

# LIBRO BLANCO DE LA CIBERSEGURIDAD EN EUSKADI 2025

Resumen ejecutivo



SPRI - Agencia Vasca de Desarrollo Empresarial (en adelante, SPRI), en aras de mostrar su compromiso constante con el sector de la ciberseguridad, publica la tercera edición de "El Libro Blanco de ciberseguridad en Euskadi" (en adelante, Libro Blanco), junto con el presente resumen ejecutivo. El Libro Blanco tiene como objetivo principal ofrecer una perspectiva de ciberseguridad dirigida, no solo a empresas, agencias, instituciones y estudiantes, sino, a quién busque mantenerse informado sobre el estado y las tendencias actuales en esta materia.

El documento presenta un análisis del mercado de la ciberseguridad mediante una visión global, europea, estatal y específica de la región de Euskadi. Asimismo, establece una metodología que permite la identificación y clasificación de los diferentes agentes que ofrecen servicios o soluciones de ciberseguridad, y que operan en Euskadi, en tres niveles diferentes: nivel Listado, nivel Acreditado y nivel Verificado.

El documento comienza con un primer apartado donde se detalla la metodología llevada a cabo en la realización del análisis y posteriormente, se procede al análisis del contexto del sector dividido en 9 apartados. La contextualización del sector abarca el estudio del valor de mercado, las inversiones en ciberseguridad, la oferta y demanda en relación con la ciberseguridad, el emprendimiento, las tendencias actuales en ciberdelitos y sus repercusiones, las tendencias en ciberseguridad, las regulaciones vigentes, los diferentes sellos de calidad existentes y sus características, así como las principales agencias de ciberseguridad tanto a nivel estatal como a nivel regional.

Más adelante, se efectúa un análisis específico sobre la ciberseguridad en el entorno industrial, además de hacer un repaso sobre algunos de los diferentes instrumentos de apoyo promovidos por diversas instituciones públicas y que van dirigidos a favorecer al crecimiento y fortalecimiento del sector, pudiendo resultar de gran ayuda para las empresas del territorio.

En esta edición, al igual que en anteriores, se presenta una sección detallada que enumera empresas y soluciones relacionadas con la ciberseguridad en Euskadi. Esto abarca desde entidades de naturaleza pública, asociaciones, centros tecnológicos y universidades hasta centros de formación profesional, así como una diversidad de empresas que abarcan consultoras, integradores, fabricantes y distribuidores.

Posteriormente, se exponen las conclusiones alcanzadas en la elaboración de este Libro Blanco, junto con las perspectivas futuras en el ámbito de la ciberseguridad en Euskadi.

Finalmente, se ofrece una visión general de eventos de interés a nivel mundial y regional en materia de ciberseguridad. Desde SPRI se generará un observatorio sectorial donde se recogerán y se actualizarán en detalle los eventos y los diversos agentes que forman el ecosistema de ciberseguridad de Euskadi.



A black and white photograph showing the back of a man's head and shoulders. He is looking towards the left side of the frame, where a large server rack is visible. The server rack is filled with various components like hard drives and network cards. The lighting is dramatic, with strong highlights on the man's hair and the server components.

**SPRI.**  
Agencia Vasca de  
Desarrollo Empresarial





El papel del Departamento de Desarrollo Económico, Sostenibilidad y Medioambiente (DESMA) del Gobierno Vasco, a través de SPRI, ha resultado fundamental en los últimos años a la hora de promover y desarrollar una cultura vinculada a la ciberseguridad en Euskadi. En este tiempo, ambos organismos han afianzado su postura y erigido como actores clave a la hora de dinamizar la actividad empresarial y favorecer al crecimiento y fortalecimiento del sector en el territorio.

De esta manera, SPRI, a lo largo de este tiempo, lleva mostrando un fuerte compromiso con el sector de la ciberseguridad, alimentado por medio de una estrategia clara y plenamente alineada con las particularidades y la realidad del tejido empresarial de la Comunidad Autónoma de Euskadi. Esta estrategia tiene un objetivo claramente dual. Por un lado, tratar de

contribuir a la mejora o el incremento del nivel de ciberseguridad del tejido empresarial de Euskadi por medio de la aplicación de tecnologías vinculadas a la ciberseguridad, teniendo en especial consideración a las empresas que focalizan su actividad dentro de los 3 ámbitos RIS3 de especialización inteligente de Euskadi (Industria Inteligente, Energías Limpias y Salud Personalizada). Mientras que, por otro lado, se pretende seguir favoreciendo al crecimiento del sector de la ciberseguridad en sí, tratando de posicionar a Euskadi como un hub de referencia en materia de ciberseguridad industrial, el cual cuente con reconocimiento a nivel internacional y que permita posicionar al sector también en el extranjero.

**DESMA y SPRI: fuerte compromiso con el sector de la ciberseguridad, alimentado por una estrategia clara y plenamente alineada con la realidad del tejido empresarial de Euskadi**

Para la consecución de dichos objetivos, aprovechándose de las diferentes capacidades del Grupo, SPRI lleva impulsando algunas iniciativas e instrumentos de apoyo concretos dirigidos al fortalecimiento del sector y que abarcan ámbitos temáticos específicos tales como el I+D, la innovación, el emprendimiento, la internacionalización, o el acceso a financiación entre otros. Este apoyo institucional diferencial a lo largo de todos estos años ha hecho erigirse a SPRI como entidad o agente de referencia en Euskadi en todo lo relacionado con la ciberseguridad vinculada al ámbito empresarial, y más concretamente, al ámbito industrial. Al mismo tiempo que ha contribuido de forma directa al crecimiento tan notable que ha experimentado el sector en los últimos años.

SPRI lleva tiempo trabajando diferentes líneas. Esto incluye por ejemplo el apoyo a proyectos de investigación y desarrollo (I+D) dentro del ámbito de la ciberseguridad, a través de sus programas HAZITEK o ELKARTEK. Financiación para la creación o acondicionamiento de infraestructuras científico-tecnológicas que favorezcan la experimentación dentro del ámbito de la ciberseguridad, a través del programa AZPITEK. La posibilidad de utilizar estas infraes-

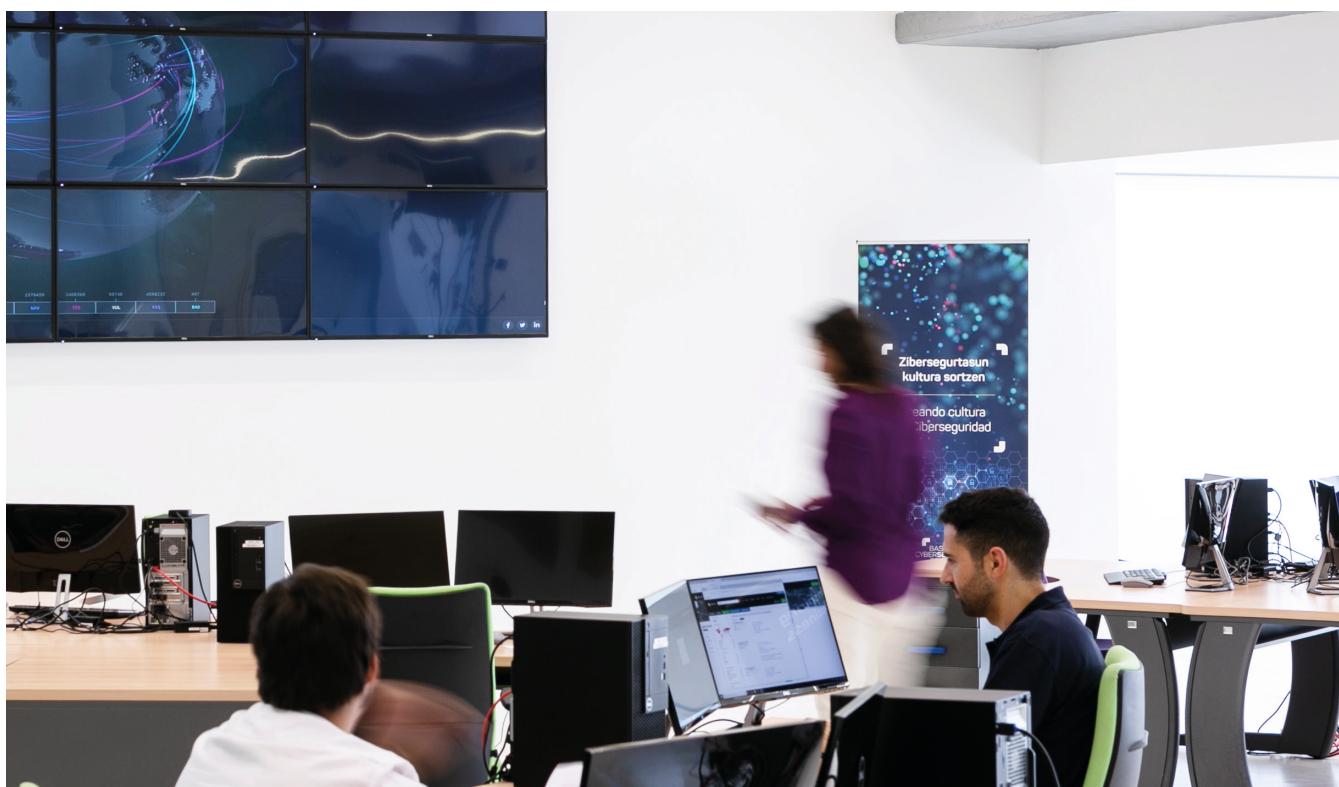


tructuras u otro tipo de activos tecnológicos para la experimentación de nuevas soluciones o productos de ciberseguridad a través del programa BDIH Konexio y enmarcado dentro del Nodo de Ciberseguridad del Basque Digital Innovation Hub, consolidando así el posicionamiento estratégico de SPRI en este sector. El apoyo para la puesta en marcha y maduración de proyectos de Emprendimiento dentro del ámbito de la ciberseguridad a través de la red de Business Innovation Centers (BICs) y a través de diferentes programas e iniciativas de apoyo como EKINTZAILE, BARNEKINTZAILE, BIND 4.0 Open Innovation Platform o Basque Tek Ventures entre otros. Apoyo financiero y estratégico para la creación y expansión de empresas especializadas en el sector a través de diferentes fondos gestionados por entidades colaboradoras del Grupo SPRI, así como por su sociedad de referencia en esta materia, GESTIÓN DE CAPITAL RIESGO DEL PAÍS VASCO, SGEIC, S.A. Programas de capacitación específicos en el ámbito de la ciberseguridad, impartidos desde la red de "Centros Empresa Digitala" en los Parques Tecnológicos de Euskadi.

Adicionalmente, cabe señalar una de las iniciativas emblemática, que no hace más que reforzar el liderazgo de SPRI en Euskadi dentro del ámbito de la ciberseguridad dirigida a la empresa. Se trata del programa Ciberseguridad Industrial, el cual tiene por objetivo apoyar proyectos que contribuyan a mejorar o elevar el nivel de ciberseguridad de las empresas de Euskadi de forma significativa. Dentro del marco de este programa, el cual ya va por su sexta edición, se han apoyado más de 1.610 proyectos en los últimos años, que han supuesto una inversión en empresas del sector, de aproximadamente 32 millones de euros, habiendo sido realizados estos proyectos por más de 155 proveedores de ciberseguridad diferentes, los cuales ofrecen soluciones o servicios de este tipo dentro de la Comunidad Autónoma de Euskadi.

Al mismo tiempo, SPRI ha favorecido también y participado activamente en la creación, maduración y consolidación de algunas iniciativas público-privadas que sin duda han contribui-

SPRI pretende afianzar su posición como agente de referencia en todo lo relacionado con la ciberseguridad aplicada a la empresa





do también al crecimiento vertiginoso que ha experimentado el sector durante estos últimos años. Hablamos de iniciativas tales como la creación de Cybasque, asociación que representa a las Industrias de Ciberseguridad de Euskadi, la creación del BRTA, alianza de innovación que aglutina 17 centros de I+D de Euskadi fomentando la cooperación y la excelencia científica y en donde una de las líneas de investigación y de actividad principales es sin duda la ciberseguridad, o la participación activa en ECSO (European Cyber Security Organisation), a través de la cual se ha realizado una labor importante por posicionar al sector de la ciberseguridad de Euskadi en el panorama internacional. Adicionalmente, desde el Departamento de Desarrollo Económico, Sostenibilidad y Medioambiente del Gobierno Vasco , con la inestimable colaboración de Grupo SPRI, también se han incurrido en otra serie de iniciativas en los últimos tiempos, que, si bien no van expresamente dirigidas a la ciberseguridad, sin duda están contribuyendo a la generación de nuevos negocios y a la aparición de nuevos productos vinculados a ámbitos temáticos o sectores específicos. Algunas de estas iniciativas: 5G Euskadi (ciberseguridad orientada al 5G), ADI – Atlantic Data Infrastructure, Robotekin (Asociación Vasca de Robótica y Automatización), BasqueCCAM (Centro Vasco de Movilidad Conectada y Autónoma), o el BAM (Basque Automotive Manufacturing Center) entre otros. Estas iniciativas e infraestructuras sin duda servirán para que las empresas de ciberseguridad de Euskadi puedan avanzar hacia nichos de especialización concretos, traduciéndose en un mayor grado de diferenciación respecto a sus principales competidores tanto a nivel local como internacional.

Todo este recorrido, el know-how adquirido en todo este tiempo, así como el disponer de los mecanismos e instrumentos de apoyo adecuados, hacen vislumbrar a SPRI y encarar el futuro de la ciberseguridad en Euskadi desde una posición privilegiada, afianzándose de forma indiscutible como agente o entidad de referencia en todo lo relacionado con la ciberseguridad aplicada al ámbito empresarial en Euskadi.

De esta manera, desde el Departamento de Desarrollo Económico, Sostenibilidad y Medioambiente, y a través de Grupo SPRI, se quiere continuar con el despliegue de su estrategia y con su firme apuesta por la ciberseguridad a lo largo de los próximos años, con el objetivo de avanzar hacia la consecución de los objetivos o el objetivo primordial mencionado anteriormente, que no es otro que el seguir avanzando hacia la consolidación del tejido empresarial de Euskadi como ecosistema “ciberseguro”, por medio del crecimiento y fortalecimiento del sector de la ciberseguridad de Euskadi.

The background of the image is a dark, low-light server room. On the right side, a person wearing glasses and a light-colored shirt is visible, looking towards the left. The server racks are filled with numerous small lights and ventilation grilles.

# Metodología





Para la elaboración de la tercera edición del Libro Blanco, se ha llevado a cabo la siguiente metodología:

## Metodología aplicada en el Libro Blanco

### 01. Obtención de información

#### Obtención inicial de la información

Búsqueda de información relativa de los diferentes ámbitos temáticos vinculados a la ciberseguridad, tanto a nivel mundial, europeo, estatal, como regional.

### 02. Análisis del contexto global

#### Análisis del contexto global

Ánalisis de los datos obtenidos relativos a los diferentes ámbitos temáticos relacionados con la ciberseguridad e inclusión de la información en el Libro Blanco

### 03. Análisis exhaustivo de Euskadi

#### Análisis exhaustivo del sector de la ciberseguridad en Euskadi

Ánalisis detallado sobre el sector de la ciberseguridad en Euskadi.

### 04. Definición de la taxonomía

Definición de un sistema de clasificación que permita organizar y agrupar los diferentes agentes de ciberseguridad en categorías, en función de sus características y naturaleza. Se define también un diccionario para la clasificación de los diferentes servicios/productos ofrecidos por los mismos.

### 05. Identificación y Análisis de agentes

Identificación, así como contacto con los agentes de ciberseguridad para la recopilación de información para su posterior análisis. Agentes que disponen de al menos una oficina de manera permanente en Euskadi y, ofrezcan servicios o productos de ciberseguridad en el territorio.

### 06. Clasificación de los agentes

Definición del listado de agentes de ciberseguridad de Euskadi, así como la clasificación de los mismos. La clasificación se realiza a dos niveles. Uno, en función de la naturaleza de cada agente. Dos, en función del grado de exhaustividad o de detalle en lo relativo a la información facilitada por los mismos. En este punto, también se determinan los productos o soluciones de ciberseguridad que ofrecen cada uno de ellos.

Figura 1. Metodología aplicada. Fuente: elaboración propia



**1. Obtención inicial de información.** Búsqueda global de información en materia de ciberseguridad relacionada con el valor del mercado, las inversiones, las iniciativas de emprendimiento, la educación, los profesionales dedicados, las tendencias dentro del sector, el impacto del cibercrimen, así como las nuevas regulaciones que están surgiendo para hacerle frente y las agencias de ciberseguridad.

**2. Análisis del contexto Global.** Análisis de la información obtenida de las diferentes fuentes a nivel mundial, europeo y regional, seleccionando aquella que es relevante o de interés para esta edición del Libro Blanco.

**3. Análisis exhaustivo del ecosistema vasco de ciberseguridad en Euskadi.** Realización de un análisis más detallado sobre el sector de la ciberseguridad en Euskadi.

**4. Definición de la taxonomía.** Establecimiento de un sistema de clasificación basado en la naturaleza y características de cada agente, que permite identificar y agrupar a los mismos facilitando así su estudio. Del mismo modo, se define también un diccionario para la clasificación de los diferentes productos o servicios ofrecidos por los agentes.

**5. Identificación y Análisis de los diferentes agentes.** Identificación, así como obtención de información a través del contacto directo con los agentes de ciberseguridad. Se han identificado y analizado los diferentes agentes que teniendo su origen o no en Euskadi, disponen de al menos una oficina de manera permanente en cualquiera de los tres territorios históricos de la Comunidad Autónoma de Euskadi y, ofrecen servicios o productos de ciberseguridad.

**6. Clasificación de los agentes.** Tras el análisis de la información de los agentes de ciberseguridad, se clasifican los agentes en función de sus características, naturaleza, así como en función del grado de exhaustividad o nivel de detalle de la información facilitada.

En lo relativo a esto último, se establecen diferentes niveles (nivel Listado, nivel Acreditado y nivel Verificado) de clasificación. Cada nivel determina un grado de certeza o nivel de confianza en lo que se refiere a la información facilitada por cada uno de los agentes. De esta manera, los agentes del nivel más alto (nivel Verificado) por ejemplo, son aquellos que además de trasladar que ofrecen diferentes productos o servicios de ciberseguridad, también han aportado datos y evidencias suficientes que así lo acrediten. Del mismo modo, los agentes presentes en este nivel también han facilitado referencias de clientes o proyectos en los que haber implantado este tipo de productos u ofrecidos este tipo de servicios.

Por lo tanto, para los agentes de ciberseguridad presentes en este nivel, el grado de certeza respecto a la información facilitada y publicada resulta considerablemente mayor. Dicho esto, a continuación, se especifican los requisitos necesarios para la obtención de los diferentes niveles.



Nivel listado	Nivel acreditado	Nivel verificado
Ser un agente que proporciona productos/servicios de ciberseguridad.	Ser un agente que proporciona productos/servicios de ciberseguridad.	Ser un agente que proporciona productos/servicios de ciberseguridad.

*Figura 2. Niveles de clasificación de los agentes. Fuente: elaboración propia.*

Debe destacarse que, tras la publicación del presente Libro Blanco, a través de un observatorio se va a realizar un seguimiento continuo de los agentes. Por lo que, en caso de que alguna organización cumpla con los requisitos establecidos y no aparezca representada en esta edición del Libro Blanco, podrá solicitar su incorporación de cara a próximas ediciones. Para ello, deberán dirigirse a la siguiente dirección de correo electrónico: **libroblanco.ext@spri.eus**



# Contextualización del sector





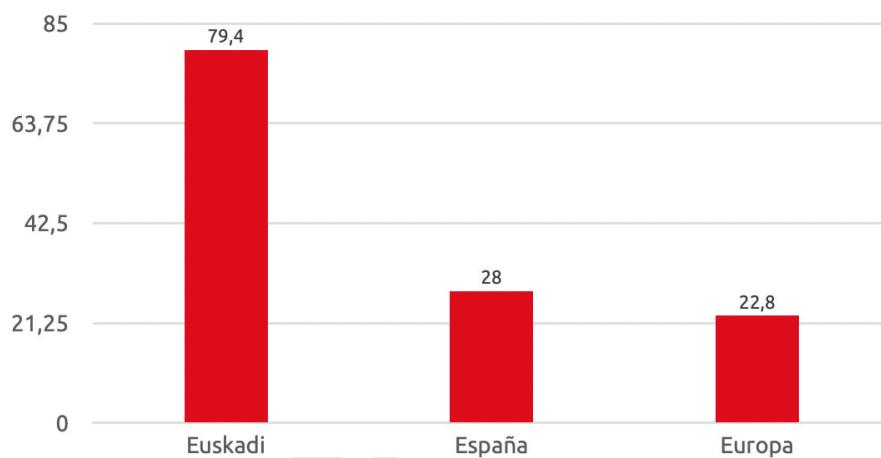
En el presente resumen ejecutivo, se muestra el **análisis de la situación actual del ecosistema de ciberseguridad a nivel global, europeo, estatal y específico de Euskadi**, resaltando aspectos clave, retos y oportunidades para fortalecer la región. Además, se abordan diferentes ámbitos temáticos, entre los que se incluyen el valor de mercado, inversión, empleo y educación, emprendimiento, cibercrimen, tendencias en ciberseguridad, regulaciones, sellos de ciberseguridad, agencias especializadas, ciberseguridad industrial, así como los agentes de ciberseguridad que operan en Euskadi.

## Valor de mercado

Con la hiperconectividad como una de las causas principales, el valor de mercado en materia de ciberseguridad superó los 126.000 millones de dólares a nivel global en 2022, suponiendo un crecimiento del 18% en los últimos cuatro años. Se proyecta a nivel global, un aumento anual de 8,7% en el mercado de la ciberseguridad hasta 2026, con un valor estimado en 260.000 millones de dólares en 2023. Atribuyéndose este aumento a la demanda creciente de soluciones y servicios de seguridad digital, respaldados por un ambiente propicio para la innovación y la tecnología.

Este incremento se hace patente en Europa y, de manera específica, en Euskadi, donde se observa un notable aumento en la inversión y el interés hacia la ciberseguridad. Todo ello ha derivado en que la concentración de empresas especializadas en ciberseguridad en la región de Euskadi sea significativamente mayor que la media tanto a nivel estatal como europeo. La media de empresas por millón de habitantes en Euskadi es de 79 frente a las 28 y 22 de España y Europa respectivamente, reflejándose así una importante presencia y relevancia del sector de la ciberseguridad en la región.

### Media de empresas por cada millón de habitantes



*Figura 3. Media de empresas por cada millón de habitantes.*  
Fuente: European Cybersecurity Investment Platform



## Inversión

El constante crecimiento del mercado mundial de ciberseguridad, impulsado entre otras causas por la hiperconectividad y el aumento de la actividad delictiva en este ámbito, está generando un incremento en términos de inversión en el sector.

Siendo Euskadi un foco para la inversión en ciberseguridad, las estrategias públicas y los programas de inversión en Euskadi se enfocan en fomentar la innovación y el desarrollo en el sector. **La apuesta por la innovación es la seña de identidad de Euskadi**, apuesta que le ha reportado reconocimiento y recursos en el ámbito europeo. En esta línea, tal y como recoge el “Informe sobre la Ciencia en Euskadi 2022”, **Euskadi es la comunidad autónoma del Estado que lidera la inversión en I+D, con un 2,2% sobre el producto interior bruto**.

A su vez, Euskadi es considerada región fuertemente innovadora, según el European Innovation Scoreboard. También lidera el retorno per cápita de fondos europeos, casi triplicando la media estatal, haciendo de Euskadi una región atractiva en la que invertir.

Euskadi cuenta con diversas entidades de inversión de naturaleza pública entre las que destacan: Gestión Capital Riesgo Euskadi y Seed Capital Bizkaia

Las fortalezas en **innovación, educación, y colaboración empresarial respaldadas por ventajas fiscales**, posicionan a Euskadi como un punto de notable interés para diversa tipología de inversores en un sector emergente y con gran proyección como es el de la ciberseguridad. Además, en lo que a la inversión de naturaleza pública se refiere, Euskadi dispone de **diversas entidades que focalizan su actividad en esta materia, entre las que destacan: Gestión Capital Riesgo Euskadi y Seed Capital Bizkaia**.

Euskadi se presenta como un territorio atractivo para la inversión en ciberseguridad, con varias iniciativas de colaboración público-privada y un entorno fiscal favorable. Este beneficioso escenario ha favorecido al incremento de agentes inversores en el territorio

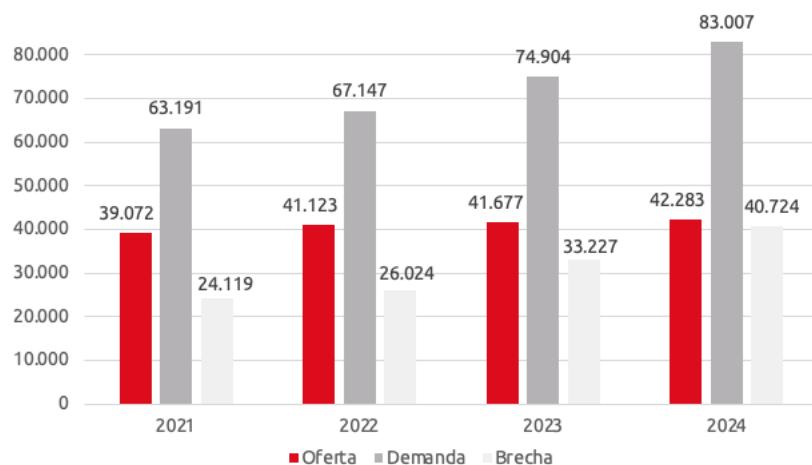


## Empleo y educación

El avance acelerado de las tecnologías, la digitalización, la dependencia hacia los sistemas TIC y la necesidad de protegerlos ante los riesgos y amenazas de ciberseguridad, ha generado la necesidad de cada vez más profesionales en este sector. A pesar de la cantidad considerable de expertos en ciberseguridad en Euskadi, existe una marcada escasez de talento debido al aumento notorio de la demanda de profesionales. En respuesta a esta situación, el Gobierno Vasco impulsa la educación STEM mediante la estrategia STEAM Euskadi, con el propósito de fomentar la formación y el desarrollo de habilidades en el sector.

En esta línea, y pese a la aparición en los últimos tiempos de diversas iniciativas y estrategias dirigidas a tratar de equilibrar la ferviente demanda con la oferta de profesionales en el sector, se observa una tendencia a que la brecha entre ambas dimensiones continue aumentando. Esto es debido a que la **demandas de profesionales del sector sigue un crecimiento considerablemente superior en comparación al incremento que está experimentando la oferta de profesionales en el sector**, de manera que dicha brecha no se termina de cerrar.

**Proyección de empleo en España**



*Figura 4. Proyección de empleo en España. Fuente: ObservaCIBER*

Para poder paliar y reducir esta brecha en cuanto a necesidad de profesionales, **se está contemplando en las empresas el uso de medidas de reskilling** (perfiles que pese no a estar actualmente familiarizados con el ámbito de la ciberseguridad, se forman y adquieren conocimientos en esta materia). Adicionalmente, en este sector **también se están impulsando una serie de iniciativas por parte de la red de educación de Euskadi a fin de paliar la falta de talento y aumentar el número de profesionales en esta materia**.

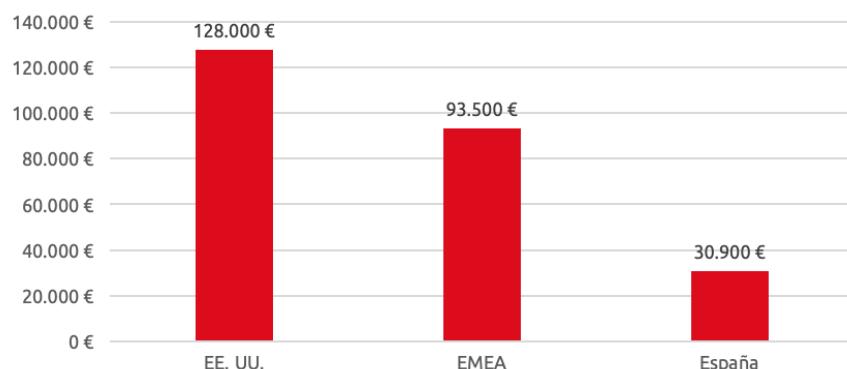


**Las 5 universidades de Euskadi** (UPV/EHU, Universidad de Deusto, Mondragon Unibertsitatea, Tecnun y EUNEIZ) **ofrecen estudios en materia de ciberseguridad** y disciplinas afines, mostrando su compromiso continuo con el desarrollo en este ámbito. Entre ellos, la universidad EUNEIZ ha presentado recientemente su **Grado en Ciberseguridad de 240 ECTS**. Esta iniciativa no solo representa un avance en la diversificación y mejora de la educación en este campo, sino que también ejemplifica el esfuerzo continuo por fortalecer y ampliar las oportunidades de formación en áreas clave como la ciberseguridad, respondiendo así a las demandas cambiantes del entorno socioeconómico y tecnológico de Euskadi.

En lo respectivo al ámbito profesional, a pesar de que el perfil típico de la ciberseguridad se encuentre ligado al perfil técnico de la ingeniería, se trata de un terreno cada vez más amplio, donde, se ha visto acrecentada también la demanda de profesionales que dominen otros ámbitos como puede ser, el jurídico.

Asimismo, se observa una **diferencia salarial notable a nivel regional y estatal en comparación con Europa y EE. UU.**, lo que podría influir en la retención de talento. Esto genera una movilidad considerable entre expertos en búsqueda de compensaciones más acordes con sus expectativas. Sin embargo, es destacable que **en los últimos años se está mostrando en la región una tendencia al alza en lo que a los sueldos en materia de ciberseguridad se refiere, ofreciendo salarios cada vez más competitivos** en la región para expertos en protección de datos, análisis de riesgos y otras áreas clave de la ciberseguridad.

### Salario medio trabajador de ciberseguridad



*Figura 5. Salario medio de trabajadores en ciberseguridad por ámbito geográfico.  
Fuente: (ISC)2 e Indeed*



# Emprendimiento

**Euskadi ha surgido como un territorio destacado para el emprendimiento a nivel estatal**, especialmente en el ámbito de la ciberseguridad vinculada al sector digital. Con un entramado que abarca **más de 100 entidades tanto públicas como privadas**, respaldada por una red de inversores activos, centros tecnológicos de vanguardia, y un apoyo institucional diferencial, Euskadi se erige como un entorno ideal para la gestación, crecimiento y consolidación de startups tecnológicas e innovadoras, incluyendo aquellas especializadas en ciberseguridad. A su vez, este potente ecosistema ha atraído en los últimos tiempos una diversidad de actores privados y públicos, fomentando así un entorno multidisciplinario propicio para el espíritu emprendedor, respaldado por una sólida base normativa, financiera e institucional.

La estrategia institucional, que evoluciona desde los años 80, ha culminado en el **Plan Interinstitucional de Emprendimiento (PIE) 2021-2024**, el tercer ciclo enfocado en proveer herramientas y recursos para el emprendimiento. Iniciativas como la **red de Business Innovation Centers (BICs)** o **BIND 4.0. Basque Open Innovation Platform con sus tres líneas de actividad (4.0, SME Connection y Govtech)**, han ayudado en la aceleración de startups, entre las que destacan aquellas dedicadas a la ciberseguridad, fomentando la innovación y establecido colaboraciones internacionales, evidenciando el carácter innovador y proyectando a nivel global el ecosistema emprendedor de Euskadi.

**Up!Euskadi** se muestra como otra iniciativa relevante en este ámbito. Esta nueva plataforma basada en una innovadora tecnología de machine learning e ingeniería de datos, aporta información de valor, dando visibilidad a las startups y a todos los agentes del ecosistema y posicionando Euskadi como hub de emprendimiento avanzado. En la misma, se muestran también las principales empresas emergentes dedicadas a la ciberseguridad en Euskadi, que, en estos momentos, ascienden a un total de más de 50 atendiendo a los datos que figuran en la plataforma.

**BAT – B Accelerator Tower**, iniciativa respaldada por las instituciones públicas vascas, destaca también en este ámbito por su enfoque personalizado, ofreciendo un **acompañamiento integral desde la concepción de una empresa hasta la búsqueda de colaboradores**, fortaleciendo así la trayectoria hacia el éxito empresarial. Esta combinación de valores distintivos coloca a BAT como un **centro crucial para el emprendimiento e innovación en la región**, comprometido con el crecimiento empresarial y su proyección internacional, trazando una ruta clara hacia el éxito sostenible.

El apoyo brindado mediante estos instrumentos, el respaldo de las instituciones públicas y el constante flujo de inversiones han sido **fundamentales para el crecimiento sostenido del ecosistema de startups de ciberseguridad en Euskadi**. Estas compañías dentro del ecosistema vasco están enfocadas en la innovación, mejorando y fortaleciendo sus servi-

Desde las instituciones públicas de Euskadi, se ofrecen diversos programas y estrategias de apoyo al emprendimiento como son las siguientes: PIE 2023; BICs; BIND; Up!Euskadi; BAT; Beaz Acceleration Program



cios para potenciar el sector y enfrentar un futuro repleto de oportunidades. Gracias a este apoyo y al impulso continuo, la región ha visto florecer a más de **50 empresas emergentes dedicadas a la ciberseguridad**, logrando elevar el valor total de mercado de estas compañías a **142 millones de euros**, previéndose una tendencia similar para los próximos años.

Adicionalmente, cabe señalar que Euskadi cuenta con un **amplio abanico de iniciativas respaldadas por entidades públicas cruciales a la hora de fomentar y favorecer el emprendimiento en la región**. Entre algunas de estas iniciativas de apoyo dirigidas al impulso del emprendimiento destacan: **Ekintzaile, Ekintzaile+, Barnekintzaile, BIND, Basque Fondo, Aurrera, Reto 2030, Basque Tek Ventures, otras**.

### Valor de las startups en Euskadi

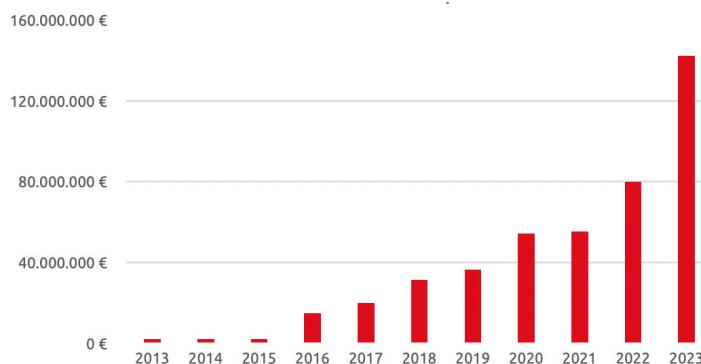


Figura 6. Valor de startups en Euskadi. Fuente: UP!Euskadi

Este conjunto de herramientas, han tenido un impacto significativo en el desarrollo y fortalecimiento de nuevas empresas emergentes de ciberseguridad. Además, alianzas como **BRTA o el Basque Digital Innovation Hub (BDIH)** proveen laboratorios y recursos para apoyar la experimentación necesaria en este sector, con el objetivo de ayudar a diferentes tipologías de empresas en el desarrollo y mejora de sus productos o sus procesos, entre las que destacan también las empresas del tipo startup.



# Cibercrimen

En 2022, la Ertzaintza fue conocedora de un total de 20.147 infracciones penales en el ciberespacio, un 25% más que el año anterior, siendo el más originado el delito de estafa, con un total de 18.107 delitos de esta modalidad

La cibercriminalidad, en constante ascenso a nivel global, se ha convertido en una preocupación primordial en la era digital. El **phishing** y el **ransomware** destacan como amenazas principales, con informes que señalan un récord de **3,4 millones de ataques de phishing en 2022, conllevando a un costo global de 8 trillones de dólares**.

A nivel estatal, se experimentó un aumento del 22.9% en delitos informáticos en 2022, reflejando una realidad similar en Euskadi. Los **informes de la Ertzaintza indican un crecimiento del 25% en los ciberdelitos, con más de 20.000 infracciones en 2022**. El phishing y otras estafas representan el 20.3% de los actos delictivos, evidenciando la importancia de abordar esta problemática.

(CVSS), mostrando un aumento del 31% en los ciberdelitos durante el primer semestre de 2023, siendo la mayoría relacionados con ciberestafas.

En este contexto, resulta **imperativo para regiones como Euskadi adoptar prácticas y medidas de seguridad alineadas con estándares internacionales**. Esto no solo fortalece la protección de datos y sistemas, sino que también contribuye a salvaguardar la integridad digital de comunidades y sectores frente a un panorama global de riesgos en constante evolución.

**Delitos informáticos en Euskadi**



*Figura 7. Delitos informáticos en Euskadi 2021-2022. Fuente: Ertzaintza*



# Tendencias ciberseguridad

El crecimiento en la adopción de tecnologías y el uso extendido de dispositivos electrónicos ha ampliado la superficie de ataque, generando nuevas vulnerabilidades para los cibercriminales. En 2023, los diferentes tipos de malware, como el cryptojacking, el malware IoT y las amenazas de cifrado, han aumentado significativamente, registrando incrementos de hasta un 799% a nivel europeo. El ransomware en particular, muestra un aumento considerable en Euskadi y en otros países, convirtiéndose en una amenaza crítica para infraestructuras y cadenas de suministro.

La profesionalización de los atacantes está llevando a un enfoque más específico en la extorsión, centrado en el cifrado de datos y el robo de información confidencial, buscando obtener compensaciones económicas. Se espera que las técnicas de ransomware y phishing se sofistiquen aún más, incluso desafiando las medidas de protección actuales, como la autenticación multifactorial. Esto subraya la importancia de que las empresas cumplan con las regulaciones de privacidad y ciberseguridad a nivel mundial, europeo y estatal, así como el aumento en la demanda de servicios como Cyber Threat Intelligence (CTI).

La ciberseguridad está ganando un papel esencial en las organizaciones, con un enfoque creciente en roles como el Chief Information Security Officer (CISO) y un incremento en las inversiones en este campo. Las empresas también están intensificando programas de concienciación y formación para mejorar su preparación contra los ciberataques.

El ransomware y el cryptojacking se convierten en las amenazas principales del 2023



Figura 8. Tendencias de ciberseguridad. Fuentes: CCN-CERT, Sealpath y TÜV SÜD



En Euskadi, se proyecta un escenario similar en términos de ciberseguridad. Las tendencias muestran una **sincronización a nivel global, lo que refleja desafíos y avances compartidos en esta materia**. Se prevé un aumento continuo de ciberamenazas en los próximos años, a consecuencia del mayor uso de dispositivos electrónicos conectados a la red y el uso de servicios en la nube, entre otros. Por consiguiente, mantenerse actualizado y progresar hacia un entorno digital más seguro se vuelve fundamental para enfrentar este panorama en constante evolución.

## Entorno regulatorio

El progreso tecnológico representa un **desafío para la ciberseguridad, enfatizando la necesidad de ajustar regulaciones y normativas** ante la evolución de los métodos de ciberataque y afrontar los nuevos retos y riesgos existentes.

Destaca las regulaciones a nivel mundial o europeo, así como su evolución en respuesta al desarrollo tecnológico, mencionando la importancia de la colaboración internacional para abordar las ciberamenazas. Se enfoca en **regulaciones clave como el RGPD de la UE**, que busca proteger la privacidad y seguridad de los datos personales, y el **DORA**, que fortalece la seguridad informática en el sector financiero europeo. Además, se señalan otras normas y directivas, como **CRA – Cyber Resilience Act**, encargada de reforzar las normas de seguridad de cara a que los productos hardware y software sean más seguros; NIS 2 (Network and Information Systems) que, define las normas mínimas relativas al funcionamiento de un marco normativo común, facilitando un mecanismo de cooperación entre las autoridades competentes de cada Estado miembro o, la reciente propuesta de Ley de Inteligencia Artificial que, refleja el objetivo de la UE por liderar en la promoción de un enfoque legislativo integral para respaldar el uso confiable y responsable de los sistemas de IA.

El constante avance en materia tecnológica acarrea retos en materia de ciberseguridad que demandan la adaptación de las regulaciones



EEUU	ESPAÑA
<b>The Cibersecurity Information Sharing Act:</b> <ul style="list-style-type: none"><li>Tiene como objetivo mejorar la ciberseguridad de EEUU</li><li>Fomentar el intercambio de información</li></ul> <b>Strengthening American Cybersecurity Act of 2022:</b> <ul style="list-style-type: none"><li>Objetivo de obligar a los operadores de infraestructuras críticas a notificar a la CISA</li></ul>	<b>Real Decreto 311/2022</b> <ul style="list-style-type: none"><li>Nueva actualización del Esquema Nacional de Seguridad</li></ul> <b>Ley Orgánica 3/2018:</b> <ul style="list-style-type: none"><li>Protección de Datos Personales y garantía de los derechos digitales</li></ul> <b>Real Decreto 43/2021:</b> <ul style="list-style-type: none"><li>Seguridad de las redes y sistemas de información</li></ul> <b>Ley Orgánica 7/2021:</b> <ul style="list-style-type: none"><li>Materia de protección de datos</li></ul>
<b>EUROPA</b>	
<b>RGPD</b> <ul style="list-style-type: none"><li>Garantizar la privacidad y seguridad de los datos de los ciudadanos y armonizar las leyes de privacidad en toda la UE</li></ul> <b>DORA:</b> <ul style="list-style-type: none"><li>Desarrollar plan de respuesta de incidentes</li><li>Programa de evaluación de riesgos</li></ul>	<ul style="list-style-type: none"><li>Notificación de incidentes para evaluar vulnerabilidades.</li></ul> <b>Cyber Resilience Act:</b> <ul style="list-style-type: none"><li>Obligar a los fabricantes a mejorar la seguridad de sus productos durante su ciclo de vida.</li><li>Aumentar la transparencia de las propiedades de seguridad</li></ul>
	<b>NIS2:</b> <ul style="list-style-type: none"><li>Cambiar la directiva actual.</li><li>Objetivo de establecer la base para las medidas de gestión de riesgos de ciberseguridad y las obligaciones de notificación en todos los sectores.</li></ul> <b>Propuesta de Reglamento-Ley de Inteligencia Artificial:</b> <ul style="list-style-type: none"><li>Impone diferentes obligaciones a todos los actores en la cadena de valor de la IA.</li><li>Aplicable a todos los sistemas de IA que afecten a personas en la UE</li></ul>

Figura 9. Regulaciones de ciberseguridad. Fuente: CISA, Comisión Europea, Parlamento Europeo, BOE

En relación con Euskadi, se destaca una evaluación positiva en cuanto a su marco jurídico en ciberseguridad. Este territorio opera bajo el marco estatal de España y la Unión Europea, situándose en el cuarto lugar del Global Cybersecurity Index (GCI). Esto indica que Euskadi cuenta con uno de los marcos legislativos más completos, obteniendo la máxima puntuación en legislación.

Estas regulaciones **impactan significativamente en el entorno empresarial de Euskadi**. En la Administración Pública, se busca salvaguardar datos sensibles y garantizar la integridad de los sistemas, lo que implica implementar estándares más altos de seguridad. En el sector privado, representan tanto un desafío como una oportunidad. Por un lado, imponen requisitos adicionales que las empresas deben cumplir, lo que implica inversiones en tecnología, recursos y formación del personal. Pero, por otro lado, las regulaciones en ciber-



seguridad también podrían generar oportunidades para empresas especializadas en ofrecer soluciones de seguridad, consultoría o servicios relacionados, erigiéndose como nuevos nichos de oportunidad o áreas de negocio para estas.

El tejido empresarial industrial en Euskadi, importante en su economía, debe cumplir con regulaciones como el **Cyber Resilience Act** o la **NIS2**. El cumplimiento de estas normativas puede generar confianza entre clientes y socios comerciales, fortaleciendo la reputación y credibilidad de las empresas en el mercado.

En resumen, las regulaciones en ciberseguridad impulsan a las organizaciones en Euskadi a mejorar sus prácticas de seguridad, adoptando medidas proactivas para proteger la información y contribuyendo a un entorno empresarial más robusto y seguro.

## Sellos de ciberseguridad

---

La evolución de la ciberseguridad ha dado origen a la creación de diversos sellos y estándares destinados a certificar el cumplimiento de requisitos de seguridad informática en productos, servicios y empresas. Estos sellos se fundamentan en criterios estrictos y sólidos establecidos por organizaciones emisoras y ofrecen visibilidad y reconocimiento a quienes los obtienen.



CYBERSECURITY  
MADE IN EUROPE™

Cybersecurity  
made in Europe



Cybersecurity  
Label



Cybersecurity  
Labelling Scheme

Figura 10. Sellos de ciberseguridad. Fuente: elaboración propia

**En Euskadi, cabe señalar que Cybasque puede emitir el sello exclusivo “Cybersecurity Made in Europe”** en los productos de cualquier empresa de ciberseguridad de Europa lo que permite aumentar la visibilidad de las empresas vascas frente a otras compañías y ante los usuarios finales, clientes o diferentes inversores con actividad en el sector. Obtener este tipo de distintivos no solo valida el cumplimiento con normativas exigentes, sino que también proyecta confianza y compromiso con la protección de datos y sistemas digitales.

Los sellos, alineados con estándares de seguridad digital, no solo impulsan la competitividad de las organizaciones, sino que también ofrecen certeza a clientes y colaboradores sobre el compromiso con la seguridad y la integridad de la información en un contexto europeo de confianza digital.



# Agencias de ciberseguridad

Debido al progreso de las nuevas tecnologías, se ha experimentado un aumento significativo en los últimos tiempos en lo que las comunicaciones electrónicas entre ciudadanos, empresas y las diversas Administraciones Públicas se refiere, lo que ha llevado a una mayor exposición frente a diferentes tipos de ciberamenazas. Por ello, resulta fundamental establecer un marco que asegure el adecuado funcionamiento de las infraestructuras digitales, proporcionando una protección efectiva contra las diversas ciberamenazas a las que están expuestas.

El papel de las agencias de ciberseguridad resulta fundamental para fortalecer un entorno ciberseguro

A nivel global, la agencia de referencia es la Cybersecurity and Infrastructure Security Agency (CISA), mientras que a nivel europeo destaca la **Agencia de la Unión Europea para la Ciberseguridad (ENISA)**. En España, el Instituto Nacional de Ciberseguridad (INCI-BE) juega un papel clave en la promoción de la seguridad digital. Otras agencias estatales, como el CCN-CERT, CNPIC y AEPD, también contribuyen al fortalecimiento de la protección digital.

La CAE, lleva varios años implicados en iniciativas y actividades de fomento y apoyo a la ciberseguridad, teniendo especial relevancia los organismos que prestan servicios al Gobierno Vasco, a las Diputaciones Forales, a las principales entidades regionales, así como también a las empresas del territorio.

En este sentido, existen diversos planes de acción orientados a respaldar tanto a los ciudadanos como a las empresas. Entre los organismos destacables en esta materia, se encuentra **SPRI**, que ha venido fomentando arduamente la **cultura de ciberseguridad fundamentalmente entre las empresas del País Vasco**. De esta manera, SPRI, a lo largo de estos últimos años, lleva mostrando un fuerte compromiso con el sector de la ciberseguridad, alimentado por medio de una estrategia clara y plenamente alineada con las particularidades y la realidad del tejido empresarial de la Comunidad Autónoma de Euskadi. Esta estrategia persigue el objetivo primordial de tratar de seguir avanzando hacia la consolidación del tejido empresarial de Euskadi como ecosistema “ciberseguro”, por medio del crecimiento y fortalecimiento del sector de la ciberseguridad de Euskadi.

Para la consecución de dicho objetivo, aprovechándose de las diferentes capacidades del Grupo, SPRI promueve algunas iniciativas e instrumentos de apoyo concretos dirigidos al fortalecimiento del sector y que abarcan ámbitos temáticos específicos tales como el I+D, la innovación, el emprendimiento, la internacionalización, o el acceso a financiación entre otros. Este **apoyo institucional diferencial hace erigirse a SPRI como entidad o agente de referencia en Euskadi** en todo lo relacionado con la ciberseguridad vinculada al ámbito





empresarial, y más concretamente, al ámbito industrial. Al mismo tiempo que favorece y contribuye de forma directa al crecimiento tan notable que está experimentando el sector en los últimos tiempos.

Por otro lado, es preciso mencionar el Centro de Ciberseguridad Industrial de Gipuzkoa, conocido como **ZIUR** y creado por la Diputación Foral de Gipuzkoa, tiene como objetivo principal fortalecer la protección de las empresas industriales y sus productos o servicios frente a ciberataques. Su enfoque se centra en mejorar la capacidad de ciberseguridad de las empresas en la región, ayudándolas a identificar sus necesidades en ciberseguridad y encontrar soluciones adecuadas.



Se destaca la creación de la *Agencia Vasca de Ciberseguridad, llamada "Cyberzaintza"*. Euskadi ha decidido desarrollar un proyecto común con el objetivo de fortalecer y dirigir la coordinación de los recursos disponibles y así, elevar a un nivel superior el nivel de madurez de ciberseguridad en el territorio, creando "Cyberzaintza". Esta nueva agencia ubicada en el Parque Tecnológico de Araba (Miaño), nace para lidiar con las amenazas procedentes del uso de internet y las nuevas tecnologías en Euskadi. La agencia depende del Departamento de Seguridad del Gobierno Vasco y, en coordinación con la Ertzaintza vigilará y coordinará la lucha contra el cibercrimen y los ciberataques dentro del territorio.

Entre otras funciones específicas, destacan la de **trabajar en conjunción con los organismos nacionales o internacionales para disminuir los efectos y los daños causados por posibles ataques** como equipo de respuesta a emergencias (CERT) y de respuesta ante incidentes de ciberseguridad (CSIRT).

En resumen, las iniciativas llevadas a cabo por las instituciones públicas en materia de ciberseguridad resultan fundamentales para abordar los desafíos actuales y futuros en el ámbito digital. El trabajo conjunto de estas entidades promueve un entorno más seguro y confiable, garantizando la protección de los datos y la continuidad de las operaciones tanto a nivel nacional como internacional.



# Ciberseguridad Industrial





La Industria Inteligente ha marcado un cambio transcendental en el panorama global, impulsada por una conectividad y automatización sin precedentes.

Sin embargo, tal y como se indica a lo largo del presente estudio, esta transformación no está exenta de desafíos. La creciente **interconexión de los sistemas** y el importante incremento en cuanto a dispositivos industriales conectados a Internet, ha abierto las puertas a un **aumento significativo en el número vulnerabilidades**, posicionando a la ciberseguridad industrial como un pilar fundamental en la protección de sistemas y de cara a garantizar la continuidad de las empresas que operan en este tipo de entornos.

El mercado de la ciberseguridad industrial, valorado en 15,1 mil millones de dólares en 2022, **proyecta un crecimiento exponencial**, con una CAGR del 5,1% hasta 2032. En este sentido, las pymes, a pesar de dominar el mercado, se enfrentan a una mayor exposición de ataque debido a sus limitaciones financieras y a la falta de recursos.

En cuanto a los ataques se refiere, desde hace varios años se está produciendo un **incremento de ataques hacia infraestructuras industriales**, directamente relacionados con las vulnerabilidades presentes en estos entornos. Ha sido notorio en este sentido, los ataques a aquellas infraestructuras industriales que cuentan con sistemas SCADA, además, este tipo de ataques no se producen hacia un sector en concreto, sino que, son generalizados.

En el año 2022, se registraron un total de 338 incidentes de ciberseguridad industrial a nivel estatal, caracterizados por vulnerabilidades recurrentes como la validación incorrecta de parámetros de entrada, el Cross-Site Scripting y el desbordamiento de búfer basado en pila, lo que subraya la necesidad de utilizar las mejores prácticas a la hora de desarrollar software industrial. Además, muchos de estos fallos vienen derivados del mundo de TI, por lo que es posible seguir ejemplos de desarrollo para evitar cometer los mismos errores.

Cabe destacar que la **limitación presupuestaria se presenta como un desafío significativo** para la materialización efectiva de estrategias de ciberseguridad de aplicación en estos entornos industriales. En este contexto, normativas europeas, como la Directiva 2008/114/CE, se erigen con el propósito de fomentar la adopción de medidas más robustas en materia de ciberseguridad en estos entornos. Estándares reconocidos, como la norma **IEC 62443** y guías específicas, como el NIST SP 800-82, son también empleados con el fin de elevar los estándares en la gestión de ciberseguridad industrial.

De esta manera, las actualizaciones normativas van cobrando cada vez mayor relevancia. En este sentido, el organismo ISA99 desarrolló una serie de estándares, los IEC 62443 que deben ser aplicados a todos los sistemas de control industrial ICS. El estándar describe los requisitos básicos para minimizar los riesgos de seguridad de los fabricantes de componentes, los integradores de sistemas y los exportadores.

Euskadi, a través del BDIH, cuenta con un nodo específico en ciberseguridad compuesto por 5 laboratorios mediante los que poder dar respuesta a la especialización en este ámbito



Asimismo, la Guía **NIST SP 800-82** de diseño y configuración de redes industriales es un documento de orientación publicado por el Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos. Aborda la seguridad en los sistemas de control industrial, facilitando una visión general de los ICS y las características típicas de los sistemas, identificando amenazas y vulnerabilidades, y las medidas preventivas correspondientes.

En cuanto a los desafíos futuros de la ciberseguridad industrial, se vislumbra la necesidad de la integración de soluciones de seguridad en la nube como la principal tendencia. Adicionalmente, se anticipa un aumento global de ciberataques en el sector industrial, entre las que destacan, las amenazas como cambios en las APT, el incremento de precios en hardware y energía, las inconsistencias en la nube debido al uso de múltiples proveedores, los riesgos asociados al trabajo híbrido, los ataques de ingeniería social y el enfoque en vulnerabilidades de autenticación multifactorial (MFA).

Por su parte, a la hora de hablar del ecosistema de ciberseguridad industrial, es digno de mención el panorama emergente en cuanto a hubs de ciberseguridad. A nivel europeo, se cuenta con los **European Digital Innovation Hubs** (EDIH) que destacan por su enfoque en digitalización aplicada a la industria. En este sentido, se encuentra con un ecosistema escaso y sin hubs específicos o concretos de ciberseguridad industrial. No obstante, encontramos varios hubs dedicados a la digitalización e innovación en el entorno industrial, como por ejemplo: FactoryXChange, AI5production hub o DIH4AIsec.

A nivel estatal, diversos hubs concentran sus esfuerzos en la transformación digital y la ciberseguridad industrial, sirviendo como ejemplo de ello los siguientes: Digital Impulse hub, Agora DIH, EDIH Madrid Region o InnDIH.

Euskadi busca posicionarse como un hub en ciberseguridad industrial de reconocimiento internacional, respaldado por la sinergia entre la madurez digital de su sector industrial, la fortaleza de su ecosistema tecnológico y el excepcional nivel de competencia en ciberseguridad

**A nivel regional, en Euskadi, cabe mencionar el BDIH (Basque Digital Innovation HUB)** que se configura como una iniciativa que responde a la especialización inteligente RIS3 del territorio con el objetivo de apoyar al tejido empresarial en la experimentación de innovaciones digitales y sostenibles. Esta iniciativa está compuesta por una red de activos y servicios para la formación, investigación, testeo y validación de tecnologías a disposición de las empresas. El BDIH cuenta con un **nodo específico en ciberseguridad** compuesto por 5 laboratorios distintos distribuidos por los tres territorios históricos Araba, Gipuzkoa y Bizkaia, que tienen como objetivo incentivar y fomentar la experimentación y la I+D+i dentro de este ámbito.

En Euskadi, la **rica trayectoria industrial** ha servido como impulso para la implementación de estándares de seguridad y para la colaboración entre distintos sectores, reconociendo que la ciberseguridad juega un papel crucial en la continuidad y competitividad de la industria. Esta conexión entre la herencia industrial y el foco actual en ciberseguridad evidencia que Euskadi no solo abraza su legado industrial, sino que también se esfuerza por adaptarse y resguardarse en un entorno cada vez más digitalizado y susceptible a las ciberamenazas.



Este **enfoque proactivo** en el ámbito de la ciberseguridad responde a la conciencia de las empresas e instituciones en Euskadi sobre la importancia de mantenerse a la vanguardia en este campo. No solo buscan proteger sus operaciones sino salvaguardar la estabilidad y confiabilidad de las infraestructuras críticas que sustentan la economía local. Estos esfuerzos continuos se materializan en acciones concretas, como el fortalecimiento de sistemas, la promoción de una cultura de ciberseguridad y la atención constante a las innovaciones y tendencias que puedan influir en la seguridad de las operaciones industriales de la región.

**En Euskadi, la ciberseguridad industrial ocupa un lugar prioritario** debido a su histórico enfoque industrial. El ecosistema tecnológico en Euskadi destaca por su robustez, actuando como un catalizador para consolidar al territorio como un hub en ciberseguridad industrial de referencia internacional. Este entorno propicio, no solo **facilita la adopción de soluciones de vanguardia, sino que también promueve la colaboración entre empresas, instituciones y centros de investigación.**

La estrategia de Euskadi para posicionarse como un hub de reconocimiento internacional en ciberseguridad industrial recibe respaldo de la **sinergia entre la madurez digital de su sector industrial, la fortaleza de su ecosistema tecnológico y el excepcional nivel de competencia en ciberseguridad**. Esta combinación única de factores no solo fortalecerá la resiliencia del entorno industrial regional, sino que también permitirá proyectar el territorio como un referente a nivel mundial en lo relacionado con la protección de la industria. En este contexto, Euskadi cuenta con todos los elementos necesarios para materializar su visión de liderazgo en los próximos años dentro del ámbito de la ciberseguridad industrial.



# Instrumentos de apoyo a la ciberseguridad





Tanto a nivel estatal como regional, las instituciones públicas han implementado diversos programas y ayudas destinadas a impulsar la transformación digital, integrando en ellos iniciativas específicas relacionadas con la ciberseguridad. En relación con los instrumentos de apoyo a la ciberseguridad que impactan en Euskadi, a nivel nacional convendría mencionar la Agenda Digital de España. Esta agenda tiene como objetivo mejorar las capacidades de ciberseguridad en el Estado, impulsar el desarrollo empresarial en el sector (industria, investigación, desarrollo e innovación, y talento) y consolidar el liderazgo internacional en seguridad digital.

Por otro lado, se encuentra el **Plan de Recuperación, Transformación y Resiliencia (PRTR)**, uno de los ejes transversales de España Digital. Este plan integral busca la recuperación económica tras la crisis generada por la pandemia con el objetivo de modernizar el tejido productivo, fomentar la innovación y fortalecer la resiliencia del país. La ciberseguridad se integra transversalmente en varios componentes del Plan de Recuperación, reconociendo su importancia en un entorno digital cada vez más presente. Este reconocimiento se debe al aumento de la presencia de ciudadanos, empresas y administraciones públicas en el mundo digital, donde la seguridad cobra una importancia crucial.

La “**Adenda**”, segunda fase del Plan de Recuperación busca impulsar **inversiones alineadas** a la estrategia digital europea y se enfoca en tres áreas clave: infraestructuras y/o tecnología, economía y personas. Además, con el objetivo de fortalecer el entorno de seguridad digital y **ciber resiliencia**, entre otros, nacen programas de impacto económico, como el **Programa Kit Digital** impulsado por **red.es**. Este programa ha sido creado para respaldar la transformación digital de pequeñas empresas, microempresas y autónomos y tiene como objetivo acompañarlos en la adopción de soluciones y productos digitales que mejoren su madurez digital, destacándose entre ellos, la presencia de productos y soluciones de ciberseguridad.

Es preciso mencionar también las **Redes Territoriales de Especialización Tecnológica (RETECH)**, que, impulsadas por el Plan de Recuperación, Transformación y Resiliencia de España, son herramientas clave para llevar a cabo la transformación digital a nivel nacional.

RETECH representa una iniciativa impulsada por la Secretaría de Estado de Digitalización e Inteligencia Artificial del Gobierno de España en agosto de 2022, la cual persigue una cooperación interregional entre diferentes Comunidades Autónomas, al mismo tiempo que va destinada a impulsar el desarrollo de ecosistemas tecnológicos. En particular, RETECH Ciberseguridad, coordinado por INCIBE, es una iniciativa estratégica que impulsa el ecosistema de ciberseguridad en España. En su primera etapa, involucra a 15 comunidades autónomas con un presupuesto inicial de 149 millones de euros y se encuentra estructurado en 3 nodos, en donde **Euskadi forma parte del primer nodo** junto con otras Comunidades Autónomas (Andalucía, Castilla y León, y Comunidad de Madrid). Enfocado en movilidad, aeroespacial, industria inteligente, energía, salud y Smart Cities, el proyecto correspondiente a este primer nodo integra nuevas infraestructuras, equipos y recursos para promover su especialización y facilitar la integración de la ciberseguridad en sectores considera-

Euskadi cuenta con un ecosistema robusto en lo que a instrumentos de apoyo se refiere. Dirigidos a diferentes ámbitos tecnológicos, en donde la ciberseguridad cuenta con un papel protagonista



dos como estratégicos para cada una de estas regiones. De esta manera, cada comunidad adopta un sector específico, siendo la industria inteligente y la energía los sectores específicos en el de Euskadi.

El enfoque de RETECH Ciberseguridad no solo se limita a reunir a las comunidades autónomas, sino que también busca establecer una **colaboración entre INCIBE y las comunidades autónomas para fortalecer la ciberseguridad** en sectores productivos estratégicos. Esta estructura, con la participación de las comunidades autónomas y sus ecosistemas de ciberseguridad, se integra en la Comunidad Nacional Española asociada al Centro Europeo de Competencia en Ciberseguridad, donde INCIBE asume el rol de Centro de Coordinación Nacional (NCC-ES).

Además, en este contexto, las universidades y el ámbito de la investigación desempeñan un papel esencial. Se reconoce que, sin investigación, desarrollo e innovación, la ciberseguridad no puede avanzar, y sin ciberseguridad, la transformación digital se enfrenta a obstáculos significativos. De esta manera, INCIBE ha promovido la creación de la **Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC)** como una asociación sectorial nacional que actúa como representante del ámbito investigador estatal en ciberseguridad. RENIC está compuesta por centros de investigación, instituciones tecnológicas y universidades tanto públicas como privadas, convirtiéndose en un espacio abierto, inclusivo y participativo que brinda servicios a toda la comunidad investigadora en el ámbito de la ciberseguridad a nivel nacional.

Otro de los programas, a nivel nacional, es el programa **Activa Ciberseguridad** que, impulsado por el Ministerio de Industria y Turismo del Gobierno de España, la secretaría General de Industria ha puesto en marcha junto con la Escuela de Organización Industrial. Orientado a todo tipo de pymes, el objetivo del programa no es otro que apoyar la realización de evaluaciones o diagnósticos en empresas en materia de ciberseguridad, con el fin de comprender su nivel de protección, así como con vistas a desarrollar un Plan de Ciberseguridad adaptado a las necesidades particulares de cada una de estas empresas.

A nivel de **Euskadi**, se cuenta con varios planes estratégicos orientados principalmente a la innovación y transformación digital. Asimismo, existen otra serie de planes que, si bien no son específicamente de tecnología y que, pese a no haber sido objeto del presente estudio, favorecen también al crecimiento y mejora de la competitividad de cualquier tipo de empresas como, por ejemplo, de empresas que focalizan su actividad dentro del ámbito de la ciberseguridad.

**El Plan de Ciencia, Tecnología e Innovación (PCTI) 2030** es la pieza clave que simboliza la decidida apuesta de Euskadi por la investigación y la innovación. Más allá de ser un documento estratégico, encarna el compromiso arraigado de la sociedad vasca por forjar un futuro prometedor. Su visión se centra en **potenciar la ciencia, la tecnología y la innovación para agilizar la transición hacia una Euskadi que sea digital, sostenible e inclusiva**. Este plan abarca tres áreas: tecnológica y digital, energética y climática, social y sanitaria.

Por otro lado, la **Estrategia para la Transformación Digital de Euskadi 2025 (ETDE2025)** representa un nuevo paradigma en la relación entre la Administración Pública Vasca y los sectores económicos y sociales, buscando abordar de manera conjunta los desafíos globales a través de la transformación digital. Esta estrategia se basa en tres dimensiones clave: palancas tecnológicas (6), habilitadores de apoyo (10) y ámbitos de aplicación (14). La selección de las palancas tecnológicas se ha realizado considerando su potencial disruptivo a corto, medio y largo plazo en relación con los desafíos planteados en las tres transiciones principales. Siendo una de estas palancas tecnológicas, la ciberseguridad.



Las **líneas de actividad** principales de estos planes estratégicos se materializan en forma de **instrumentos de apoyos para las empresas**, favoreciendo la aparición y ejecución de proyectos tecnológicos que contribuyan al desarrollo económico de la región. Estos instrumentos se dirigen a diferentes ámbitos tecnológicos, en donde la ciberseguridad cuenta con un papel claramente protagonista. A continuación, se presentan algunos de estos instrumentos de apoyo:

### **Hazitek**

Se trata de ayudas dirigidas a grandes empresas, pymes y asociaciones de empresas vascas para apoyar la ejecución de proyectos de investigación industrial o desarrollo experimental competitivos y estratégicos en el tejido empresarial del País Vasco y en las áreas de especialización del Plan Euskadi 2030 de Ciencia, Tecnología e Innovación. Cuenta con un presupuesto total de 90.000.000€ para dos líneas de apoyo diferenciadas:

- **Proyectos I+D de carácter competitivo:** orientados a la introducción de nuevos negocios de base científica y tecnológica, así como nuevos productos, procesos y servicios. Se pueden realizar de forma independiente o colaborativa, y se necesita un presupuesto mínimo de 100.000€.
- **Proyectos de carácter estratégico I+D:** concebidos por la dirección empresarial y ejecutados con el apoyo de las capacidades científicas y tecnológicas del País Vasco. Deben llevarse a cabo por no menos de 4 millones de euros y por no más de tres años.

### **Elkartek**

El propósito del programa de subvenciones para la investigación colaborativa Elkartek 2023 es fomentar Proyectos de Investigación Fundamental Colaborativa, Investigación con alto Potencial Industrial y otras actividades complementarias de especial relevancia, centradas en mejorar la competitividad en áreas como la industria inteligente, las energías más limpias y la salud personalizada. Estas subvenciones se dividen en tres tipos de proyectos:

- **Proyectos de Investigación Fundamental Colaborativa.** Estos proyectos innovadores de carácter estratégico son desarrollados por entidades dentro de la RVCTI y buscan expandir los conocimientos en áreas clave como la industria inteligente, la energía y la salud. El presupuesto total por proyecto debe ser de al menos 1 millón de euros.
- **Proyectos de Investigación con Alto Potencial Industrial.** Estos proyectos se enfocan en la investigación fundamental orientada o la investigación industrial y son liderados por Unidades de I+D Empresariales pertenecientes a la RVCTI, con una alta capacidad para influir y penetrar en el mercado. El presupuesto total de por proyecto debe ser de al menos 200.000 euros.
- **Acciones Complementarias de Especial Interés.** Iniciativas de intermediación entre la oferta y la demanda tecnológica, exclusivamente desarrolladas por Organismos de Intermediación Oferta-Demanda y Organismos de Difusión de la RVCTI, tales como: estudios de prospectiva y vigilancia; acciones para fomentar la cooperación y brindar asesoramiento para proyectos I+D+i; Gestión de I+D+i y transferencia vinculadas a proyectos; Actividades de internacionalización relacionadas con proyectos de investigación fundamental e industrial.



## Azpitek

Apoyo a los agentes de la RCVTI (Red Vasca de Ciencia, Tecnología e Innovación) para la adquisición e instalación de equipamiento científico-tecnológico. El programa ofrece subvenciones de hasta el 100% de la inversión en infraestructura científico-tecnológica, con el objetivo de promocionar e impulsar nuevas líneas de investigación y desarrollo en materias estratégicas como la Industria Inteligente, Energías más limpias y Salud Personalizada. Del mismo modo, también persigue el poder avanzar en la transición tecnológico-digital, dentro de la cual la ciberseguridad destaca como una de las líneas maestras.

## BDIH Konexio

Un total de 992.360 € para apoyar a aquellas empresas industriales y de servicios conexos ligados al producto-proceso industrial. Se trata del apoyo a la incorporación de tecnologías digitales y sostenibles en el diseño y desarrollo de bienes y servicios prestados por las empresas manufactureras a través de proyectos de estudio de viabilidad, orientación y asistencia técnica sobre los recursos que componen BDIH en las áreas de robótica flexible y colaborativa, fabricación aditiva, ciberseguridad, máquinas conectadas, materiales avanzados, dispositivos médicos, salud y electricidad digitales.

## Programa Kloud

Con un presupuesto de 800.000 € dirigidos a empresas del sector industrial y de servicios conexos ligados al producto-proceso industrial, para apoyarlas en la migración de equipos presentes en sus salas técnicas y CPDs On-premise a entornos cloud, que como se ha comprobado a lo largo de estos años proporcionan con carácter general niveles más altos en términos de ciberseguridad.

## Smart Industry

Representa una evolución de Basque Industry 4.0 y respalda proyectos de Investigación Industrial y Desarrollo Experimental, ofreciendo hasta 300.000 € para proyectos que se centren en la transferencia de tecnología desde instituciones I+D hacia empresas del ámbito industrial en fabricación avanzada. El propósito principal es equipar a las empresas vascas con los recursos y herramientas necesarios para incorporar innovaciones provenientes de proveedores tecnológicos, mejorando así su competitividad y posición en los mercados. Estas subvenciones están dirigidas a empresas industriales o relacionadas con la industria, así como a servicios avanzados que colaboren con instituciones I+D en proyectos centrados en las TICs aplicadas a la industria inteligente. Los proyectos a los que se dirigen deben estar relacionados con áreas como Ciberseguridad, Cloud Computing, IA, y Computación Cuántica entre otros, dentro del ámbito de los Cyber Physical Systems (CPS) aplicados a la fabricación avanzada.

Por otro lado, el Gobierno Vasco, a través del Grupo SPRI, puso en 2018 en marcha el **programa de ayudas de Ciberseguridad Industrial**. El lanzamiento del programa no fue más que otra muestra del fuerte compromiso del Departamento de Desarrollo Económico, Sostenibilidad y Medioambiente del Gobierno Vasco con la ciberseguridad, tratando de avanzar en su estrategia por favorecer al crecimiento o a la mejora de la ciberseguridad del tejido empresarial de Euskadi, por medio del fortalecimiento y el apoyo a los diferentes agentes que componen el ecosistema de la ciberseguridad en el territorio.



Figura 2. Programa ciberseguridad industrial

De esta manera, el programa va dirigido a empresas industriales o de servicios conexos ligados al producto-proceso industrial, persigue el apoyar proyectos que contribuyan a elevar o mejorar el nivel de ciberseguridad de estas empresas de forma significativa. Concretamente, el programa trata de generar una base sólida de ciberseguridad entre las empresas, con el objetivo de que puedan encarar los desafíos de ciberseguridad futuros desde una posición más privilegiada y una mayor preparación.

En lo que respecta a la modalidad y a la cuantía de estas ayudas, el presupuesto global aceptado del proyecto se constituye por la suma de gastos aprobados en Consultoría e Ingeniería, además del presupuesto aprobado en hardware y software, estableciéndose el límite de subvención en 18.000 € por empresa y año. Los proyectos objeto del programa deben de ser realizados por empresas externas y expertas en el campo de la ciberseguridad.

Hasta el momento son alrededor de 1.000 las empresas que se han podido beneficiar del programa de ayudas, lo que ha supuesto la ejecución de unos 1.610 proyectos de ciberseguridad por un valor total de alrededor de 32,5 millones de euros, y realizados por más de 155 proveedores que ofrecen soluciones o servicios de ciberseguridad en Euskadi. A nivel de presupuesto, también el programa ha sufrido un incremento importante a lo largo de estos años, hasta alcanzar una cifra de 3.5 millones de euros para apoyar proyectos en cada una de las convocatorias de 2021, 2022 y 2023. En total, teniendo en consideración las seis convocatorias, desde el Departamento de Desarrollo Económico, Sostenibilidad y Medioambiente de Gobierno Vasco, se ha destinado un total de 14,8 millones de euros al programa. Cifra nada desdeñable e indicativo de la importancia y de lo estratégico de este ámbito para el Departamento, desde el cual se quiere seguir apostando por este apoyo institucional diferencial con el objetivo de posicionar a Euskadi como hub internacional en lo referente a la ciberseguridad industrial.



A nivel de distribución geográfica, como se puede apreciar en los datos de los últimos años, prácticamente la mitad de los proyectos aprobados se corresponderían con proyectos presentados por empresas de Gipuzkoa. Algo ciertamente habitual en las diferentes líneas y programas de ayuda gestionados tanto por SPRI como por el Departamento de Desarrollo Económico, Sostenibilidad y Medioambiente.

**Proyectos aprobados 2021**  
Total: 404 expedientes

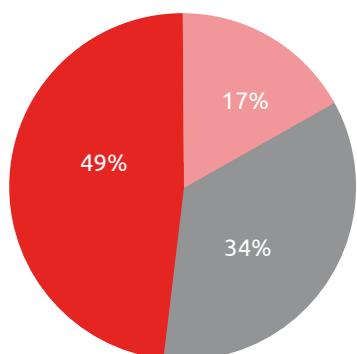


Figura 27. N.º de proyectos aprobados por territorio histórico 2021. Fuente: SPRI

**Proyectos aprobados 2022**  
Total: 349 expedientes

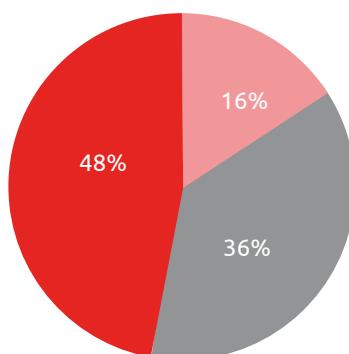


Figura 28. N.º de proyectos aprobados por territorio histórico 2022. Fuente: SPRI

**Proyectos aprobados 2023**  
Total: 362 expedientes

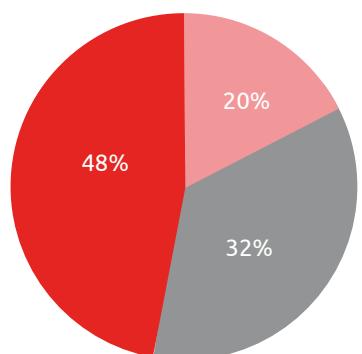


Figura 29. N.º de proyectos aprobados por territorio histórico 2023. Fuente: SPRI

■ Araba ■ Bizkaia ■ Gipuzkoa

A la hora de realizar el mismo análisis a nivel de número de empleados, cabe destacar el papel de las **empresas de entre 10 y 49 empleados, las cuales son las que más proyectos presentan y se benefician en mayor medida del programa Ciberseguridad Industrial**. Del mismo modo, atendiendo a las cifras de la última convocatoria, de ahí se extrae que el 58% de los proyectos aprobados en la convocatoria fueron en empresas de entre 1 y 49 empleados.

Estos datos, permiten entrever cierta tendencia en lo que se refiere a las empresas de menor tamaño. La ciberseguridad ha dejado de ser cuestión de solo grandes empresas, hasta el punto de que se ha convertido en una de las principales preocupaciones de las pymes. Si bien es verdad que muchas de éstas abogan por un enfoque más reactivo en términos de ciberseguridad y carecen de estrategia a largo plazo, sí que se observa al menos voluntad para mejorar dentro de este ámbito. Es el caso de las empresas que pese a tener un tamaño limitado, deciden realizar proyectos y acometer inversiones año tras año dentro de este campo. Con carácter general se trata de proyectos que, si bien no persiguen la excelencia, si resultan francamente necesarios para estas empresas. Hablamos de actuaciones tales como la implanta-



ción de dispositivos para la seguridad perimetral tipo Firewalls, o el diseño y ejecución de nuevas arquitecturas de red que permitan a estas empresas ganar en robustez frente a posibles amenazas. En ambos casos, se observa que la mayoría de los proyectos van dirigidos a entornos IT, y no tanto así a entornos operacionales.

Otro análisis interesante es el de las empresas apoyadas por Sector de Actividad. En este apartado, destacan las empresas industriales dedicadas a la manufactura. Además, se observa cierta masa crítica en otros sectores que, pese a no ser industriales, ofrecen servicios conexos a la industria ligados al producto-proceso industrial. Sectores de actividad tales como el de "Actividades profesionales, científicas o técnicas", "Comercio al por mayor", "información y comunicaciones", o "construcción".

### Proyectos Aprobados por Sector de Actividad



Figura 34. N.º de proyectos aprobados por Sector de Actividad.

Fuente: SPRI

En lo que respecta a la tipología de proyectos aprobados, es digno de mención el incremento que han experimentado los proyectos relacionados con la adopción de **buenas prácticas y procesos de certificación dirigidos a la obtención y cumplimiento** de diversas normas de Ciberseguridad industrial (por ejemplo, IEC 62443, TISAX o equivalentes) u otros estándares de gestión de la Ciberseguridad (por ejemplo, ISO 27001, CAB o equivalentes). Atendiendo a los datos de la última convocatoria, uno de cada cinco proyectos aprobados se correspondió con esta tipología.

Este auge, se entiende que viene derivado o es el resultado del contexto regulatorio o normativo actual, así como por algunos controles en forma de requisitos que están imponiendo determinados clientes a sus proveedores en sectores tales como la automoción, el sector aeronáutico o la propia administración pública. De ahí que diferentes **empresas de Euskadi tengan que hacer un esfuerzo por adecuarse a dichos requisitos** y avanzar hacia la certificación en estos estándares o en estas normas.



## Apoyo a la Ciberseguridad a nivel provincial: Iniciativas Innovadoras Impulsadas por las Diputaciones Forales en Euskadi

En los próximos años, se espera que esta tendencia siga experimentando un crecimiento importante, debido fundamentalmente a un **entorno altamente cambiante dentro del campo normativo y regulatorio**, el cual ha sufrido importantes variaciones en los últimos meses, con la llegada de directivas como la NIS2 o el CRA – Cyber Resilience Act entre otros.

En definitiva, el programa busca establecer una base sólida de ciberseguridad en las empresas del territorio para que se puedan enfrentar futuros desafíos desde una posición más sólida. Este enfoque ha generado interés y beneficios para numerosas empresas, permitiéndoles abordar proyectos de ciberseguridad que de otra manera podrían no haberse materializado debido fundamentalmente a la falta de recursos y expertise en este campo.

A nivel provincial, también se han llevado a cabo diferentes iniciativas para impulsar el mercado de ciberseguridad en la región. Concretamente, desde la **Diputación Foral de Gipuzkoa** se ofrecen diversas ayudas en innovación y tecnología, especialmente aquellas relacionadas con la ciberseguridad. Estas incluyen subvenciones específicas destinadas a distintos ámbitos:

- **Gipuzkoa digitala: Ciberseguridad en la CADENA DE VALOR.** Esta ayuda tiene como objetivo regular la asignación de subvenciones para facilitar la adaptación o implementación de normativas y certificaciones de ciberseguridad en la gestión de la información. Está dirigida a pymes que operan en Gipuzkoa y que apliquen los resultados del proyecto a estas instalaciones.
- **Gipuzkoa digitala: Ciberseguridad para EMPRESAS.** Dirigida a pymes radicadas en Gipuzkoa que desarrollen actividades industriales, servicios técnicos ligados al proceso productivo, así como a aquellas del ámbito de la sociedad de la información y las comunidades. Su objetivo es regular la concesión de subvenciones para impulsar la implantación de la ciberseguridad en estas empresas.
- **Gipuzkoa digitala: Producto industrial ciberseguro.** Su finalidad es impulsar el desarrollo de proyectos de evaluación de la seguridad de productos industriales. Las empresas beneficiarias serán aquellas que cuenten con un producto propio y desarrollen su actividad en Gipuzkoa. Es crucial que los resultados del proyecto tengan una aplicación directa en estas instalaciones.

De igual forma, la **Diputación Foral de Bizkaia** cuenta con el “**Programa Transición Digital y Verde**” que, mediante el Departamento de Promoción Económica de Bizkaia, ofrece apoyo financiero a pymes de diversos sectores para impulsar la digitalización y la sostenibilidad ambiental en las empresas del territorio. El propósito del programa es fomentar la integración de tecnologías digitales y métodos sostenibles, fortaleciendo la competitividad y la capacidad de recuperación de las empresas en un contexto económico dinámico y cambiante que contiene 4 líneas de subvención.

- **Línea 1:** desarrollo de planes para la digitalización básica, avanzada o la innovación ambiental y economía circular, con asesoramiento de expertos.
- **Línea 2:** proyectos para mejorar los procesos de valor de la empresa mediante la digitalización básica. Incluye la implementación de Tecnologías de la Electrónica, la Información y las Telecomunicaciones como: comercio electrónico, siste-



mas avanzados de gestión empresarial, control de procesos productivos, logística, ciclo de vida del producto, automatización industrial, integración de datos operativos, y **ciberseguridad**.

- **Línea 3:** proyectos para mejorar productos/servicios y procesos de valor mediante la digitalización avanzada. Implica el uso de Tecnologías de la Electrónica, la Información y las Telecomunicaciones sofisticadas, como IA, machine learning, cloud computing, blockchain, simulación 3D, integración de datos con la cadena de valor, interacción persona-máquina avanzada, sistemas ciber físicos, visión artificial, y aplicaciones de metodologías y conectores en el procesamiento de datos.
- **Línea 4:** proyectos para mejorar la sostenibilidad ambiental, alineados con la economía circular, que impacten en los procesos de valor, productos/servicios o modelo de negocio de las empresas.

En cuanto a lo referente a la **Diputación Foral de Álava**, se ofrece el programa “**Álava Innova – Digitaliza**” que cuyo objeto es promover la innovación y la digitalización en Álava mediante la concesión de subvenciones en régimen de concurrencia competitiva a aquellas entidades que realicen actuaciones que coadyuven a la modernización económica y a la mejora de la competitividad del tejido productivo alavés.

El programa está destinado a las Pymes, Autónomos y Asociaciones con domicilio en el Territorio Histórico de Álava y que realicen actuaciones que se encuadren dentro de actividades innovadoras como la introducción del uso intensivo de tecnologías digitales en todos los procesos de las empresas. Entre estas actividades se encuentra la automatización, la monitorización remota, la teleasistencia, el teletrabajo, la ciberseguridad, el big data, la fabricación aditiva e impresión 3D, la robótica colaborativa y flexible, la inteligencia artificial, la realidad aumentada y realidad virtual, **plataformas cloud, los sistemas ciberfísicos o el internet de las cosas**.

Estas ayudas demuestran el compromiso también a nivel provincial a la hora de fortalecer la ciberseguridad y promover la innovación en diversas áreas empresariales

Con todo esto, cabe reconocer a Euskadi **como una región enormemente comprometida con lo que es la transformación digital** tanto de la sociedad, como de los diferentes ámbitos o sectores que conforman la economía de la región, y en donde la **ciberseguridad resulta prioritaria e imperativa** para favorecer no solo al desarrollo económico de la región, sino también para garantizar la continuidad en todo momento del tejido empresarial de Euskadi. De esta manera, tal y como se desprende de los apartados anteriores, el progreso y avance en esta línea se ve respaldado por medio de un apoyo institucional diferencial, el cual se pone de manifiesto en forma de diferentes estrategias e instrumentos de apoyo para las empresas.

# Ecosistema de ciberseguridad en Euskadi



El ecosistema de ciberseguridad en Euskadi se compone de entidades privadas y públicas especializadas que se dedican a proveer servicios y soluciones en esta área en el que se muestra una diversidad considerable, albergando una variedad de agentes que van desde grandes corporaciones multinacionales hasta empresas de menor escala, como las pymes.

Se destaca principalmente la presencia de organizaciones dedicadas a la consultoría e integración de soluciones frente al resto de los sectores.

Por su parte, el **entramado industrial en Euskadi** demuestra una sólida capacidad para integrar diversas tecnologías ligadas a la manufactura, como la automatización y la optimización de procesos. Por eso, resulta crucial desarrollar procesos de fabricación inteligente que se adapten ágilmente a las necesidades y dinámicas de producción, así como asignar de manera más eficiente los recursos disponibles. En estos procesos, se trabaja para incorporar la ciberseguridad desde la fase inicial de diseño en los productos y servicios ofrecidos. Además, es importante ajustar los modelos de costos para que incentiven a los usuarios a considerar la ciberseguridad como un valor esencial, resaltando que no implementar medidas de protección puede acarrear graves consecuencias. La concienciación, educación y capacitación juegan un papel fundamental para garantizar un nivel adecuado de seguridad en este ámbito.

## Agentes del mercado

---

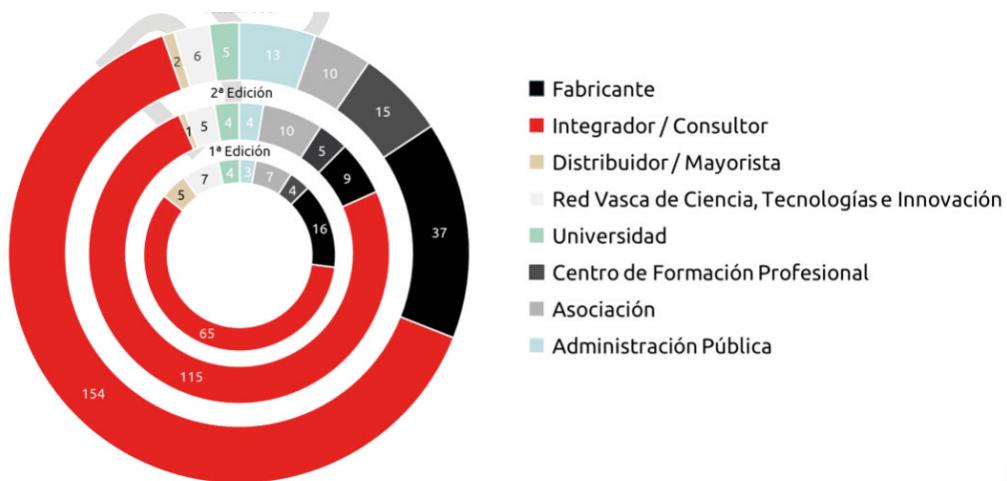
El panorama del sector de la ciberseguridad en Euskadi revela una notable diversidad, caracterizado por la coexistencia de entidades de distintas escalas, que abarcan desde grandes multinacionales hasta empresas de tamaño más reducido. En el marco de este informe, se ha llevado a cabo la identificación de una gama variada de actores del mercado, tanto aquellos involucrados en la cadena de suministro que facilitan los productos a los usuarios, como los proveedores de servicios especializados en esta esfera.

En la clasificación de los agentes del mercado de ciberseguridad en Euskadi, se ha empleado un enfoque basado en distintas tipologías, siguiendo el modelo de categorización propuesto por la European Cyber Security Organisation (ECSO)[142]. Además, se han incorporado nuevas categorías adaptadas específicamente a los diversos agentes presentes en el entorno de Euskadi, quedando la categorización de la siguiente manera:



- **Administración Pública:** son los agentes que están formados para realizar las tareas de administrar y gestionar organismos, instituciones y entes del Estado.
- **Asociación:** es una agrupación de personas que desarrollan una actividad colectiva de forma estable, democrática y sin ánimo de lucro. Pueden formar parte de una asociación tanto personas físicas como jurídicas (sociedades).
- **Centro de formación:** todos aquellos centros de formación de carácter público o privado que tengan como principal objetivo la impartición de formación de carácter no oficial.
- **Centro de formación profesional:** son centros educativos autorizados que imparten formación conducente para la obtención de títulos de Formación Profesional o Certificados de Profesionalidad. Todos aquellos centros que estén dados de alta en el Registro Estatal de Centros Docentes no Universitarios, de carácter público o privado que tengan como principal objetivo la impartición de Formación Profesional.
- **Distribuidor/Mayorista:** son proveedores que adquieren grandes cantidades, o volúmenes de licencias, de soluciones de seguridad de diversos fabricantes, comercializándolas al por mayor.
- **Fabricante:** son proveedores que fabrican o desarrollan sus propias soluciones de ciberseguridad (hardware o software). Estos agentes trabajan únicamente con sus productos, pudiendo realizar integraciones de los mismos.
- **Integrador/Consultor:** son proveedores que adquieren las soluciones a mayistas/distribuidores o directamente a los fabricantes y/o que realizan labores de consultoría e integran todo tipo de soluciones de ciberseguridad. Este tipo de agentes son los encargados de realizar proyectos de consultoría integrando productos que no son propios.
- **Red Vasca de Ciencia, Tecnología e Innovación:** entidades de investigación, desarrollo e innovación que, trabajando en red, desarrollan actividades de I+D+i equilibrado, realizando una investigación especializada y de alto valor añadido; estas deberán estar inscritas en el Registro Público de Agentes de la RVCTI articulada por el Decreto 109/2015.
- **Universidad:** institución destinada a la enseñanza superior, que está constituida por varias facultades y que concede los grados y másteres académicos correspondientes. Universidades que estén dadas de alta en el Registro de Universidades, Centros y Títulos (RUCT) del Ministerio de Universidades del Gobierno de España.

En este momento, han sido **242 agentes** los que se han decidido a formar parte del presente estudio facilitando datos para su inclusión en el mismo:



*Figura 16. Agentes listados en diferentes ediciones del Libro Blanco. Fuente: SPRI*

Del gráfico anterior puede concluirse que desde el año 2018 (año de la publicación de la primera edición del Libro Blanco), hasta hoy, las empresas con actividad en Euskadi en materia de ciberseguridad han crecido llegando a alcanzar la totalidad de 242 empresas.

	<b>1<sup>a</sup> Edición</b>	<b>2<sup>a</sup> Edición</b>	<b>3<sup>a</sup> Edición</b>
<b>Total</b>	111	153	242

Tabla 4. Número total de agentes. Fuente: SPRI

En el contexto de Euskadi, **un total de 193 empresas privadas** han facilitado sus datos para su inclusión en el presente catálogo. Estas empresas ofrecen servicios o productos relacionados con la ciberseguridad, dentro de las cuales 59 son startups. La información detallada sobre estas empresas se encuentra disponible en el Anexo - 10.3 Listados de agentes y soluciones de ciberseguridad.



*Figura 17. Agentes del mercado de ciberseguridad en Euskadi.*  
Fuente: SPRI



El siguiente gráfico ilustra la distribución de organizaciones privadas por territorio histórico:

### Distribución de organizaciones privadas por territorio histórico

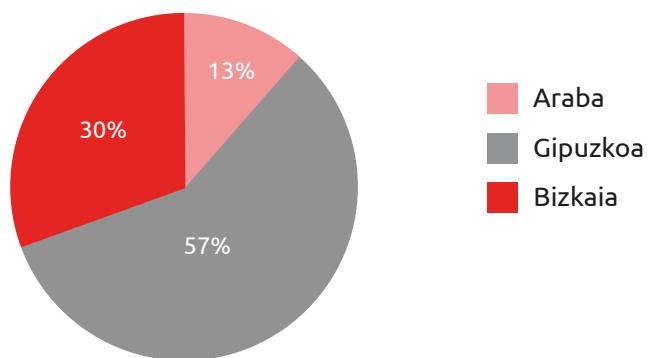


Figura 38. Distribución de agentes privados por territorio histórico.

Fuente: SPRI

Los hallazgos de este análisis demuestran un fenómeno destacado en el ámbito de la ciberseguridad en Euskadi: **una proporción considerable de los agentes especializados se concentran en las áreas urbanas**. Este patrón responde a la estrategia de ubicación adoptada por estas entidades, que optan por establecer sus sedes en estas de importancia estratégica, convirtiéndose en enclaves fundamentales que atraen a potenciales clientes clave. Asimismo, representan puntos neurálgicos en términos de interconexión a nivel global, lo que motiva a estas entidades de ciberseguridad a posicionarse estratégicamente para capitalizar sus oportunidades comerciales y maximizar su inserción en los mercados internacionales.

## Emprendimiento

La actividad emprendedora en el ámbito de la ciberseguridad en Euskadi destaca como una de las más prominentes a nivel estatal. Este hecho se evidencia a través de la proliferación de numerosas **startups especializadas en ciberseguridad** que han sido creadas en la región. En cuanto a la **tipología de las startups**, es relevante resaltar la notable presencia de empresas que desarrollan su propia tecnología.

El panorama emprendedor en ciberseguridad en **Euskadi** se encuentra en una etapa saludable y continúa generando nuevas ideas que se materializan en la creación de empresas. La concentración de startups sitúa, sin lugar a duda, como uno de los epicentros destacados del emprendimiento y la innovación en ciberseguridad en el sur de Europa.

En la siguiente figura puede observarse la distribución de las empresas emergentes de ciberseguridad en Euskadi que han proporcionado sus datos para el presente estudio.

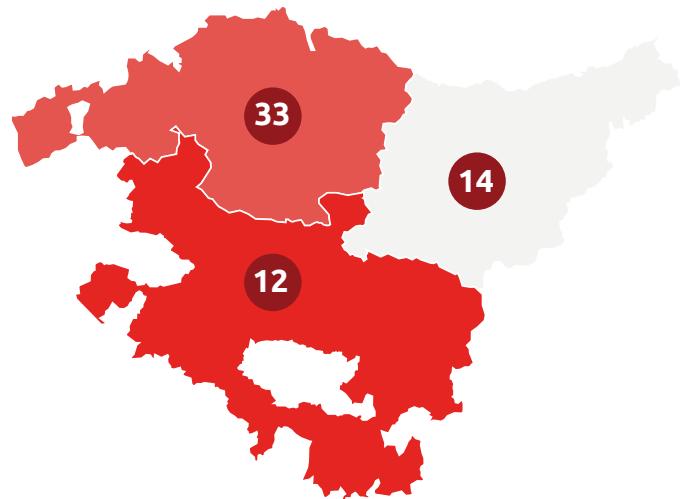


Figura 19. Startups de ciberseguridad en Euskadi. Fuente: SPRI

ADI	Ensotest Energy	Nymiz
Aga Intelligent	Software & Testing	Open Cloud Factory
Akirutek	EUROCYBCAR	Industrial Cybersecurity
Alias Robotics	Fit Learning Systems	Opscura
Appsamblea	Four9s	Orbik Cybersecurity
Assured Clarity Iberia	Gaptain. Cultura de	Osane Consulting
Barbara IoT	Ciberseguridad	Perseus Cybersecurity
Brave Corporation	Gardians Consulting	Services
Bullhost	Gemetik	Purple blob
BusMan View	Goikode	Redborder
Bytek	GPIntegral	RKL Integral
Code Contract	Grupo CYBENTIA	Sealpath
Copia Nube	HodeiCloud	Seginet
CounterCraft	Infakt21	SPCnet
Cras Vigilans Group	Ironchip	Tabira Berezi
DactilPlus	JakinCode	Talio
DATA CENTER EUSKADI	Laubor Technologies	Titanium Industrial
Dative	Lautik IT	Security
Developair	Lex Program Online	Tecnología y Personas
Dokensip	Megabi Soluciones	WSG Tech Solutions
Edatalia	Tecnológicas	Yoid Identidad Digital
Encriptia	Multiverse Computing	Zuratrust



# Red Vasca de Ciencia y Tecnología

En el territorio vasco, se hallan prominentes plataformas de investigación y desarrollo que atraen a una extensa red internacional de profesionales. Estas plataformas tienen como principal **objetivo contribuir al progreso económico y social, así como potenciar la competitividad empresarial en la región**. Se trata de agentes de difusión de la Ciencia, Tecnología e Innovación cuyo propósito principal radica en **estimular la difusión del conocimiento hacia la sociedad y facilitar la transferencia de saberes entre los actores que conforman el Sistema Vasco de Ciencia, Tecnología e Innovación**.

Además, como se ha mencionado en apartados anteriores de este estudio, Euskadi cuenta con el Basque Digital Innovation Hub, una red interconectada de recursos y servicios especializados en fabricación avanzada. Esta red dispone de infraestructuras para la formación, investigación, pruebas y validación, poniendo a disposición de las empresas conocimientos y servicios específicos en áreas como la fabricación aditiva, la robótica flexible y la ciberseguridad.

El propósito fundamental de esta iniciativa es dotar a las empresas industriales, especialmente a las pymes, de las capacidades tecnológicas esenciales para abordar los desafíos que plantea la industria inteligente. Para lograrlo, se establece una red de colaboración público-privada que incluye universidades, centros tecnológicos, unidades de investigación y desarrollo empresarial, así como una red de contactos a nivel internacional.

Esta red interconectada de recursos comprende **infraestructuras, laboratorios, herramientas, software y capacidades científico-tecnológicas innovadoras y de alta calidad en el campo de la Industria Inteligente**.

Específicamente en el campo de la ciberseguridad, se encuentra un **nodo de ciberseguridad** dentro del Basque Digital Innovation Hub, compuesto por 5 laboratorios distribuidos en los territorios históricos y vinculados entre sí. Estos laboratorios tienen como objetivo impulsar el espíritu emprendedor y la innovación, concentrándose especialmente en proyectos relacionados con smart-grid, automoción, blockchain y la evaluación/certificación de productos.

En relación con los agentes que ofrecen soluciones o servicios vinculados al ámbito de la ciberseguridad en Euskadi, la distribución es la siguiente:

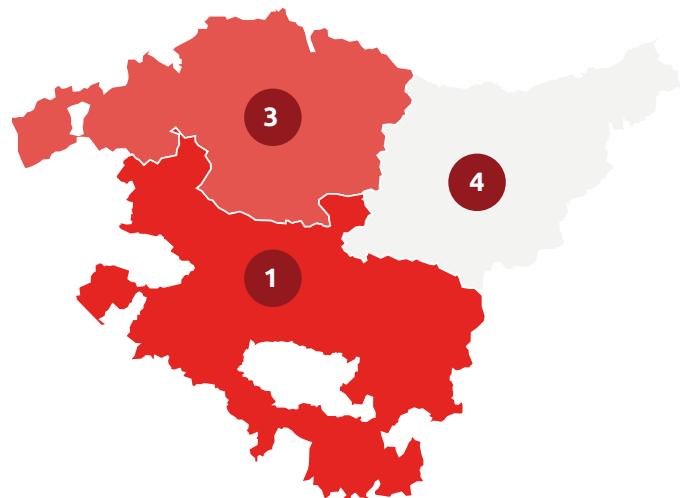


Figura 20. Distribución de centros de actividad de agentes RVCTI de ciberseguridad en Euskadi. Fuente: SPR1

Vicomtech  
Ikerlan

Tecnalia  
Ceit

Innovalia  
BCAM

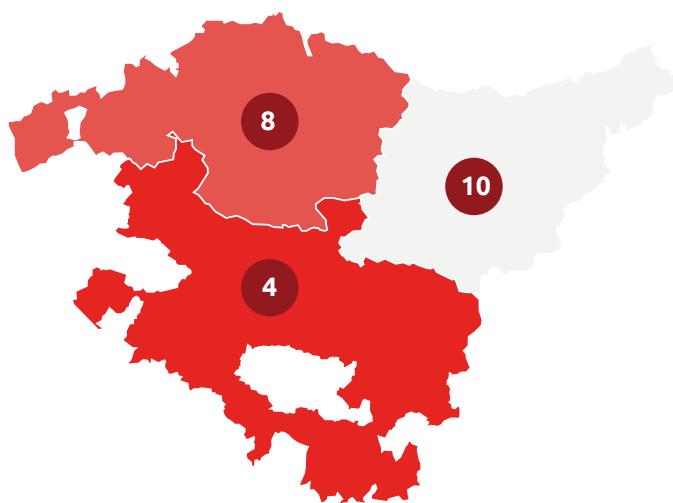
## Red de Centros de Educación

---

El ámbito educativo de Euskadi en ciberseguridad se estructura en Centros de Formación Profesional, Centros de formación y Universidades, los cuales brindan programas de estudio dedicados a esta disciplina. El principal objetivo del sistema educativo consiste en formar y capacitar a todas las personas, guiándolas y proporcionándoles las competencias y herramientas necesarias para su desarrollo profesional en materia de ciberseguridad, de forma que puedan nutrir a las empresas del sector en un futuro.

En este sentido, a día de hoy en Euskadi, se han identificado 20 centros que ofrecen formación en ciberseguridad repartidos en 23 ubicaciones por toda la región (para más detalle de los centros consultar el Anexo – 9.2 Listados de agentes y soluciones de ciberseguridad).

Estos centros educativos tienen **múltiples sedes** donde llevan a cabo sus programas académicos. La distribución se puede visualizar en la siguiente figura.



*Figura 21. Distribución en cuanto a sedes de centros de educación en materia de ciberseguridad.*  
Fuente: SPRI

<b>Centro de Formación Profesional:</b>	Izarraitz Lanbide Heziketa Laudioalde Lanbide Eskola	<b>Universidad:</b>
Centro SEIM	Lea-Artibai Ikastetxea	Mondragon Unibertsitatea
CIFP Tartanga LHII	Maristik Durango Ikastetxea	Tecnun - Universidad de Navarra
CIFP Txurdinaga	Politeknika Txorierri	Universidad de Deusto
EASO Politeknikoa	Tknika	Universidad de Vitoria-Gasteiz EUNEIZ
Egibide Vitoria-Gasteiz	Uni Eibar-Ermua	UPV/EHU
Alava	Urola Garaiko Lanbide Eskola	
FP Andra Mari		
IES Zubiri-Manteo		

## Asociaciones

En Euskadi, hay un total de 10 asociaciones enfocadas en servicios vinculados a la ciberseguridad.

Las asociaciones en Euskadi muestran un compromiso firme con la protección y fortalecimiento de la ciberseguridad en la región. A través de alianzas estratégicas, programas de concienciación y colaboración con instituciones y empresas, estas entidades trabajan incansablemente para impulsar políticas y prácticas que salvaguarden la infraestructura digital y promuevan un entorno seguro en el ámbito tecnológico. Su enfoque proactivo y la dedicación hacia la capacitación, el intercambio de conocimientos y la implementación de medidas preventivas demuestran su determinación en resguardar la integridad y confianza en el entorno cibernético de Euskadi.



- Asociación de Seguridad Informática EuskalHack
- Asociación STOP Violencia de Género Digital
- BRTA-Basque Research & Technology Alliance
- Centro de Ciberseguridad Industrial
- Cybasque
- GAIA (Asociación de Industrias de Conocimiento y Tecnología)
- Pantallas Amigas
- Puntu.eus
- SAE - Asociación Vasca de Profesionales de Seguridad - Segurtasun Adituen Euskal
- VOSTEuskadi

## Administraciones Públicas

---

Las instituciones públicas en Euskadi han asumido un papel fundamental en la promoción y concienciación sobre ciberseguridad en la región, mostrando un creciente compromiso en esta área. Su participación en campañas educativas, la organización de eventos especializados y el impulso de políticas que fomentan buenas prácticas en seguridad digital demuestran su papel esencial en el desarrollo y fortalecimiento de la ciberseguridad en Euskadi. Su liderazgo y colaboración con diversos sectores no solo elevan la conciencia colectiva sobre los desafíos cibernéticos, sino que también contribuyen significativamente a la protección de la infraestructura digital y la confianza en el entorno tecnológico de la región.

Su influencia se extiende más allá de la sensibilización al ofrecer un apoyo crucial en esta área, facilitando programas educativos especializados y respaldando el desarrollo empresarial en el campo de la ciberseguridad. Es destacable observar el creciente compromiso de estas entidades, evidenciado por su participación progresiva en iniciativas relacionadas con la ciberseguridad. Este compromiso se muestra con la **reciente creación de la Cyberzaintza en Euskadi** representa un claro esfuerzo de estas instituciones por fortalecer la seguridad digital, abordar desafíos específicos y salvaguardar los intereses tanto individuales como empresariales en el ámbito digital.

# Conclusiones y perspectivas futuras



Euskadi sobresale por su notable **potencial en ciberseguridad** debido a la heterogeneidad de agentes especializados en esta materia. El sector empresarial dedicado a la ciberseguridad en esta región se destaca por albergar una notable concentración de empresas de alto valor añadido, superando la media de empresas por millón de habitantes, tanto a nivel estatal como europeo. Este ecosistema se distingue por su **diversidad, al disponer de una amplia gama de agentes especializados lo que lo convierte en un entorno muy heterogéneo**. Además, según la clasificación realizada, se confirma que Euskadi cuenta con al menos un representante de cada tipo de agente en dicha categorización.

En este contexto, es relevante resaltar que el progreso de Euskadi en el ámbito de la ciberseguridad se atribuye, en parte, al incremento en la inversión y a las múltiples iniciativas impulsadas en el campo del emprendimiento. Esto ha propiciado un aumento en el valor de mercado de las startups dedicadas a la ciberseguridad en Euskadi durante los últimos años.

De cara a futuro, **se espera que el sector alcance un punto de estabilización**, donde es posible que las empresas no experimenten un aumento significativo en número, pero sí **destacarán por un notable incremento en su grado de especialización y valor añadido**.

En cambio, el **desafío significativo** para Euskadi en el ámbito de la ciberseguridad radica en la **escasez de talento especializado**. A pesar de los esfuerzos en la promoción de la especialización mediante oportunidades educativas bien concebidas, persiste una brecha considerable entre la oferta y la demanda de profesionales en este sector.

**El territorio muestra una clara disposición hacia la especialización en ciberseguridad**, respaldada por iniciativas educativas y programas de formación. Sin embargo, el desequilibrio entre la cantidad de profesionales cualificados disponibles y la creciente necesidad de habilidades especializadas sigue siendo una preocupación real.

Euskadi se enfrenta a la escasez de talento, mediante programas de upskilling y diversas iniciativas educativas destinadas a fortalecer sus capacidades tecnológicas y preparar a su fuerza laboral. Resultará crucial promover y expandir los programas de ayuda disponibles, enfocados en el desarrollo y la capacitación en ciberseguridad. Euskadi tiene la oportunidad de fortalecer su posición en este campo y cerrar la brecha de talento mediante estrategias integrales.

En su ámbito industrial, la ciberseguridad ha surgido como **prioridad para proteger sus infraestructuras, impulsada por su rica historia en el ámbito industrial**. Con un ecosistema tecnológico robusto y una red de colaboración entre empresas, centros de investigación y universidades, la región ha logrado consolidarse como un referente en la protección de infraestructuras industriales. La combinación de conocimientos en ciberseguridad, industria avanzada y digitalización ha colocado a Euskadi en la vanguardia, ofreciendo soluciones robustas y adaptadas a los desafíos específicos que plantea la protección de entornos industriales en un mundo cada vez más interconectado.

La consolidación de Euskadi como referente en ciberseguridad industrial requerirá de un compromiso y colaboración entre las instituciones públicas y privadas



La creciente interconexión y el consiguiente aumento de vulnerabilidades han generado un **creciente interés en la adopción de medidas de seguridad en el ámbito industrial**. La implementación de estándares de seguridad, así como la investigación y la innovación, siguen siendo áreas de enfoque clave que buscan desarrollar estrategias adaptadas a las necesidades específicas de la industria regional.

## En el ámbito Industrial: la ciberseguridad como prioridad

El futuro de Euskadi apunta a ser muy positivo, con todos los **elementos necesarios para consolidarse como un centro líder y hub de referencia en ciberseguridad industrial**. Su éxito dependerá en gran medida de su capacidad para aprovechar el talento regional, convirtiéndolo en un motor para la innovación y el desarrollo en este campo crucial en la era digital. Además, con el creciente interés en soluciones de ciberseguridad dirigidas al sector industrial, se espera un **aumento en el mercado de ciberseguridad industrial en Euskadi en los próximos años**.

La consolidación como un centro de referencia no solo es una oportunidad económica, sino también un pilar esencial para la integridad de la información, la protección de la privacidad y la seguridad de sistemas vitales en un mundo interconectado.

Sin duda, **el futuro el Euskadi en el ámbito de la ciberseguridad industrial se vislumbra prometedor**, pero su consolidación como líder indiscutible requerirá un compromiso sólido y colaborativo entre las instituciones públicas y privadas de la región. La confluencia de esfuerzos y recursos de ambos sectores será fundamental para alcanzar los objetivos trazados en este sector tan crucial en la era digital.

En este sentido, las entidades públicas han demostrado su compromiso con este ámbito en la región, destacando la **creación de "Cyberzaintza"** como un ejemplo de esta colaboración intersectorial. Asimismo, **SPRI** se destaca como un actor clave en el ámbito empresarial de la ciberseguridad en Euskadi, gracias al respaldo que ofrece al tejido empresarial local.

En definitiva, **la participación coordinada de los diferentes agentes de Euskadi es crucial para avanzar hacia una posición de liderazgo en ciberseguridad**. La unión de esfuerzos, conocimientos y recursos será el motor que impulse la innovación, la competitividad y el desarrollo sostenible en este campo, consolidando así el rol de la región como un referente destacado en la protección digital en un mundo interconectado.

En lo que al **Departamento de Desarrollo Económico, Sostenibilidad y Medioambiente del Gobierno Vasco y a SPRI** se refiere, el futuro se revela prometedor. En los próximos

Euskadi como centro líder y hub de referencia en ciberseguridad Industrial



años, DESMA y SPRI pretenden continuar avanzando en su estrategia de favorecer al incremento y mejora de la ciberseguridad del tejido empresarial de Euskadi, por medio del fortalecimiento y crecimiento del sector de la ciberseguridad del territorio, así como con su rol como **organismo referente en todo lo relacionado con la ciberseguridad aplicada al ámbito empresarial**. Para la consecución de estos objetivos, ambos organismos se comprometen a seguir avanzando con dedicación y fuerte compromiso, para continuar definiendo e impulsando nuevos instrumentos de apoyo que permitan mejorar la competitividad de las empresas del sector, contribuyendo al desarrollo económico no solo del sector, sino también de la Comunidad Autónoma de Euskadi.



# Grupo Spri, Agencia vasca de Desarrollo empresarial

