cyber zaintza | BASQUE CYBERSECURITY AGENCY

Estrategia Vasca de Ciberseguridad

2024-2029

EUSKO JAURLARITZA
GOBIERNO VASCO

Índice

Resumen ejecutivo

Resumen ejecutivo

Euskadi es un país con una sociedad moderna y con servicios avanzados que reflejan su compromiso con el progreso y la sociedad. En este contexto, está apostando de manera decidida por la transformación digital, reconociendo que la innovación tecnológica es clave para mantenerse a la vanguardia en un entorno global cada vez más interconectado.

Las nuevas tecnologías, como la inteligencia artificial (IA), están transformando radicalmente la sociedad. Desde la automatización industrial hasta los asistentes virtuales y la toma de decisiones predictivas, la IA impulsa la eficiencia y la innovación.

Sin embargo, la rápida evolución de las tecnologías y herramientas disponibles genera nuevos casos de uso y, al mismo tiempo, incrementa la superficie de exposición de las organizaciones, que puede ser aprovechada por los ciberdelincuentes para realizar nuevos ataques.

Para hacer frente a este escenario, en el que la ciberseguridad es un reto que afecta a toda la sociedad, es necesario implementar una gestión global de la ciberseguridad, así como disponer de mecanismos de coordinación que permitan alinear las actuaciones realizadas por los diferentes agentes involucrados.

En este contexto se aprueba la Ley 7/2023, de 29 de junio, de creación de la **Agencia Vasca de Ciberseguridad**. La Agencia, también denominada Cyberzaintza, está adscrita al Departamento de Seguridad del Gobierno Vasco y su objeto 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. Tras su creación, la Agencia ha liderado el diseño de una estrategia de ciberseguridad para Euskadi, con el objetivo de potenciar el alineamiento de las actuaciones en dicha materia durante los próximos años. En el proceso han participado los principales interesados en los diferentes niveles de Administración Pública de la Comunidad Autónoma Vasca, así como agentes de la Red Vasca de Ciencia Tecnología e Innovación y representantes del sector privado de la ciberseguridad.

El presente documento desarrolla la **Estrategia Vasca de Ciberseguridad** para el periodo 2024-2029.

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.

La estrategia de ciberseguridad identifica los retos del país en este ámbito, y plantea un conjunto de objetivos estratégicos. Para lograr la consecución de dichos objetivos define ocho líneas de actuación. Y a su vez, para cada una de estas líneas, concreta un conjunto de actuaciones que deberá liderar el agente competente en cada caso, para lograr la consecución de los objetivos identificados. Estas actividades involucran al conjunto de las Administraciones Públicas de Euskadi, la ciudadanía, el tejido empresarial y el propio sector de la ciberseguridad.

En la siguiente imagen se muestran los **siete retos y los cuatro objetivos estratégicos** identificados para Euskadi en el ámbito de la ciberseguridad:

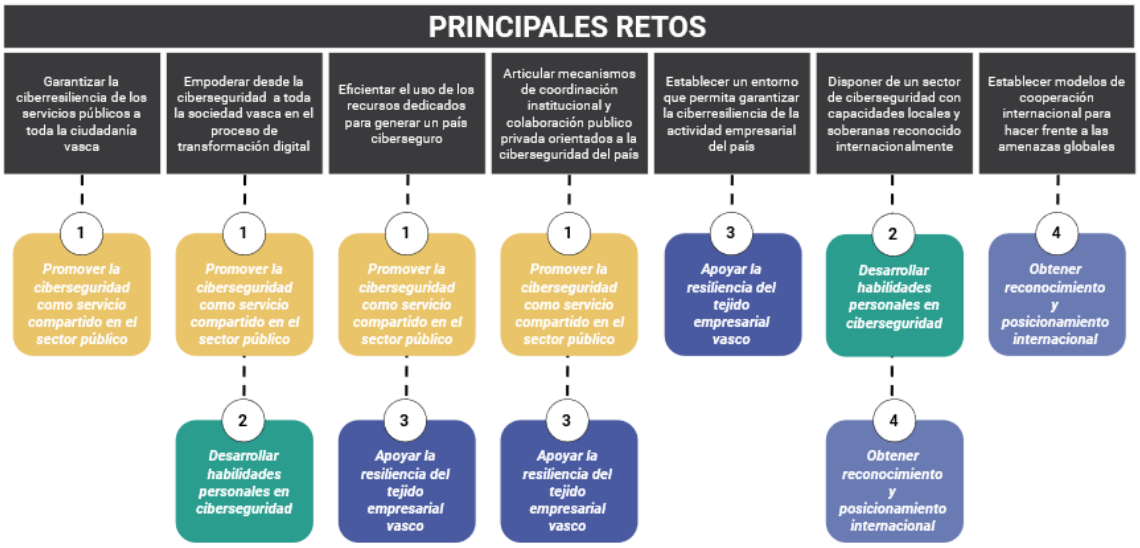

Ilustración 1:Retos y objetivos de la Estrategia Vasca de Ciberseguridad

Para alcanzar estos objetivos, se muestran a continuación las **ocho líneas de actuación** identificadas:

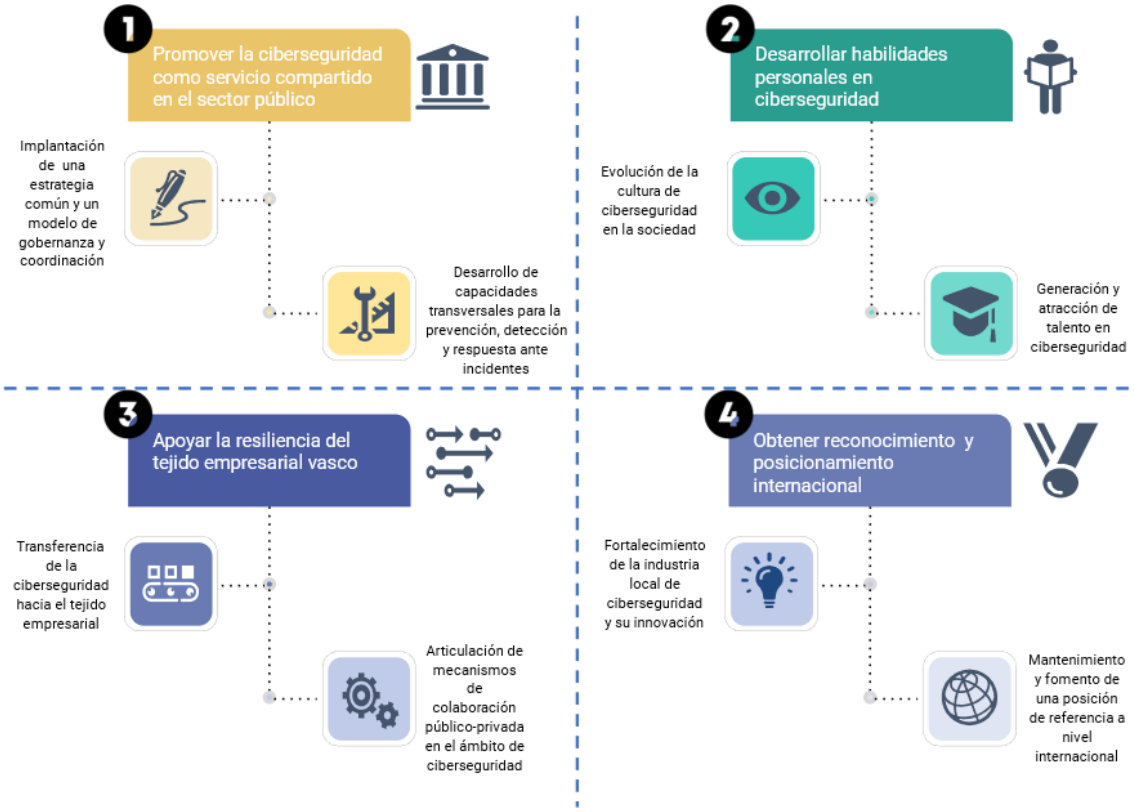

Ilustración 2: Objetivos y líneas de actuación de la Estrategia Vasca de Ciberseguridad

Para garantizar la implantación de la Estrategia de Ciberseguridad de Euskadi se ha definido un **Modelo de Gobernanza**. Este modelo permitirá integrar la actuación de los diferentes agentes intervinientes en el conjunto de acciones identificadas, así como garantizar el correcto despliegue, la eficiencia en la inversión de recursos y la coordinación interinstitucional y público-privada.

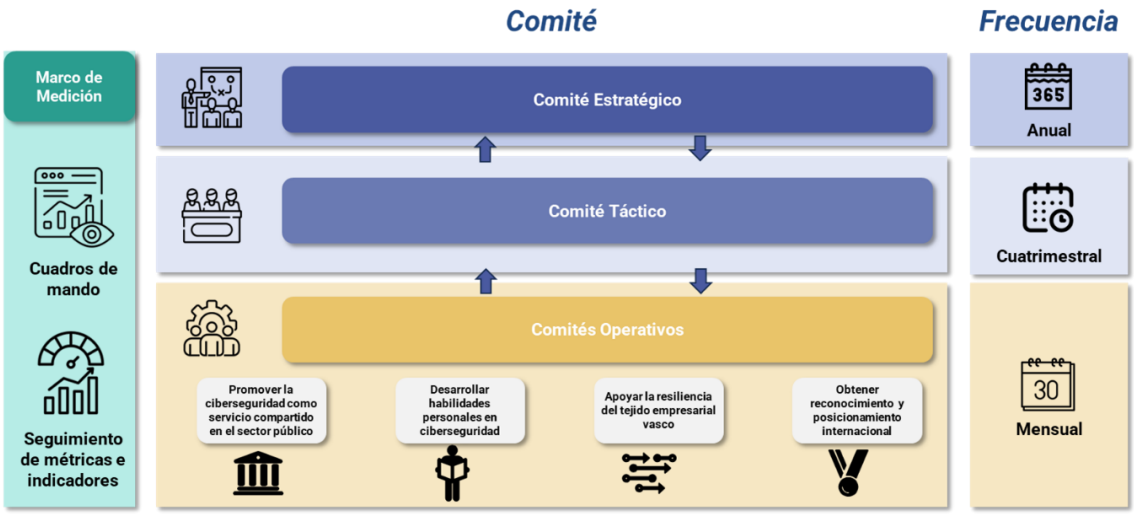

Ilustración 3: Modelo de gobernanza de la Estrategia Vasca de Ciberseguridad

Contexto global de la ciberseguridad

Contexto global de la ciberseguridad

En los últimos años, se ha observado un notable cambio en el panorama tecnológico, impulsado por el proceso de transformación digital y el continuo desarrollo de las Tecnologías de la Información y la Comunicación (TIC). Este fenómeno no solo ha revolucionado las prácticas empresariales, sino que también ha generado una dependencia de las tecnologías emergentes, promoviendo la creación de un nuevo modelo de interconexión digital en la sociedad actual. Esta situación ha supuesto un avance de lo físico a lo digital, de lo progresivo a lo inmediato, de lo tangible a lo intangible.

No obstante, esta evolución hacia un entorno cada vez más digitalizado y altamente interconectado también supone nuevas amenazas y desafíos en el ámbito de la ciberseguridad, donde la prevención, preparación y respuesta eficaz ante incidentes, que comprometan la seguridad y la privacidad de las entidades públicas, empresas privadas y ciudadanía, cobran especial relevancia.

La fuerte dependencia en las tecnologías disruptivas y la hiperconectividad, en este nuevo paradigma digital, se destacan como las principales razones del aumento de la cibercriminalidad, especialmente en lo que respecta a la Administración Pública, que se perfila como un objetivo de lo más atractivo para los ciberdelincuentes.

Bajo este contexto, con el propósito de hacer frente a este desafío, la Unión Europea (UE) ha reconocido la imperiosa necesidad de implementar medidas de seguridad para salvaguardar los sistemas y redes, poniendo especial atención en los operadores críticos y servicios esenciales.

En este sentido, la UE presentó en 2020 una estrategia de ciberseguridad, denominada “Estrategia de Ciberseguridad de la UE para la Década Digital”, cuyas principales líneas de actuación son: “aumentar la seguridad de los servicios esenciales y de los dispositivos conectados, reforzar las capacidades colectivas para responder a los principales ciberataques y cooperar con socios a nivel mundial para garantizar la seguridad internacional y la estabilidad en un ciberespacio global, abierto, estable y seguro, protegiendo los derechos humanos, las libertades fundamentales y los valores democrático”[1].

A nivel nacional, el Consejo de Seguridad Nacional aprobó en 2021 la “Estrategia de Seguridad Nacional (ESN) 2021 en la cual se describe “el contexto actual de seguridad en el mundo, e identifica cuatro dinámicas de transformación global: una mayor competición geopolítica; un entorno socioeconómico marcado por las consecuencias

1 The EU’s Cybersecurity Strategy for the Digital Decade. Fecha: Diciembre 2020.

de la COVID-19; la aceleración del ritmo de transformación provocada por la tecnología; y, por último, el proceso de transición ecológica."[2]

En línea con lo anterior, la regulación y normativa aplicable en este ámbito, también ha evolucionado de manera constante, con el objetivo de dar respuesta a este nuevo entorno digital.

En este sentido, cabe mencionar las principales regulaciones de referencia, a nivel europeo, adoptadas en materia de ciberseguridad en la UE, como son las siguientes:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales ya la libre circulación de estos datos, y por lo que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
- Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013 («Reglamento sobre la Ciberseguridad»).
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS 2).
- Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo.
- Propuesta de Ley Europea de Ciberresiliencia (Cyber Resilience Act - CRA), que tiene como objetivo proteger a los consumidores y a las empresas que compran o utilizan productos o software con un componente digital, estableciendo requisitos de ciberseguridad obligatorios para dichos productos.
- Propuesta de Ley Europea de Inteligencia Artificial, que tiene por objetivo fomentar el desarrollo y la adopción de una IA segura y fiable en todo el mercado único de la UE.

Por otro lado, las principales regulaciones de referencia en materia de seguridad, a nivel estatal, son las siguientes:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

2 Estrategia de Seguridad Nacional 2021. Fecha: Diciembre 2021.

- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

A modo de conclusión, la sociedad actual está inmersa en un proceso de cambio global derivado de la irrupción de las nuevas tecnologías. Esto influye en la forma de conformar un espacio global y ciberseguro que aborde los desafíos y amenazas emergentes.

En este contexto, los gobiernos y organismos deben focalizar sus esfuerzos en la definición e implementación de estrategias de ciberseguridad, alineadas con las principales regulaciones en este ámbito, tanto a nivel internacional como nacional, con el fin de garantizar el uso seguro de las redes, sistemas e infraestructuras, prestando especial atención a los operadores críticos y servicios esenciales, que dan soporte a los sectores clave del mundo moderno.

Situación actual en Euskadi

Situación actual en Euskadi

En un entorno cada vez más digitalizado, asegurar la protección de datos y sistemas se vuelve esencial, especialmente para aquellas organizaciones que adoptan tecnologías avanzadas. Es imperativo tomar acciones proactivas para preservar la integridad, disponibilidad y confidencialidad de la información y así prevenir posibles ataques cibernéticos.

Los sectores esenciales son aquellos que desempeñan un papel crucial para el funcionamiento y desarrollo de un país. En este contexto, la colaboración entre el sector público y privado es fundamental para enfrentar los nuevos desafíos cibernéticos y garantizar la ciberseguridad en los sectores esenciales de Euskadi.

Ante esta evolución constante de las nuevas tecnologías, resulta también imprescindible que las Administraciones Públicas de Euskadi se adapten continuamente a un entorno cambiante y cada vez más complejo, para proporcionar servicios de manera eficiente y segura a la sociedad.

En este contexto, Euskadi cuenta con una destacada concentración de empresas especializadas en ciberseguridad, sobrepasando significativamente el número de compañías por cada millón de habitantes en comparación con otras economías tanto a nivel nacional como europeo. En este mismo sentido, la actividad emprendedora en Euskadi en materia de ciberseguridad destaca como una de las más prominentes a nivel estatal, siendo notable la presencia de startups que desarrollan su propia tecnología.

Así mismo, desde el ámbito público se han articulado diversos instrumentos de internalización y programas de ayuda en ciberseguridad, cuyo objetivo es impulsar la mejora competitiva del tejido empresarial de Euskadi.

Por su parte, el sector público de Euskadi cuenta con una variedad de capacidades de ciberseguridad, cuyo propósito es mejorar la eficiencia, accesibilidad y seguridad de sus servicios.

Dichas capacidades se centran, principalmente, en actividades operativas, con algunas capacidades adicionales en promoción, asesoramiento y formulación de normativas y procesos. Sin embargo, se deben reforzar tanto el ámbito de la prevención, detección y respuesta ante incidentes como el ámbito de la estrategia, la gobernanza y la gestión coordinada de la ciberseguridad. No fortalecer estas capacidades podría implicar riesgos significativos, como la fragmentación de las capacidades o la falta de alineación estratégica con la visión nacional e internacional.

En este contexto, se ha creado Cyberzaintza, la Agencia Vasca de Ciberseguridad, cuyo propósito 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. Este organismo se erige como un

elemento clave para centralizar esfuerzos y optimizar la respuesta ante las ciberamenazas, asegurando así una acción conjunta y efectiva de todos los actores involucrados.

En la siguiente figura se representan las principales entidades públicas que actúan en el ámbito de la ciberseguridad dentro de Euskadi.

Ilustración 4. Principales entidades que actúan en el ámbito de la ciberseguridad

En este marco, resulta también destacable el Plan Estratégico de Tecnologías de la información y Comunidades para la Seguridad Pública de Euskadi (PETICSEG 2021-2024). Se trata de una iniciativa que permite establecer las directrices y objetivos para el desarrollo y la implementación de tecnologías de la información y comunicaciones (TIC) en el ámbito de la seguridad pública en Euskadi.

Asimismo, Euskadi cuenta con el Plan General de Seguridad Pública de Euskadi (2025), el cual, integra el análisis y las proyecciones generales de peligros, acciones y recursos relacionados con la seguridad ciudadana. En su vertiente de ciberseguridad, infraestructuras críticas y sensibles, el plan se enfoca en proteger los activos digitales y las infraestructuras esenciales contra amenazas cibernéticas y otros riesgos.

En base a lo expuesto anteriormente, se puede concluir que, a lo largo de los años, Euskadi ha apostado de manera decidida por la ciberseguridad, dando respuesta a los

retos y desafíos a los que se enfrente una sociedad en pleno auge de transformación digital, intentando posicionarse como un espacio confiable y ciberseguro para la sociedad vasca.

En este contexto, el crecimiento de los ciberdelitos en Euskadi marca una tendencia alcista. Esto no es un hecho aislado y refleja una tendencia global. En el siguiente gráfico, se muestran los datos de la última Memoria Delincuencial de la Euskal Polizia publicada:

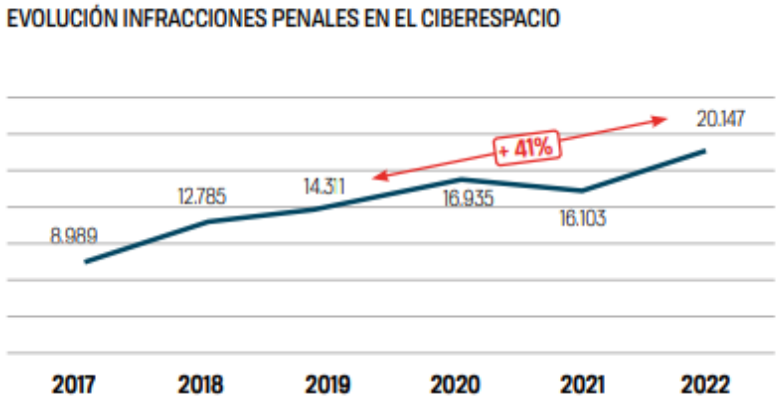

Ilustración 5: Evolución de los ciberdelitos en Euskadi

Así mismo, durante el primer semestre de 2023 esta tendencia al alza se mantuvo, con un incremento del 31% respecto al mismo periodo del año anterior. Actualmente uno de cada 4 delitos que se denuncian en Euskadi se perpetran, ya, a través de las nuevas tecnologías.

Tal y como las cifras ponen de manifiesto, los riesgos van en aumento a medida que la sociedad se digitaliza. La sofisticación de los ataques y la evolución de la tecnología han incrementado significativamente el número de amenazas existentes. Desde fraudes financieros hasta ataques de ransomware, tanto organismos públicos como empresas deben fortalecer y desarrollar nuevas medidas de seguridad para proteger su información y sus infraestructuras.

Retos de la ciberseguridad en Euskadi

Retos de la ciberseguridad en Euskadi

Tras de llevar a cabo un análisis exhaustivo, en el que han participado los principales agentes clave en el ámbito de la ciberseguridad en Euskadi, y consultar fuentes internacionales del ecosistema de la ciberseguridad, se han identificado cuales son los retos estratégicos en el ámbito de la ciberseguridad. Estos retos muestran el modo en que Euskadi, y por ende su sociedad y tejido empresarial pueden verse afectados por las amenazas globales, y son un punto de partida para establecer los objetivos estratégicos a abordar a través de la estrategia de ciberseguridad 2024-2029.

Los principales desafíos identificados, y a los que se buscará dar respuesta durante los próximos cinco años, se recogen a continuación.

GARANTIZAR LA CIBERRESILIENCIA DE LOS SERVICIOS PÚBLICOS A TODA LA CIUDADANÍA VASCA

La transformación digital del Sector Público de Euskadi está en marcha. En un país en el que la ciudadanía cuenta con servicios públicos de calidad, prestados en un contexto de seguridad jurídica y física, garantizar la ciberresiliencia de esos servicios, cada vez más digitales, es un desafío que debe abordarse correctamente.

La resiliencia de los servicios y la protección de la información debe garantizarse para toda la sociedad vasca, generando confianza en su relación con la Administración Pública. Además, esta resiliencia debe garantizarse al conjunto de la ciudadanía, independientemente del territorio histórico en el que resida, de la administración con la que se relacione, y de las características y circunstancias personales que le afecten.

Existen algunos aspectos, como la obsolescencia tecnológica de algunos entornos o el nivel de flexibilidad en otros, que deben ser considerados a la hora de afrontar este reto.

EMPODERAR DESDE LA CIBERSEGURIDAD A TODA LA SOCIEDAD VASCA EN EL PROCESO DE TRANSFORMACIÓN DIGITAL

La ciberseguridad no es un campo completamente tecnológico, la protección de los servicios y de la información debe abordarse desde diversos ámbitos de aplicación. Las medidas no se centran únicamente en la protección, sino que también existen medidas para gestionar riesgos, detectar problemas, dar respuesta a los incidentes y recuperarse de los mismos. Dotar a la sociedad de un nivel de concienciación y capacitación, que le permita ser consciente de los riesgos existentes y poder tomar decisiones informadas, es fundamental. Esto permite a las ciudadanas y los ciudadanos convertirse en agentes activos de su propia protección, y resulta clave para que puedan aprovecharse de las ventajas de la transformación digital.

Debido a la brecha digital existente en la sociedad y a las especificidades de los diferentes colectivos que la componen, este desafío debe abordarse desde una visión

global. De modo que deben contemplarse todas las particularidades que pueden existir en Euskadi, tanto desde el punto de vista personal, como social y profesional, entre otros.

EFICIENTAR EL USO DE LOS RECURSOS DEDICADOS PARA GENERAR UN PAÍS CIBERSEGURO

La Administración Pública de Euskadi ofrece a la sociedad servicios adecuados a sus necesidades, con una organización desplegada en tres niveles de actuación, cada uno de estos niveles cuentan con una estructura y unas capacidades diferentes. En este contexto, para poder optimizar los servicios públicos ofrecidos a la sociedad, la eficiencia de los recursos se convierte en un aspecto clave, también en el caso de los servicios digitales.

La ciberseguridad es una amenaza global que representa un desafío asimétrico en la protección. Así, en este ámbito también, ser más eficiente en el uso de los recursos supondrá un factor clave para poder desplegar un conjunto mayor de medidas, que permitan gestionar los riesgos de manera más efectiva.

ARTICULAR MECANISMOS DE COORDINACIÓN INSTITUCIONAL Y COLABORACIÓN PUBLICO-PRIVADA ORIENTADOS A LA CIBERSEGURIDAD DEL PAÍS

Para lograr la ciberresiliencia de Euskadi es necesario contar con un nivel de coordinación interinstitucional completamente definido y entrenado, que permita identificar una respuesta única en las ocasiones que así se requiera.

Adicionalmente, se hace fundamental articular mecanismos de colaboración público-privada, que lleven esta ciberresiliencia al conjunto del país y aumenten las posibilidades de éxito. Siendo la colaboración público-privada una de las señas de identidad de Euskadi, este desafío debe abordarse apoyándose en las fortalezas existentes que han sido identificadas durante las sesiones realizadas.

ESTABLECER UN ENTORNO QUE PERMITA GARANTIZAR LA CIBERRESILIENCIA DE LA ACTIVIDAD EMPRESARIAL DEL PAÍS

La seguridad, como concepto general, es uno de los aspectos más valorados por el tejido empresarial a la hora de desarrollar su actividad. En este contexto, el nivel de seguridad pública que existe en Euskadi hace que empresas de referencia internacional nazcan y se desarrollen en el país.

En un contexto global, en el que la transformación digital dentro del ámbito empresarial es cada vez más rápida y necesaria, el tejido empresarial debe proteger sus actividades y resultados también en el ámbito cibernético. Aunque la ciber protección de las empresas es un aspecto que debe afrontar el tejido empresarial de primera mano, Euskadi tiene el reto de disponer de las medidas necesarias que provean el mejor escenario para garantizar la ciberresiliencia de la actividad empresarial del país.

DISPONER DE UN SECTOR DE CIBERSEGURIDAD CON CAPACIDADES LOCALES Y SOBERANAS RECONOCIDO INTERNACIONALMENTE

La ciberseguridad es un reto global que debe afrontarse como tal. Existen capacidades desarrolladas en múltiples países y regiones. Euskadi actualmente cuenta con un buen

posicionamiento y consideración, y su sector de ciberseguridad ha sido capaz de generar soluciones y capacidades con proyección internacional. No obstante, desde hace tiempo, algunas de las operaciones realizadas por el entorno empresarial han resultado en que diferentes agentes de relevancia nacidos en Euskadi han llevado sus centros de decisión a otros países o regiones.

Además, las principales herramientas utilizadas en el ámbito de la protección dependen de empresas de terceros países. Aun así, Euskadi cuenta con un sector sólido, con presencia de un gran número de agentes y con un nivel de innovación destacado, algo que debe permitir afrontar este reto desde una posición optimista. Así mismo, el tejido empresarial local con importante presencia internacional puede ser un aliado clave.

ESTABLECER MODELOS DE COOPERACIÓN INTERNACIONAL PARA HACER FRENTE A LAS AMENAZAS GLOBALES

Frente a amenazas globales como el cibercrimen, que cada vez tienen un mayor impacto también en Euskadi, no es posible buscar una defensa centrada en nuestro País. Para afrontar estas amenazas desde la mejor posición, deben establecerse modelos de cooperación internacional, que nos permitan anticiparnos a las amenazas cuando sea posible y responder de la mejor manera cuando no lo sea. En este contexto, en el que todos los países se ven afectados por una amenaza común y el número de interesados es muy elevado, que los modelos de cooperación funcionen correctamente es un gran desafío. Euskadi, siendo un país pequeño tanto en superficie como en población, debe resolver este reto desde un enfoque que le permita ganar relevancia.

La posición de partida es buena, ya que actualmente Euskadi está representada en diversos foros internacionales, con especial relevancia en el contexto estatal y europeo. En términos generales, desde una posición de colaboración o desde una posición de liderazgo, es considerada una región que genera valor. Esta situación debe aprovecharse a la hora de afrontar el reto.

Propósito, principios y objetivos estratégicos

Propósito, principios y objetivos estratégicos

Una de las claves del desarrollo tanto de las sociedades como de su tejido económico, es el nivel de ciberseguridad que estas adquieren. Con unos niveles de seguridad ciudadana extraordinarios, Euskadi debe protegerse de los riesgos de ciberseguridad existentes y empoderar su sociedad para una transformación digital segura, que permita su desarrollo futuro de manera óptima.

En este contexto, como base para la construcción de los objetivos estratégicos, se han formulado el propósito y los principios que rigen la Estrategia de Ciberseguridad de Euskadi.

PROPÓSITO

El propósito principal de la Estrategia Vasca de Ciberseguridad es el de convertir a Euskadi en un país ciberresiliente, con capacidades para proteger su Administración Pública y su tejido empresarial frente a los riesgos y amenazas en el ámbito de las TIC, 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.

PRINCIPIOS

La Estrategia de Ciberseguridad de Euskadi se fundamenta en seis principios clave, que son esenciales para diseñar y ejecutar una estrategia efectiva.

Los principios clave

Ilustración 6: Principios de la Estrategia Vasca de Ciberseguridad

- **Resiliencia:** Nos adaptamos a los cambios tecnológicos y reaccionamos ante nuevas amenazas, asegurando la continuidad y eficacia de los servicios esenciales y la protección de la información sensible.
- **Colaboración:** Colaboramos para el intercambio eficaz de conocimientos, estrategias y prácticas óptimas en ciberseguridad. La meta es consolidar un frente unido que mejore la capacidad de respuesta colectiva ante las ciberamenazas, elevando así nuestro nivel de seguridad digital.
- **Eficiencia:** Implementamos procedimientos y soluciones transversales aprovechando las sinergias identificadas que nos permitan optimizar los recursos disponibles y capacidades de ciberseguridad.
- **Cercanía:** Creamos vínculos sólidos que permitan facilitar la comunicación con toda la ciudadanía, promoviendo la proximidad en nuestra labor. Fomentamos una cultura de seguridad digital accesible y comprensible para todos, facilitando así la participación y el compromiso de la sociedad en las iniciativas de ciberseguridad.
- **Liderazgo:** Impulsamos y guiamos las acciones en materia de seguridad digital a través de la toma de decisiones proactiva y la definición de objetivos estratégicos claros inspirando y motivando hacia el logro de objetivos comunes.
- **Innovación y mejora continua:** Promovemos la adopción de las últimas tecnologías y tendencias que nos permitan abordar nuevos desafíos y optimizar los diferentes procesos.

OBJETIVOS

Ante esta situación, Euskadi debe conseguir alcanzar cuatro objetivos estratégicos principales en el periodo 2024-2029.

Cada uno de estos objetivos estratégicos, está vinculado a uno o más retos, como se muestra en la siguiente figura:

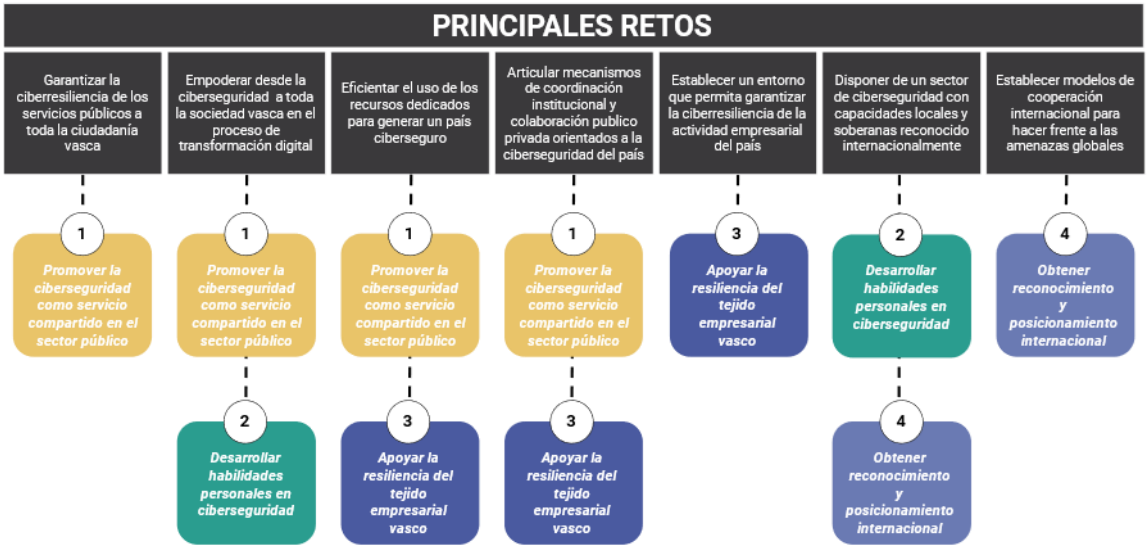

Ilustración 7: Objetivos de la Estrategia Vasca de Ciberseguridad

- **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 adecuado 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 ciberseguridad 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.

Líneas de actuación

Líneas de actuación

A continuación, se describen las diferentes líneas de actuación que permitirán resolver los principales desafíos identificados en la Estrategia.

En este sentido, cada línea de actuación está compuesta por una serie de actividades principales que pretenden dar cobertura a la consecución de los objetivos establecidos para para el periodo 2024 – 2029.

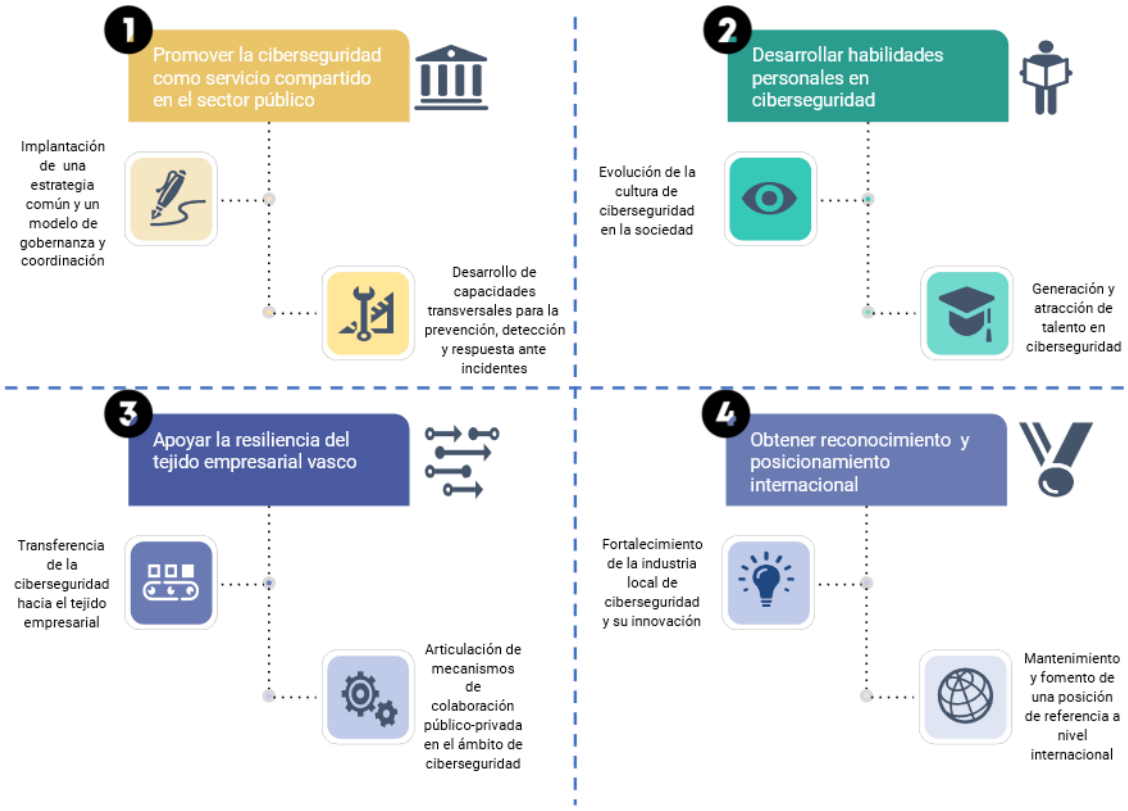

Ilustración 8: Líneas de actuación de la Estrategia Vasca de Ciberseguridad

LÍNEA DE ACTUACIÓN 1

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

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.

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.

LÍNEA DE ACTUACIÓN 2

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

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.

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.

LÍNEA DE ACTUACIÓN 3

Evolución de la cultura de ciberseguridad en la sociedad

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

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.

LÍNEA DE ACTUACIÓN 4

Generación y atracción de talento en ciberseguridad

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.

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.

LÍNEA DE ACTUACIÓN 5

Transferencia de la ciberseguridad hacia el tejido empresarial

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.

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.

LÍNEA DE ACTUACIÓN 6

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

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.

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.

LÍNEA DE ACTUACIÓN 7

Fortalecimiento de la industria local de ciberseguridad y su innovación

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

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.

LÍNEA DE ACTUACIÓN 8

Mantenimiento y fomento de una posición de referencia a nivel internacional

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

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.

Modelo de gobernanza

Modelo de gobernanza

La implantación exitosa de la Estrategia Vasca de Ciberseguridad requiere de un modelo de gobernanza sólido y bien estructurado, en el que estén incluidos todos los agentes involucrados en las líneas de actuación definidas.

Para ello, se ha establecido un modelo de comités y mecanismos de reacción basado en tres niveles y apoyados por un marco de medición que permitirá realizar un seguimiento de la estrategia.

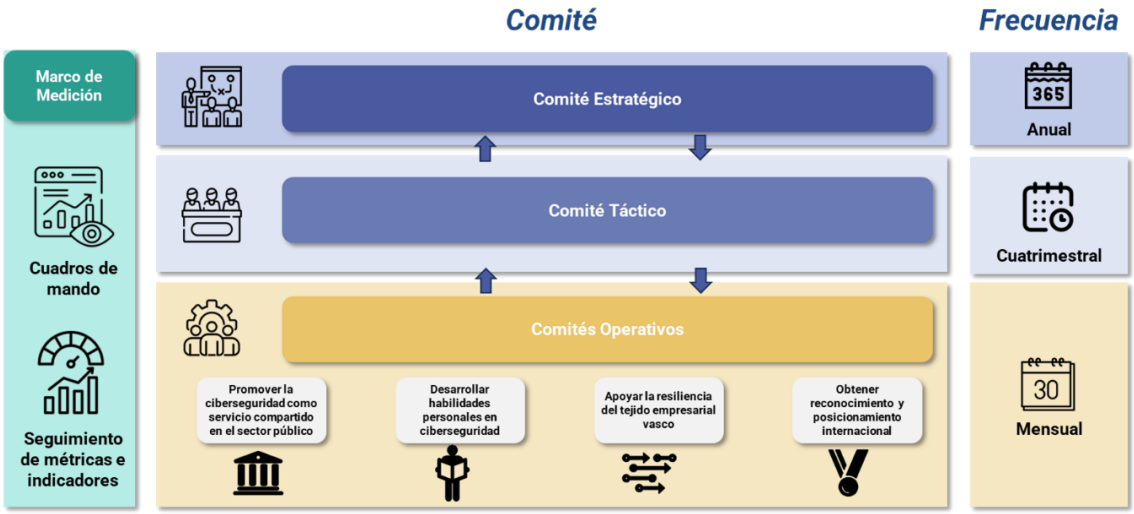

Ilustración 9: Modelo de gobernanza de la Estrategia Vasca de Ciberseguridad

Para llevar a cabo las funciones de monitorización y vigilancia del estado de los diferentes indicadores definidos en la estrategia se designará un órgano de seguimiento y coordinación.

A continuación, se detallan las presidencias de cada uno de los comités, las personas que lo deben integrar, sus funciones, su periodicidad y el ámbito de actuación definidos:

Comité Estratégico
Presidencia
🧍 Persona que lidere el Departamento de Seguridad en calidad de Consejero o Consejera.
Miembros
🧍 Dirección General de la Agencia Vasca de Ciberseguridad, actuando también como enlace con el Comité Táctico. 🧍 La persona que ostente la presidencia del Comité Estratégico determinará el resto de la composición y las normas de organización de este.
Funciones
• Será función de la presidencia del Comité Estratégico la aprobación del Modelo de Medición de la Estrategia cuyo seguimiento presentará al Comité Estratégico cuando este se reúna. • Seguimiento del cumplimiento de los objetivos de la Estrategia. • Toma de decisiones estratégicas. • Análisis global de indicadores relevantes. • Supervisión de riesgos. • Resolución de problemas escalados.
Periodicidad
❖ Anual.
Ámbitos de actuación
✓ Transversal.

Comité Táctico
Presidencia
⚷ Dirección General de la Agencia Vasca de Ciberseguridad.
Miembros
⚷ Dirección de Estrategia de la Agencia Vasca de Ciberseguridad, actuando también como enlace con los Comités Operativos. ⚷ La persona que ostente la presidencia del Comité Táctico determinará el resto de la composición y las normas de organización de este.
Funciones
• Propuesta del modelo de medición que permita monitorizar el avance en el despliegue de la Estrategia. • Medición del cumplimiento de los objetivos de la Estrategia. • Análisis y gestión de presupuestos. • Seguimiento y coordinación de las líneas de actuación. • Análisis de las actividades e hitos completados. • Planificación de nuevas actividades. • Toma de decisiones tácticas. • Definición y supervisión de indicadores. • Gestión de riesgos. • Resolución de problemas.
Periodicidad
❖ Cuatrimestral.
Ámbitos de actuación
✓ Transversal.

Comité Operativo
Presidencia
⚷ La persona que ostente la Dirección de Estrategia de la Agencia Vasca de Ciberseguridad o 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.
Miembros
⚷ La persona que ostente la Dirección de Estrategia de la Agencia Vasca de Ciberseguridad determinará la composición y las normas de organización de los Comités.
Funciones
• Implementación y mantenimiento del Modelo de Medición de la Estrategia. • Ejecución de presupuestos. • Seguimiento detallado de actividades y tareas asociadas. • Definición de metodologías de trabajo y acciones operativas. • Análisis de las tareas completadas. • Planificación de nuevas tareas. • Toma de decisiones operativas. • Medición y mantenimiento de indicadores. • Escalado de riesgos y problemas.
Periodicidad
❖ Mensual.
Ámbitos de actuación
✓ Promover la ciberseguridad como servicio compartido en el sector público. ✓ Desarrollar habilidades personales en ciberseguridad. ✓ Apoyar la resiliencia del tejido empresarial vasco. ✓ Obtener reconocimiento y posicionamiento internacional.

Seguimiento y evaluación

Seguimiento y evaluación

Para asegurar un seguimiento efectivo y preciso del avance en el despliegue de la Estrategia de Ciberseguridad de Euskadi, es fundamental contar con un modelo de seguimiento eficaz. Este modelo permitirá evaluar el progreso, identificar desviaciones y tomar medidas correctivas para garantizar que se alcancen los objetivos establecidos.

El **Modelo de Medición** deberá incluir métricas, indicadores y un cuadro de mando que posibiliten evaluar y supervisar el progreso en la implantación de la Estrategia de manera efectiva.

Será responsabilidad del Comité Táctico proponer el modelo que permita medir el avance en el despliegue de la Estrategia.

Será función de la presidencia del Comité Estratégico la aprobación del Modelo de Medición cuyo seguimiento presentará al Comité Estratégico cuando este se reúna.

EUSKO JAURLARITZA
GOBIERNO VASCO