



Plan Estratégico de Cyberzaintza 2025-2028

Índice

1	Introducción	4
1.1	Objetivo del documento	4
1.2	Contexto	4
1.2.1	Sobre Cyberzaintza	4
1.2.2	Estrategia Vasca de Ciberseguridad	4
2	Principios	6
2.1	Misión	6
2.2	Propuesta de valor	6
2.3	Ámbitos de actuación	6
2.4	Público objetivo	7
2.1	Canales	7
3	Plan de acción	8
3.1	Líneas de acción	8
3.2	Plan de despliegue	9
3.2.1	Servicios	9
3.2.2	Situación actual	13
3.2.3	Hoja de ruta	49
3.2.4	Modelo de entrega de servicios	52
4	Modelo de gobernanza	53
4.1	Consejo de administración	53
4.2	Comité de dirección	53
4.3	Áreas	54
5	Seguimiento y evaluación	55
5.1	Sistema de seguimiento	55
5.2	Mecanismos de seguimiento	55
5.2.1	Reuniones de Área	55
5.2.2	Reuniones del Comité de Dirección	55
5.2.3	Reuniones del Consejo de Administración	55
5.3	Herramientas de evaluación	55
5.3.1	Monográfico	56
5.3.2	Cuadro de mando	56

5.3.3 Catálogo de indicadores.....	56
Anexo I - Catálogo de indicadores del Plan Estratégico de Cyberzaintza 2025-2028.....	57
Anexo II - Indicadores de gestión de Gobierno (2025)	63

1 Introducción

1.1 Objetivo del documento

Este documento presenta el Plan Estratégico de Cyberzaintza para el período 2025-2028, marcando un hito significativo como el primer plan desarrollado tras aprobación de la Ley 7/2023, de 29 de junio, de creación de la Agencia Vasca de Ciberseguridad.

El Plan Estratégico ha sido elaborado con el propósito de establecer un marco estructurado que guíe las actividades y objetivos de la Agencia durante los próximos cuatro años, garantizando su alineación con sus funciones establecidas por ley, así como con la Estrategia de Ciberseguridad de Euskadi, la cual define las prioridades y metas de la región en materia de ciberseguridad.

1.2 Contexto

1.2.1 Sobre Cyberzaintza

La Agencia Vasca de Ciberseguridad, Cyberzaintza, es un ente público de derecho privado del sector público de la Comunidad Autónoma Vasca, con personalidad jurídica propia, adscrita al Departamento de Seguridad.

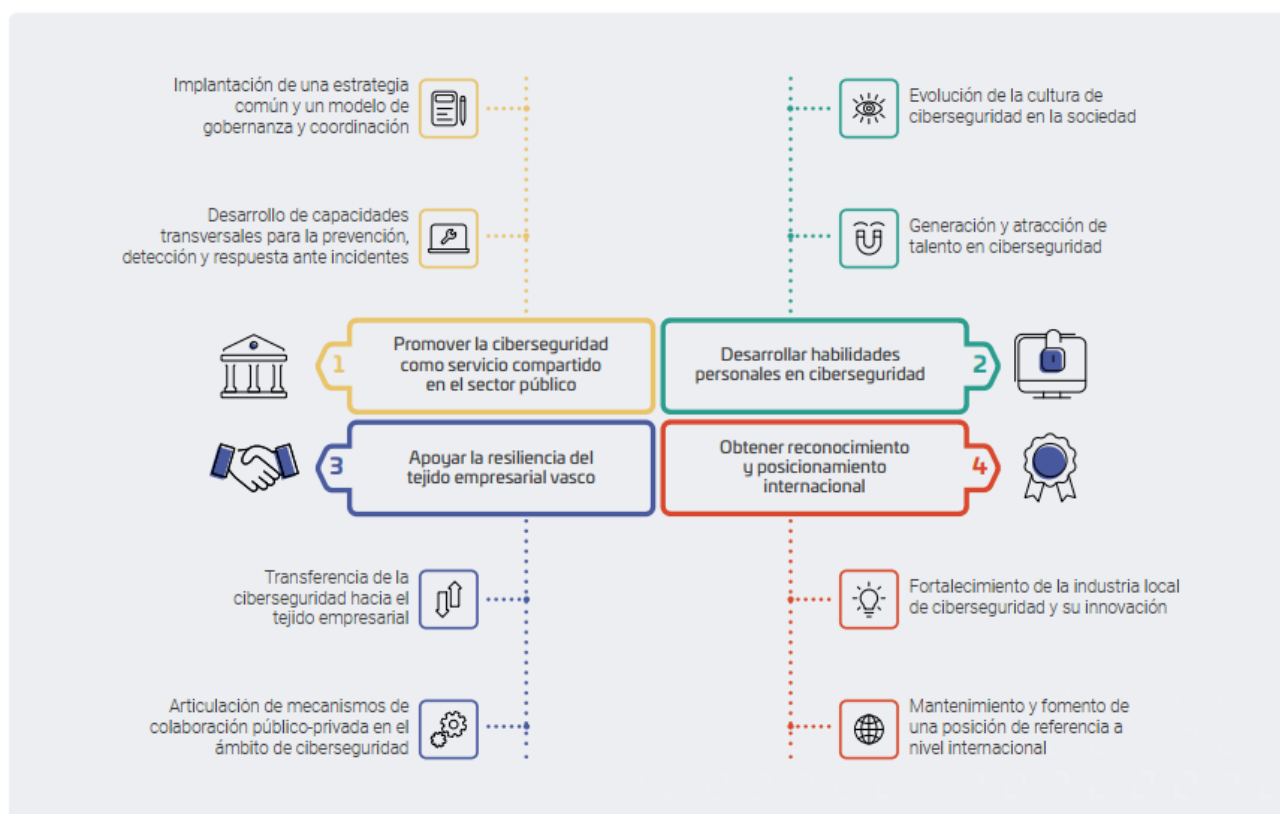
El objeto de Cyberzaintza es promover y coordinar la ciberseguridad en el sector público vasco en el ámbito de la seguridad de los sistemas de información y de las redes electrónicas de competencia de dicho sector, y apoyar e impulsar la capacitación en ciberseguridad y el desarrollo digital seguro de la Comunidad Autónoma Vasca, de su Administración pública, de su ciudadanía y de su tejido empresarial.

La [LEY 7/2023, de 29 de junio, de creación de la Agencia Vasca de Ciberseguridad](#) en su Artículo 2 establece las funciones que corresponden a la Agencia para el cumplimiento de su objeto.

1.2.2 Estrategia Vasca de Ciberseguridad

La Estrategia Vasca de Ciberseguridad 2024-2029 aborda los desafíos de País en este ámbito y establece cuatro objetivos estratégicos. Para alcanzar estos, define ocho líneas de actuación, cada una con un conjunto específico de acciones que deberán ser lideradas por los agentes competentes. Las actividades contempladas en esta Estrategia no solo involucran a las Administraciones Públicas de Euskadi, sino también a la ciudadanía, al tejido empresarial y al sector de la ciberseguridad en su conjunto.

El propósito de la estrategia es convertir a Euskadi en un país ciberresiliente, con capacidades para proteger su Administración Pública y su tejido empresarial frente a los riesgos cibernéticos, promoviendo el empoderamiento de la sociedad en el proceso de transformación digital y aportando dichas capacidades para desarrollar la ciberseguridad global, ocupando un lugar de referencia en el ámbito internacional.



Objetivos y líneas de actuación de la Estrategia Vasca de Ciberseguridad

El Plan Estratégico de Cyberzaintza 2025-2028 se alinea de manera integral con la Estrategia Vasca de Ciberseguridad 2024-2029, asegurando que las acciones y medidas propuestas refuercen la misión de Cyberzaintza y se correspondan con los objetivos y líneas de actuación establecidos en la estrategia de País.

2 Principios

2.1 Misión

La misión de la Agencia tiene es promover y coordinar la ciberseguridad en el sector público vasco delimitado en la Ley 3/2022, de 12 de mayo, del Sector Público Vasco, en el ámbito de la seguridad de los sistemas de información y de las redes electrónicas de competencia de dicho sector, y apoyar e impulsar la capacitación en ciberseguridad y el desarrollo digital seguro de la Comunidad Autónoma Vasca, de su Administración pública, de su ciudadanía y de su tejido empresarial.

2.2 Propuesta de valor

Cyberzaintza presenta su propuesta de valor con el objetivo de cumplir su misión y alinearse con el desarrollo de la Estrategia de Ciberseguridad de Euskadi. Esta propuesta busca impulsar medidas y acciones que fortalezcan la ciberseguridad en Euskadi, promoviendo la colaboración, la concienciación y la protección de los sistemas informáticos y datos sensibles.

- Promovemos la ciberseguridad en Euskadi.
- Coordinamos la ciberseguridad con otros dentro y fuera de Euskadi.
- Nos alineamos con la estrategia vasca de ciberseguridad y con el marco legal aplicable.
- Elaboramos estándares y directrices.
- Damos servicios de gobernanza, prevención, detección y respuesta.
- Nos orientamos al sector público vasco, al tejido empresarial y a la ciudadanía.

2.3 Ámbitos de actuación

La actividad de Cyberzaintza se clasifica en cuatro ámbitos de actuación. Estos no solo definen los espacios de intervención, sino que también establecen un marco estructurado para abordar de manera integral las diversas facetas de la ciberseguridad, alineándose con estándares de buenas prácticas reconocidos internacionalmente.

A continuación, se describen los cuatro ámbitos de actuación:

- **Prevención:** abarca todos los servicios destinados a evitar posibles incidentes de seguridad antes de que ocurran.
- **Detección:** identificación temprana de incidentes de seguridad a través del uso de sistemas y herramientas. La detección temprana permite una respuesta más rápida y efectiva ante cualquier amenaza.
- **Respuesta:** engloba los servicios necesarios una vez que se ha detectado un incidente de seguridad.
- **Gobernanza:** establece las directrices y estructuras necesarias para gestionar la ciberseguridad de forma integral.

2.4 Público objetivo

Cyberzaintza orienta sus servicios a un público objetivo diverso, que incluye al sector público vasco, al tejido empresarial y a la ciudadanía. La oferta de servicios se segmenta en diferentes verticales para satisfacer las necesidades específicas de cada sector. El propósito fundamental de esta segmentación es abordar de manera específica las necesidades de ciberseguridad en cada entorno y adaptar los servicios a esas necesidades particulares.

A continuación, se listan las verticales definidas hasta la fecha:

Público Objetivo	Vertical
Sector Público	Sector público – Administración Seguridad Salud Educación
Empresas	Empresas estratégicas Empresas con obligación en materia de autoprotección Otras Empresas+
Ciudadanía	Menores Personas Adultas

2.5 Canales

La entrega de servicios a las diferentes verticales se realiza directamente desde Cyberzaintza o a través de diversos canales que aseguren su llegada a la organización destinataria. Este proceso se lleva a cabo siguiendo las siguientes premisas:

- Los servicios al sector público son proporcionados directamente por Cyberzaintza, con las siguientes excepciones:
 - La transferencia de conocimientos se gestiona a través de acuerdos con la **Academia de Policía y Emergencias**, el **IVAP y otras entidades o iniciativas públicas que trabajen con ese foco**.
 - Para los servicios destinados a ayuntamientos con menos de 20.000 habitantes, Cyberzaintza se coordinará con la **Diputación Foral** correspondiente.
- La entrega de servicios a empresas se efectúa directamente desde Cyberzaintza, sin perjuicio de que también puedan establecerse acuerdos temporales con **clústeres, asociaciones empresariales y otras entidades o iniciativas públicas que trabajen con ese foco**.
- Los servicios a la ciudadanía se ofrecen de manera unidireccional desde Cyberzaintza y mediante acciones específicas que se puedan canalizar a través de acuerdos con el departamento de **Educación, Ertzaintza, Lanbide, KZ-Gunea, Tknika, asociaciones y entidades sin ánimo de lucro**.

3 Plan de acción

3.1 Líneas de acción

Siguiendo los principios establecidos, se han definido once líneas de acción para cumplir con la misión y funciones de Cyberzaintza. Una línea de acción es un conjunto de actividades específicas dirigidas a alcanzar un objetivo particular en el ámbito de la ciberseguridad. A continuación, se incluye una breve descripción de las mismas:

- **Auditoría**

La línea de acción de auditoría está destinada a evaluar y asegurar el cumplimiento de las normativas clave en ciberseguridad, así como a facilitar su seguimiento y mantenimiento.

- **Concienciación**

El objetivo principal de la línea de acción de concienciación es fomentar una cultura sólida de ciberseguridad y elevar el nivel de conocimiento y comprensión tanto de individuos como de organizaciones sobre los riesgos digitales presentes en el entorno actual. Además, busca promover comportamientos seguros y responsables en la utilización de la tecnología.

- **Consultoría**

La línea de acción de consultoría tiene como objetivo principal mejorar la comprensión de la problemática en materia de ciberseguridad y apoyar en la gestión de proyectos específicos.

- **Coordinación estratégica**

El objetivo principal de la línea de coordinación estratégica es coordinar los recursos de ciberseguridad existentes, desde una perspectiva transversal, con el fin de optimizar y mejorar su eficiencia.

- **Gestión del riesgo**

La línea de acción de gestión del riesgo tiene como objetivo principal identificar, evaluar y mitigar los riesgos tecnológicos y organizativos relacionados con la ciberseguridad. Este enfoque integral permite a las organizaciones obtener una visión clara y transversal de su nivel de riesgo, facilitando la toma de decisiones informadas y la implementación de medidas de protección adecuadas.

- **Inteligencia de Amenazas**

La línea de acción de inteligencia de amenazas tiene como objetivo principal proporcionar a las organizaciones información relevante y procesable sobre posibles amenazas en el ámbito de la ciberseguridad. Esto les facilita anticiparse a ataques, tomar decisiones informadas y reforzar su protección.

- **Modelo de Seguridad de Euskadi**

La línea de acción de modelo de seguridad de Euskadi tiene como objetivo principal establecer un marco integral de ciberseguridad que sirva como base para garantizar un entorno digital seguro y resiliente frente a las ciberamenazas. Este modelo para el espacio digital estará alineado con el Plan General de Seguridad pública de Euskadi y formará, por tanto, parte de un Modelo de Seguridad Integral más amplio que responda a los retos del Territorio.

- **Operaciones de seguridad (SOC)**

La línea de acción de SOC tiene como objetivo principal proteger las infraestructuras tecnológicas de las organizaciones mediante la monitorización continua, lo que reduce el tiempo de respuesta ante posibles incidentes de ciberseguridad.

- **Respuesta a incidentes (CSIRT)**

El objetivo principal de la línea de acción del Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) es asistir a las organizaciones en la gestión de sus incidentes de seguridad. Con un enfoque integral, se pretende coordinar la respuesta ante incidentes que impacten a múltiples entidades y compartir información crucial para salvaguardar al resto.

- **Seguridad ofensiva**

El objetivo principal de la línea de seguridad ofensiva es identificar amenazas y vulnerabilidades en los sistemas de las organizaciones antes de que lo haga un atacante, fortaleciendo así su capacidad defensiva frente a posibles ciberataques.

- **Transferencia del conocimiento**

La línea de acción de transferencia del conocimiento tiene como objetivo principal fomentar la especialización y el desarrollo de habilidades en ciberseguridad, así como exportar operativas y casos de éxito a los diferentes públicos de Cyberzaintza. Además, se busca exportar maneras de proceder, documentación, clausulado, etc., de entidades con un nivel de madurez mayor a otras con un nivel de madurez menor, promoviendo así un intercambio de conocimientos y prácticas que eleve el estándar general de ciberseguridad.

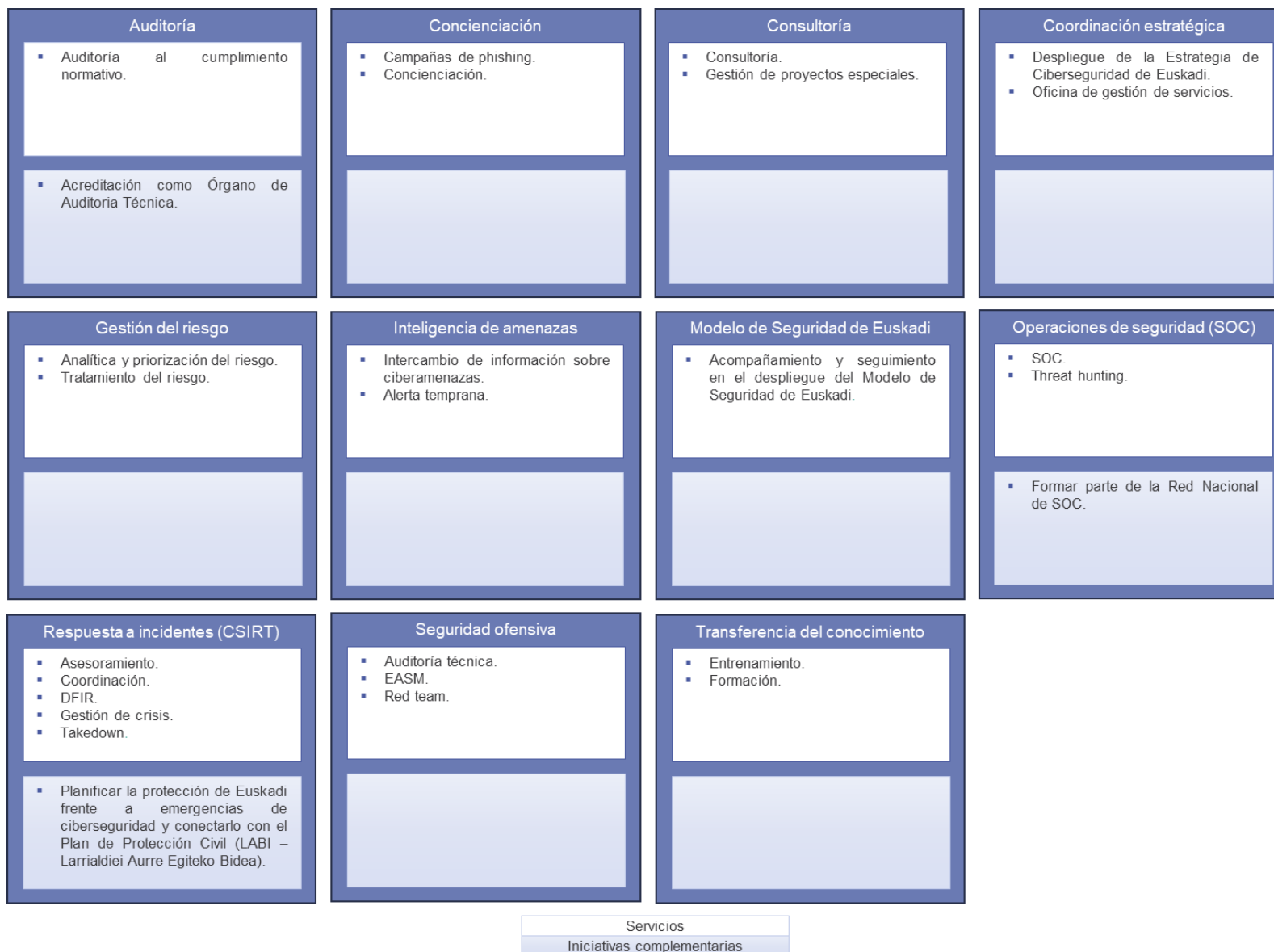
3.2 Plan de despliegue

3.2.1 Servicios

Las líneas de acción se implementarán principalmente como servicios. Cada línea de acción está alineada con una línea de servicio, la cual está compuesta por múltiples servicios individuales con características similares y un objetivo común. De esta manera, se garantiza una coherencia estratégica en la ejecución.

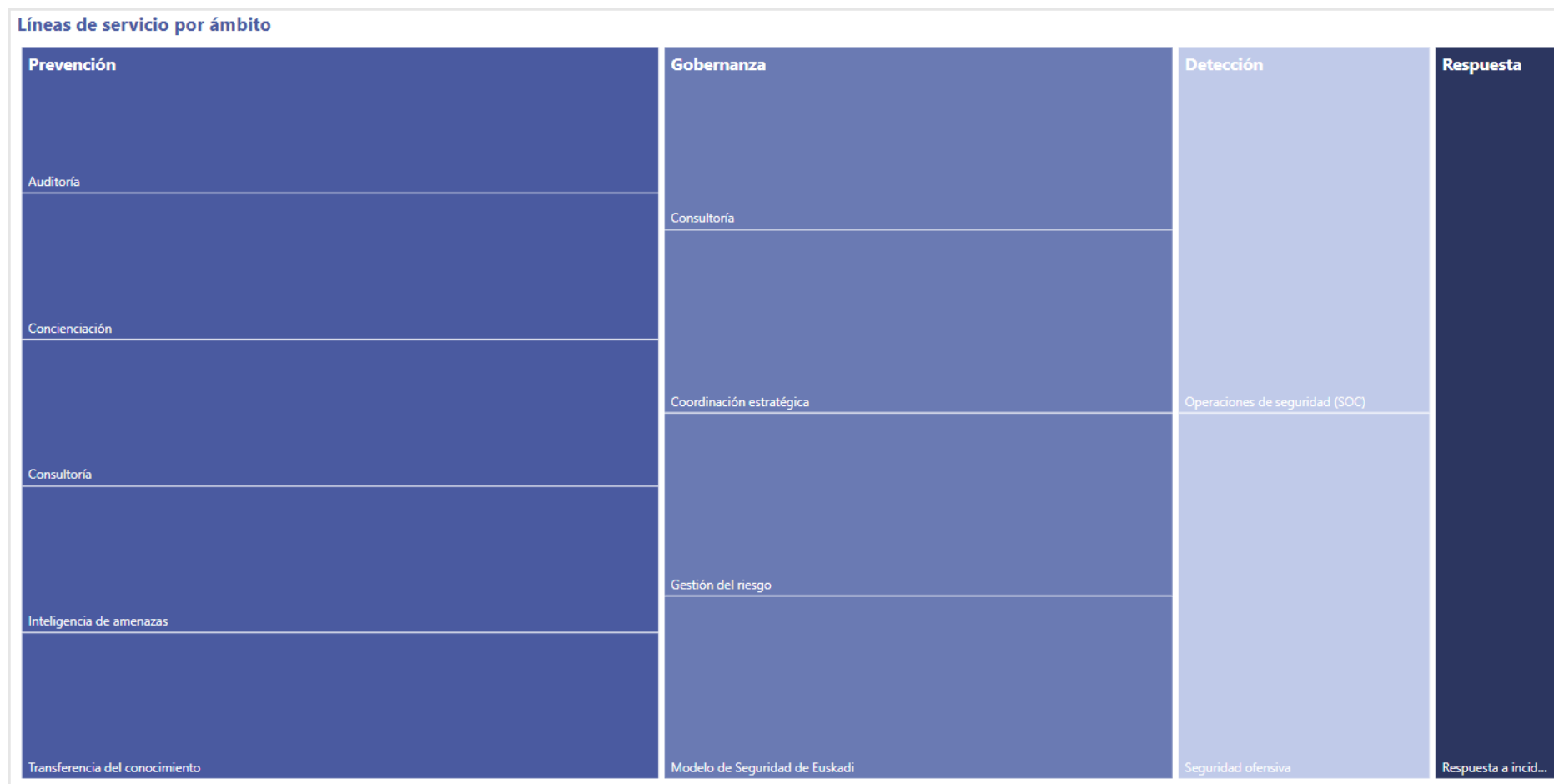
Para aquellas actividades puntuales que no estén cubiertas por los servicios, las líneas de acción se desplegarán mediante iniciativas complementarias.

En la siguiente tabla se resumen los servicios agrupados por línea y las iniciativas complementarias identificadas hasta la fecha:



3.2.1.1 Líneas de servicio por ámbito

En el siguiente gráfico se muestra cómo se distribuyen las líneas de servicios en base a los ámbitos de actuación definidos:



3.2.1.2 Servicios internos

Para poder desarrollar todas estas actividades, se requieren una serie de servicios internos que posibiliten la operativa y aseguren el correcto funcionamiento de Cyberzaintza. Estos servicios internos comprenden las áreas de soporte fundamentales para la implementación efectiva de las acciones propuestas. A continuación, se describen los servicios internos:

Administración y servicios

- El objetivo del servicio es gestionar los aspectos económicos y de personal, asegurar el cumplimiento del régimen jurídico aplicable, y proporcionar los servicios generales necesarios para apoyar el funcionamiento integral de la Agencia.

Apoyo al desarrollo de proyectos de innovación en I+D+i en ciberseguridad

- El objetivo del servicio es fomentar la participación en consorcios europeos, promover la adopción temprana de soluciones innovadoras, e identificar casos de uso para la protección de las Administraciones Públicas (AAPP).

Cumplimiento normativo Cyberzaintza

- El objetivo del servicio es el cumplimiento de la normativa aplicable para la propia Agencia Vasca de Ciberseguridad.

Desarrollo y despliegue del Plan Estratégico de Cyberzaintza

- El objetivo del servicio es desarrollar y ejecutar el Plan Estratégico de Cyberzaintza con el fin de asegurar una alineación estratégica efectiva. Esto incluye la elaboración de un plan de acción para implementar la estrategia definida, así como la evaluación y monitoreo continuo de su implementación.

Seguridad corporativa

- El objetivo del servicio es garantizar la administración eficiente de la infraestructura de la organización, proteger los activos físicos y digitales de la Agencia, e implementar controles de seguridad informática que aseguren la integridad y confidencialidad de la información.

Servicio de comunicación

- El objetivo del servicio es facilitar la interacción entre Cyberzaintza y sus diferentes públicos objetivos, asegurando que la información relevante se transmita de manera clara y accesible. Esto incluye informar sobre políticas, programas y servicios, a la vez que busca construir y mantener una buena imagen institucional, gestionar la comunicación interna y externa, responder a las inquietudes de la comunidad y fortalecer la confianza entre el organismo y la sociedad.

3.2.2 Situación actual

El catálogo de servicios consta de 24 servicios individuales, organizados en 11 líneas de servicio. Se ha determinado qué servicios se ofrecerán a cada público objetivo. La oferta se muestra en la siguiente tabla:

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.

Las líneas de servicio con un rombo rojo no están disponibles, mientras que las marcadas con un círculo verde sí lo están. Actualmente, se han activado el 28,37% de los servicios definidos. Para la obtención de este valor se ha considerado la oferta de servicios segmentada por vertical.

A continuación, se presenta la información detallada para cada uno de los servicios: incluyendo la línea correspondiente, una descripción del servicio, el detalle de las verticales en las que se entrega el servicio y el ámbito de actuación en el cual se enmarca dicho servicio.

Auditoría

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

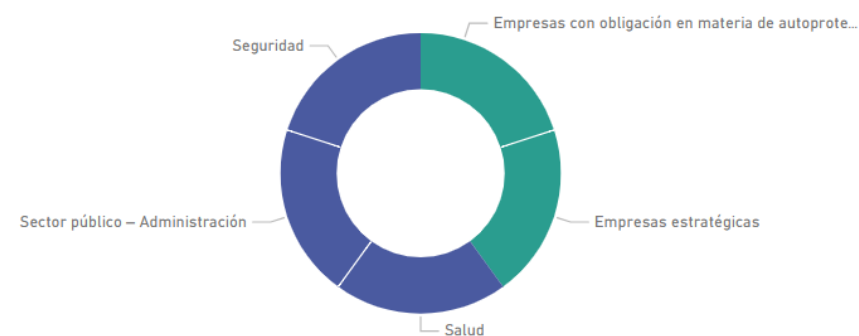
Auditoría

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.



Concienciación



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

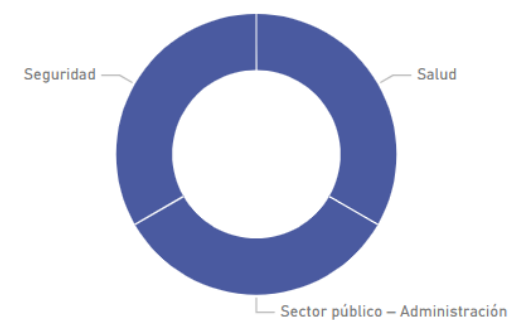
Concienciación

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

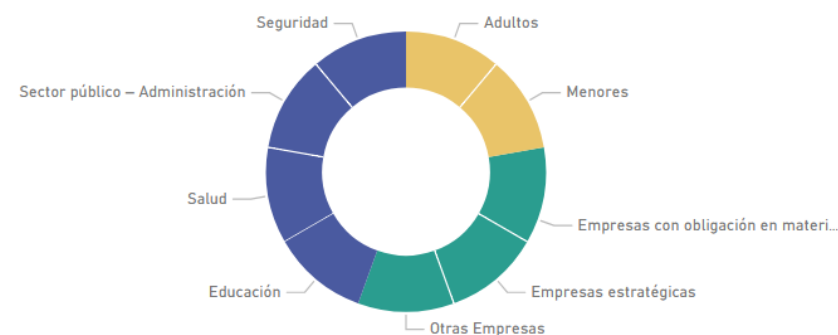
Descripción del servicio

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



Consultoría

Línea del servicio	Empresas	Sector Público
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

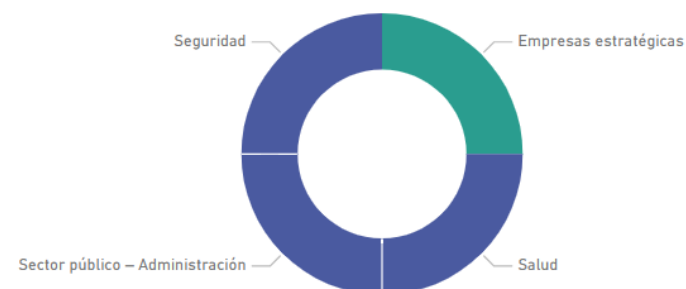
Consultoría

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

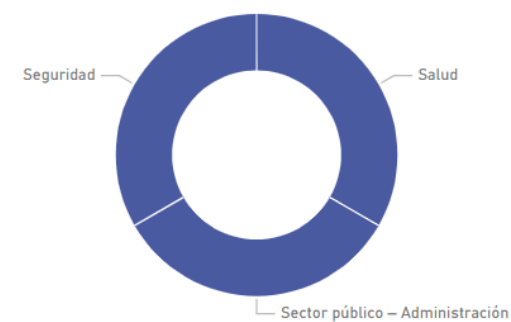
Consultoría

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.



Coordinación Estratégica

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

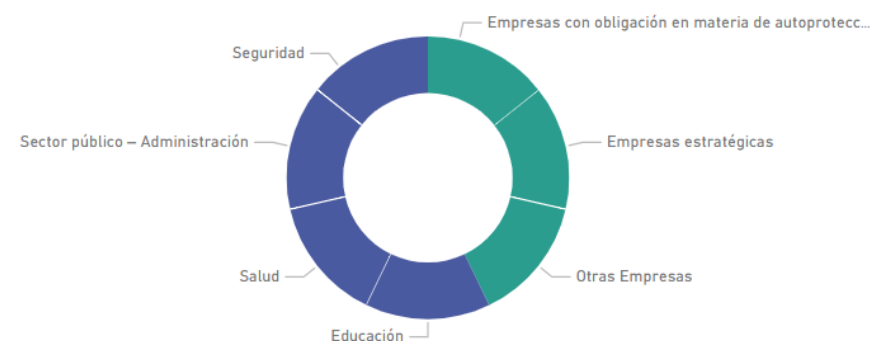
Coordinación estratégica

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

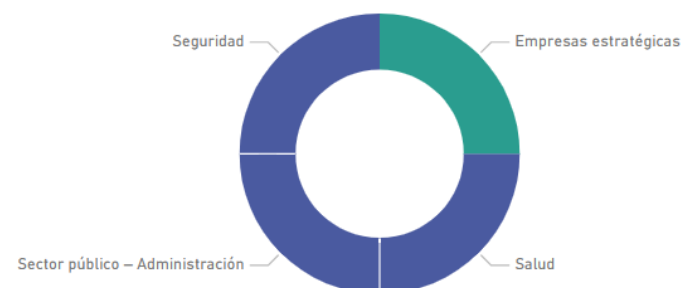
● Empresas ● Sector Público

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.



Gestión del riesgo

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

Ficha de servicio

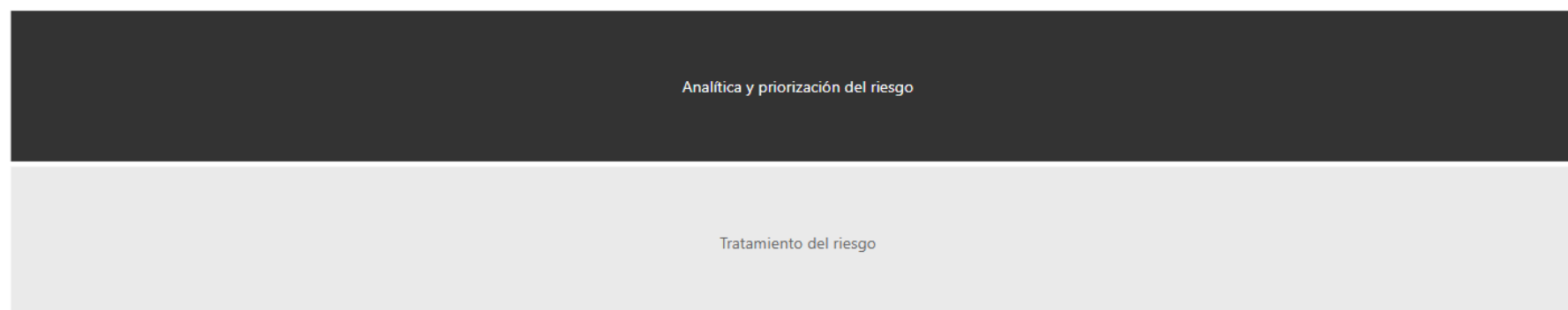
Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Gestión del riesgo

Servicios



Ámbito

Gobernanza

Línea del servicio

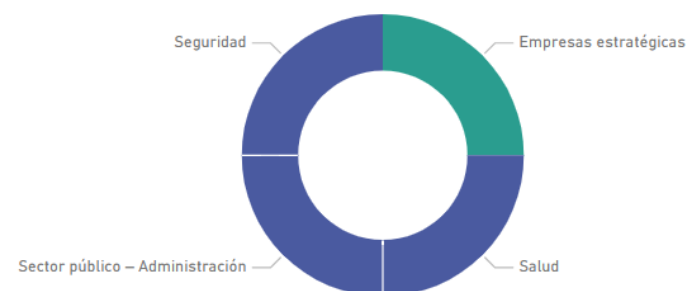
Gestión del riesgo

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

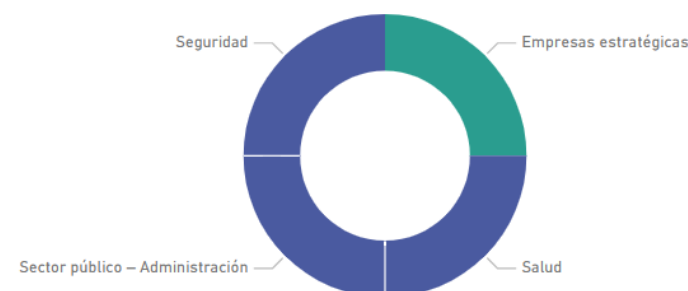
Gestión del riesgo

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.



Inteligencia de Amenazas

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

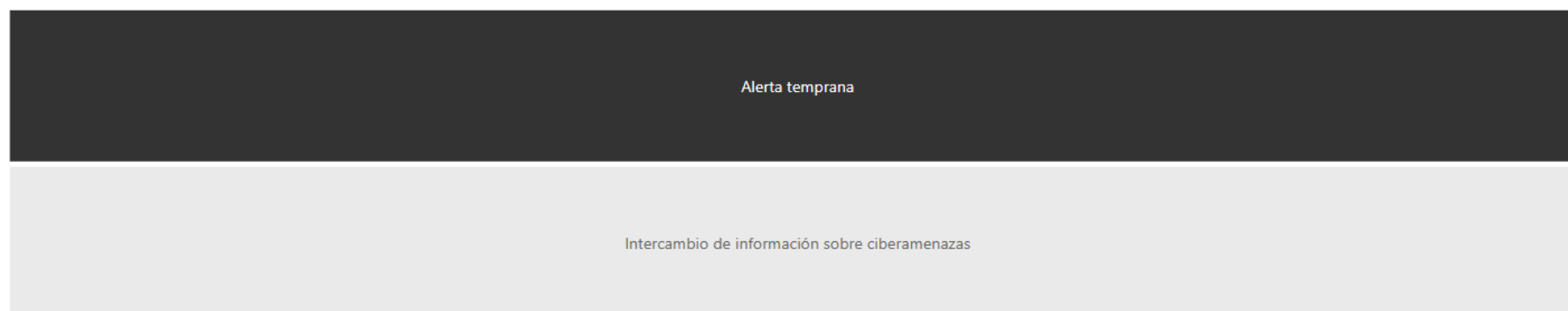
Ficha de servicio

Información detallada de los servicios

Filtro por línea del servicio

Inteligencia de amenazas

Servicios



Ámbito

Prevención

Línea del servicio

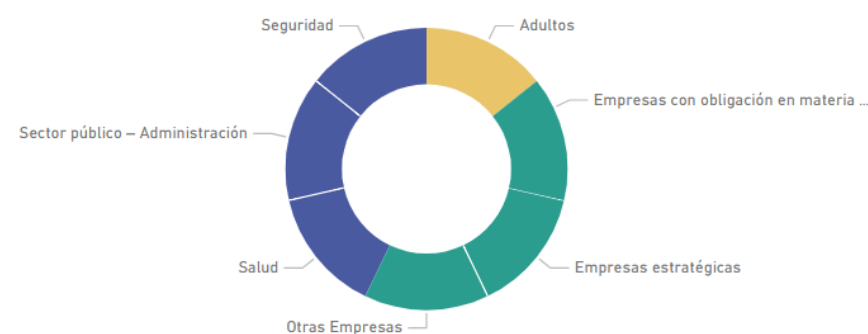
Inteligencia de amenazas

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

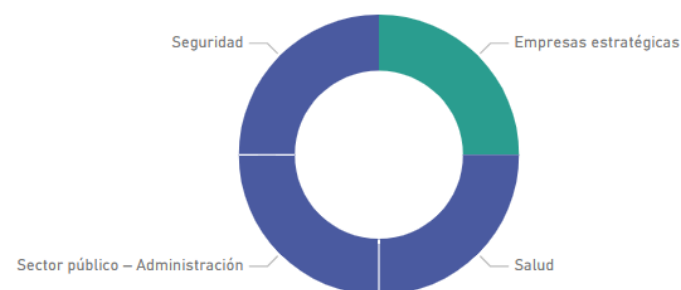
Inteligencia de amenazas

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.



Modelo de Seguridad de Euskadi

Línea del servicio	Empresas Sector Públ	
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

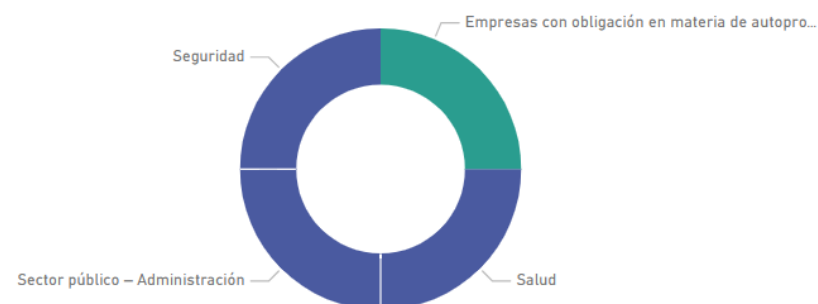
Verticales

● 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.



Operaciones de seguridad (SOC)

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

Ficha de servicio

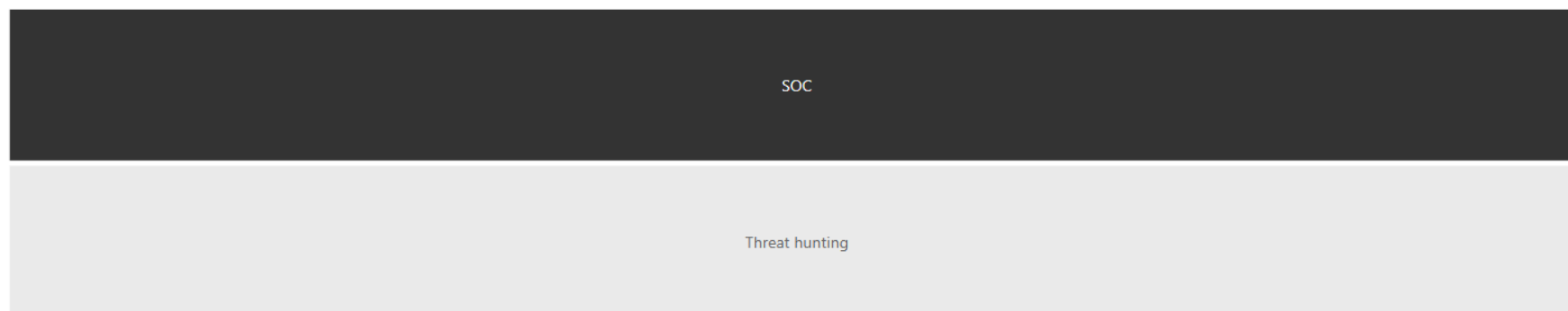
Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Operaciones de seguridad (SOC)

Servicios



Ámbito

Detección

Línea del servicio

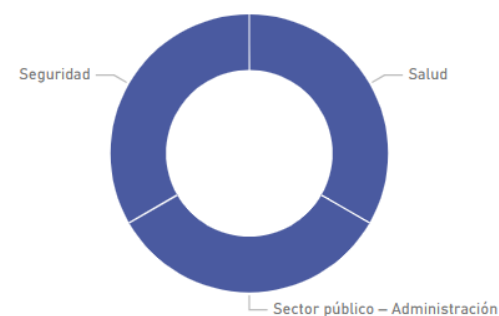
Operaciones de seguridad (SOC)

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

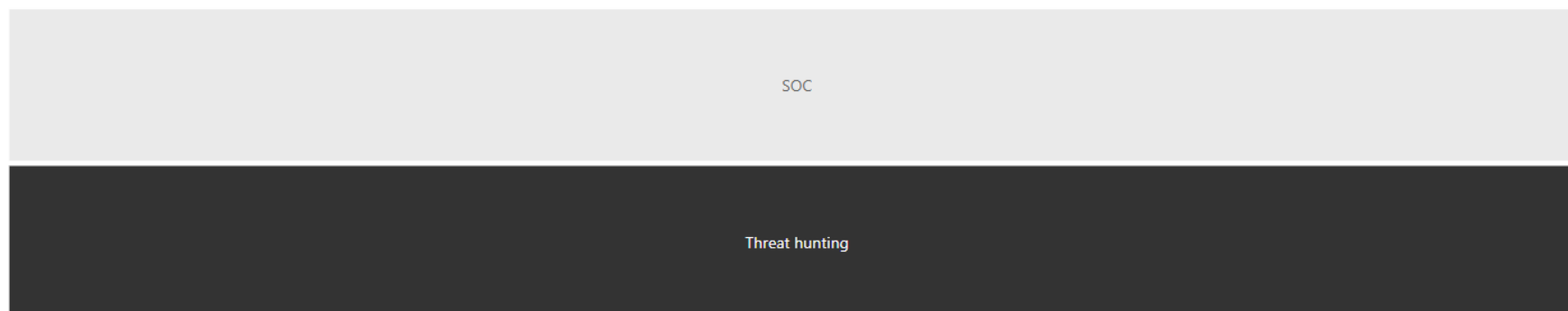
Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Operaciones de seguridad (SOC)

Servicios



Ámbito

Detección

Línea del servicio

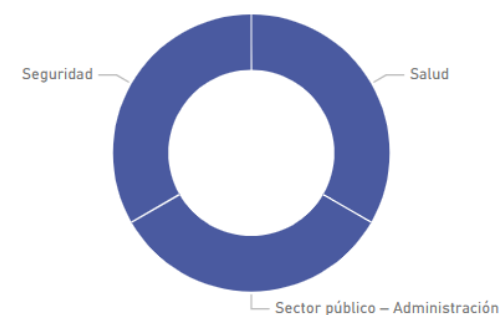
Operaciones de seguridad (SOC)

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.



Respuesta a incidentes (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

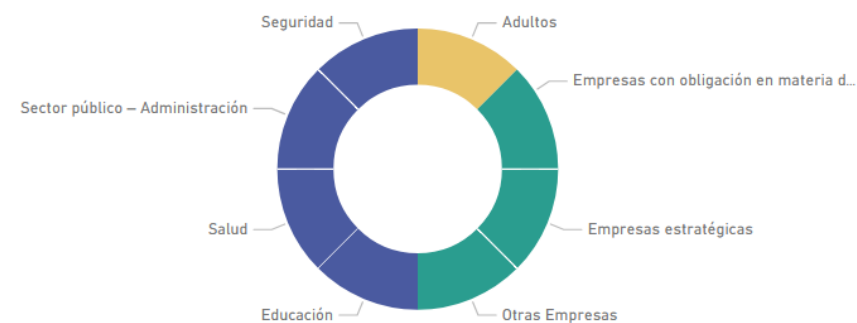
Respuesta a incidentes (CSIRT)

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

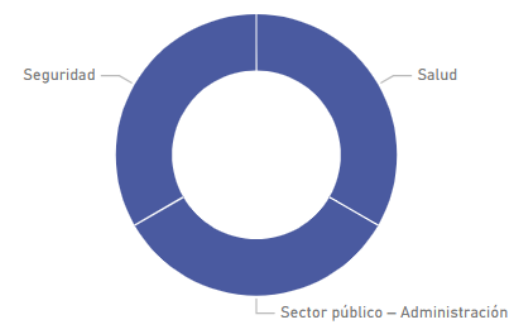
Respuesta a incidentes (CSIRT)

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

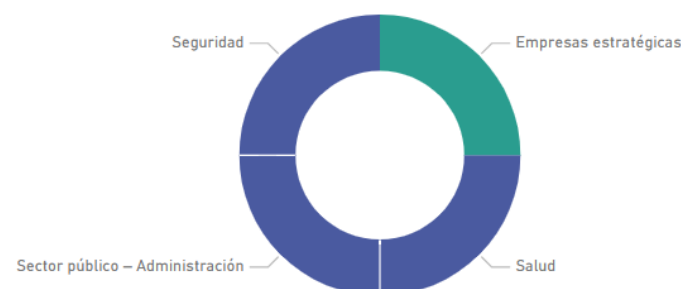
Respuesta a incidentes (CSIRT)

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

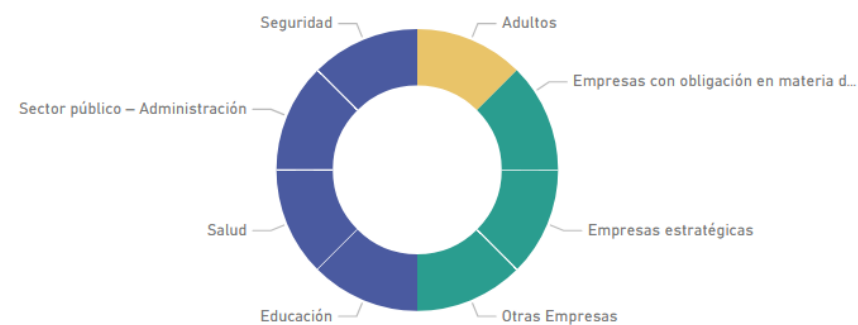
Respuesta a incidentes (CSIRT)

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

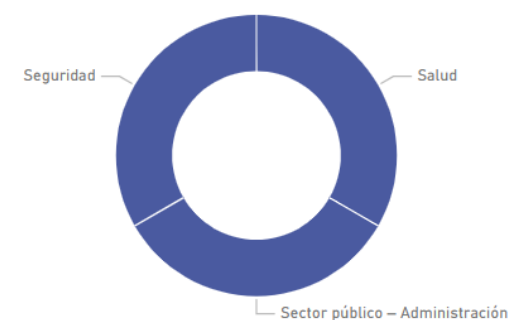
Respuesta a incidentes (CSIRT)

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.



Seguridad Ofensiva

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

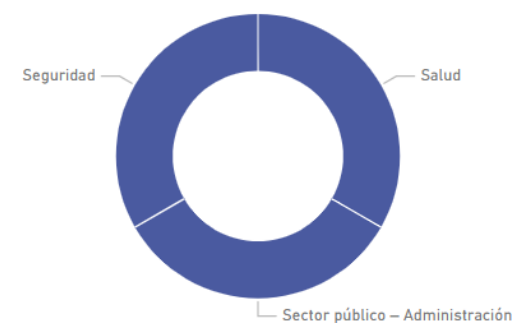
Seguridad ofensiva

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

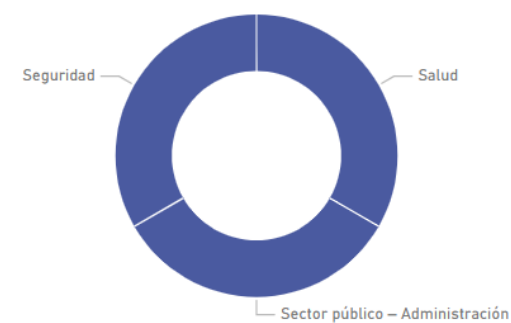
Seguridad ofensiva

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

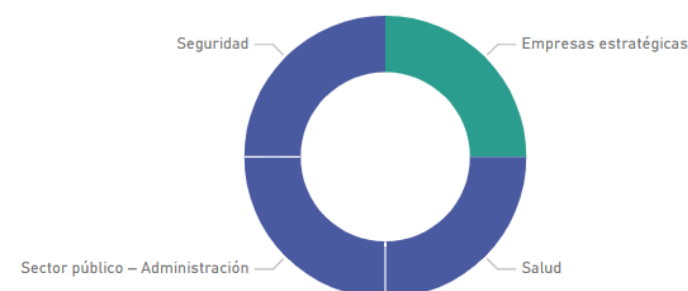
Seguridad ofensiva

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



Transferencia del conocimiento

Línea del servicio	Empresas	Sector Público
Transferencia del conocimiento		
Entrenamiento	◆	◆
Formación	◆	◆

Ficha de servicio

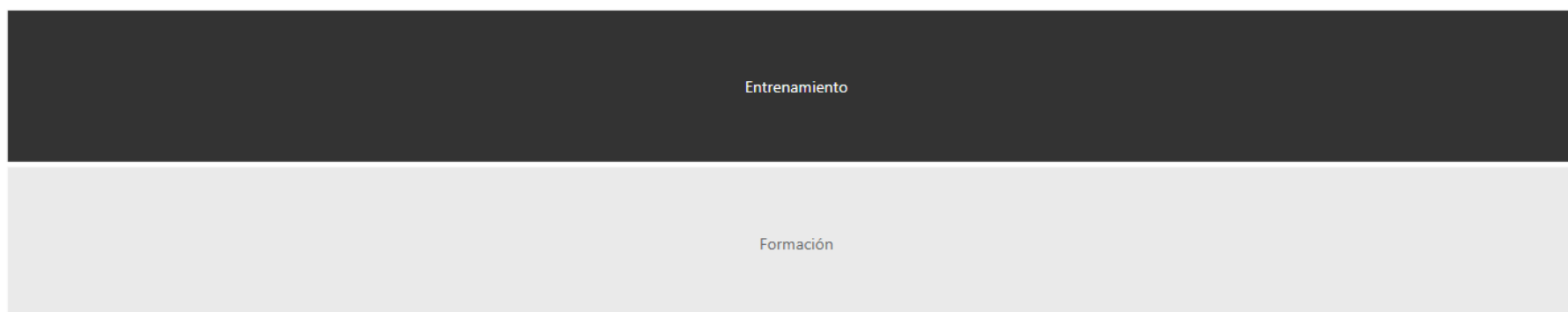
Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Transferencia del conocimiento

Servicios



Ámbito

Prevención

Línea del servicio

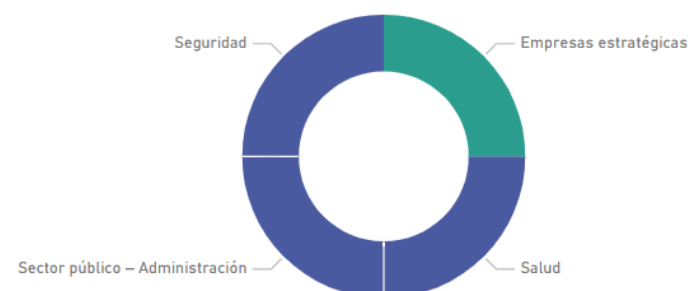
Transferencia del conocimiento

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

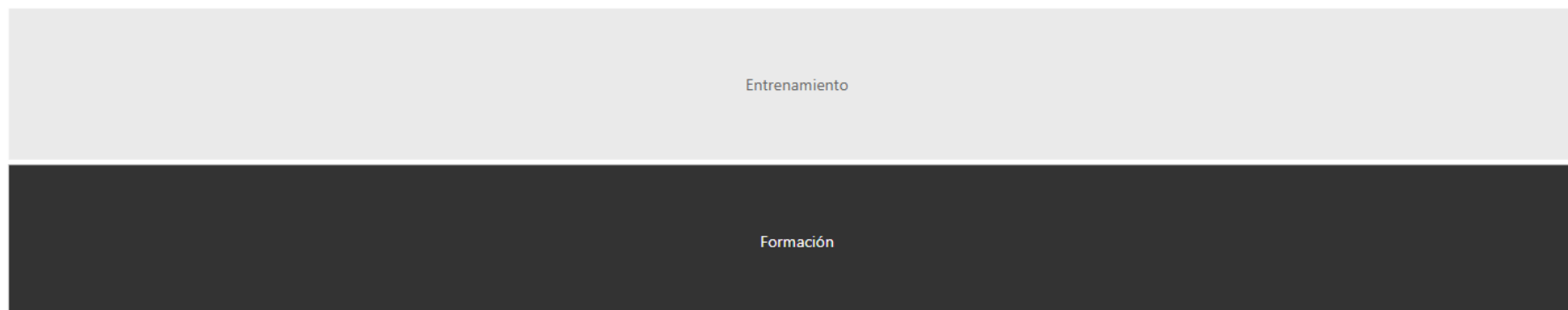
Información detallada de los servicios

Inactivo

Filtro por línea del servicio

Transferencia del conocimiento

Servicios



Ámbito

Prevención

Línea del servicio

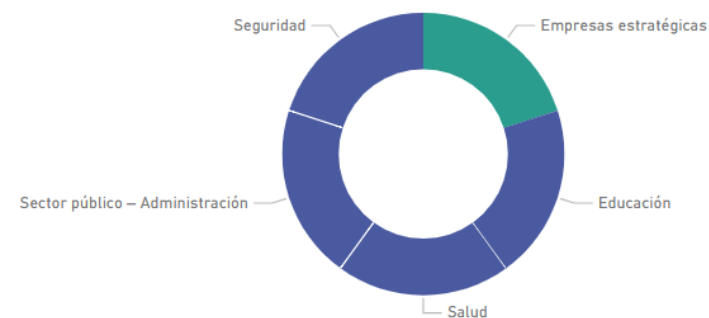
Transferencia del conocimiento

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.

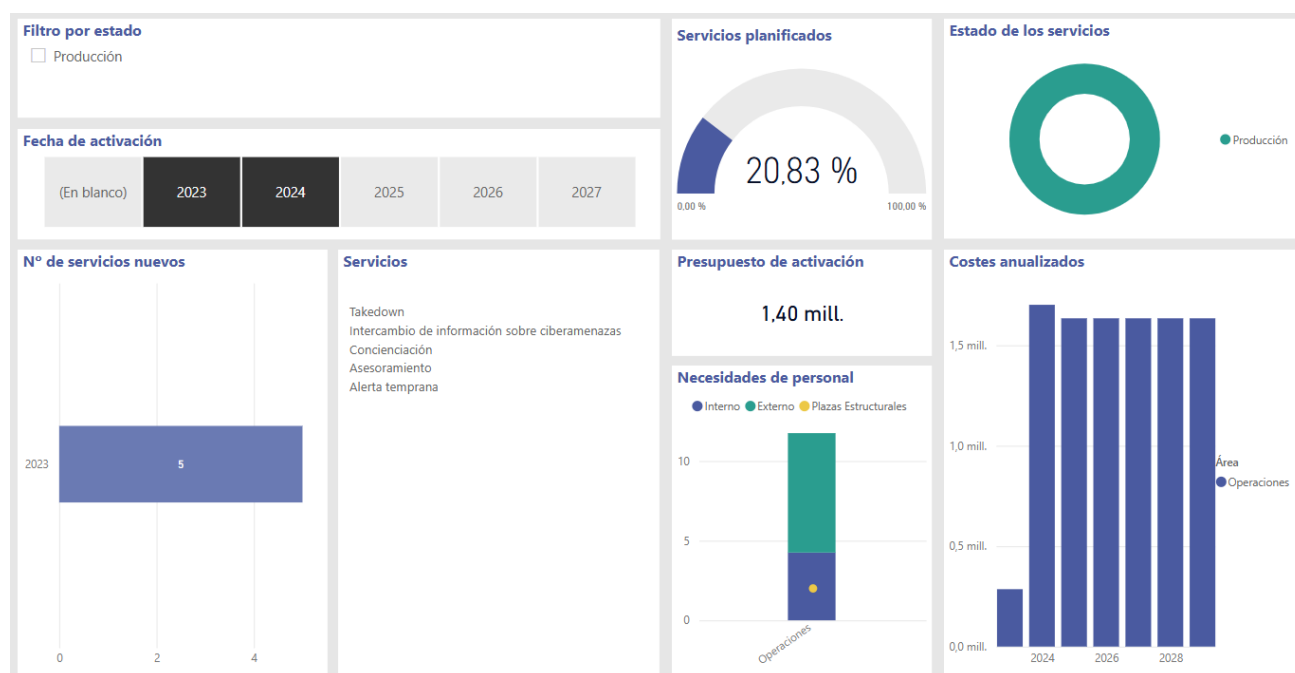


3.2.3 Hoja de ruta

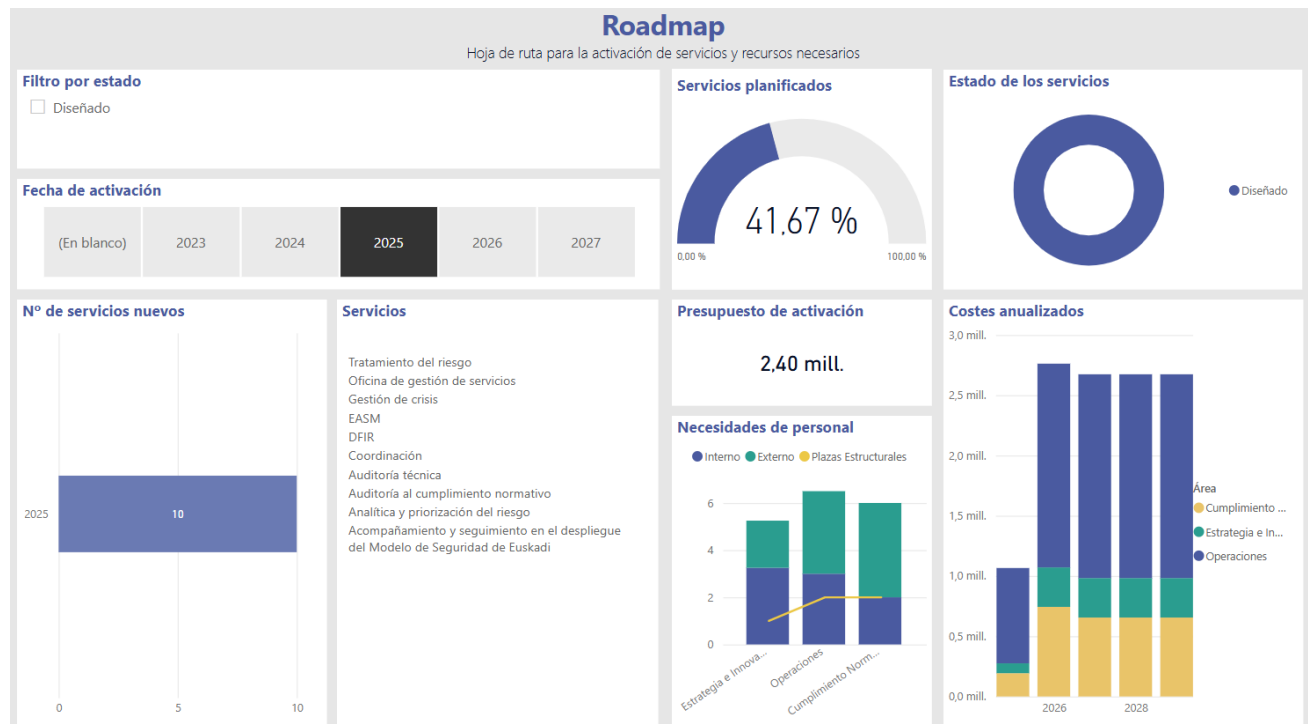
A continuación, se detalla la hoja de ruta para la activación de servicios, incluyendo la relación de servicios planificados y la estimación de recursos necesarios para su implementación. Se han estimado tanto las necesidades de personal como las necesidades presupuestarias, considerando el coste de puesta en marcha y el coste de mantenimiento anual del servicio.

Situación inicial

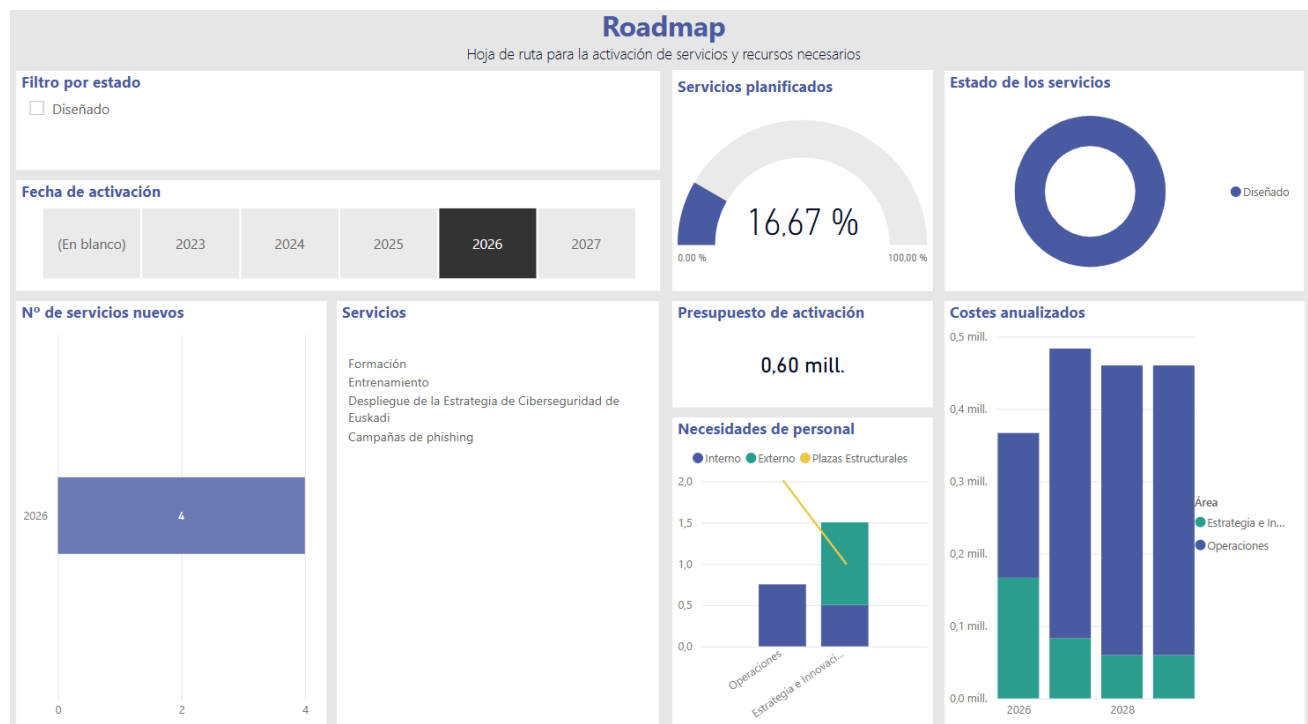
A continuación, se resume la situación inicial de los servicios, previa a la aprobación del presente Plan:



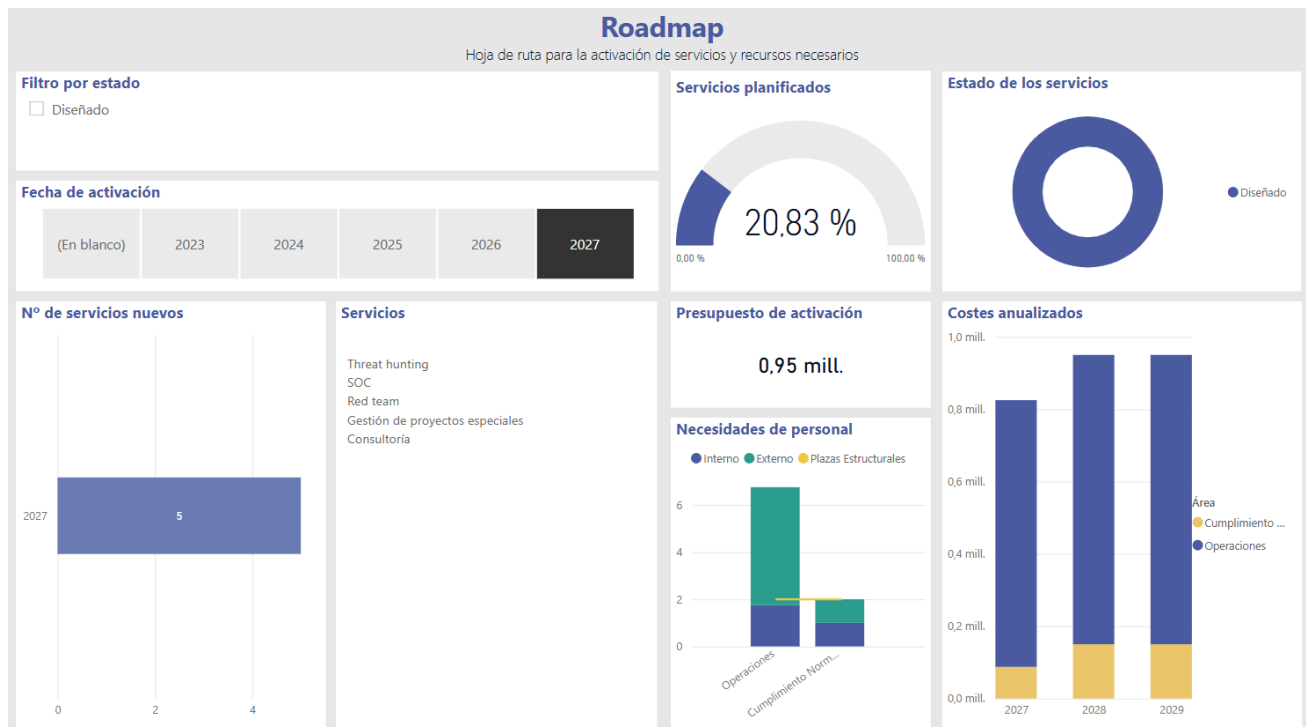
2025



2026

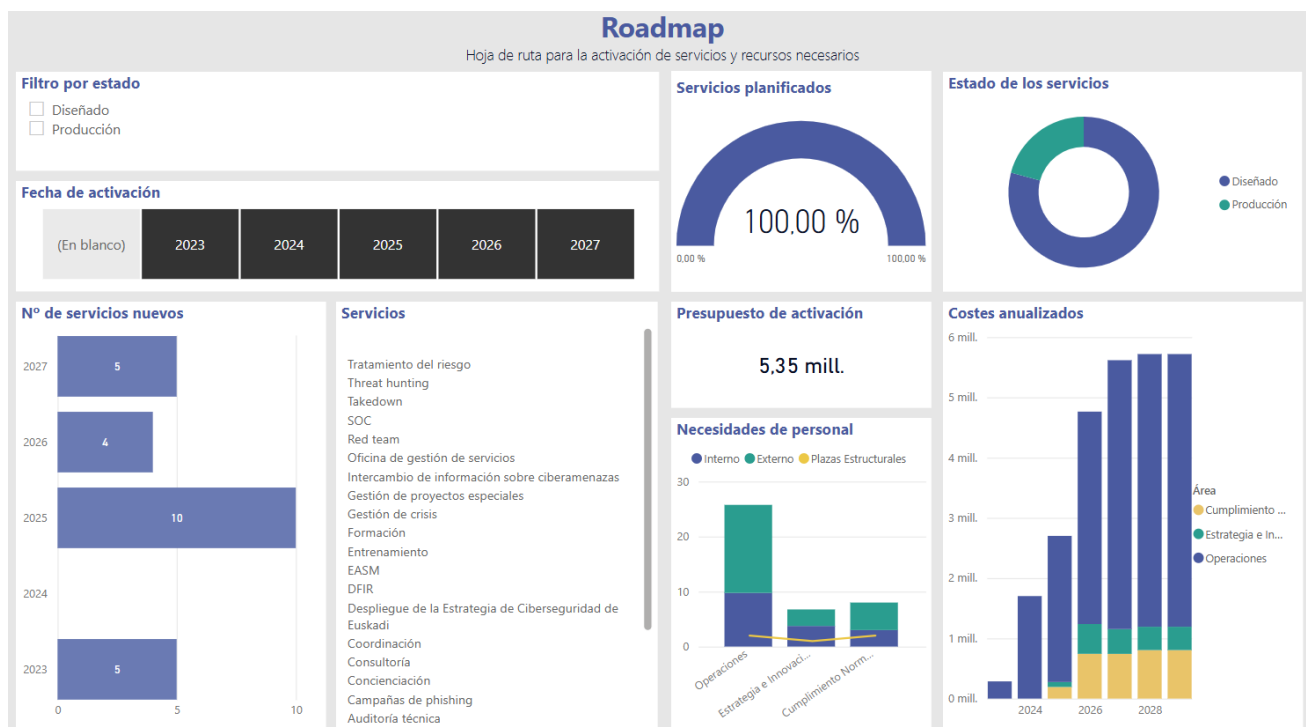


2027



Situación final

A continuación, se presenta el resumen final de la situación de los servicios, tras la activación de todos los servicios planificados:



3.2.4 Modelo de entrega de servicios

El modelo de entrega de servicios es fundamental para asegurar una operación eficiente y eficaz de Cyberzaintza. Este modelo se ha diseñado para garantizar que los servicios se proporcionen de manera coherente y alineada con los objetivos estratégicos de la organización.

A continuación, se presenta el esquema del modelo de entrega de servicios definido:



4 Modelo de gobernanza

El Plan Estratégico de Cyberzaintza cuenta con tres niveles de gobernanza diseñados para garantizar su implementación y supervisión:



4.1 Consejo de administración

El Consejo de Administración es el órgano superior de la Agencia, compuesto por dieciséis miembros que representan los tres niveles de la Administración Pública de la Comunidad Autónoma Vasca. Entre su principales funciones se encuentran la aprobación de planes y presupuestos anuales, la memoria de actividades, y la propuesta de plantillas del personal y régimen retributivo. Además, se encarga de proponer modificaciones de estatutos, supervisar la gestión de la Dirección, autorizar participaciones en otras entidades, aprobar convenios y acuerdos, informar al Gobierno Vasco sobre sus actividades, y ejercer otras funciones legales y estatutarias.

Respecto al Plan Estratégico de Cyberzaintza, el Consejo de Administración tiene la responsabilidad de aprobarlo y hacer un seguimiento periódico de su desarrollo. Además, velará porque la Agencia tenga los recursos necesarios para su desarrollo, aprobando los planes de actividades y presupuestos que soportan el desarrollo del Plan y proponiendo y escalando a Gobierno las plantillas de personal necesario para llevar a cabo las acciones planificadas.

Así mismo, informará periódicamente al Gobierno Vasco sobre el progreso y las actividades de la Agencia, garantizando así una supervisión continua.

4.2 Comité de dirección

El Comité de Dirección está liderado por la persona que ostenta la Dirección General de Cyberzaintza. Este comité cuenta con representación permanente de las Direcciones de Estrategia e Innovación, Operaciones y Equipo de Respuesta, Comunicación y Relaciones Institucionales, y Cumplimiento Normativo y Gobierno del Riesgo, así como de las Jefaturas de División de Administración y Servicios y Asesoría Jurídica. Además, la Jefatura de División de Seguridad e Infraestructuras tiene representación invitada.

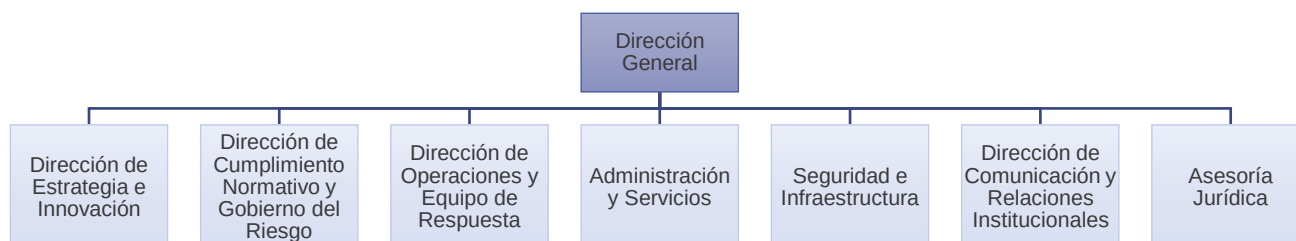
Entre sus funciones se encuentran la elaboración del Plan Estratégico y la documentación táctica necesaria para asegurar el cumplimiento anual de los objetivos, incluyendo el Plan de Gestión, el Plan de Actuación y el Presupuesto, entre otros. Asimismo, el Comité de Dirección supervisa y guía todas

las actividades relacionadas con el desarrollo y la ejecución de las líneas de acción definidas en el Plan Estratégico.

El Comité de Dirección reporta al Consejo de Administración a través de la Dirección General.

4.3 Áreas

En el siguiente gráfico se detalla la estructura de áreas de Cyberzaintza:



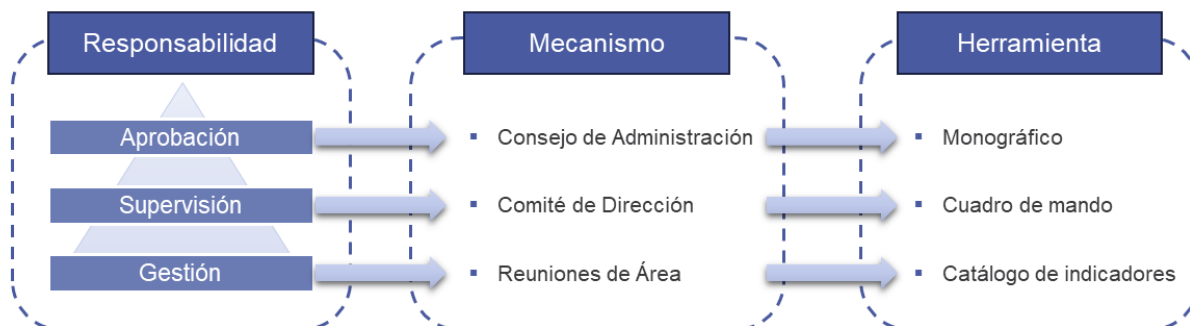
Cada área es responsable de ejecutar las actividades necesarias para implementar las líneas de acción definidas en el Plan Estratégico que correspondan a su ámbito. Además, deben asegurar que todas las acciones se gestionen de manera eficiente y estén alineadas con los principios establecidos.

Las áreas reportan al Comité de Dirección a través de sus respectivos responsables.

5 Seguimiento y evaluación

5.1 Sistema de seguimiento

Se define la siguiente sistemática para el seguimiento y revisión del Plan Estratégico de Cyberzaintza 2025-2028:



5.2 Mecanismos de seguimiento

5.2.1 Reuniones de Área

- **Frecuencia:** Semanal.
- **Responsable:** Persona responsable del área.
- **Objetivo:** Gestionar el avance de las actividades del área, revisar el estado de los KPIs, identificar desviaciones y proponer acciones correctivas, asegurando el cumplimiento de los objetivos operativos.

5.2.2 Reuniones del Comité de Dirección

- **Frecuencia:** Mensual.
- **Responsable:** Dirección de Estrategia de Cyberzaintza.
- **Objetivo:** Supervisar de forma integral el avance del Plan Estratégico, evaluar las acciones correctivas propuestas, y asegurar que las líneas de acción se implementen de manera efectiva y alineada con los principios estratégicos.

5.2.3 Reuniones del Consejo de Administración

- **Frecuencia:** Anual, durante el último trimestre del año.
- **Responsable:** Dirección General de Cyberzaintza.
- **Objetivo:** Recibir información sobre el progreso anual del Plan Estratégico, analizar su rendimiento y resultados, y aprobar los planes y la asignación de recursos necesarios para asegurar la continuidad de las líneas de acción en el próximo periodo.

5.3 Herramientas de evaluación

La evaluación del Plan Estratégico se basará en siguientes herramientas principales, detalladas a continuación:

5.3.1 Monográfico

El monográfico es un informe de balance anual elaborado por el Comité de Dirección de Cyberzaintza. Este informe tiene como objetivo realizar una evaluación exhaustiva del progreso de las acciones del Plan Estratégico a lo largo del año. Se analizan los logros alcanzados, las desviaciones respecto a los objetivos planteados y se proponen medidas correctivas para asegurar el cumplimiento de las metas establecidas.

5.3.2 Cuadro de mando

El cuadro de mando es una herramienta que agrupa un conjunto de indicadores diseñados para evaluar tanto las líneas de acción como los principios estratégicos del Plan. Estos indicadores permiten una visualización clara y concisa del estado de avance de las diferentes iniciativas, facilitando la toma de decisiones informadas por parte del Comité de Dirección. El cuadro de mando se actualiza periódicamente para reflejar los cambios y avances en tiempo real.

5.3.3 Catálogo de indicadores

El catálogo de indicadores incluye los indicadores clave de rendimiento (KPIs), que son fundamentales para el seguimiento continuo del Plan Estratégico. En todo caso los indicadores del Plan Estratégico están alineados con el sistema de indicadores de gestión del Gobierno.

El catálogo proporciona una descripción detallada de cada indicador, incluyendo la siguiente información:

Campo	Descripción
Id.	Identificador único del indicador.
Línea de acción	Línea de acción a la que pertenece el indicador.
Fuente del indicador	Origen de los datos (servicio, iniciativa complementaria, etc.).
Servicio/Iniciativa asociada	Nombre del servicio, iniciativa, etc. de la que se obtiene el indicador.
Responsable del indicador	Persona o departamento responsable de la medición y reporte del indicador.
Memoria presupuestaria	Indicador incluido en la memoria de presupuestos (sí/no).
Descripción del indicador	Descripción del indicador.
Valor objetivo	Valor objetivo que se espera alcanzar con el indicador.
Valor actual	Valor actual del indicador, obtenido en la última medición.
Fecha de medición	Fecha de la última medición del indicador.
Fórmula cálculo cumplimiento	Fórmula utilizada para calcular el grado de cumplimiento del indicador.
% Cumplimiento	Grado de cumplimiento del indicador expresado en %.

En el Anexo I se incluye los indicadores incluidos en el Catálogo de Indicadores.

En el Anexo II se incluyen los indicadores de gestión de Gobierno para el ejercicio 2025.

Anexo I - Catálogo de indicadores del Plan Estratégico de Cyberzaintza 2025-2028

Línea de acción	Fuente del indicador	Servicio/Iniciativa asociada	Responsable del indicador	Memoria presupuestaria	Descripción del indicador	Valor objetivo	Frecuencia	Fórmula cálculo cumplimiento	% Cumplimiento
Auditoría	Servicio	Auditoría al cumplimiento normativo	Cumplimiento Normativo y Gobierno del Riesgo	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/10/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Auditoría	Iniciativa complementaria	Acreditación como Órgano de Auditoría Técnica	Cumplimiento Normativo y Gobierno del Riesgo	No	Obtención del reconocimiento como OAT del Sector Público para la realización de Auditorías de Certificación de la Conformidad con el ENS	4	Trimestral	1=En estudio; 2=Cumplimiento requisitos previos; 3=Cumplimiento requisitos internos; 4=Acreditación OAT.	25%
Concienciación	Servicio	Campañas de phishing	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/01/2026	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Concienciación	Servicio	Concienciación	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para la renovación del servicio inferior a 90 días.	01/01/2026	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Consultoría	Servicio	Consultoría	Cumplimiento Normativo y Gobierno del Riesgo	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/06/2027	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Consultoría	Servicio	Gestión de proyectos especiales	Cumplimiento Normativo y Gobierno del Riesgo	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/06/2027	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Coordinación estratégica	Servicio	Despliegue de la Estrategia de Ciberseguridad de Euskadi	Estrategia e Innovación	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/03/2026	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	

Línea de acción	Fuente del indicador	Servicio/Iniciativa asociada	Responsable del indicador	Memoria presupuestaria	Descripción del indicador	Valor objetivo	Frecuencia	Fórmula cálculo cumplimiento	% Cumplimiento
Coordinación estratégica	Servicio	Oficina de gestión de servicios	Estrategia e Innovación	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/10/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Gestión del riesgo	Servicio	Analítica y priorización del riesgo	Cumplimiento Normativo y Gobierno del Riesgo	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/10/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Gestión del riesgo	Servicio	Tratamiento del riesgo	Cumplimiento Normativo y Gobierno del Riesgo	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/10/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Inteligencia de amenazas	Servicio	Alerta temprana	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para la renovación del servicio inferior a 90 días.	01/04/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Inteligencia de amenazas	Servicio	Intercambio de información sobre ciberamenazas	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para la renovación del servicio inferior a 90 días.	01/04/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Interno	Servicio	Administración y servicios	Administración y Servicios	No	Porcentaje de ejecución presupuestaria realizada por Cyberzaintza.	100%	Trimestral	$(\text{Valor medido} / \text{Objetivo}) \times 100$	0%
Interno	Servicio	Apoyo al desarrollo de proyectos de innovación en I+D+i en ciberseguridad	Estrategia e Innovación	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/06/2027	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Interno	Servicio	Cumplimiento normativo Cyberzaintza	Administración y Servicios	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/10/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Interno	Servicio	Cumplimiento normativo Cyberzaintza	Seguridad e Infraestructura	No	Obtención del certificado de cumplimiento del ENS con nivel medio	4	Trimestral	1=GAP; 2=Plan de adecuación; 3=Implantación del plan; 4=Obtención certificado.	25%

Línea de acción	Fuente del indicador	Servicio/Iniciativa asociada	Responsable del indicador	Memoria presupuestaria	Descripción del indicador	Valor objetivo	Frecuencia	Fórmula cálculo cumplimiento	% Cumplimiento
Interno	Servicio	Desarrollo y despliegue del Plan Estratégico de Cyberzaintza	Estrategia e Innovación	No	Aprobación del Plan Estratégico de Cyberzaintza 2025-2028.	4	Trimestral	1=Elaborado; 2=Validado direcciones; 3=Aprobado Comité de Dirección; 4=Aprobado Consejo de Administración.	50%
Interno	Servicio	Desarrollo y despliegue del Plan Estratégico de Cyberzaintza	Estrategia e Innovación	No	Entrega de servicios garantizando el desarrollo de todos los ámbitos de actuación (gobernanza, detección, prevención y respuesta), asegurando que al menos el 10% del coste total se distribuya en cada uno de ellos.	4	Trimestral	1=1 ámbito; 2=2 ámbitos; 3=3 ámbitos; 4=4 ámbitos.	50%
Interno	Servicio	Desarrollo y despliegue del Plan Estratégico de Cyberzaintza	Estrategia e Innovación	No	Entrega de servicios garantizando la llegada a todos los públicos objetivo (sector público, empresas y ciudadanía), asegurando que al menos un 50% de servicios se ofrecen al sector público, 30% a las empresas y 10% a la ciudadanía.	3	Trimestral	1=1 público objetivo; 2=2 públicos objetivos; 3=3 públicos objetivos.	66%
Interno	Servicio	Desarrollo y despliegue del Plan Estratégico de Cyberzaintza	Estrategia e Innovación	No	Entrega de servicios implementando el modelo de entrega de servicios definido por Cyberzaintza.	4	Trimestral	1=Elaborado; 2=Validado direcciones; 3=Aprobado Comité de Dirección; 4=Implantado.	0%
Interno	Servicio	Desarrollo y despliegue del Plan Estratégico de Cyberzaintza	Estrategia e Innovación	No	Número de reuniones del Comité de Dirección para supervisar el avance del Plan Estratégico.	4	Trimestral	(Valor medido / Objetivo) x 100	25%
Interno	Servicio	Desarrollo y despliegue del Plan Estratégico de Cyberzaintza	Estrategia e Innovación	No	Número de reuniones del Consejo de Administración para recibir información del progreso anual del Plan Estratégico.	1	Trimestral	(Valor medido / Objetivo) x 100	0%

Línea de acción	Fuente del indicador	Servicio/Iniciativa asociada	Responsable del indicador	Memoria presupuestaria	Descripción del indicador	Valor objetivo	Frecuencia	Fórmula cálculo cumplimiento	% Cumplimiento
Interno	Servicio	Desarrollo y despliegue del Plan Estratégico de Cyberzaintza	Estrategia e Innovación	No	Porcentaje de servicios iniciados en comparación con los identificados en el Plan Estratégico para su implementación en 2025.	63%	Trimestral	$(\text{Valor medido} / \text{Objetivo}) \times 100$	33%
Interno	Servicio	Desarrollo y despliegue del Plan Estratégico de Cyberzaintza	Estrategia e Innovación	No	Porcentaje de servicios iniciados en comparación con los identificados en el Plan Estratégico para su implementación en 2026.	79%	Trimestral	$(\text{Valor medido} / \text{Objetivo}) \times 100$	26%
Interno	Servicio	Desarrollo y despliegue del Plan Estratégico de Cyberzaintza	Estrategia e Innovación	No	Porcentaje de servicios iniciados en comparación con los identificados en el Plan Estratégico para su implementación en 2027.	100%	Trimestral	$(\text{Valor medido} / \text{Objetivo}) \times 100$	21%
Interno	Servicio	Desarrollo y despliegue del Plan Estratégico de Cyberzaintza	Estrategia e Innovación	No	Porcentaje de servicios que pueden entregarse a través de un canal que son efectivamente prestados mediante dicho canal.	75%	Trimestral	$(\text{Valor medido} / \text{Objetivo}) \times 100$	67%
Interno	Servicio	Desarrollo y despliegue del Plan Estratégico de Cyberzaintza	Estrategia e Innovación	No	Porcentaje de las líneas de actuación identificadas en el Plan Estratégico iniciadas.	100%	Trimestral	$(\text{Valor medido} / \text{Objetivo}) \times 100$	25%
Interno	Servicio	Seguridad corporativa	Seguridad e Infraestructura	No	Desvío en la fecha prevista para la renovación del servicio inferior a 90 días.	01/07/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Interno	Servicio	Servicio de comunicación	Comunicación y Relaciones Institucionales	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/07/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Modelo de Seguridad de Euskadi	Servicio	Acompañamiento y seguimiento en el despliegue del Modelo de Seguridad de Euskadi	Estrategia e Innovación	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/10/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Operaciones de seguridad (SOC)	Servicio	SOC	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/01/2027	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Operaciones de seguridad (SOC)	Iniciativa complementaria	SOC	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para formar parte de la Red Nacional de SOC inferior a 90 días.	01/06/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 101$	

Línea de acción	Fuente del indicador	Servicio/Iniciativa asociada	Responsable del indicador	Memoria presupuestaria	Descripción del indicador	Valor objetivo	Frecuencia	Fórmula cálculo cumplimiento	% Cumplimiento
Operaciones de seguridad (SOC)	Servicio	Threat hunting	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/01/2027	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Respuesta a incidentes (CSIRT)	Servicio	Asesoramiento	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para la renovación del servicio inferior a 90 días.	01/09/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Respuesta a incidentes (CSIRT)	Servicio	Coordinación	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/10/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Respuesta a incidentes (CSIRT)	Servicio	DFIR	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/10/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Respuesta a incidentes (CSIRT)	Servicio	Gestión de crisis	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/10/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Respuesta a incidentes (CSIRT)	Servicio	Takedown	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/11/2023	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Respuesta a incidentes (CSIRT)	Iniciativa complementaria	Planificar la protección de Euskadi frente a emergencias de ciberseguridad y conectarlo con el LABI	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para incluir las crisis ciber como uno de los eventos que podrían activar el LABI inferior a 90 días.	01/06/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Seguridad ofensiva	Servicio	Auditoría técnica	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/05/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Seguridad ofensiva	Servicio	EASM	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/10/2025	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Seguridad ofensiva	Servicio	Red team	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/06/2027	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	
Transferencia del conocimiento	Servicio	Entrenamiento	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/09/2026	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	

Línea de acción	Fuente del indicador	Servicio/Iniciativa asociada	Responsable del indicador	Memoria presupuestaria	Descripción del indicador	Valor objetivo	Frecuencia	Fórmula cálculo cumplimiento	% Cumplimiento
Transferencia del conocimiento	Servicio	Formación	Operaciones y Equipo de Respuesta	No	Desvío en la fecha prevista para la puesta en marcha del servicio inferior a 90 días.	01/09/2026	Trimestral	$(1 - \text{Días de desvío} / 90) \times 100$	

Anexo II - Indicadores de gestión de Gobierno (2025)

HELBURUA EKINTZA ADIERAZLEA	MAGNITUDEA MAGNITUD	OBJETIVO ACCION INDICADOR
1. ARLOAN ESKUMENAK DITUZTEN HAINBAT ORGANISMOREN BITARTEZ HEDATUTAKO ZIBERSEGURTASUNeko 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 PRINTZIOIOAK 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 ebaluatzeraz 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. Lankidetzak 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 ziberintzidentek 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).



www.ciberseguridad.eus

