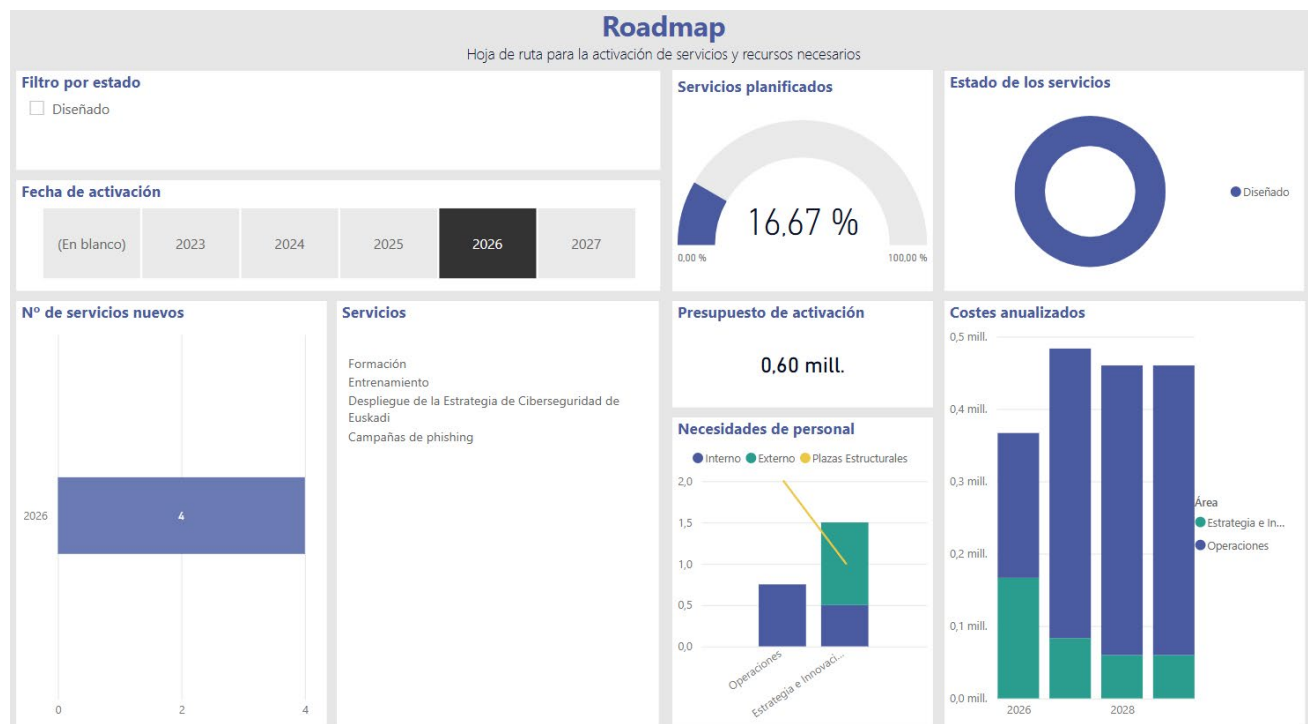
Hona hemen zerbitzuen hasierako egoera, plan hau onetsi aurrekoa:



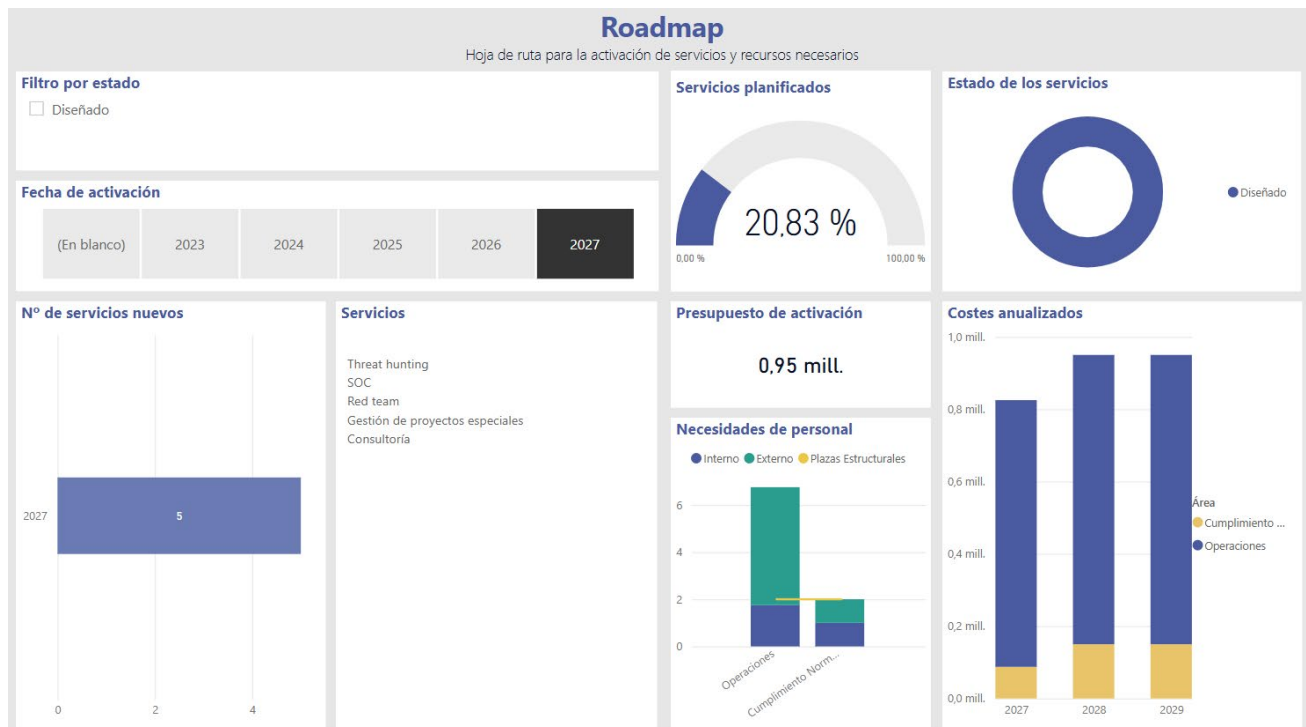
2025



2026

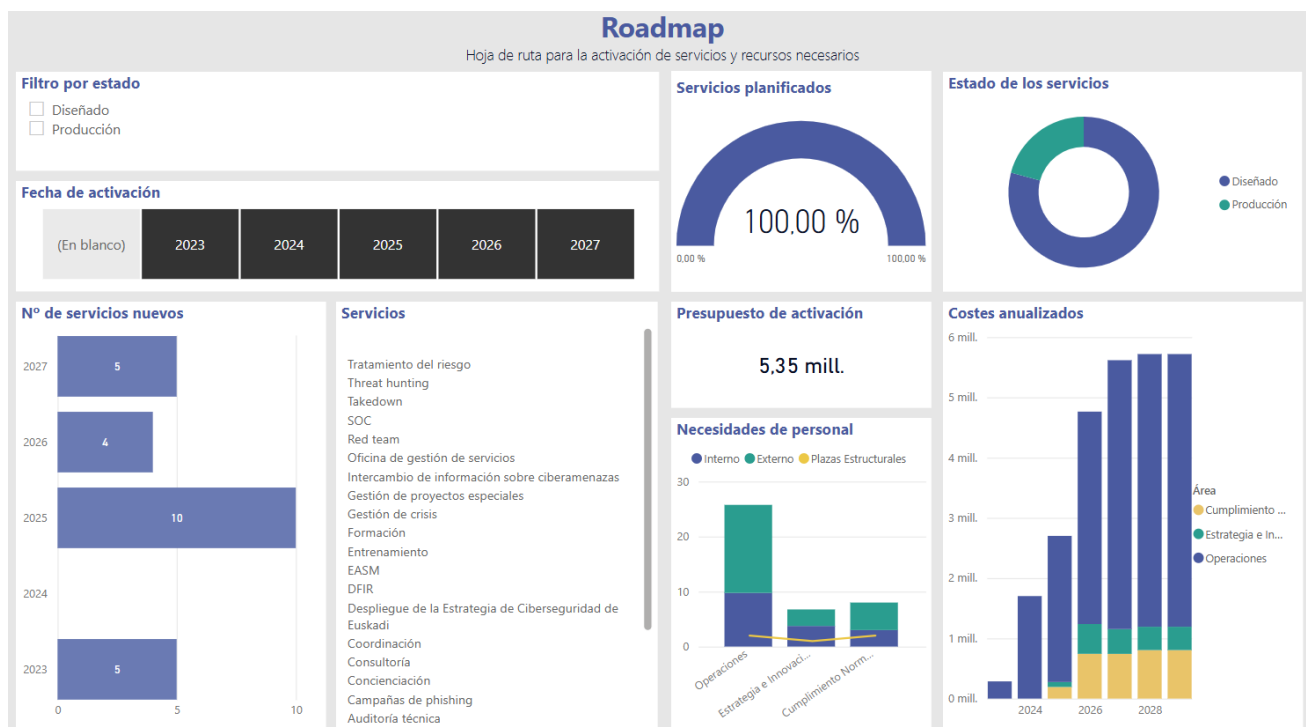


2027



Amaierako egoera

Hona hemen zerbitzuen amaierako egoeraren laburpena, planifikatutako zerbitzu guztiak aktibatu ostekoa:



3.2.4 Zerbitzuak emateko eredua

Zerbitzuak emateko eredua funtsezkoa da Cyberzaintzak efizientziaz eta efikaziaz jardutea ziurtatzeko. Zerbitzuak modu koherentean eta antolakundearen helburu estrategikoekin bat etorrira ematea bermatzeko xedez diseinatu da eredu hau.

Horra zerbitzuak emateko zehaztu den ereduaren eskema:



4 Gobernantza-eredua

Cyberzaintzaren Plan Estrategikoak hiru gobernantza-maila dauzka, ezarpena eta ikuskapena bermatzeko diseinatuak:



4.1 Administrazio Kontseilua

Administrazio Kontseilua agentziaren organo gorena da, eta Euskal Autonomia Erkidegoko Administrazio Publikoaren hiru mailak ordezkatzen dituzten hamasei kidek osatzen dute. Eginkizun nagusien artean dago urteko planak eta aurrekontuak, jardueren memoria eta plantillen nahiz ordainsari-araubidearen proposamena onestea. Halaber, estatutu-aldaketak proposatzen ditu, Zuzendaritzaren kudeaketa gainbegiratzeko, beste entitate batzuetan parte hartzeko baimenak ematen ditu, hitzarmenak eta akordioak onesten ditu, Eusko Jaurlaritzari jardueren berri ematen dio, eta lege- eta estatutu-arloko beste eginkizun batzuk betetzen ditu.

Cyberzaintzaren Plan Estrategikoari dagokionez, Administrazio Kontseiluak dauka plana onesteko eta planaren garapenaren aldizkako jarraipena egiteko ardura. Horretaz gainera, agentziak garatzeko behar dituen baliabideak edukitzea zainduko du, eta, horretarako, plana garatzeko jardura-planak eta aurrekontuak onetsiko ditu eta planifikatutako ekintzak gauzatzeko behar den plantilla-eskala Eusko Jaurlaritzari proposatuko dio.

Era berean, Agentziaren bilakaerari eta jardueri buruzko informazioa emango dio Eusko Jaurlaritzari, aldizka, ikuskapen etengabea bermatzeko.

4.2 Zuzendaritza Batzordea

Cyberzaintzako zuzendari nagusia da Zuzendaritza Batzordeko burua. Batzorde honetan, ordezkaritza iraunkorra dute hauek: Estrategia eta Berrikuntza Zuzendaritza, Eragiketen eta Erantzuteko Lantaldearen Zuzendaritza, Komunikazioko eta Erakundeekiko Harremanetarako Zuzendaritza, Arauak Betetzeko eta Arriskuak Gobernatzeko Zuzendaritza, Administrazio eta Zerbitzuen Dibisioko Burutza eta Aholkularitza Juridikoaren Dibisioko Burutza. Bestetik, Segurtasun eta Azpiegituretako Dibisioko Burutza ordezkarari gonbidatua da.

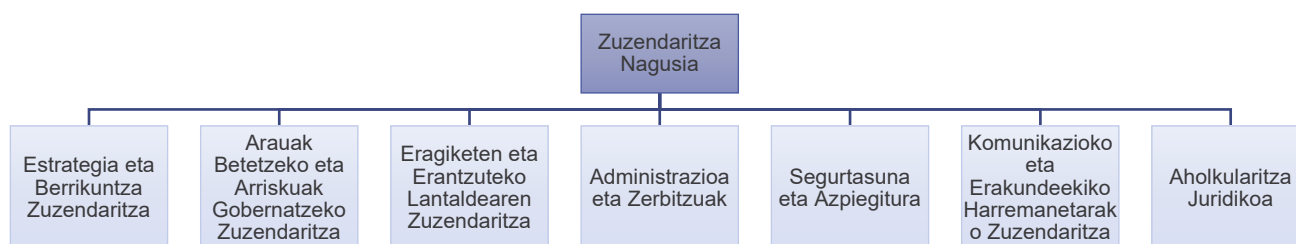
Batzordearen eginkizunen artean daude Plan Estrategikoa egitea eta helburuak urtez urte betetzeko behar den dokumentazio taktikoa biltzea, baita, besteak beste, kudeaketa-plana, jarduketa-plana eta

aurrekontua egitea ere. Halaber, Zuzendaritza Batzordeak Plan Estrategikoan zehaztutako ekintza-ildoak garatu eta gauzatzearekin zerikusia daukaten jarduera guztiak gainbegiratu eta bideratzen ditu.

Zuzendaritza Batzordeak informazioa ematen dio Administrazio Kontseiluari, Zuzendaritza Nagusiaren bidez.

4.3 Arloak

Grafiko honetan, Cyberzaintzaren arloen egitura xehatzen da:



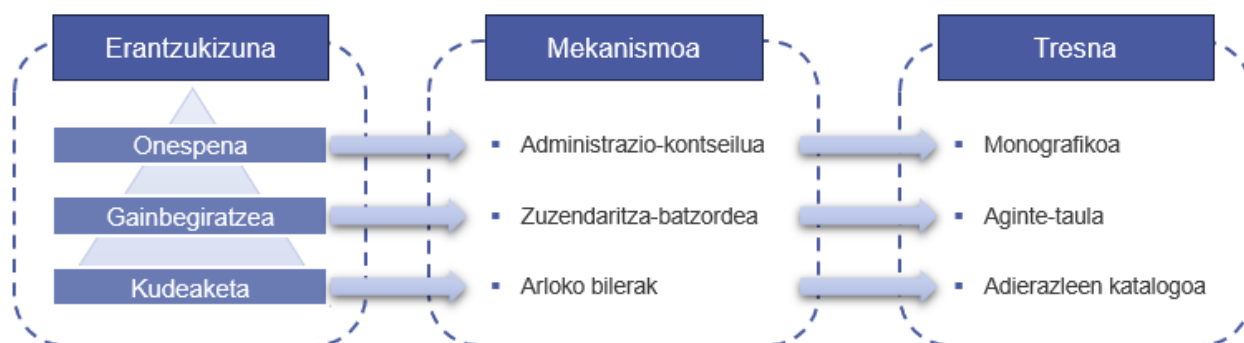
Arlo bakoitza arduratzen da Plan Estrategikoan bere eremurako zehaztutako ekintza-ildoak ezartzeko behar diren jarduerak burutzeaz. Halaber, ekintza guztiak modu efizientean kudeatzen direla eta ezarritako printzipioekin bat datozela ziurtatu behar dute.

Arloek Zuzendaritza Batzordeari ematen diote informazioa, arduradunen bidez.

5 Jarraipena eta ebaluazioa

5.1 Jarraipen-sistema

Sistematika hau zehaztu dugu Cyberzaintzaren 2025-2028 aldirako Plan Estrategikoari jarraipena egin eta plana bera berrikusteko:



5.2 Jarraipena egiteko mekanismoak

5.2.1 Arloko bilerak

- **Maiztasuna:** astean behin.
- **Arduraduna:** arloko arduraduna.
- **Helburua:** arloko jardueren aurrerapen-maila kudeatzea, KPlen egoera berrikustea, desbiderapenak identifikatzea eta horiek zuzentzeko ekintzak proposatzea, helburu operatiboak betetzea ziurtatzeko.

5.2.2 Zuzendaritza Batzordearen bilerak

- **Maiztasuna:** hilean behin.
- **Arduraduna:** Cyberzaintzaren Estrategiaren Zuzendaritza.
- **Helburua:** Plan Estrategikoaren aurrerapen-maila osoa gainbegiratzea, proposatutako zuzenketa-ekintzak ebaluatzea eta ekintza-ildoak eraginkortasunez eta printzipio estrategikoen arabera ezartzen direla ziurtatzea.

5.2.3 Administrazio Kontseiluaren bilerak

- **Maiztasuna:** urtean behin, urteko azken hiruhilekoan.
- **Arduraduna:** Cyberzaintzaren Zuzendaritza Nagusia.
- **Helburua:** Plan Estrategikoaren urteko bilakaerari buruzko informazioa jasotzea, errendimendua eta emaitzak aztertzea eta ekintza-ildoek hurrengo aldian jarraitzeko beharko diren planak eta baliabide-esleipena onestea.

5.3 Ebaluazio-tresnak

Plan Estrategikoaren ebaluazioa tresna nagusi hauetan oinarrituko da:

5.3.1 Monografikoa

Txosten monografikoak urteko balantzea jasotzen du, eta Cyberzaintzaren Zuzendaritza Batzordeak egiten du. Plan Estrategikoko ekintzek urtean izandako bilakaera zorrotz ebaluatzea da txostenaren helburua. Monografikoan, egindako lorpenak eta planteatutako helburuekiko desbiderapenak aztertu, eta ezarritako jomugak betetzea ziurtatzeko zuzenketa-neurriak proposatzen dira.

5.3.2 Aginte-aula

Aginte-aulak adierazle multzo bat biltzen du, planaren ekintza-ildoak nahiz printzipio estrategikoak ebaluatzeko propio diseinatutako adierazleen multzo bat. Adierazle horiek modua ematen dute egitasmoen aurrerapen-maila argi eta zehatz ikusteko, eta horrek erabaki informatuak hartzea errazten dio Zuzendaritza Batzordeari. Aginte-aula aldizka eguneratzen da, aldaketak eta aurrerapenak denbora errealean islatzeko.

5.3.3 Adierazleen katalogoa

Adierazleen katalogoak barruan hartzen ditu errendimenduaren gako-adierazleak (KPIak), ezinbestekoak direnak Plan Estrategikoari jarraipen etengabea egiteko. Nolanahi ere, Plan Estrategikoaren adierazleak bat etorri beharko dute Jaurlaritzaren kudeaketa-adierazleen sistemarekin.

Katalogoak adierazle bakoitzaren deskribapen xehatua jasotzen du, informazio honekin:

Eremua	Deskribapena
Id.	Adierazlearen identifikatzaile bakarra.
Ekintza-ildoak	Adierazlea zer ekintza-ildori dagokion.
Adierazlearen iturria	Datuen jatorria (zerbitzua, egitasmo osagarria eta abar).
Lotutako zerbitzua/egitasmoa	Adierazlea zer zerbitzu edo egitasmotik eskuratu den.
Adierazlearen arduraduna	Adierazlea neurtzeaz eta horren berri emateaz arduratzen den pertsona edo saila.
Aurrekontu-memoria	Adierazlea aurrekontu-memorian sartuta dagoen (bai/ez).
Adierazlearen deskribapena	Adierazlearen deskribapena.
Helburu-balioa	Adierazlearekin lortu nahi den helburu-balioa.
Oraingo balioa	Adierazlearen oraingo balioa, azken neurketakoa.
Neurketaren data	Adierazlearen azken neurketaren data.
Betetze-maila kalkulatzeko formula	Adierazlearen betetze-maila kalkulatzeko erabilitako formula.
Betetze-mailaren ehunekoa	Adierazlearen betetze-maila, ehunekotan (%) adierazita.

I. eranskinean, adierazleen katalogoan sartutako adierazleak jasotzen dira.

II. eranskinean, Jaurlaritzaren 2025erako kudeaketa-adierazleak jasotzen dira.

I. eranskina - Cyberzaintzaren 2025-2028 aldirako Plan Estrategikoaren adierazleen katalogoa

Ekintza-ildoak	Adierazlearen iturria	Lotutako zerbitzua/egitasmoa	Adierazlearen arduraduna	Aurrekontu-memoria	Adierazlearen deskribapena	Helburu-balioa	Maiztasuna	Betetze-maila kalkulatzeko formula	Betetze-mailaren ehunekoa
Auditoretza	Zerbitzua	Arau-betetzearen gaineko auditoretza	Araudia betetzea eta arriskua gobernatzea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2025-10-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Auditoretza	Egitasmo osagarria	Auditoretza Teknikoko Organo gisa akreditatzea	Araudia betetzea eta arriskua gobernatzea	Ez	Sektore publikoko Auditoretza Teknikoko Organoaren (ATO) aitortza jasotzea, ziurtapen-auditoretzak Segurtasunaren Eskema Nazionalaren (ENS) arabera egiteko	4	Hiru hilean behin	1=Aztertzen; 2=Aurretiko betekizunak betetzea; 3=Barne-betekizunak betetzea; 4=ATO izendatzea	% 25
Kontzientziazioa	Zerbitzua	Phishing-kanpainak	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2026-01-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Kontzientziazioa	Zerbitzua	Kontzientziazioa	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena zerbitzua martxan jartzeko aurreikusitako egunari dagokionez.	2026-01-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Aholkularitza	Zerbitzua	Aholkularitza	Araudia betetzea eta arriskua gobernatzea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2027-06-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Aholkularitza	Zerbitzua	Proiektu berezien kudeaketa	Araudia betetzea eta arriskua gobernatzea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2027-06-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	

Ekintza-ildoak	Adierazlearen iturria	Lotutako zerbitzua/egitasmoa	Adierazlearen arduraduna	Aurrekontu-memoria	Adierazlearen deskribapena	Helburu-balioa	Maiztasuna	Betetze-maila kalkulatzeko formula	Betetze-mailaren ehunekoa
Koordinazio estrategikoa	Zerbitzua	Zibersegurtasunaren Euskal Estrategia hedatzea	Estrategia eta Berrikuntza	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2026-03-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Koordinazio estrategikoa	Zerbitzua	Zerbitzuak kudeatzeko bulegoa	Estrategia eta Berrikuntza	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2025-10-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Arriskuaren kudeaketa	Zerbitzua	Arriskuak aztertu eta lehenestea	Araudia betetzea eta arriskua gobernatzea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2025-10-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Arriskuaren kudeaketa	Zerbitzua	Arriskuaren tratamendua	Araudia betetzea eta arriskua gobernatzea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2025-10-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Mehatzuen alorreko inteligentzia	Zerbitzua	Alerta goiztiarra	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako egunari dagokionez.	2025-04-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Mehatzuen alorreko inteligentzia	Zerbitzua	Zibermehtxuei buruzko informazioa trukatzeko	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako egunari dagokionez.	2025-04-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Barrukoa	Zerbitzua	Administrazioa eta Zerbitzuak.	Administrazioa eta zerbitzuak	Ez	Cyberzaintzaren aurrekontuaren betearazpen-maila (%)	% 100	Hiru hilean behin	(Neurtutako balioa / Helburu-balioa) x 100	% 0
Barrukoa	Zerbitzua	Zibersegurtasuneko I+G+B berrikuntza-proiektuak garatzen laguntzea	Estrategia eta Berrikuntza	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2027-06-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Barrukoa	Zerbitzua	Cyberzaintzaren arau-betetzea	Administrazioa eta Zerbitzuak	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2025-10-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	

Ekintza-ildoak	Adierazlearen iturria	Lotutako zerbitzua/egitasmoa	Adierazlearen arduraduna	Aurrekontu-memoria	Adierazlearen deskribapena	Helburu-balioa	Maiztasuna	Betetze-maila kalkulatzeko formula	Betetze-mailaren ehunekoa
Barrukoa	Zerbitzua	Cyberzaintzaren arau-betetzea	Segurtasuna eta Azpiegitura	Ez	Segurtasunaren Eskema Nazionala maila ertainean betetzen delako ziurtagiria lortzea	4	Hiru hilean behin	1=Arrakalen azterketa egitea; 2=Egokitzapen-plana egitea; 3=Plana ezartzea; 4=Ziurtagiria lortzea.	% 25
Barrukoa	Zerbitzua	Cyberzaintzaren Plan Estrategikoa garatu eta hedatzea	Estrategia eta Berrikuntza	Ez	Cyberzaintzaren 2025-2028 aldirako Plan Estrategikoa onesta	4	Hiru hilean behin	1=Eginda; 2=Zuzendaritzek baliozkotuta; 3=Zuzendaritza Batzordeak onetsita; 4=Administrazio Kontseiluak onetsita.	% 50
Barrukoa	Zerbitzua	Cyberzaintzaren Plan Estrategikoa garatu eta hedatzea	Estrategia eta Berrikuntza	Ez	Zerbitzuak ematea, jarduketa-eremu guztiak (gobernantza, detekzioa, prebentzioa eta erantzuna) garatzea bermatuta eta guztizko kostuaren % 10 gutxienez eremu bakoitzean banatzea ziurtatuta.	4	Hiru hilean behin	1=1 eremu; 2=2 eremu; 3=3 eremu; 4=4 eremu.	% 50
Barrukoa	Zerbitzua	Cyberzaintzaren Plan Estrategikoa garatu eta hedatzea	Estrategia eta Berrikuntza	Ez	Zerbitzuak ematea, xede-publiko guztiei (sektore publikoa, enpresak eta herritarrek) iristea bermatuta eta zerbitzuen % 50 gutxienez sektore publikoari, % 30 enpresei eta % 10 herritarrei eskaintzea ziurtatuta.	3	Hiru hilean behin	1=1 hartzaile; 2=2 hartzaile; 3=3 hartzaile.	% 66
Barrukoa	Zerbitzua	Cyberzaintzaren Plan Estrategikoa garatu eta hedatzea	Estrategia eta Berrikuntza	Ez	Zerbitzuak ematea, Cyberzaintzak zerbitzuak emateko ezarritako eredua ezarri.	4	Hiru hilean behin	1=Eginda; 2=Zuzendaritzek baliozkotuta; 3=Zuzendaritza Batzordeak onetsita; 4=Ezarrita.	% 0
Barrukoa	Zerbitzua	Cyberzaintzaren Plan Estrategikoa garatu eta hedatzea	Estrategia eta Berrikuntza	Ez	Zuzendaritza Batzordeak Plan Estrategikoaren aurrerapen-maila gainbegiratzeko egindako bilerak.	4	Hiru hilean behin	(Neurtutako balioa / Helburu-balioa) x 100	% 25

Ekintza-ildo	Adierazlearen iturria	Lotutako zerbitzua/egitasmoa	Adierazlearen arduraduna	Aurrekontu-memoria	Adierazlearen deskribapena	Helburu-balioa	Maiztasuna	Betetze-maila kalkulatzeko formula	Betetze-mailaren ehunekoa
Barrukoa	Zerbitzua	Cyberzaintzaren Plan Estrategikoa garatu eta hedatzea	Estrategia eta Berrikuntza	Ez	Administrazio Kontseiluak Plan Estrategikoaren urteko bilakaerari buruzko informazioa jasotzeko egindako bilerak.	1	Hiru hilean behin	(Neurtutako balioa / Helburu-balioa) x 100	% 0
Barrukoa	Zerbitzua	Cyberzaintzaren Plan Estrategikoa garatu eta hedatzea	Estrategia eta Berrikuntza	Ez	Abian jarritako zerbitzuen ehunekoa, Plan Estrategikoak 2025ean ezartzeko identifikatutakoen aldean.	% 63	Hiru hilean behin	(Neurtutako balioa / Helburu-balioa) x 100	% 33
Barrukoa	Zerbitzua	Cyberzaintzaren Plan Estrategikoa garatu eta hedatzea	Estrategia eta Berrikuntza	Ez	Abian jarritako zerbitzuen ehunekoa, Plan Estrategikoak 2026an ezartzeko identifikatutakoen aldean.	% 79	Hiru hilean behin	(Neurtutako balioa / Helburu-balioa) x 100	% 26
Barrukoa	Zerbitzua	Cyberzaintzaren Plan Estrategikoa garatu eta hedatzea	Estrategia eta Berrikuntza	Ez	Abian jarritako zerbitzuen ehunekoa, Plan Estrategikoak 2027an ezartzeko identifikatutakoen aldean.	% 100	Hiru hilean behin	(Neurtutako balioa / Helburu-balioa) x 100	% 21
Barrukoa	Zerbitzua	Cyberzaintzaren Plan Estrategikoa garatu eta hedatzea	Estrategia eta Berrikuntza	Ez	Kanal baten bidez eman daitezkeen zerbitzuen ehunekoa, kanal horren bidez benetan emandakoen aldean.	% 75	Hiru hilean behin	(Neurtutako balioa / Helburu-balioa) x 100	% 67
Barrukoa	Zerbitzua	Cyberzaintzaren Plan Estrategikoa garatu eta hedatzea	Estrategia eta Berrikuntza	Ez	Plan Estrategikoan identifikatutako jarduketaren ehunekoa, abian jarritakoen aldean.	% 100	Hiru hilean behin	(Neurtutako balioa / Helburu-balioa) x 100	% 25
Barrukoa	Zerbitzua	Segurtasun korporatiboa	Segurtasuna eta Azpiegitura	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako egunari dagokionez.	2025-07-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Barrukoa	Zerbitzua	Komunikazio-zerbitzua	Komunikazioa eta Erakundeekiko harremanak	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2025-07-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
EAEko segurtasun-eredua	Zerbitzua	EAEko segurtasun-eredua hedatzen laguntzea eta jarraipena egitea	Estrategia eta Berrikuntza	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2025-10-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	

Ekintza-ildoak	Adierazlearen iturria	Lotutako zerbitzua/egitasmoa	Adierazlearen arduraduna	Aurrekontu-memoria	Adierazlearen deskribapena	Helburu-balioa	Maiztasuna	Betetze-maila kalkulatzeko formula	Betetze-mailaren ehunekoa
Segurtasun-arloko operazioak (SOC)	Zerbitzua	SOC	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2027-01-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Segurtasun-arloko operazioak (SOC)	Egitasmo osagarria	SOC	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena SOCen Sare Nazionaleko kide izateko aurreikusitako egunari dagokionez.	2025-06-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 101	
Segurtasun-arloko operazioak (SOC)	Zerbitzua	Threat hunting	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2027-01-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Gertakariei erantzutea (CSIRT)	Zerbitzua	Aholkularitza	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako egunari dagokionez.	2025-09-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Gertakariei erantzutea (CSIRT)	Zerbitzua	Koordinazioa	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2025-10-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Gertakariei erantzutea (CSIRT)	Zerbitzua	DFIR	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2025-10-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Gertakariei erantzutea (CSIRT)	Zerbitzua	Krisien kudeaketa	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2025-10-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Gertakariei erantzutea (CSIRT)	Zerbitzua	Takedown	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2023-11-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	
Gertakariei erantzutea (CSIRT)	Egitasmo osagarria	EAE zibersegurtasuneko larrialdietatik babesteko modua planifikatzea eta LABIrekin konektatzea	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena, ziberkrisia LABI aktiba lezaketzen gertakari gisa sartzeko aurreikusitako datari dagokionez.	2025-06-01	Hiru hilean behin	(1-Desbideratze-egunak / 90) x 100	

Ekintza-ildoak	Adierazlearen iturria	Lotutako zerbitzua/egitasmoa	Adierazlearen arduraduna	Aurrekontu-memoria	Adierazlearen deskribapena	Helburu-balioa	Maiztasuna	Betetze-maila kalkulatzeko formula	Betetze-mailaren ehunekoa
Segurtasun ofentsiboa	Zerbitzua	Auditoretza teknikoa	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2025-05-01	Hiru hilean behin	$(1 - \text{Desbideratze-egunak} / 90) \times 100$	
Segurtasun ofentsiboa	Zerbitzua	EASM	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2025-10-01	Hiru hilean behin	$(1 - \text{Desbideratze-egunak} / 90) \times 100$	
Segurtasun ofentsiboa	Zerbitzua	Red team	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2027-06-01	Hiru hilean behin	$(1 - \text{Desbideratze-egunak} / 90) \times 100$	
Ezagutzaren transferentzia	Zerbitzua	Entrenamendua	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2026-09-01	Hiru hilean behin	$(1 - \text{Desbideratze-egunak} / 90) \times 100$	
Ezagutzaren transferentzia	Zerbitzua	Prestakuntza	Eragiketak eta Erantzuteko lantaldea	Ez	90 egun baino gutxiagoko desbiderapena, zerbitzua martxan jartzeko aurreikusitako datari dagokionez.	2026-09-01	Hiru hilean behin	$(1 - \text{Desbideratze-egunak} / 90) \times 100$	

II. eranskina – Jaurlaritzaren kudeaketa-adierazleak (2025)

HELBURUA EKINTZA ADIERAZLEA	MAGNITUDEA MAGNITUD	OBJETIVO ACCION INDICADOR
1. ARLOAN ESKUMENAK DITUZTEN HAINBAT ORGANISMOREN BITARTEZ HEDATUTAKO ZIBERSEGURTASUNEO ESTRATEGIA KOMUN BATEN BARRUAN INTEGRATUTA DAUDEN ADMINISTRAZIO PUBLIKOAK IDENTIFIKATZEA.		1. IDENTIFICAR LA INTEGRACIÓN DE LAS ADMINISTRACIONES PÚBLICAS DE EUSKADI EN UNA ESTRATEGIA DE CIBERSEGURIDAD COMÚN DESPLEGADA A TRAVÉS DE LOS DIFERENTES ORGANISMOS CON COMPETENCIAS EN EL ÁMBITO.
1. Zibersegurtasunaren Euskal Estrategia abian jartzea.		1. Poner en marcha la Estrategia Vasca de Ciberseguridad.
Hasitako jarduera ildoak.	25%	Líneas de actuación iniciadas.
Abian jarritako jarduera estrategikoen kopurua.	5	Número de actuaciones estratégicas puestas en marcha.
Estrategiari atxikitako eragileekin espazioak dinamizatzeko ekintzen kopurua.	4	Número de acciones para la dinamización de espacios con los agentes adheridos a la estrategia.
2. EUSKADIKO SEKTORE PUBLIKOKO ORGANISMO GUZTIEK EZARRIKO DITUZTEN PRINTZPIOAK BILDUKO DITUEN ESTANDARREN, JARRAIBIDEEN ETA ARAU TEKNIKOEN ESPARRUA ESKAINTZEA, BETIERE LEGEDI APLIKAGARRIA ERRESPETATUZ.		2. DOTAR DE UN MARCO DE ESTÁNDARES, DIRECTRICES Y NORMAS TÉCNICAS CUYOS PRINCIPIOS SEAN ADOPTADOS POR EL CONJUNTO DE ORGANISMOS DEL SECTOR PÚBLICO VASCO, SIEMPRE RESPETANDO LA LEGISLACIÓN APLICABLE.
1. Euskal sektore publikoan arriskua gobernatzeko estandar-esparru bat definitzea.		1. Definir un marco de estándares para el gobierno del riesgo en el sector público vasco.
Banatutako zibersegurtasuneko euskal ereduko elementuen kopurua.	2	Número de elementos del modelo vasco de ciberseguridad distribuidos.
3. EUSKADIKO SEKTORE PUBLIKOAN ZIBERSEGURTASUNAREN EGOERA ZEIN DEN EGIAZTATZEA.		3. VERIFICAR EL ESTADO DE LA CIBERSEGURIDAD EN EL SECTOR PÚBLICO VASCO.
1. Euskal sektore publikoa babesteko protokoloa definitzea.		1. Definir el protocolo de protección del sector público vasco.
EAEn eta atxikitako euskal sektore publikoko administrazioetan hedatutako gaitasunen egoera orokorraren maila ebaluatzea bideratutako jardueren kopurua.	2	Número de actuaciones orientadas a evaluar el nivel del estado general de capacidades desplegadas en la CAV y en las diferentes administraciones del sector público vasco adheridas.

"Euskadiko Zibersegurtasunaren Behatokiak" argitaratutako txostenen kopurua.	2	Número de informes publicados por el "Observatorio de Ciberseguridad de Euskadi".
4. EUSKADIKO GIZARTEAK DUEN ZIBERSEGURTASUNEN KULTURAREN MAILA SUSTATZEA. 1. Zibersegurtasuneko jardunbide egokien gidak eta gomendioak egitea eta zabaltzea. Egindako ekintzen guztizko kopurua. 100 Ekintza presentzialetan edo birtualetan parte hartu duten pertsonen kopurua, guztira. 2.500		4. IMPULSAR EL NIVEL DE CULTURA DE CIBERSEGURIDAD DE LA SOCIEDAD VASCA. 1. Elaborar y difundir guías de buenas prácticas y recomendaciones de ciberseguridad. Número total de acciones realizadas. Número total de personas participantes en acciones presenciales o virtuales.
5. EUSKADIKO ENPRESA EHUNDURAREN ZIBER RESILIENTZIA SUSTATZEA 1. Enpresa estrategikoentzako babes-eredua definitzea. Lankidetzaren publiko pribatuaren esparruan azpiegitura sentikorrek eta Autobabeserako Euskal Arauak eragindako erakundeak babestera bideratutako jardueren kopurua. 10		5. IMPULSAR LA CIBER RESILIENCIA DEL TEJIDO EMPRESARIAL VASCO. 1. Definir el modelo de protección para las empresas estratégicas. Número de actuaciones realizadas en el ámbito de colaboración público-privada orientadas a la protección de infraestructuras sensibles y a organizaciones afectadas por la Norma Vasca de Autoprotección.
6. EUSKADIN FINKATUTAKO ERAKUNDEEI EDO EUSKADIN BIZI DIREN PERTSONEI ERAGITEN DIETEN ZIBERJAZOERAK HAUTEMATEA. 1. Euskadin eragina duten ziberintzidientek kudeatzea. Erantzun-ekipoan erregistratutako intzidenteen kopurua (CERT). 1.000		6. DETECTAR CIBERINCIDENTES QUE AFECTEN A ORGANIZACIONES ESTABLECIDAS O PERSONAS RESIDENTES EN EL TERRITORIO DE EUSKADI. 1. Gestionar los ciberincidentes que afecten a Euskadi. Número de incidentes registrados en el equipo de respuesta (CERT).



<https://zibersegurtasun.euskadi.eus/hasiera/>

