Estrategia Vasca de Ciberseguridad

Marzo 2024

Índice

1

Análisis de situación

Iturria: Irekia/Eusko Jaurlaritza
Egilea: Mikel Arrazola

1. Análisis de situación

El mundo está viviendo una **transformación global** sin precedentes, donde la rápida evolución de la tecnología ha cambiado la forma de interactuar y compartir información entre las personas, dando lugar a **nuevos riesgos y desafíos**. Para hacer frente a este nuevo escenario, **gobiernos y organismos**, tanto a nivel nacional como europeo, han definido **estrategias, políticas y regulaciones en el ámbito de la ciberseguridad**, de cara a proteger a la sociedad en su conjunto y combatir el cibercrimen.

Las administraciones públicas vascas son conscientes de que este escenario requiere de una visión integrada y de país en materia de ciberseguridad, que permita elevar el nivel de concienciación de la sociedad y proteger la administración y el tejido empresarial para facilitar su óptimo desarrollo. En este contexto, lideradas por Cyberzaintza, han participado en un ejercicio de análisis conjunto, en el que se han identificado las principales fortalezas y debilidades del país y las principales oportunidades y amenazas existentes a la hora de abordar el reto que la trasformación digital conlleva en términos de ciberseguridad. El resultado de este análisis es el punto de partida de la estrategia de ciberseguridad.

Gobierno Vasco y organismos dependientes

Lehendakaritza · Departamento de Seguridad · Departamento de Educación · Departamento de Salud · Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente · Departamento de Gobernanza Pública y Autogobierno · Departamento de Economía y Hacienda

cyberzaintza · Ertzaintza · GRUPO spri · Osakidetza · Datuak Babesteko Euskal Agintaritza Autoridad Vasca de Protección de Datos · EJIE · IVAP

Diputaciones forales y organismos dependientes

Bizkaia foru aldundia diputación foral · araba álava foru aldundia diputación foral · Gipuzkoako Foru Aldundia Diputación Foral de Gipuzkoa · Bizkaia lantik · ZIUR · izfe GipuzkoaTIK

Ayuntamientos y organismos dependientes

Bilbao UDALA AYUNTAMIENTO · DONOSTIA SAN SEBASTIÁN · Ayuntamiento de Vitoria-Gasteiz · EUDEL EUSKADIKO UDALEN ELKARTEA ASOCIACIÓN DE MUNICIPIOS VASCOS · BilbaoTIK · DONOSTIA SAN SEBASTIÁN DonostiaTIK

Otras entidades

CYBASQUE · BRTA BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Representantes independientes del Comité Consultivo

1. Análisis de situación

El ejercicio DAFO-CAME realizado dentro del análisis de resultados ha mostrado que Euskadi cuenta con un conjunto de fortalezas relevante que permitirían al país aprovechar las oportunidades del entorno y afrontar gran parte de las amenazas del contexto. No obstante, se han identificado debilidades que podrían dificultar el abordaje de las principales amenazas del contexto actual y futuro, siendo esta la primera actuación que debe afrontarse.

Fortalezas

- Cyberzaintza
- Apoyo institucional
- Tejido industrial
- Capacidad para llegar a la ciudadanía
- Capacidades tecnológicas

Debilidades

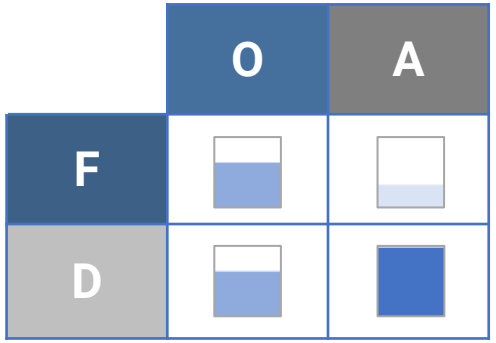
- Falta de concienciación y sensibilización en materia de ciberseguridad
- Falta de flexibilidad
- Falta de estrategia y trabajo común
- Falta de recursos, talento y capacidades en ciberseguridad
- Obsolescencia tecnológica

Oportunidades

- Entorno regulado
- Digitalización
- Tejido empresarial de ciberseguridad fuerte
- Aprendizaje en base a lecciones aprendidas
- Aprovechamiento de fondos

Amenazas

- Entorno cambiante con riesgo al alza
- Ciberdelincuencia
- Brecha Digital
- Aumento de superficie de exposición
- Falta de soberanía tecnológica



2

Propósito y principios estratégicos

Iturria: Irekia/Eusko Jaurlaritza
Egilea: Mikel Arrazola

2. Propósito y principios estratégicos

1. **Resiliencia**
2. **Colaboración**
3. **Eficiencia**
4. **Cercanía**
5. **Liderazgo**
6. **Innovación y mejora continua**

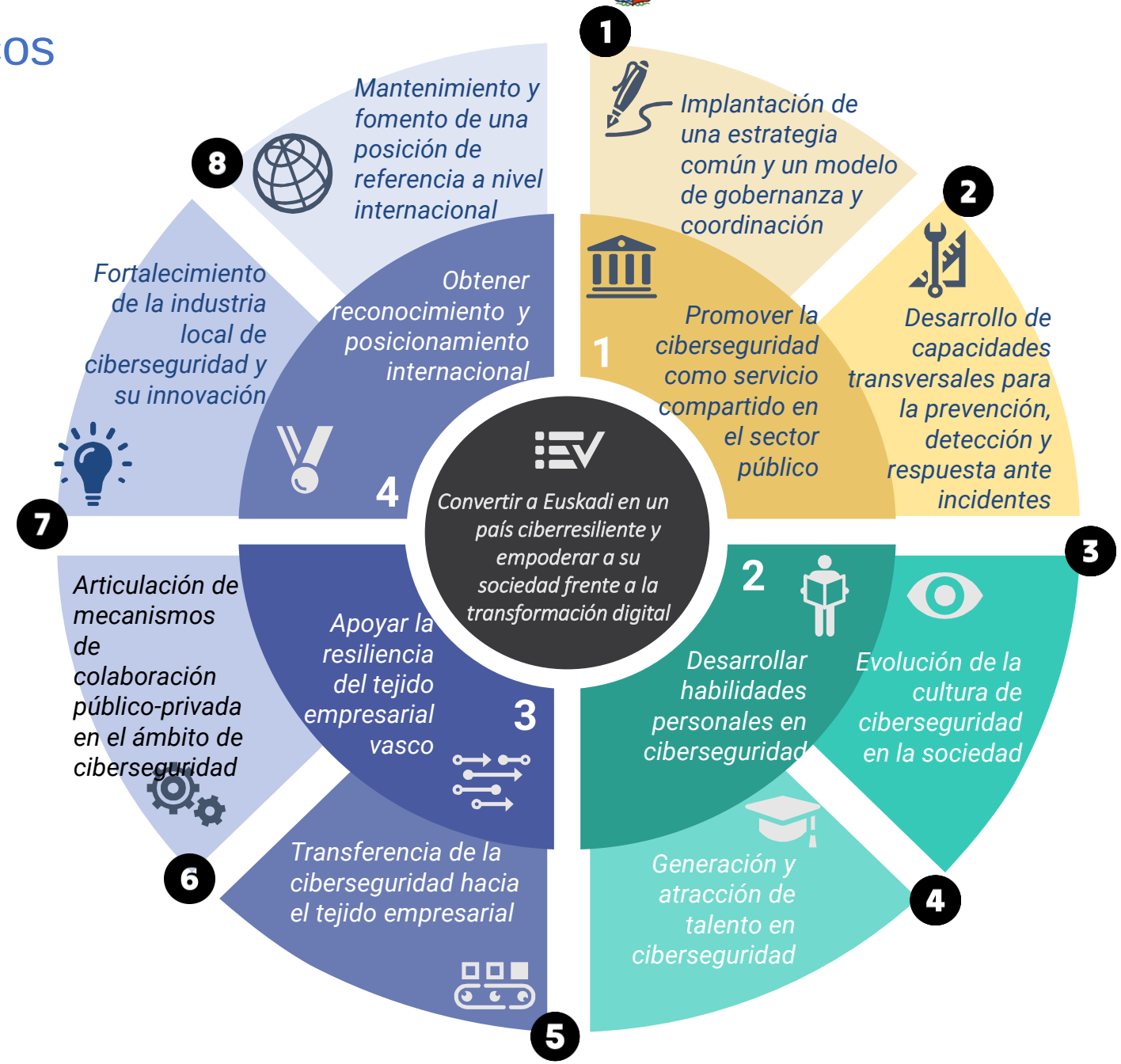
Convertir a Euskadi en un país ciberresiliente, con capacidades para proteger su administración pública y su tejido empresarial frente a los riesgos cibernéticos, promoviendo el empoderamiento de la sociedad en el proceso de transformación digital y aportando dichas capacidades para desarrollar la ciberseguridad global ocupando un lugar de referencia en el ámbito internacional.

Hemendik + ***Gure gizartearentzat*** + ***Elkarlanean*** = ***Sarean ere, auzolana***

2. Propósito y principios estratégicos

La estrategia definida contiene los **objetivos estratégicos y las líneas de actuación** que permitirán resolver las principales debilidades y amenazas existentes, así como aprovechar las oportunidades y fortalezas en el periodo **2024-2029**, para **dotar al país de capacidades y recursos que permitan ofrecer al conjunto de la sociedad una correcta protección contra los riesgos de ciberseguridad y empoderamiento frente a la transformación digital**. La estrategia involucra tanto al conjunto de administraciones públicas de Euskadi, como la ciudadanía, el tejido empresarial y el sector de la ciberseguridad existente.

Para ello, Euskadi debe conseguir alcanzar cuatro **objetivos estratégicos principales**, centrados en la propia **administración** y su relación digital con la sociedad; la generación de **talento** y las capacidades que permitan al país ser soberano y resiliente frente a los riesgos existentes; aportar valor al conjunto del sector de la **ciberseguridad**, convirtiéndose en un **agente relevante** para el mismo; y ser capaz de transferir los logros al conjunto de la sociedad vasca y, especialmente, a su **tejido empresarial e industrial**, como valor diferencial y fuente de riqueza.



3

Objetivos estratégicos

Iturria: Irekia/Eusko Jaurlaritza
Egilea: Mikel Arrazola

3. Objetivos estratégicos

Convertir a Euskadi en un país ciberresiliente y empoderar a su sociedad frente a la transformación digital

Una de las claves del desarrollo de las sociedades y su tejido económico es el nivel de seguridad que adquieren. Con unos niveles de seguridad ciudadana extraordinarios, Euskadi debe protegerse de los riesgos de ciberseguridad y empoderar su sociedad para una transformación digital segura, que permita su desarrollo futuro de manera óptima. En este contexto, se deben alinear todos los factores, incluyendo las personas y las capacidades soberanas, en la estrategia, para impulsar la obtención de un reconocimiento internacional que redundará en el beneficio de la protección del país y de su economía.

Promover la ciberseguridad como servicio compartido en el sector público

Las Administraciones Públicas de Euskadi, lideradas por el Gobierno Vasco, deben desplegar las capacidades y mecanismos de colaboración necesarios, tanto internos como con otros agentes, para garantizar a la ciudadanía, el tejido empresarial y el conjunto de la sociedad vasca un nivel de ciberseguridad adecuados para su correcto desarrollo y protección de sus derechos.

Desarrollar habilidades personales en ciberseguridad

Las personas son un aspecto central para conseguir empoderar a la sociedad en la transformación digital. En este contexto, la estrategia debe permitir dotar a las personas de las habilidades y cultura suficientes para desenvolverse libremente en un entorno de riesgo creciente, y generar el conocimiento necesario dentro de nuestro país.

Apoyar la resiliencia del tejido empresarial vasco

A través de la estrategia de ciberseguridad se debe impulsar que el tejido empresarial del país encuentre el mayor nivel de protección, que le permita ser resiliente ante escenarios de riesgos complejos. La colaboración público-privada y la puesta a disposición de las capacidades existentes para el conjunto del tejido empresarial, partiendo de las empresas tractoras, deben marcar la actuación en este ámbito.

Obtener reconocimiento y posicionamiento internacional

Ser un agente relevante y confiable dentro del ecosistema de ciberseguridad internacional permite articular mejores mecanismos de colaboración en un entorno complejo y asimétrico. Dotar al país de capacidades de ciberserguidad soberanas, a través de una industria de seguridad puntera, y formar parte de los organismos clave a nivel internacional permitirá desplegar una protección más completa.

4

Líneas estratégicas

Iturria: Irekia/Eusko Jaurlaritza
Egilea: Mikel Arrazola

4. Líneas estratégicas

1. Implantación de una estrategia común y un modelo de gobernanza y coordinación

Propósito:

Unificar la actuación del sector público en materia de ciberseguridad con una perspectiva de país, en el que toda la sociedad reciba los servicios públicos con el mismo nivel de seguridad independientemente de la administración pública con la que interactúe.

Descripción:

En la actualidad se utilizan distintas aproximaciones para abordar los retos de la ciberseguridad en el sector público de Euskadi, existiendo múltiples modelos con distintos niveles de desarrollo y madurez.

En este contexto, se considera clave definir una estrategia común, que permita implantar un modelo de gobernanza adecuado para responder a estos retos de forma coordinada, logrando así optimizar y mejorar la eficiencia de los recursos existentes.

Así mismo, es necesario establecer mecanismos que permitan gestionar los riesgos y verificar el nivel de cumplimiento en materia de ciberseguridad, facilitando así la prestación de unos servicios públicos de calidad y seguros, y velando por la privacidad y confidencialidad de la información de ciudadanos y empresas.

Actuaciones principales:

- *Despliegue de una **estrategia común** para potenciar y coordinar el alineamiento del sector público de Euskadi en materia de ciberseguridad.*
- *Despliegue de un **modelo de gobernanza** que permita modelar los servicios necesarios, en el ámbito de la ciberseguridad, para el conjunto de las administraciones públicas de Euskadi.*
- *Desarrollo de los **roles y responsabilidades** en el ámbito de la ciberseguridad dentro del sector público de Euskadi que permita implementar un modelo de actuación conjunta.*
- *Desarrollo de un **modelo de referencia** de políticas de seguridad, normas técnicas y medidas de protección, que complemente las normativas de ciberseguridad existentes, y se alinee con las necesidades particulares del conjunto de administraciones públicas de Euskadi para facilitar su despliegue.*
- *Creación de un modelo de revisión que permita identificar, evaluar y gestionar los **riesgos cibernéticos** a los que están expuestos los servicios públicos.*
- *Establecimiento de un **marco para la adopción de tecnologías** apoyado en las capacidades transversales y herramientas comunes, y aportando criterios unificados para las nuevas adopciones teniendo en consideración diferentes aspectos, como los lingüísticos.*
- *Evaluación periódica del **cumplimiento y estado de la ciberseguridad** en el conjunto de las administraciones públicas de Euskadi.*
- *Creación de **mecanismos de cooperación** activa, en el ámbito de la seguridad integral, y de procesos unificados y homogéneos para las actuaciones que así lo requieran.*
- *Fomento de un plan de alineamiento con el **plan de seguridad pública de Euskadi**.*

4. Líneas estratégicas

2. Desarrollo de capacidades transversales para la prevención, detección y respuesta ante incidentes

Propósito:

Dotar el sector público de Euskadi con las capacidades necesarias para hacer frente a los riesgos y amenazas en materia de ciberseguridad desde un punto de vista holístico y eficiente.

Descripción:

Las capacidades para hacer frente a los diferentes riesgos y amenazas en materia de ciberseguridad abarcan un espectro muy amplio de necesidades, entre ellas: tecnología y herramientas especializadas, sistemas y modelos de seguimiento específicos, profesionales altamente cualificados, etc. Esta situación dificulta que cada organismo público pueda disponer de todas estas capacidades de manera individual y con un nivel de servicio óptimo.

En este contexto, se identifica la necesidad de disponer de ciertas capacidades de ciberseguridad desplegadas desde una perspectiva transversal, y que presten servicios de manera interinstitucional al conjunto del sector público, consiguiendo así aportar valor a toda la sociedad.

Actuaciones principales:

- ***Refuerzo de las capacidades de CERT de Cyberzaintza** ampliando sus servicios y enfocándose, tanto a la prevención y detección de ciberincidentes, como a la protección del sector público de Euskadi, y apoyando así la resiliencia del país.*
- *Desarrollo de las capacidades necesarias para la gestión y **respuesta coordinada ante ciberincidentes** ocurridos en el sector público de Euskadi.*
- *Establecimiento de un **procedimiento de Gestión de Crisis** a nivel de país que contemple todos los agentes de Euskadi.*
- *Desarrollo de un modelo de **vigilancia digital y alerta temprana**, para el conjunto de administraciones públicas, incluyendo el **desarrollo de un mapa de riesgo / país** adaptado a Euskadi.*
- *Implementación de medidas de soporte a iniciativas estratégicas orientadas a **colectivos sensibles,** de manera focalizada y en coordinación con los responsables de estos.*
- *Aumento de las **capacidades de investigación** de ciberincidentes, para la protección del conjunto de la sociedad y persecución de delitos cibernéticos de la policía integral de Euskadi.*
- *Desarrollo de un **modelo de compartición de información** sobre ciberincidentes y ciberamenazas.*
- *Despliegue y entrenamiento de un **modelo de gestión de crisis** de ciberseguridad, coordinado con el plan de emergencias de Euskadi.*
- *Definición de un **plan de resiliencia** de los servicios públicos y esenciales de Euskadi para priorizar y adecuar su protección.*
- *Puesta en marcha de un servicio de apoyo a las diferentes administraciones públicas de Euskadi para la **ejecución de proyectos especiales** de ciberseguridad y la gestión de terceros.*

4. Líneas estratégicas

3. Evolución de la cultura de ciberseguridad en la sociedad

Propósito:

Promover la sensibilización y concienciación en materia de ciberseguridad entre la ciudadanía para mejorar la cultura de ciberseguridad del país.

Descripción:

La ciberseguridad es un ámbito que alcanza y tiene impacto en todo el conjunto de la sociedad. En un entorno cada vez más complejo, interconectado y con mayores riesgos, impulsar una cultura de ciberseguridad en todos los niveles de la sociedad resulta clave para poder hacer frente a las amenazas existentes y futuras.

Esta cultura es imprescindible para poder llevar a cabo una transformación digital segura, en la que la sociedad se encuentre empoderada a todos los niveles en el uso de las tecnologías.

Esta línea busca, por tanto, fomentar una cultura de ciberseguridad en toda la ciudadanía que sea, además de una protección frente a los riesgos actuales, la base del talento futuro.

Actuaciones principales:

- *Fomento de **programas educativos** que aborden la ciberseguridad desde una **edad temprana**, que permitan desarrollar una cultura de ciberseguridad en Euskadi orientada al empoderamiento de la ciudadanía en la transformación digital.*
- *Desarrollo **campañas de concienciación** que aborden la ciberseguridad, destacando prácticas seguras y consecuencias de comportamientos de riesgo. Utilizar canales de comunicación accesibles para llegar a un público amplio.*
- *Creación de un programa de **concienciación** en ciberseguridad para los miembros de la Ertzaintza y los cuerpos de Policía de Euskadi que se incluya dentro de la formación en la **Academia Vasca de Policía y Emergencias**.*
- *Creación de un programa de **concienciación y sensibilización** en ciberseguridad para los **trabajadores públicos**, así como para el **cuerpo político**.*
- *Diseño de **programas de sensibilización** y concienciación adaptados los **diferentes perfiles de la ciudadanía** existentes en Euskadi.*
- *Fomento de la **participación activa de la sociedad** en la protección de la ciberseguridad, fomentando la denuncia de incidentes y promoviendo la ética digital. Crear una **cultura de responsabilidad compartida** refuerza la ciberseguridad en todos los niveles de la sociedad.*

4. Líneas estratégicas

4. Generación y atracción de talento en ciberseguridad

Propósito:

Potenciar el talento y las competencias de ciberseguridad entre los profesionales a través de la atracción de este, los planes de desarrollo y la reorientación de perfiles en el ámbito de la ciberseguridad.

Descripción:

El rápido crecimiento de la demanda y la amplitud del alcance de la ciberseguridad han supuesto que el número de profesionales disponibles sea inferior a la demanda existente. Dada la evolución prevista para el sector, si no se actúa adecuadamente, es posible que en un futuro el escenario empeore en este ámbito. Teniendo en cuenta la relevancia del talento para el desarrollo del sector y para la protección de la sociedad, promover la atracción y generación de talento es una de las claves que permitirá a Euskadi disponer de las capacidades necesarias para alcanzar el nivel de resiliencia esperado.

Para conseguir este talento, se han identificado varias oportunidades que conllevarán la integración de todos los mecanismos disponibles, desarrollando actuaciones en diferentes áreas.

Actuaciones principales:

- *Despliegue de **mecanismos que faciliten la atracción** de talento en ciberseguridad provenientes de otras regiones y culturas a través del refuerzo de la integración en nuestra sociedad.*
- *Lanzamiento de un modelo de **colaboración estrecha entre instituciones educativas y empresas**, facilitando programas de mentoría y proyectos conjuntos para que los estudiantes tengan la oportunidad de aplicar sus conocimientos en entornos empresariales reales.*
- *Establecimiento de un modelo **reorientación de perfiles** hacia ciberseguridad mediante capacitación técnica, certificaciones y experiencia práctica y formación no reglada. Facilitar programas de reentrenamiento para profesionales de TI o campos relacionados que deseen cambiar a la ciberseguridad*
- *Desarrollo de un **modelo de capacitación especializada** en el conjunto de **campos de ciberseguridad** en conjunto con las universidades y centros de formación profesional.*
- ***Impulso a la vocación** en el ámbito de la ciberseguridad, tanto a los perfiles que muestren interés en la temática como a los colectivos con una menor representación, a través de iniciativas específicas.*

4. Líneas estratégicas

5. Transferencia de la ciberseguridad hacia el tejido empresarial

Propósito:

Establecer mecanismos que permitan al tejido empresarial del país dotarse de capacidades de ciberseguridad para afrontar los riesgos y amenazas a los que se enfrentan.

Descripción:

La ciberseguridad afecta a todos los sectores de actividad económica y a todos los elementos de la cadena de valor de los productos y servicios. En un entorno tan amplio, los eslabones más débiles pueden afectar en cadena al conjunto del tejido empresarial de Euskadi. En este contexto, se hace necesario articular mecanismos que permitan garantizar que las capacidades de seguridad llegan a todo el tejido empresarial, de modo que se proteja no solo la ciudadanía en el uso de los productos y servicios, sino también la economía del país.

Realizar esta transferencia apostando por capacidades locales se convertirá, además, en un mecanismo de impulso del sector de la ciberseguridad y a su vez, el éxito del tejido empresarial local será un factor clave de éxito para el posicionamiento estatal e internacional del mismo.

Actuaciones principales:

- *Despliegue de un programa que permita a las organizaciones **incorporar capacidades locales de ciberseguridad** dentro de su actividad, y apostar por una internacionalización de las tecnologías y productos locales a través de las propias empresas.*
- *Puesta en marcha de **observatorios sectoriales** que permitan identificar la madurez y la posición competitiva del tejido empresarial, desde una perspectiva del valor de la ciberseguridad para sus clientes.*
- *Establecimiento de una **línea de apoyo y asesoramiento** para la incorporación de capacidades de ciberseguridad para el tejido empresarial vasco, sin entrar en competencia con el propio sector de ciberseguridad de Euskadi.*
- *Creación de grupos de trabajo que fomenten la **colaboración entre los agentes relevantes** del sector.*
- *Despliegue de una **red de contactos apoyada en los ayuntamientos**, para la llegada de la ciberseguridad a todo el tejido empresarial de Euskadi.*

4. Líneas estratégicas

6. Articulación de mecanismos de colaboración público-privada en el ámbito de ciberseguridad

Propósito:

Promover mecanismos de colaboración entre las entidades públicas y el ecosistema privado para fortalecer la resiliencia y reducir el impacto de los incidentes en la sociedad y el tejido económico del país.

Descripción:

La colaboración es un factor clave de éxito a la hora de hacer frente a las ciberamenazas. Siendo la colaboración público-privada una seña de identidad de Euskadi, la articulación de este tipo de mecanismos de colaboración también en el ámbito de la protección es un aspecto clave y un valor diferencial.

Los modelos de colaboración público-privada pueden ser una herramienta valiosa para facilitar la mejora del nivel de seguridad del sector público, posibilitando que la administración pueda aprovechar todo el potencial y las capacidades desarrolladas por el ámbito privado y, a su vez, este pueda realimentarse y seguir evolucionando sus servicios a través de la experiencia adquirida. La compartición de información y el apoyo en la lucha frente a los incidentes estarán en el eje de dichos mecanismos.

Actuaciones principales:

- *Apuesta por los mecanismos de la colaboración público-privada para garantizar la **resiliencia del tejido empresarial y los servicios esenciales** de Euskadi a través de **programas específicos** y del apoyo y complemento de programas existentes como PISE.*
- *Promoción de **iniciativas público-privadas** y órganos de consulta de ciberseguridad.*
- ***Fomento de la transparencia y la confianza** entre el sector público y privado al compartir información sobre el ecosistema de la ciberseguridad y trabajar conjuntamente para abordar los desafíos.*
- *Establecimiento de **canales de comunicación** para la compartición de información sobre ciberamenazas y vulnerabilidades.*
- *Definición de protocolos y **mecanismos de coordinación** para facilitar la colaboración entre las entidades públicas y las privadas.*

4. Líneas estratégicas

7. Fortalecimiento de la industria local de ciberseguridad y su innovación

Propósito:

Fortalecer el sector empresarial de la ciberseguridad, promover la soberanía de este y apoyar su internacionalización.

Descripción:

Contar con un sector de ciberseguridad con capacidades y reconocimiento en el ámbito estatal e internacional favorecerá el posicionamiento y la relevancia de Euskadi frente a terceros, a la vez que supondrá un impulso económico para el país gracias a un sector de actividad cada vez mayor.

Partiendo del elevado reconocimiento actual, poder dotar al sector de un mayor nivel de soberanía, en la que los principales agentes tecnológicos y de innovación mantengan sus centros de decisión en Euskadi, se convierte en un reto a afrontar.

Garantizar el apoyo al sector y promover instrumentos financieros y mecanismos de tracción que fomenten dicha soberanía permitirá al país afrontar los retos de ciberseguridad a partir de un nivel de soberanía tecnológica que puede ser clave a largo plazo.

Actuaciones principales:

- *Creación de **herramientas orientadas al crecimiento de las empresas** innovadoras que permitan la sostenibilidad de estas y su crecimiento consolidado como empresa vasca.*
- *Identificación y puesta en marcha de un **observatorio que permita identificar oportunidades de negocio**, desarrollar ideas innovadoras y la creación de nuevas empresas locales, proporcionando los recursos, la experiencia y los contactos necesarios.*
- *Desarrollo de un **catálogo de servicios y proveedores** locales homologados, que permita facilitar el proceso de identificación de potenciales organizaciones durante los procesos de contratación.*
- *Definición de **programas de colaboración con la industria,** que permitan la colaboración entre los diferentes agentes y las empresas locales, para promover la **investigación aplicada** y el desarrollo de nuevas soluciones en ciberseguridad, favoreciendo la **transferencia tecnológica** al mercado.*

4. Líneas estratégicas

8. Mantenimiento y fomento de una posición de referencia a nivel internacional

Propósito:

Consolidar y promocionar activamente la posición destacada de Euskadi en el ámbito de ciberseguridad a nivel estatal e internacional.

Descripción:

La colaboración internacional y de personal especializado resulta clave a la hora de hacer frente a las ciberamenazas globales. El reconocimiento por parte de otros agentes resulta un factor clave de éxito para poder formar parte de los círculos de actividad más relevantes en la protección frente a las ciberamenazas y en la resolución de ciberincidentes.

En este contexto, Euskadi debe esforzarse en pertenecer a los principales foros especializados nacionales e internacionales y en tomar parte en ellos de una manera activa y colaborativa, de manera que el reconocimiento obtenido sea sostenible en el tiempo y su posicionamiento se consolide.

Actuaciones principales:

- *Definición e implementación de los mecanismos necesarios que permitan la **participación de las organizaciones vascas en foros**, conferencias y eventos internacionales relevantes en el ámbito de la ciberseguridad que permitan divulgar las capacidades y los servicios locales en Euskadi.*
- *Incorporación de **Cyberzaintza en los principales foros** y asociaciones internacionales y estatales de ciberseguridad como agente de referencia para la colaboración y generación de valor.*
- *Identificación de organizaciones líderes para el establecimiento de **alianzas estratégicas** que faciliten el acceso a recursos, **nuevas fuentes de conocimiento y mercados** con mayor visibilidad.*
- *Apoyo al sector de ciberseguridad vasco en sus labores de **posicionamiento y crecimiento internacional**.*
- *Implantación de **mecanismos para visibilizar** y poner a disposición de la sociedad internacional los **avances y capacidades desarrolladas** en Euskadi.*
- *Creación de una **red de personas referentes** en el ámbito estatal, europeo e internacional relacionadas con Euskadi que **apoyen el reconocimiento y posicionamiento de Euskadi**.*

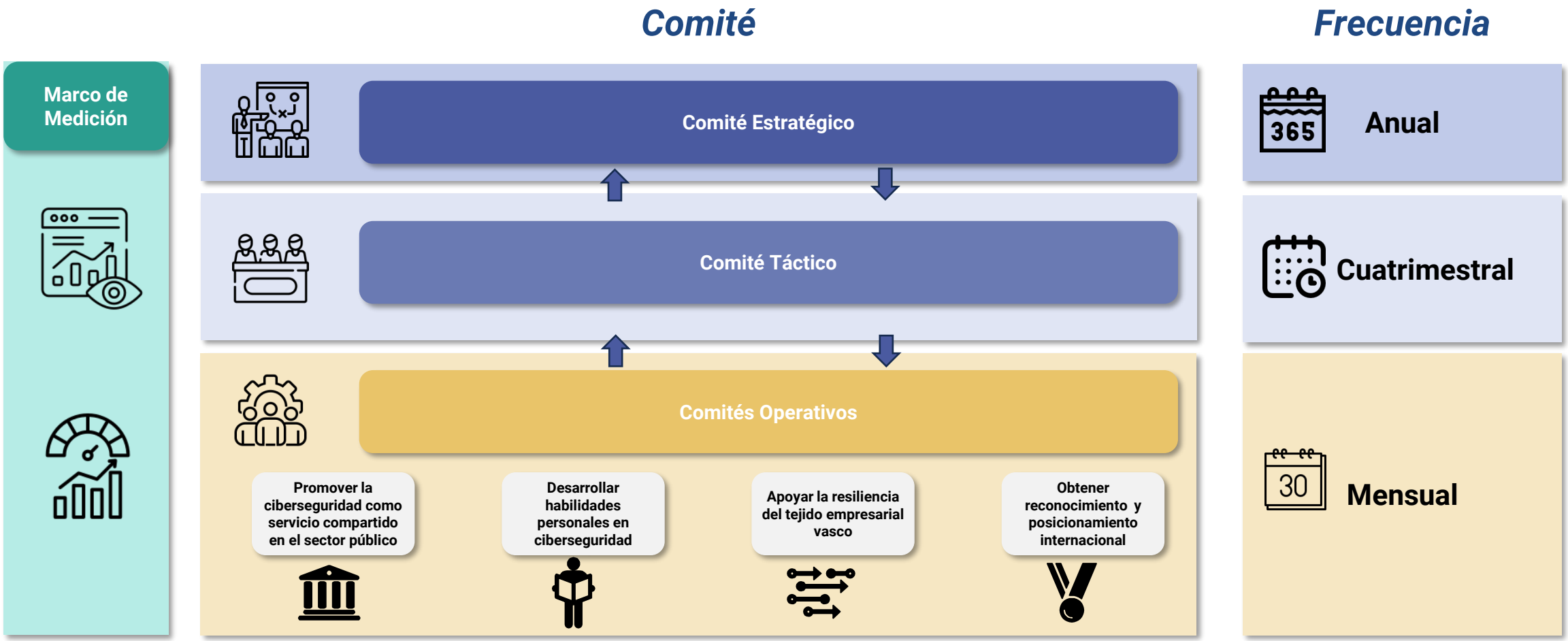
5

Modelo de gobernanza y seguimiento

Iturria: Irekia/Eusko Jaurlaritza
Egilea: Mikel Arrazola

4. Modelo de gobernanza y seguimiento

Para la implementación de la Estrategia Vasca de Ciberseguridad resulta imprescindible desplegar un modelo de gobernanza y seguimiento en el que estén involucrados los principales actores relevantes.



5. Modelo de gobernanza y seguimiento

Para la implementación de la Estrategia Vasca de Ciberseguridad resulta imprescindible desplegar un modelo de gobernanza y seguimiento en el que estén involucrados los principales actores relevantes.

Comité Estratégico: *estará presidido por la persona que lidere el Departamento de Seguridad en calidad de Consejero o Consejera quien determinará la composición del Comité y las normas de organización del mismo.*

Comité Táctico: *estará presidido por la persona que ostente la Dirección General de la Agencia Vasca de Ciberseguridad quien determinará la composición del Comité y las normas de funcionamiento.*

Comités Operativos: *estarán presididos por la persona que ostente la Dirección de Estrategia de la Agencia Vasca de Ciberseguridad o por la persona en la que elija delegar, pues podría haber varios Comités, teniendo para ello en cuenta el ámbito de actuación al que se dirija cada Comité individual.*

Marco de Medición:

- *Será responsabilidad del Comité Táctico proponer un marco que permita medir el avance en el despliegue de la Estrategia.*
- *Será función de la presidencia del Comité Estratégico la aprobación del Marco de Medición cuyo seguimiento presentará al Comité Estratégico cuando este se reúna.*


EUSKO JAURLARITZA
GOBIERNO VASCO


cyber
zaintza
BASQUE CYBERSECURITY AGENCY