LIBRO BLANCO DE LA **CIBERSEGURIDAD** EN EUSKADI 2024

3ª edición

GRUPO spri TALDEA

EUSKO JAURLARITZA
GOBIERNO VASCO

EKONOMIAREN GARAPEN, JASANGARRITASUN ETA INGURUMEN SAILA

DEPARTAMENTO DE DESARROLLO ECONÓMICO, SOSTENIBILIDAD Y MEDIO AMBIENTE

Índice

Índice de figuras

Índice de tablas

Introducción

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). Este 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.

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.

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

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.

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 Businness 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 Enpresa Digitala" en los Parques Tecnológicos de Euskadi.

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

Adicionalmente, cabe señalar una de las iniciativas emblema, 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-

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, 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 Infrastucture, 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.

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
Análisis 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
Análisis 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. 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. Proporcionar datos y evidencias sobre sus productos/servicios que acrediten la información facilitada.	Ser un agente que proporciona productos/servicios de ciberseguridad. Proporcionar datos y evidencias sobre sus productos/servicios que acrediten la información facilitada. Aportar evidencias en cuanto a referencias de clientes o proyectos en los que haber implantado este tipo de productos u ofreciendo este tipo de servicios.

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 ponerse en contacto a través de **spri.eus**

Contextualización del sector

En los últimos años, el ámbito empresarial ha experimentado una **notable transformación tecnológica**, **traduciéndose en** un mayor desarrollo y una mejora de procesos y servicios en las organizaciones. Este cambio no solo supone una revolución en las prácticas empresariales, sino también un incremento significativo en la dependencia de la tecnología por parte de las organizaciones. La hiperconectividad resultante de esta mayor dependencia se erige como una de las causas principales del aumento de la cibercriminalidad, **elevando los riesgos asociados a la ciberseguridad,** impactando no solo la integridad, confidencialidad y disponibilidad de la información gestionada, sino también los servicios ofrecidos por estas entidades.

Debido a esta situación, los cibercriminales están aprovechando los nuevos escenarios, lo que ha ocasionado que el **número de ciberataques** aumente considerablemente.

En este contexto, el cibercrimen y el mercado derivado del mismo son las principales causas por las que el sector de la ciberseguridad está cobrando mayor visibilidad y trascendencia social. Se prevé que el coste anual global del ciberdelito alcance los 8 billones de dólares en 2023. Adicionalmente, se debe sumar el creciente coste de los daños resultantes del ciberdelito, que se espera que alcance los 10,5 billones de dólares en 2025 [1].

Del mismo modo, el avance constante de las nuevas tecnologías de información ha generado un gran ascenso en la consecución de ciberdelitos, caracterizándose este aumento por la gran **variedad de nuevas técnicas** utilizadas y cada vez más **personalizadas**, como puede ser el caso del phishing. Con el objetivo de hacerlas frente, uno de los retos actuales más importantes de la sociedad se encuentra en la creación de una **conciencia de ciberseguridad** en la sociedad, así como entre las empresas.

Como respuesta al incremento del cibercrimen, **desde los diferentes estados se están dedicando esfuerzos** a la revisión y actualización de la legislación en materia de ciberseguridad. Esta revisión se vuelve imperativa con el propósito de fortalecer las capacidades de las entidades a la hora de resguardar a la población de las ciberamenazas. Asimismo, en el ámbito organizacional, la adopción de tecnologías emergentes, como la integración de nuevos elementos en los sistemas de autenticación convencionales, ha contribuido a ampliar la protección contra potenciales ataques por parte de ciberdelincuentes. No obstante, el aumento de incidentes, tales como los dirigidos por ransomware, ante los cuales muchas empresas aún no han implementado las medidas de seguridad necesarias, genera inquietud y destaca la urgencia de tomar acciones preventivas.

Ante esta situación, las instituciones públicas y privadas están aumentando sus inversiones e incrementando los recursos económicos destinados a la formación y concienciación del personal con el objetivo final de prevenir la consecución de estos ataques y, en su caso, hacer frente a los daños físicos, lógicos, económicos y morales derivados de los mismos.

Por todo ello, a lo largo del presente apartado, se analizan aquellos factores que resultan de especial interés en el ámbito de la ciberseguridad abordándose aspectos cruciales como el valor de mercado, inversión, empleo y educación, emprendimiento, cibercrimen, tendencias, entorno regulatorio, sellos de ciberseguridad y las agencias especializadas en ciberseguridad.

Este análisis, realizado a nivel internacional, europeo, estatal y especialmente, a nivel regional, permite obtener una visión de los desafíos y oportunidades para cada uno de estos campos en la región de Euskadi, facilitando así la implementación de estrategias adaptadas y efectivas para fortalecer la seguridad en este amplio espectro.

Valor de mercado

Con la hiperconectividad como una de las causas principales, el valor de mercado en materia de ciberseguridad superó los 126 mil millones de dólares a nivel global en 2022, suponiendo un crecimiento del 18% en los últimos cuatro años

Los Sistemas de Información son fundamentales para el funcionamiento eficiente de diversas industrias, impulsando la automatización y el control de procesos críticos. A medida que aumenta su importancia y conexión con redes globales, se enfrentan a más vulnerabilidades en un entorno cibernético en constante cambio. Las amenazas digitales, representan un riesgo para la integridad y continuidad de estos sistemas vitales. Esta situación, influenciada también por la creciente hiperconectividad, genera una mayor necesidad de protección, donde organizaciones y gobiernos trabajan conjuntamente para mantener la estabilidad y seguridad de las industrias frente a una variedad creciente de ciberamenazas sofisticadas.

Como consecuencia del crecimiento de los ciberdelitos en los últimos tiempos, el valor de mercado en materia de ciberseguridad superó los **126 mil millones de dólares** a nivel global en 2022, lo que supuso un crecimiento del 18% en los últimos cuatro años.

Valor mundial de la ciberseguridad en mil millones de $

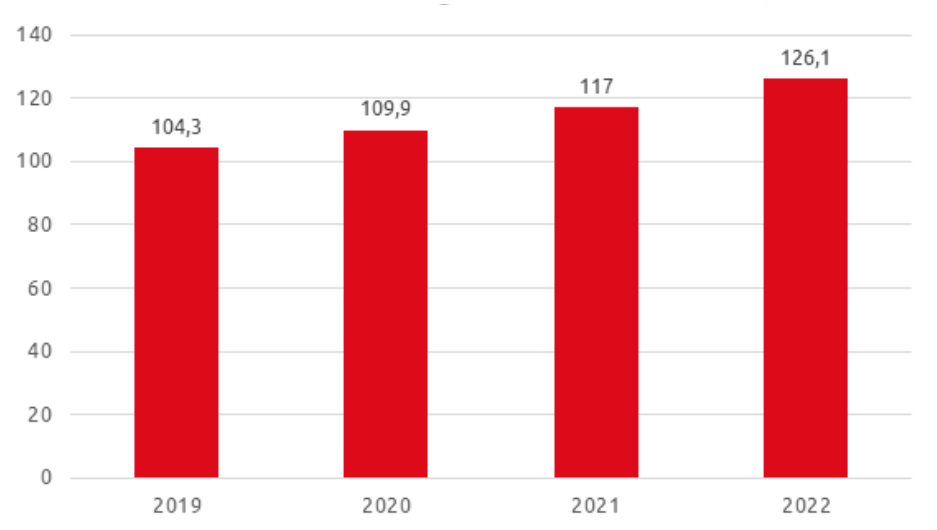


Figura 3. Valor mercado ciberseguridad. Fuente: Mordor Intelligence

A nivel **europeo**, el valor del mercado de la ciberseguridad en 2022 fue de 39 mil millones de euros [2]. Además, en virtud de lo señalado en el "Europe Cyber Security Market Report" se estima que el valor de mercado llegue a los 103.51 billones de dólares en el año 2028 [3].

Euskadi sobrepasa significativamente la media de compañías por cada millón de habitantes en comparación tanto con España como Europa

En lo que respecta al valor de mercado a **nivel estatal**, España alcanzó los 1.950 millones de euros en 2022, lo que supuso un crecimiento del 14,7% respecto al año anterior y un 30% respecto a los dos años anteriores. Ello demuestra el empujón que está experimentando este negocio ante el aumento imparable de las ciberamenazas. Dos tercios de la facturación sectorial provinieron de la prestación de servicios y, el tercio restante fue atribuible a la venta de hardware y software relacionado con la seguridad. Según estimaciones de Observatorio Sectorial DBK, las firmas de consultoría representan aproximadamente el 72% del valor total de mercado (1.400 millones) y son las firmas especializadas junto con otros tipos de negocios los que constituyen el 28% restante (550 millones) [4].

A continuación, el **siguiente gráfico expone a modo de comparativa la media de empresas de ciberseguridad por millón de habitantes en Euskadi, España y Europa** [2].

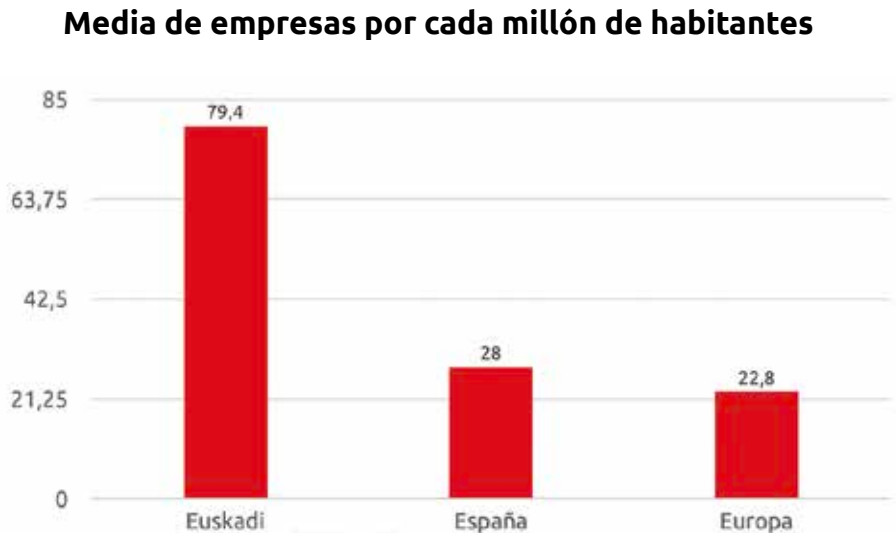


Figura 4. Media de empresas por cada millón de habitantes.
Fuente: European Cybersecurity Investment Platform

Como puede observarse en el gráfico de arriba, en Euskadi se observa una destacada concentración de empresas especializadas en ciberseguridad, sobrepasando significativamente la media de compañías por cada millón de habitantes en comparación tanto con España como Europa. Esta disparidad resalta la notable presencia y relevancia del sector de la ciberseguridad en la región, demostrando una proporción considerablemente superior de entidades dedicadas a abordar los desafíos digitales por cada unidad poblacional. Esta situación no solo destaca el compromiso regional con la vanguardia en seguridad informática, sino que también subraya el liderazgo de Euskadi en la protección de la información y la tecnología, superando el promedio establecido tanto a nivel estatal como europeo.

Inversión

La inversión en el mercado de la ciberseguridad ha tomado una tendencia alcista en los últimos años, llegando a valorarse en 261.010 millones de dólares en 2023 y se espera que crezca a una tasa de crecimiento anual compuesta (CAGR) del 8,7% durante el periodo de previsión 2023-2026 [5]. Es previsible que esta tendencia se vea reforzada en los años venideros debido al contexto geopolítico, con crecientes amenazas tanto de tipo híbrido, como tecnológico, con una mayor penetración de las nuevas amenazas, a las que se exponen las sociedades a lo largo de todo el mundo en general y las occidentales en particular. En este sentido, según la prestigiosa revista Forbes, la convergencia de la automatización y la toma de decisiones basada en datos en el panorama de la ciberseguridad ayuda a transformarla en **una inversión estratégica** en lugar de una perspectiva de coste [6].

La ciberseguridad es un sector notablemente resistente. Hasta ahora, se ha visto que los mercados de ciberseguridad se han movido en una dirección, a pesar de las crisis financieras, las recesiones y otro tipo de desastres. Por lo general, a las empresas les resulta difícil justificar el recorte de su inversión en seguridad, lo que hace que algunos expertos observen que la ciberseguridad es un sector a prueba de recesiones, que, a su vez, lo hace atractivo para inversores.

Es innegable que, en los últimos años, la ciberseguridad ha atraído más atención de lo habitual. La mayor afluencia de capital procedió de inversores en crecimiento que vieron en ella una forma de diversificar y ampliar sus inversiones en SaaS y ofertas de infraestructura.

A la hora de hablar de inversores de capital riesgo, es necesario mencionar que existen **diversas maneras de segmentar las empresas de capital riesgo:** por tamaño del fondo, etapa, sector vertical, tesis de inversión, etc. En este sentido, se podría hablar de dos tipos de empresas de capital riesgo [7]:

- **Sociedades de capital riesgo generalistas:** las que invierten en una amplia gama de segmentos, geografías, mercados, etc. (por ejemplo, empresas globales de distintos mercados).
- **Sociedades de capital riesgo especializadas:** las que optan por especializarse en un mercado concreto (por ejemplo, ciberseguridad), un subsegmento industrial (por ejemplo, tecnología de cumplimiento), una geografía (por ejemplo, EE. UU.) o una superposición de unos pocos (por ejemplo, ciberseguridad en fase inicial en Israel).

Entre las sociedades de capital riesgo generalistas, la mayoría de las firmas más relevantes tienen una práctica bien establecida en ciberseguridad: Accel, Bessemer Venture Partners, Andreessen Horowitz, Sequoia, Sands Capital, entre otras. Estas sociedades cuentan con personal dedicado exclusivamente a la ciberseguridad, por lo que la naturaleza de sus inversiones en ciberseguridad es tan específica como la de las empresas de capital riesgo especializadas en ciberseguridad [7].

En julio de 2023, los inversores de capital riesgo ya habían invertido 4.700 millones de dólares en empresas europeas de ciberseguridad, mostrándose la tendencia a superar el valor de las operaciones registradas en el año 2022, cuando el total alcanzó los 7.600 millones de dólares

En lo que a las **sociedades de capital riesgo especializadas en ciberseguridad** se refiere, éstas conocen ampliamente el mercado y mantienen excelentes relaciones con otras sociedades de capital riesgo líderes en seguridad [7]. Esto les facilita la conexión con clientes potenciales, socios, asesores e inversores que pueden participar en operaciones futuras, ofreciendo a las empresas de este ámbito inversores especializados en la materia. Este hecho se considera una ventaja ya que les brinda la experiencia necesaria para entender a lo que se dedica concretamente una empresa de ciberseguridad, siendo esto de gran importancia especialmente en las primeras fases de, por ejemplo, una startup, empresas en crecimiento que no disponen de muchos números ni resultados, sino de una visión, un equipo y en ocasiones, únicamente de un MVP (Minimum Viable Product).

Desde un punto de vista más cuantitativo, se indican algunas cifras que diferentes agentes económicos o distintos tipos de inversores generan con su actividad:

En los primeros siete meses de 2023, los inversores de capital riesgo se acercaron al total de **5.000 millones de dólares invertidos en empresas europeas de ciberseguridad.** La estimación para finales de 2023 esperaba superar el valor de las operaciones registradas en el año anterior, cuando fueron alcanzados los 7.600 millones de dólares.

En Estados Unidos, sin embargo, la actividad de acuerdos de capital riesgo en ciberseguridad ha disminuido considerablemente en comparación con el año 2022. A finales de julio, el valor de las operaciones de este tipo ascendía a 4.600 millones de dólares, menos de una décima parte de los 50.900 millones alcanzados en 2022 [8].

Inversión capital privado en millones de dólares

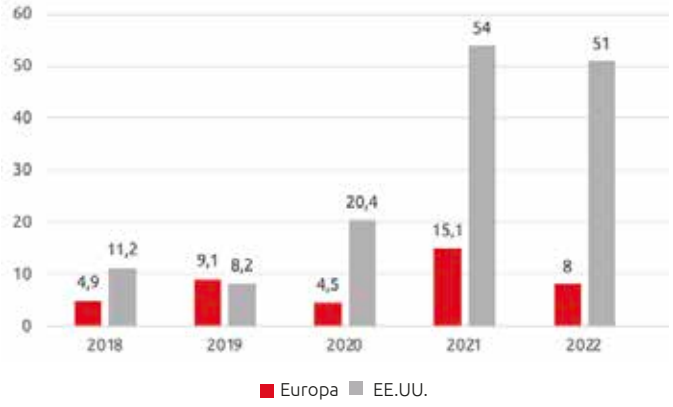


Figura 4. La inversión de capital privado en ciberseguridad. Fuente: PitchBook

A nivel de operaciones, durante los siete primeros meses de 2023, se produjeron 117 operaciones de capital riesgo de ciberseguridad en todo el mundo, frente a las 266 de todo 2022. Europa representa el 41% de ese total, con 48 operaciones durante los siete primeros meses de 2023, frente al 33% de operaciones del año pasado. A su vez, en EE. UU. se han producido 52 operaciones en 2023, lo que representa el 44% del recuento global de operaciones, frente al 58% del recuento total de operaciones del año pasado [8].

El valor de las operaciones en EE. UU. en 2023 se resintió debido entre otras cosas a la escasez de grandes operaciones. Por ejemplo, fue en el año 2022 cuando se produjo la compra apalancada de Citrix Systems, con sede en Florida, por valor de 16.500 millones de dólares, la mayor compra apalancada de ciberseguridad registrada hasta la fecha de desarrollo del presente documento. A fecha de julio de 2023, la única gran operación que se cerró fue la de KnowBe4 por 4.600 millones de dólares, anunciada por primera vez en septiembre del 2022.

En Europa, además de no haberse producido grandes operaciones de capital riesgo en ciberseguridad, el valor de las operaciones tiende también a ser inferior en comparación al de Estados Unidos. La mayor operación europea revelada durante 2023 fue la adquisición por parte de Lutech del negocio italiano de Atos por 467 millones de euros (aproximadamente 500 millones de dólares), que, tras anunciarse en noviembre de 2022, se cerró en marzo del siguiente año [8].

Como se ha podido ver, **el auge del mercado inversor en ciberseguridad se manifiesta de diferentes maneras en los distintos mercados geográficos**. Además, por todo lo mencionado anteriormente, y debido a su menor tamaño en comparación con el mercado de los EE. UU., el crecimiento del mercado europeo resulta más notable.

Pese a este crecimiento, sigue existiendo un gap o brecha de financiación en el mercado europeo frente al estadounidense, similar al caso a nivel estatal y en Euskadi. En el ámbito de la financiación de nuevas empresas emergentes (startups), estas se segmentan en series que corresponden a la fase en la que se encuentra cada organización [9]:

- Seed (semilla): hasta 500.000€.
- Serie A: desde 500.000€ hasta 5M€.
- Serie B: desde 5M€ hasta 15M€.
- Serie C: desde 15M€ hasta 50M€.
- Serie D: de 50M€ en adelante.

La cantidad de acuerdos cerrados por compañías de ciberseguridad tiende a disminuir a medida que estas avanzan en sus etapas de financiamiento. Es notable que se generan más operaciones en etapas tempranas de inversión de capital de riesgo, como Seed y Serie A. Este patrón se explica por el hecho de que las rondas de inversión en etapas más avanzadas suelen involucrar montos financieros más elevados, y por lo tanto, la cantidad de fondos o entidades que disponen de músculo y recursos económicos suficientes para poder hacer frente a inversiones de semejante magnitud, resulta también considerablemente más limitado.

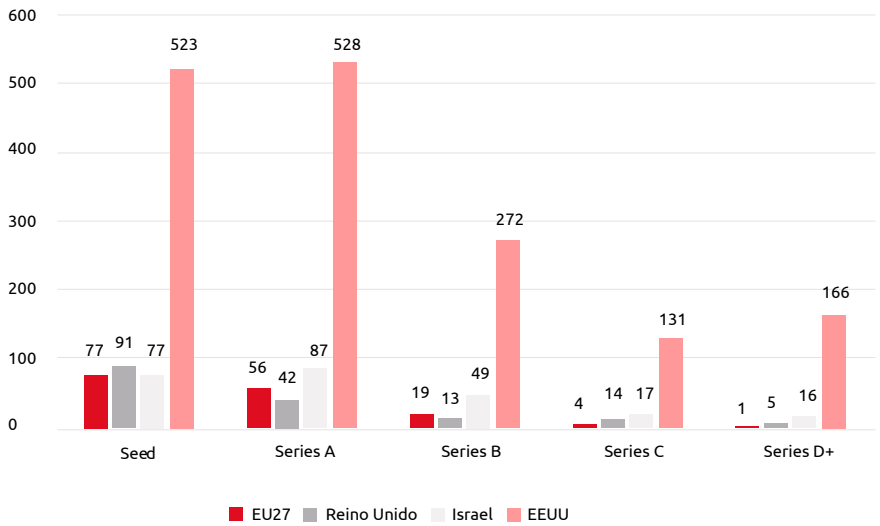


Figura 5. Número de operaciones realizadas por tamaño de empresa. Fuente: adaptación propia de European Community Investment Partners

Las compañías de la Unión Europea registraron un número considerable de acuerdos en la etapa de inversión de Seed, al igual que en Israel. Sin embargo, el número de acuerdos en Series A y B es significativamente menor en comparación con Israel y los Estados Unidos, y casi inexistente en las etapas de Series C y D+ (con solo un acuerdo de Serie D+ registrado en la UE en los últimos seis años). Esto resalta aún más la escasez de inversiones de capital de riesgo en ciberseguridad destinadas a empresas más consolidadas en la Unión Europea [9]. Situación que se puede extrapolar a la realidad de la comunidad autónoma de Euskadi.

Por otro lado, es importante resaltar que además de la inversión de origen privado, **la inversión de origen público cobra también un papel relevante en el ecosistema de la ciberseguridad.** Siguiendo esta idea, a lo largo del presente apartado se muestran algunos de los datos e iniciativas de inversión más relevantes a nivel de Europa, del estado y de Euskadi, tanto de naturaleza pública como privada.

En **Europa**, una de las iniciativas de inversión pública más relevantes, ha sido la creada para el periodo 2021-2027 en el marco del programa Europa Digital [8][9]. Se trata de un instrumento de financiación para apoyar el crecimiento de las capacidades fundamentales para salvaguardar y garantizar la economía digital y sociedad europea, con el fin de mejorar el potencial industrial y la competitividad en materia de ciberseguridad. Así pues, tanto el sector público como el privado de la UE estarán mejor capacitados para fomentar la confianza y defender a sus ciudadanos y empresas de las ciberamenazas. Para ello, la UE se compromete a invertir 1.600 millones de euros en capacidades y en implantación de infraestructuras y herramientas de ciberseguridad tanto para administraciones públicas como para empresas y particulares [10].

A nivel europeo, en cuanto a **la inversión de naturaleza privada** se refiere, nos encontramos con diferentes firmas de capital de riesgo que invierten en ciberseguridad en Europa y **también en Euskadi.** Esto resulta especialmente relevante para los actores del sector de ciberseguridad en Euskadi, ya que se trata de firmas que pudieran tener en el radar a otras empresas de ciberseguridad del territorio. Entre otras nos encontramos con:

- **Adara Ventures**: con sede en Luxemburgo, es una sociedad de capital riesgo con 180 millones de euros bajo gestión que realiza inversiones en empresas deep tech en fase inicial de Europa Occidental y del Sur (España, Portugal, Francia, Reino Unido, Italia e Irlanda). Invierte en áreas como ciberseguridad, plataformas de aplicaciones e infraestructura de datos, DevOps, componentes y salud digital, entre otras. En su tercer fondo de 80 millones de euros, que cerró en 2020, es donde invierte actualmente. Adara Ventures basa su criterio de inversión en tres pilares: que las empresas sean startups tecnológicas, con modelos B2B y en fase de financiación semilla y serie A. Además, pretende que las empresas en las que invierte cuenten con alguna ventaja tecnológica sobre sus rivales para que, de esta manera, puedan competir en mercados de todo el mundo, normalmente en Estados Unidos o Europa. Adara Ventures ha invertido en 37 empresas en total, entre las que se encuentra la empresa vasca CounterCraft como una de las startups en las que invirtieron [11].

- **Accel Partners:** es una empresa que gestiona inversiones y activos, principalmente a través de fondos de capital riesgo. A cambio de una participación accionarial, invierte dinero en nuevas empresas emergentes en áreas como Ciberseguridad, Cloud y SaaS, entre otros, en el ámbito global. Esta entidad, basa su filosofía de inversión en respaldar equipos e ideas en las primeras etapas de su desarrollo. Durante los últimos diez años, Accel Partners ha invertido en más del 70% de las empresas de su cartera como inversor principal o fundador. [12].

- **33N Ventures:** es una empresa de capital riesgo especializada en ciberseguridad y **software de infraestructura.** Su primer fondo invierte en Europa, Israel y EE.UU. en empresas en etapas iniciales de crecimiento que desarrollan y comercializan soluciones tecnológicas emergentes en ciberseguridad y software de infraestructura. 33N Ventures tiene un enfoque activo para apoyar a las empresas en su expansión global, con un equipo internacional experimentado y una extensa red de empresarios, expertos y consultores en ciberseguridad líderes en todas las industrias [13][14].

La inversión en startups no se limita únicamente a los fondos de capital riesgo. Más allá de estas entidades financieras, surge una modalidad cada vez más prominente: el corporate venturing. Este enfoque implica la participación directa de empresas consolidadas en el respaldo a startups emergentes, aportando no solo capital, sino también recursos, experiencia y una red de contactos inestimable.

Para el caso de estas corporates, pese a que sus operaciones suelen en muchas ocasiones tratarse de una forma sumamente confidencial y con notable secretismo, tienden a encontrarse muy activas también dentro del segmento de la ciberseguridad, a través de sus diferentes instrumentos de inversión. Dado que las operaciones en muchos casos no trascienden, resulta complicado identificar ejemplos o evidencias de corporates que hayan invertido en empresas del ámbito de la ciberseguridad. No obstante, como ejemplo de algunas de las actividades adoptadas por algunas de ellas nos encontramos con los siguientes ejemplos.

En una apuesta para buscar soluciones a los actuales retos en ciberseguridad empresarial, el Banco Santander invertirá hasta 300 millones de euros en tres iniciativas conjuntas. Una de ellas, es la creación del Forgepoint Capital International (FPCI), una nueva gestora de venture capital para invertir en startups de ciberseguridad [15].

El FPCI será lanzado en 2023 y tendrá como propósito promover la innovación en el ámbito de la ciberseguridad, a través de un fondo que estará abierto a inversores del sector público y privado. Con este capital, las entidades buscarán startups y compañías en Europa, Latinoamérica e Israel que se dediquen al desarrollo de soluciones innovadoras para los actuales desafíos empresariales en materia de seguridad [15].

Por otro lado, resulta destacable también el Fondo Perseo de Iberdrola (en adelante, Perseo). Se trata de un instrumento de innovación abierta de Iberdrola, que colabora con startups en el que actualmente gestiona una cartera de nueve compañías emergentes. Estas han sido seleccionadas entre más de 300 empresas internacionales evaluadas anualmente con el objetico de encontrar oportunidades de negocio, contribuyendo así a un ecosistema que abarca cerca de 7.500 emprendimientos [16].

Desde 2008, un total de 25 empresas han sido respaldadas por Perseo, abarcando áreas como la inteligencia artificial para la digitalización y automatización de procesos, soluciones inteligentes de eficiencia energética, infraestructura de recarga para vehículos, proyectos solares en economías emergentes o la ciberseguridad. Con más de quince años dedicados, se ha consolidado como una referencia en el ámbito corporativo de startups en la industria energética. Entre las startups en las que han invertido se encuentra la empresa vasca Barbara IoT [16].

En lo que respecta a las inversiones privadas a **nivel estatal**, nos encontramos con entidades de capital de riesgo entre las que se encuentran [17][18]:

- **JME Ventures:** con sede en Madrid se trata de una entidad que invierte en empresas innovadoras que utilizan la tecnología para escalar globalmente, en su etapa inicial, en el ámbito estatal. Buscan fundadores increíblemente inteligentes y motivados que persigan una oportunidad potencialmente enorme en el momento adecuado, con un producto o una tecnología y distribución excelentes, un modelo de negocio escalable, que genere ventajas acumulativas y, por lo general, cierta tracción medible. Además de apoyar a las empresas a lo largo de gran parte de su ciclo de vida de financiación, comparten su experiencia tecnológica o sectorial en potenciación de marcas y capacidades financieras a largo plazo [19][20].

- **Kibo Ventures:** nacida en 2012 con la misión de capacitar a emprendedores tecnológicos europeos para abordar desafíos significativos y facilitar su expansión. El equipo reúne a especialistas en operaciones e inversión con extensas conexiones internacionales en Europa y EE. UU., incluyendo a algunos de los líderes destacados en fundación de empresas, inversiones y corporaciones. Además, recientemente Kibo Ventures presentó Nzyme, un nuevo fondo de capital privado tecnológico de 200 millones de euros, enfocado en la enorme oportunidad de transformar industrial fragmentadas y carentes de innovación donde la tecnología puede desempeñar un papel crucial [21][17].

- **Caixa Capital Risc:** es la rama de Venture Capital de CriteriaCaixa y uno de los principales inversores de capital riesgo en España. Fundada en 2007, invierte en empresas innovadoras en sus fases iniciales de crecimiento, principalmente en España y Portugal. Ya ha invertido en más de 100 empresas con alto potencial de crecimiento en los sectores de ciencia biológicas, tecnología digital e industrial. Entre sus inversiones se encuentran las empresas de ciberseguridad de Euskadi Opscura y Barbara IoT [22].

A pesar de la citada brecha entre Estados Unidos y Europa en lo que a la inversión de ciberseguridad se refiere, son varias las regiones europeas que cuentan con un potencial considerable y podrían ser interesantes para recibir inversiones en materia de ciberseguridad, **entre las que se encuentra Euskadi.**

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

Dentro de los estados miembros de la UE, la apuesta por la innovación es la seña de identidad de **Euskadi**, una apuesta que le ha reportado reconocimiento y recursos en el ámbito europeo. Tal es así que, durante los últimos años se ha observado la atracción de inversores (Adara Ventures, Anzu Partners, Baron Capital, Caixa Capital Risc, CDTI, Datadog, DTI, ECapital, ECAPITAL, EIT FAN Helsinki (Food Accelerator Network), Elewit, European Innovation Council, Eurostars SME programme, Evolution Equity Partners, GoHub Ventures, INCIBE Cybersecurity Ventures, In-Q-Tel, LORCA, Mundi Ventures, NCSC For Startups, Orza Investments, Red Eléctrica de España, techUK, Telefónica Innovation Ventures, Wayra, entre otros.) o como grandes empresas multinacionales han mostrado interés llegando a adquirir empresas originarias de Euskadi [23].

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 [1].

También lidera el retorno per cápita de fondos europeos, casi triplicando la media estatal, haciendo de Euskadi una región atractiva en la que invertir.

De lo anterior se deduce que **Euskadi** se presenta como un **territorio atractivo** para la inversión, pudiendo ello atribuirse a las **particularidades distintivas** que este territorio ofrece en ámbitos tales como la innovación tecnológica, las ventajas fiscales y el talento especializado, entre otros factores relevantes.

Cabe destacar también el entorno colaborativo fuerte y comprometido del sector TEIC en Euskadi, el cual facilita y refuerza la creación o consolidación de empresas de ciberseguridad. Algunas de las asociaciones o iniciativas más relevantes en este sentido son: Red de Business Innovation Centers (BICs), Basque Artificial Intelligence Center (BAIC), Cybasque, BAT (B Acceleration Tower), Basque, Quantum Ecosystem, BMH – Basque Microelectronics Hub, UP! Euskadi, Robotekin, BasqueCCAM, ADI – Atlantic Data Infrastructure etc.

Otro de los aspectos relevantes a la hora de invertir en Euskadi, es la fiscalidad del territorio. Gracias a la autonomía Fiscal de Euskadi y su sistema Tributario propio, el territorio cuenta con capacidad normativa y de gestión propia y es por ello por lo que siguiendo lo señalado por el Instituto de Estudios Económicos en uno de sus informes, la Comunidad Autónoma de Euskadi (en adelante, CAE), es una de las comunidades autónomas con menos presión fiscal y, cuenta con un escenario tributario más favorable para las empresas.

En lo que respecta al Impuesto de Sociedades, actualmente, la CAE presenta un tipo impositivo en Euskadi de un 24% para empresas medianas y grandes, frente al 25% del resto de España. En el caso de las empresas pequeñas, la diferencia se incrementa un poco más, las haciendas vascas cuentan con un 20% mientras que en el resto del territorio cuenta con un

tipo impositivo del 25% [26][27][28]. Además, en el caso de las microempresas, cuando existen compensaciones tributarias, como por ejemplo la que corresponde a proyectos de I+D, el tipo puede llegar a reducirse hasta el 18%.

Otro de los beneficios con los que cuenta este territorio es que se puede obtener una deducción por inversiones de hasta el 25%, y la libertad de amortización de bienes se complementa con la deducción por creación de empleo de 5.000 euros por persona y año, incluso llegando a poder deducir el doble de lo anterior si la persona se encuentra en alguno de los colectivos de especial dificultad de inserción [26][27][28]. Estas condiciones incluyen principalmente que las inversiones superen los 48 mil euros y supongan un incremento patrimonial de al menos un 25%.

Bajo esta perspectiva, y en lo que a la **inversión de naturaleza pública** se refiere, Euskadi dispone de dos entidades diferenciales, Gestión Capital Riesgo Euskadi y Seed Capital Bizkaia.

Gestión Capital Riesgo Euskadi constituye una entidad gestora de fondos de capital riesgo fundada en 1985 por el Gobierno Vasco e integrada dentro del Grupo SPRI, que nace con el propósito de fomentar e impulsar la actividad de Capital Riesgo en Euskadi. Su función principal es la inversión en empresas en sus diferentes etapas de desarrollo, desde startups hasta empresas consolidadas, proporcionando financiación a cambio de participación en el capital de estas compañías. Su objetivo es impulsar el crecimiento y desarrollo mediante inversiones estratégicas que ayuden a fortalecer el tejido empresarial y fomentar la innovación y el emprendimiento en Euskadi. Esta entidad gestiona fondos de inversión con un alcance temporal de entre 5 y 10 años, tanto en empresas de nueva creación como en empresas ya constituidas con un plan de expansión o desarrollo. Además, sus inversiones están centradas exclusivamente en empresas con sede social y fiscal en Euskadi, que cuenten con proyectos prometedores, pero requieran un apoyo sólido para su ejecución. Su estrategia se encuentra alineada con la estrategia de especialización inteligente RIS3 de Gobierno Vasco, priorizando la búsqueda de empresas que focalizan su actividad dentro de los sectores de industria inteligente, energías limpias y salud personalizada. **Del mismo modo, también resultan de especial interés las empresas dedicadas a favorecer la transición tecnológica-digital, la transición energética-medioambiental y la transición social y sanitaria que debe afrontar Euskadi. De esta manera, Gestión Capital Riesgo Euskadi, incluye en su área tecnológico-digital sectores como la Ciberseguridad o la Inteligencia Artificial entre otros, donde destaca su inversión en diversas startups de ciberseguridad del territorio, como es el caso de Opscura [28].**

Del mismo modo, **Seed Capital Bizkaia** es un programa de inversión que se centra en proporcionar financiación inicial (seed capital) a startups y proyectos empresariales en el territorio de Bizkaia. Esta iniciativa tiene como objetivo apoyar el desarrollo y la consolidación de nuevas empresas en etapas tempranas de su crecimiento, ofreciendo recursos financieros y, en ocasiones, asesoramiento para impulsar sus ideas y proyectos innovadores. La idea es facilitar el acceso a capital en sus fases más incipientes, promoviendo así la creación de empleo, el fomento de la innovación y el fortalecimiento del tejido empresarial en la región de Bizkaia [29].

En referencia a su política de inversión, se aplican criterios generales a la hora de realizar la selección de proyectos. De esta manera, se requiere que las empresas tengan su domicilio social y una presencia física en Bizkaia, además de una implicación económica por parte del equipo promotor en el proyecto. Si bien se consideran proyectos de diversos sectores, se excluyen las sociedades financieras, inmobiliarias y aquellas centradas principalmente en la comercialización. Además, cada fondo tiene requisitos específicos adaptados a las herramientas particulares de financiación [29]. Un ejemplo destacado de su compromiso con la inversión en ciberseguridad se evidencia a través de su respaldo a startups como Barbara IoT, Sealpath y Open Cloud Factory, entre otras.

Por otro lado, en cuanto a la inversión de naturaleza privada, Euskadi cuenta con varias entidades de inversión que operan en sectores como la ciberseguridad [17]:

- **Inveready:** con más de 15 años de trayectoria, este venture capital con sede en Donostia, invierte en empresas dinámicas para respaldar sus ambiciones de crecimiento. Su enfoque se encuentra en cuatro áreas principales: tecnología digital, ciencias de la vida, fintechs orientadas a la deuda y fintechs que combinan distintas formas de financiamiento. Actualmente gestionan 1.000 millones de euros, con más de 64 salidas materializadas y una cartera actual de 203 empresas que supera los 300 millones de euros. Algunas de las empresas en las que han invertido han sido adquiridas por multinacionales como Intel, Symantec, IBM, Facebook y reconocidos fondos internacionales. Además, otros han seguido cotizando en los principales mercados públicos como Nasdaq, BME Growth, AIM London, Euronext, etc. Especial mención requiere también su inversión en la vasca Ironchip [30].

- **ORZA:** sede en Donostia, es una entidad de inversión directa, perteneciente a los fondos de pensiones Elkarkidetza y Geroa, dedicada a la toma de acciones de empresas. A través de la internacionalización, operaciones MBO y MBI, proyectos de desarrollo empresarial, resolución de problemas de sucesión empresarial y sustitución de socios minoritarios, apoya al tejido empresarial vasco. Además, toma parte en la gestión de las participaciones de las empresas teniendo presencia activa en los Consejos de Administración de cada una de ellas, aportando experiencia, conocimiento, red de contactos y relaciones entre las propias empresas en las que participa, pudiendo crear sinergias decisivas para las mismas. Esta entidad opera principalmente en Bizkaia, Gipuzkoa, Araba y Navarra, encontrándose en su alcance la empresa CounterCraft [31].

- **All Iron Ventures:** sede en Bilbao, invierte en la transformación de la economía real a través de la automatización, los mercados, los datos y la infraestructura relacionada. Se centran en proyectos generadores de ingresos en Europa y América con fundadores visionarios, modelos de negocio validados y desafíos de escala. La obtención y asignación eficiente de capital son fundamentales para su tesis de inversión, siendo estas por norma general de 2 millones de euros. También realizan inversiones estratégicas y de seguimiento específicas de hasta 5 millones de euros por empresa [32].

- **Easo Ventures:** Sociedad de Capital Riesgo Vasca y Privada que, nace con el objetivo de acompañar a personas y empresas que tienen un claro proyecto de crecimiento, aportando inversión, asesoramiento y experiencia. Se centran en la inversión en pymes con potencial de crecimiento. Se estructura en 3 fases (fase 0, fase 1 y fase 2) invirtiendo cantidades diferentes dependiendo en la fase en la que se encuentren cada una. En la fase 0 hacen inversiones de 50.000 euros condicionada al paso por el programa de aceleración de BerriUp. En la fase 1 y 2, las inversiones son desde 10.000 euros hasta 1.000.000 de euros. Además, se reserva un porcentaje del capital disponible para valorar futuros follow-on de las compañías que evolucionen positivamente [33].

- **Talde Private Equity:** sede en Bilbao, gestiona Capital Privado que invierte fundamentalmente en pymes estatales a las que apoyan en el diseño y ejecución de sus planes estratégicos. Se centran en el crecimiento tanto nacional como internacional y consolidación sectorial [34].

- **Stellum Capital:** es una firma gestora de fondos de capital privado independiente, perteneciente a Artizarra Fundazioa, una fundación creada por un grupo de empresarios del País Vasco y Navarra. La misión de la fundación es respaldar a pequeñas y medianas empresas en la planificación y ejecución de sus planes de crecimiento, ya sea de forma orgánica o inorgánica. Toman participaciones minoritarias en empresas de diversos sectores entre los que se encuentra la ciberseguridad, con el objetivo de ayudarles en su crecimiento y desarrollo a través de una participación activa en su gestión [35].

Como hemos mencionado con anterioridad, durante los próximos años, se podrá observar un incremento en las inversiones materia de ciberseguridad, que sin duda **tendrá un impacto considerable dentro del ecosistema de la ciberseguridad de Euskadi,** afectando a empresas de diferente tipología y tamaño.

Empleo y educación

El avance de las nuevas tecnologías y la transformación digital acelerada en los últimos años ha provocado el aumento del tráfico de información y datos en la red, lo que ha llevado a la sociedad a demandar cada vez más profesionales expertos en la materia.

A su vez, la situación en cuanto a la oferta-demanda de profesionales no es la idónea, siendo la brecha de talento un factor clave. Habiéndose consultado los siguientes datos en el 2023, en Europa faltan 317.050 profesionales en ciberseguridad. Además, pese a haberse alcanzado en 2022 más de 4,7 millones de profesionales del sector, se ha detectado, una escasez de 3,4 millones de trabajadores a nivel global [36].

En el siguiente gráfico, se puede observar la representación del número de trabajadores en el ámbito de la ciberseguridad tanto a nivel **mundial**, como a nivel **europeo**, viéndose como ha ido aumentando en los últimos años.

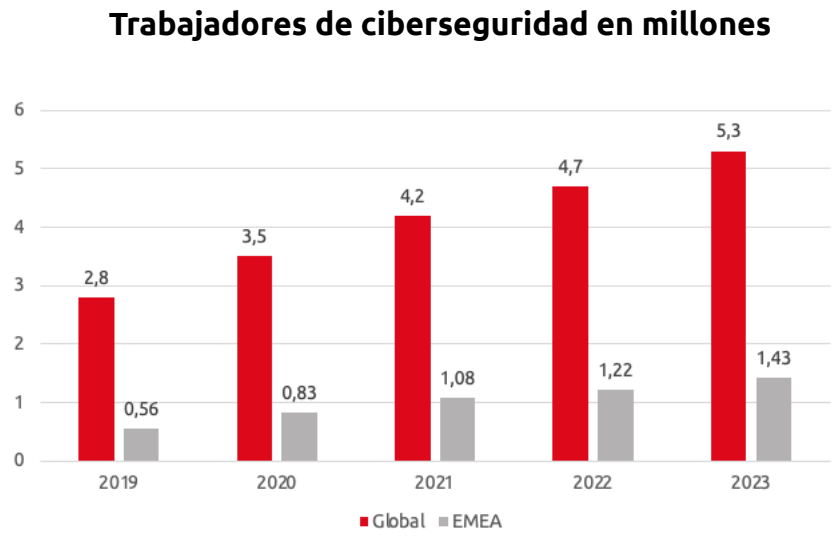


Figura 6. Trabajadores de ciberseguridad. Fuente: (ISC)2

Las últimas décadas han estado marcadas por la realización de una gran parte de nuestras actividades multidimensionales en el ciberespacio. Además de los propios beneficios que esto trae, posee una parte negativa relativa a los riesgos a los que se expone toda la civilización. Por ello, tal y como define ENISA en su modelo de capacidades, para mitigar estos riesgos se necesitan más especialistas en ciberseguridad, especialistas capaces de dar respuesta a las más sofisticadas formas de ataque y, responsables de crear una arquitectura de ciberseguridad necesaria [37]. Siguiendo en la línea de lo declarado por el Cybersec Hub, la clave para proporcionar ciberseguridad tanto en el sector público como en el privado es adaptar el sistema educativo a estos nuevos retos a largo plazo, así como a las necesidades del mercado de formar a un número cada vez mayor de ciber especialistas. Actualmente es difícil cerrar la creciente brecha de empleo en el sector TIC, formar expertos que adapten las políticas y leyes de las instituciones estatales a la ciberseguridad o, fomentar la cooperación internacional en este campo.

A nivel **estatal**, se cuenta con aproximadamente 149.000 trabajadores en esta materia [38]. No obstante, como se puede apreciar en el siguiente gráfico, sigue siendo notoria la escasez de trabajadores que se encuentran en lo que a la oferta y demanda de este sector se refiere. Brecha que surge porque la demanda de profesionales sigue siendo mayor que la oferta de trabajadores existentes. Es apreciable que, a pesar de encontrarse con una oferta mayor cada vez mayor, esta no crece a un ritmo suficiente como para abastecer a esta industria. En el gráfico que se muestra a continuación se puede observar como la brecha entre estos dos universos (oferta y demanda) sigue acrecentándose año tras año.

Proyección de empleo en España

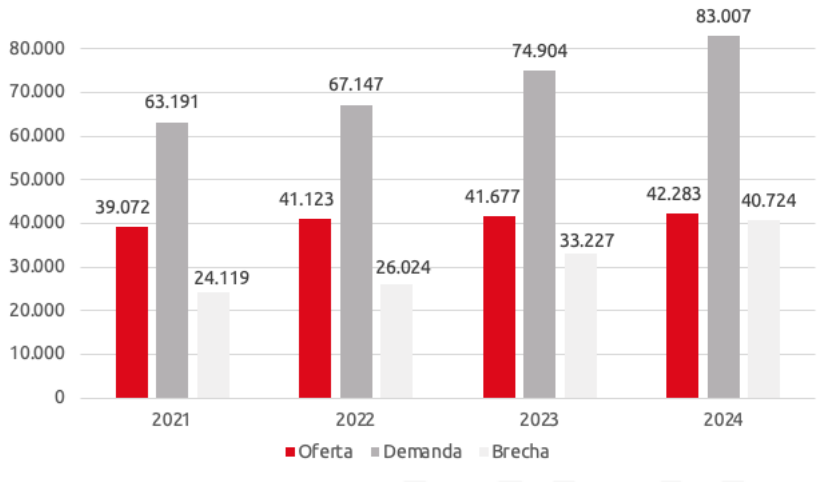


Figura 7. Proyección de empleo en España. Fuente: ObservaCIBER

De esta manera, 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). Entre los perfiles más demandados en la actualidad destacan los siguientes [37]:

Chief Information Secuirty Officer

Gestor de incidentes

Cumplimiento normativo en materia de ciberseguridad

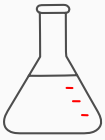
Especialista en ciberinteligencia

Arquitecto de ciberseguridad

Auditor de ciberseguridad

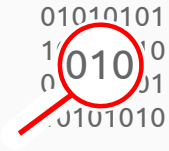
Formador en ciberseguridad

Implementador



Investigador de ciberseguridad

Asesor de riesgos



Forense digital

Analista de amenazas

Adicionalmente, otra de las técnicas que se está llevando a cabo desde las empresas es lo que se conoce como el upskilling, concepto que hace referencia al proceso de aprender y potenciar habilidades que ayuden a los empleados a mejorar su productividad y a ser más competitivos dentro de sus respectivas áreas de trabajo, como por ejemplo dentro del campo de la ciberseguridad.

En línea con estas tendencias en términos de capacitación, conviene resaltar algunas de las iniciativas impulsadas por las diferentes instituciones públicas de Euskadi. A modo de ejemplo, el Departamento de Desarrollo Económico, Sostenibilidad y Medioambiente del Gobierno Vasco, a través de SPRI lleva tiempo impulsando estas disciplinas por medio de diferentes programas y servicios de apoyo a profesionales, contribuyendo así a su capacitación y formación dentro del ámbito de la ciberseguridad. Un caso de éxito en este campo son los diferentes talleres y jornadas que se organizan desde la red de centros ENPRESA DIGITALA de SPRI, y que abarcan un amplio espectro de materias como el Pentesting, el Hacking Ético, el CRA (Cyber Resilience Act) o la LOPD, entre otras.

A nivel de Euskadi, puede observarse que la demanda de empleo de ciberseguridad está experimentando un fuerte crecimiento. Principalmente, se requieren profesionales que hayan obtenido estudios de nivel superior, tanto estudios universitarios como estudios de Formación Profesional.

En lo que respecta a la demanda de perfiles de estudios de Grados Superiores de Informática y Telecomunicaciones, como se aprecia en el siguiente gráfico, se ha producido un aumento significativo en la demanda de estos perfiles por parte de las empresas vascas del sector [39].

Demanda de graduados de Formación Profesional

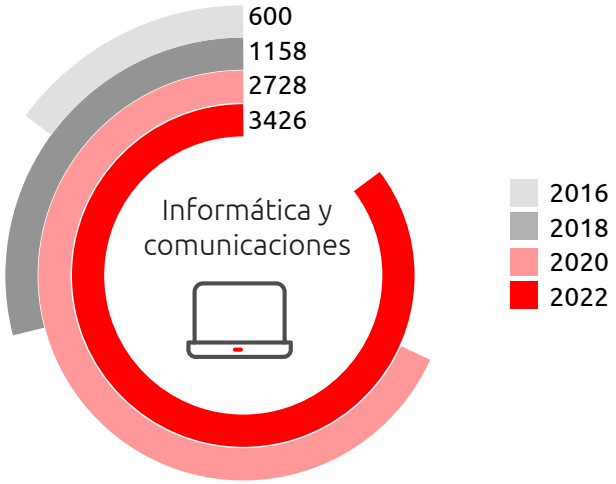


Figura 9. Demanda de Formación Profesional en Euskadi. Fuente: Cybasque

En la misma línea, se encuentra la demanda de perfiles de profesionales con estudios universitarios.

Demanda de universitarios en Euskadi

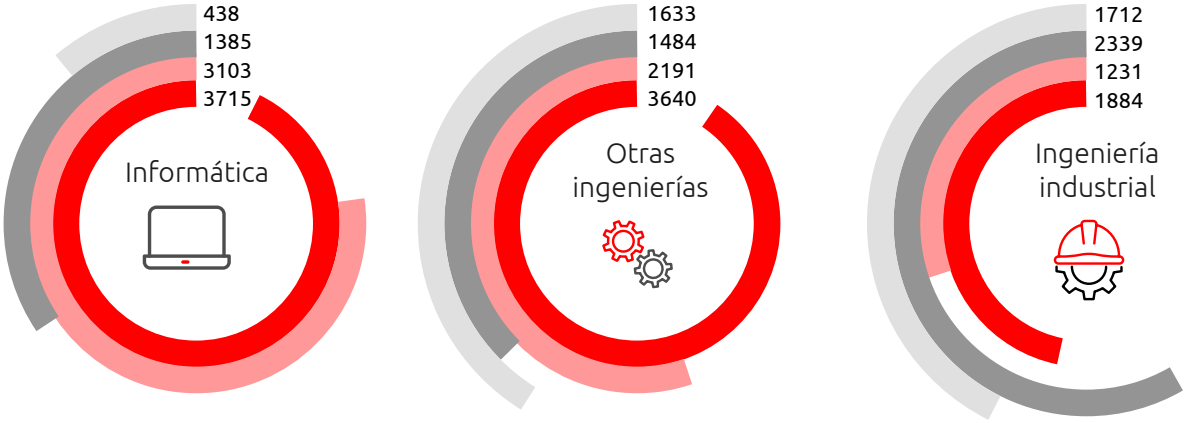


Figura 10. Demanda universitarios en Euskadi. Fuente: Cybasque

En cuanto a la brecha entre profesionales y la oferta laboral en materia de ciberseguridad, es crucial mencionar las iniciativas promovidas por diversos organismos públicos, así como explorar la gama de programas educativos disponibles en el ámbito de la ciberseguridad actualmente en Euskadi.

En línea con esto último, y con el objetivo de tratar de disminuir la brecha existente en cuanto oferta-demanda, el Gobierno Vasco lanzó la estrategia STEAM Euskadi en el año 2018 [40]. Se trata de una estrategia que cuenta con el objetivo de impulsar la educación y formación científico-técnica en todas las etapas educativas. Esta iniciativa busca promover la educación en ciencia y tecnología en todos los niveles educativos. En este sentido, Euskadi busca cumplir los siguientes objetivos con esta estrategia [41]:

- **Impulsar la educación y formación** científico-técnica en todas las etapas educativas.
- **Inspirar vocaciones y aspiraciones profesionales** en el ámbito STEM, con especial atención en las alumnas, para una preparación adecuada ante los retos de futuro.
- **Promocionar la divulgación** y la cultura científico-tecnológica entre la ciudadanía vasca.

Por otro lado, la atracción de talento de fuera de la Comunidad Autónoma de Euskadi también se erige como una palanca fundamental a la hora de combatir esta falta o escasez de nuevos profesionales de ciberseguridad. Bajo esta perspectiva, es digno de mención la estrategia denominada "Basque Talent", que Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco, en colaboración con SPRI, ha puesto en marcha, con el objetivo de abordar el reto del talento para su desarrollo, fidelización, atracción y acogida, dando lugar a una iniciativa única y común en toda Euskadi. Se espera que a través de esta iniciativa se pueda favorecer también a que profesionales de la ciberseguridad de fuera de la CAE puedan recalar en el territorio con el objetivo de nutrir a las diferentes empresas que conforman el ecosistema de ciberseguridad de Euskadi.

> Las diferentes universidades de Euskadi están realizando un importante esfuerzo, tratando año tras año de adaptar, mejorar e incluir nuevos estudios en materia de ciberseguridad

En materia de ciberseguridad, para el profesional que se dedique a ello, resulta imprescindible que éste sea conocedor de diferentes aspectos técnicos relacionados con la informática. Por este motivo, se valora de forma muy positiva el haber cursado o disponer de algún tipo de ciclo formativo de grado superior en la familia de la informática y las comunicaciones o de estudios universitarios en estas áreas. Del mismo modo, estos profesionales deben poseer también ciertos conocimientos en el campo de la seguridad informática aplicada a diferentes entornos (Industrial, IoT, etc.), que se pueden obtener a través de másteres u otra serie de estudios de postgrado en ciberseguridad.

En este sentido, **Euskadi cuenta con diferente oferta educativa en la materia**. En términos de educación superior, nos encontramos con la posibilidad de realizar estudios tanto a nivel de Formación Profesional como a nivel Universitario en Euskadi.

Actualmente Euskadi cuenta **con dos grados superiores de Formación Profesional** que son impartidos en 12 centros diferentes [42]:

Curso de Especialización en Ciberseguridad en entornos de las Tecnologías de la Información	Ciberseguridad en Entornos de las Tecnologías de Operación
CPIFP Egibide LHIPI CIFP Txurdinaga LHII CPIFP Maristak Durango LHIPI CIFP Tartanga LHII CIFP Izarraitz Lanbide Heziketa LHII IES Xabier Zubiri-Manteo BHI CIFP UNI Eibar-Ermua LHII	CIFP Andra Mari Lanbide Heziketa LHII CIFP Easo Politeknikoa LHII IES Laudioalde Lanbide Eskola BHI CPIFP Lea-Artibai LHIPI CIFP Urola Garaiko Lanbide Eskola LHIPI

Figura 11. Oferta de Grados Superiores de Formación Profesional. Fuente: elaboración propia

Además de los centros previamente listados, nos encontramos con otros centros que, toman parte en **diferentes iniciativas e imparten cursos profesionales relacionados** con la materia. En este sentido es preciso destacar la presencia del **Centro de Estudios SEIM** que, cuenta con dos cursos concretos en materia de ciberseguridad, el "Curso de Hacking Ético" y el "Máster de Ciberseguridad" [43]. Este último se configura como un Máster Título Propio que tiene como objetivo nutrir y actualizar los conocimientos de los profesionales en materia de detección, protección y prevención de delitos informáticos [44].

Por otro lado, el Centro de Formación Profesional **Politeknika Txorierri,** imparte cursos profesionales tales como el "Curso de Ciberseguridad. Entornos Ubicuos y Móviles" con el objetivo de que su alumnado pueda obtener los conocimientos necesarios para la protección de redes y sistemas, y sepan detectar y evaluar vulnerabilidades que pudieran ser explotadas por ciberatacantes [43].

Resulta destacable también su iniciativa en la materia, ya que este centro forma parte del proyecto DICYSTECH. Este proyecto llevado a cabo entre 2021 y 2023, reúne a cinco socios de la Unión Europea provenientes de Grecia, Portugal, Italia y España. Su objetivo es desarrollar módulos de formación accesibles y laboratorios remotos de ciberseguridad. Estos recursos tienen un doble propósito: satisfacer las demandas de la Smart Industry y ofrecer una experiencia educativa innovadora en la era digital [45][46].

Otro de los claros ejemplos es Tknika que, al igual que Politeknika Txorierri, imparte cursos profesionales en materia de ciberseguridad, como por ejemplo los siguientes: "Bases de la Ciberseguridad OT"; "Ciberseguridad en instalaciones automatizadas" y "Principales amenazas de ciberseguridad en nuestro centro" [47]. Es destacable también que este centro cuenta con un espacio **Cyber Range.** En él, el alumnado puede acercarse a las instalaciones para realizar entrenamientos, ejercicios o competiciones de ciberseguridad en un entorno controlado donde poner en práctica las habilidades y conocimientos adquiridos.

En cuanto a la oferta formativa y educativa a nivel universitario, desde las diferentes universidades de Euskadi se está realizando un importante esfuerzo, tratando año tras año de adaptar, mejorar e incluir nuevos estudios relacionados con la ciberseguridad. Un claro ejemplo de ello es el de **Universidad EUNEIZ**, universidad privada, reconocida por Ley 8/2021, de 11 de noviembre y que, en el curso 2022/2023 comenzó a impartir de forma gradual una

amplia oferta de enseñanzas universitarias en todos sus niveles. A este respecto, cabe destacar su nuevo **Grado en Ciberseguridad** de 240 ECTS, iniciativa que muestra claramente el compromiso del centro con la ciberseguridad y la necesidad de ir creando itinerarios y programas formativos específicos que permitan un mayor grado de especialización entre los estudiantes de la Comunidad Autónoma de Euskadi y posibiliten el nutrir a las empresas del sector de nuevos profesionales en la materia [48].

De forma adicional, la **oferta universitaria** en Euskadi resulta mucho más extensa. De esta manera, a continuación, se presentan algunos de los grados, másteres y cursos de postgrado específicos de ciberseguridad que se han identificado y que se imparten desde las diferentes universidades de la Comunidad Autónoma de Euskadi:

Universidad de Vitoria-Gasteiz EUNEIZ	Grado universitario en Ciberseguridad
eman ta zabal zazu UPV EHU	Máster en Protección de datos personales, ciberseguridad y derecho de las TICs Máster en Ciberseguridad 4.0
Mondragon Unibertsitatea	Máster en análisis de datos, ciberseguridad y computación en la nube Curso online en Ciberseguridad en las flotas de vehículos Curso online en Normativa de ciberseguridad para vehículos UNECE/R155 Curso online en Ejecutivo de ciberseguridad corporativa GRC Curso online en Ciberseguridad: Mecanismos de protección y defensa Curso online en Ciberseguridad industrial Curso online en Gestión de incidentes de ciberseguridad
Deusto Universidad de Deusto Deustuko Unibertsitatea	Curso superior de ciberseguridad

Figura 12. Oferta universitaria. Fuente: elaboración propia

Por otro lado, en este punto es importante destacar también la oferta en cuanto a grados universitarios en ámbito STEM, por ser académicamente troncales a la ciberseguridad. En este aspecto, Euskadi cuenta con diferentes centros en los que poder realizar diferentes grados universitarios de esta naturaleza. A continuación, se muestran dichos grados y másteres:

UPV EHU	Grado en Ingeniería de Gestión y Sistemas de Gestión y Sistemas de Información Grado en Ingeniería Informática Grado en Ingeniería en Tecnología de Telecomunicación
Deusto	Grado en Ingeniería Informática Doble Grado en ADE + Ingeniería Informática Doble Grado en Ingeniería Electrónica industrial y automática + ingeniería informática Doble Grado en Ingeniería informática + ciencia de datos e inteligencia artificial
Mondragon Unibertsitatea	Grado en IngenieríaInformática
Universidad de Navarra	Grado en Ingeniería en Sistemas de Telecomunicación Máster en Innovación tecnológica

Figura 13. Oferta grados universitarios ámbito STEM. Fuente: elaboración propia

A pesar de que el perfil típico o tradicional de la ciberseguridad se encuentre ligado al perfil de la ingeniería, se trata de un terreno mucho más amplio. De esta manera, aunque gran parte de las especializaciones son de carácter técnico, se ha visto acrecentada también la demanda en cuanto a profesionales de la ciberseguridad que dominen otros ámbitos como el jurídico. El campo normativo y legislativo cada vez tiene más relevancia en la ciberseguridad, claro ejemplo de ello son los estándares normativos o las regulaciones como el Reglamento General de Protección de Datos (en adelante, RGPD) [49] o la Directiva de la UE Network and Information Security [50].

Otro aspecto para tener en cuenta a la hora de hablar de la oferta y demanda de empleo en materia de ciberseguridad es el salario medio por trabajador a nivel mundial, europeo, estatal y regional.

La siguiente representación gráfica exhibe el salario promedio de expertos en ciberseguridad, detallando su variación geográfica y considerando diversos perfiles profesionales dentro del sector.

Salario medio trabajador de ciberseguridad

Figura 14. Salario medio de trabajadores en ciberseguridad por ámbito geográfico. Fuente: (ISC)2 e Indeed

Del gráfico anterior se puede deducir que, **Euskadi** al igual que España, **se enfrenta al riesgo de fuga de talento debido a la significativa disparidad salarial,** principalmente en comparación con Europa y los EE. UU. Según se muestra, el salario promedio para profesionales de ciberseguridad es de 135.000 dólares en EE. UU., 93.500 euros en Europa, y entorno a los 30.000 euros a nivel estatal y regional [36][51].

A nivel de Euskadi, por lo tanto, es importante poner el foco en la amenaza latente de pérdida de talento en el ámbito de la ciberseguridad debido a la presente brecha salarial con respecto al resto de la región EMEA y los EE. UU. Esta disparidad se traduce en sueldos inferiores, generando una situación de riesgo en la retención de profesionales altamente cualificados. La competitividad salarial ha desencadenado una rotación considerable de expertos, quienes buscan oportunidades con compensaciones más atractivas, creando así movimiento constante de talento entre organizaciones en busca de mejores condiciones económicas. 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.

Tendencia alcista en Euskadi en lo que a los sueldos en materia de ciberseguridad se refiere

Emprendimiento

El emprendimiento y las estrategias para incentivarlo son un pilar fundamental que un ecosistema de cualquier sector debe poseer, muy especialmente un sector tan incipiente, relevante y transversal como es el de la ciberseguridad. Por ello, este apartado destaca las competencias e iniciativas que deben existir en este ámbito. Entre ellas, se encuentran aspectos clave como el respaldo a las nuevas empresas mediante diferentes iniciativas, como, por ejemplo, aceleradoras o incubadoras de startups. Esto implica la creación de programas de asesoramiento especializado, donde se brinda orientación técnica a emprendedores. Asimismo, se habla sobre el respaldo financiero, ya que, el acceso a fondos de inversión, subvenciones y recursos económicos que permitan a estas nuevas empresas despegar, se configura como fundamental.

En cuanto al ecosistema de incubadoras y aceleradoras de apoyo al emprendimiento en ciberseguridad a nivel internacional, a continuación, se muestra un listado que recoge numerosas incubadoras y aceleradoras de startups que conforman el ecosistema internacional de apoyo al emprendimiento en el ámbito de la industria de la ciberseguridad.

Nombre	Descripción	País	Web
A1 Start Up Campus	A1 Start Up Campus es un lugar en el que tres expertos especializados trabajan estrechamente con las startups y buscan nuevos socios potenciales que puedan ayudarles a crecer.	Austria	https://a1startup.net
Ääkköset Oy	Apoya a personas con mentalidad emprendedora en su búsqueda de soluciones a problemas relacionados con la ciberseguridad.	Finlandia	https://www.scanabc.com/
Accelerator Frankfurt	Accelerator Frankfurt es un programa de tres meses que ayuda a las empresas tecnológicas de software B2B a comercializar sus productos con mayor rapidez.	Alemania	https://www.accelerator-frankfurt.com/
Bing Fund	El fondo de riesgo de Microsoft invierte en empresas de software empresarial en fase inicial, centrándose en Inteligencia Artificial aplicada, aplicaciones empresariales, infraestructura, seguridad y tecnologías de vanguardia.	Estados Unidos	https://m12.vc/
Crosspring	Crosspring es un inversor semilla en fases tempranas e invierte en startups de tecnología digital. Están activos en los campos de FinTech, Al, B2B, SaaS, Ciberseguridad, AgriTech, AR/VR, Alimentación y Horti-tech.	Países Bajos	https://crosspring.com/startups/
CTM insights	CTM Insights es una empresa que ayuda a las startups de ciberseguridad con el desarrollo de proyectos y dinero.	Estados Unidos	https://ctminsights.com/
Cyberport Hong Kong	Cyberport Hong Kong es un centro de tecnologías de la información y la comunicación que da acceso a instalaciones y servicios de red de banda ancha a startups y empresarios del sector de las TIC.	Hong Kong	https://cyberport.hk/en

CyLon	CyLon es el principal inversor en fase inicial en seguridad y resiliencia de Europa, invierten utilizando su propio capital para permitirse estar alineados de manera única con los fundadores.	Reino Unido	https://www.cylonventures.com/
CyRise	CyRise Bootcamp ayuda a las startups de ciberseguridad y a las personas que trabajan internamente en ciberseguridad a mejorar, más rápido.	Australia	https://www.cyrise.co/#
Energia Ventures	Energia Ventures es una aceleradora intensiva de tres meses para emprendedores con negocios innovadores en los sectores de la energía, redes inteligentes, inteligencia artificial, tecnologías limpias y ciberseguridad.	Canadá	https://www.energiaventures.com/
Exponential Impact	Exponential Impact es una aceleradora de startups dirigida por mentores y centrada en tecnología Al, blockchain y ciberseguridad.	Estados Unidos	https://www.exponentialimpact.com/
Founders.ai	Founders.ai invierte en startups de pre-semilla y semilla que utilizan Al y datos para cambiar la empresa. Su enfoque: IA /NLP/Machine Learning, Data/Analytics, Cloud Infrastructure, Cybersecurity, Future of Work.	Estados Unidos	https://www.failory.com/startups/cyber-security-accelerators-incubators#31-taqadam
Future Labs	Forma parte de NYU Tandon Future Labs, una red de programas de innovación que ayuda a las empresas emergentes del mañana con recursos y tutoría; Áreas de interés: IA, RA, computación en nube, ciberseguridad, datos y analítica.	Estados Unidos	https://futurelabs.nyc/
ICE71	Innovation Cybersecurity Ecosystem es el primer lugar para emprendedores en ciberseguridad de la zona.	Singapur	https://ice71.sg/accelerate/
ICE71 Accelerate	Innovation Cybersecurity Ecosystem at BLOCK71 (ICE71) es el primer centro de emprendedores en ciberseguridad de la zona.	Singapur	https://ice71.sg/accelerate/
International Security Accelerator	CorkBIC es una organización creada hace casi 30 años para encontrar y crear empresas intensivas en conocimiento basadas en tecnologías prometedoras y personas inteligentes y creativas.	Irlanda	https://isa.corkbic.com/
KOISRA Seed Partners	KOISRA Seed Partner es una aceleradora coreano-israelí que se centra en campos industriales como la telefonía móvil, la ciberseguridad, Internet, la IoT, la robótica, la medicina, el comercio electrónico y las telecomunicaciones.	Corea Del Sur	http://www.koisraseedpartners.com/

L-SPARK	L-SPARK Accelerator es el lugar donde las empresas de SaaS y cloud que están listas para salir al mercado pueden reunirse con expertos en SaaS de Canadá.	Canadá	https://www.l-spark.com/
MACH37	MACH37TM una aceleradora de ciberseguridad centrada en el mercado de Estados Unidos.	Estados Unidos	https://www.mach37.com/
MARL 5G Accelerator	MARL 5G es un programa acelerador para startups que se centran en fabricar productos y servicios DeepTech para clientes empresariales que funcionan con 5G.	Estados Unidos	https://marlaccelerator.com/
NCSC Cyber Accelerator	El objetivo del NCSC Cyber Accelerator es acelerar las nuevas ideas e innovaciones en ciberseguridad en el REINO UNIDO.	Reino Unido	https://www.ncsc.gov.uk/section/ncsc-for-startups/overview
Orevon Partners	Orevon Partners es un nuevo fondo y plataforma de inversión tecnológica para la próxima generación de líderes en DeepTech y Healthlech.	Luxemburgo	https://www.failory.com/startups/cyber-security-accelerators-incubators#24-conscious-venture-lab
OXO Cybersecurity Lab	OXO Cybersecurity Lab es una incubadora independiente de OXO Labs creada para apoyar la innovación en ciberseguridad.	Budapest	https://cybersecurity.oxolabs.eu/
Startup Wise Guys	Startup Wise Guys es el principal inversor y acelerador de startups B2B en fase inicial de Europa, con más de 400 empresas en su cartera de inversiones, en diversos sectores (SaaS, Fintech, Sostenibilidad, Realidad XR, Ciberseguridad).	Estonia	https://www.failory.com/startups/cyber-security-accelerators-incubators#34-foundersai
Startupbootcamp Fintech Singapore	Startupbootcamp es una red global de aceleradoras centradas en la industria. Ayudan a globalizar startups dándoles acceso directo a una red internacional de los socios, inversores y mentores más relevantes de su sector. Numerosos temas, incluida la ciberseguridad.	Singapur	https://www.startupbootcamp.org/accelerator/fintech-singapore/
StartupX-seed Ventures	Comenzaron con el objetivo de crear un ecosistema más completo para startups y emprendedores en la India; Con inversiones desde SaaS hasta Space (Tech), incluyendo las áreas de Ciberseguridad, Semicon, Al/ML, Drones y Startups de Nueva Frontera en la India con un Enfoque Global.	India	https://startupx-seed.in/

Taqadam	Tagadam ha ayudado a las startups a crecer dándoles acceso a expertos y mentores locales, inversores y redes profesionales, así como hasta 140.000 dólares de financiación; Al, Data Science, CberSecurity y loT.	Arabia Saudí	https://taqadam.kaust.edu.sa/
Viveka	Viveka es una aceleradora de servicios completos que diseña, desarrolla y lleva a cabo programas de preincubación, incubación y aceleración, incluida la ciberseguridad.	Turquía	https://www.viveka.com.tr/
Wise Guys Cyber	Wise Guys Cyber está formado por un grupo diverso de personas amantes de la tecnología, mentores, expertos y fundadores.	Estonia	https://startupwise-guys.com/verticals/cybersecurity/
Xpreneurs	XPRENEURS es un programa de incubación de tres meses a tiempo completo. Numerosos temas, incluida la ciberseguridad	Alemania	https://xpreneurs.io/

Tabla 1. Incubadoras y aceleradoras de apoyo al emprendimiento en ciberseguridad a nivel mundial. Fuente: elaboración propia

Reparando en actuaciones promovidas por entidades estatales, la principal iniciativa de apoyo al emprendimiento de la ciberseguridad es el Programa para el desarrollo de ideas de negocio, incubación y aceleración de proyectos de ciberseguridad (INCIBE Emprende 2023-2026) [52].

INCIBE Emprende forma parte de El Plan Estratégico 2021-2025 de INCIBE, en línea con la agenda España Digital 2026 y el Plan de Recuperación, Transformación y Resiliencia, que tiene entre sus objetivos el fortalecimiento de las capacidades de ciberseguridad de ciudadanos, pymes y profesionales, y el impulso del ecosistema del sector ciberseguridad.

Los objetivos de este programa son los siguientes [52]:

- Acompañar a los emprendedores y a las startups estatales.
- Impulsar el desarrollo de los proyectos a lo largo de las fases del proceso emprendedor.
- Apoyar el emprendimiento en ciberseguridad y la ciberseguridad en el emprendimiento.

Dotado con un presupuesto superior a 45 millones de euros, de los cuales 30 millones son para la Inversión Pública y, más de 15 millones en ayudas para los emprendedores. Estas partidas se canalizarán a través del Plan de Recuperación, Transformación y Resiliencia, y la Agenda Digital 2026 [53].

La nueva invitación pública permitirá seleccionar las entidades colaboradoras que ejecutarán las acciones de emprendimiento de manera conjunta con INCIBE. Entre sus principales objetivos se pueden destacar la promoción del emprendimiento en ciberseguridad en todo

el territorio nacional, con especial incidencia en las provincias y regiones menos desarrolladas empresarialmente.

Cabe resaltar que este centro, con el objetivo de impulsar el emprendimiento en ciberseguridad, hoy en día, ya ha acelerado 35 startups, se han incubado 57 proyectos y se han creado 160 puestos de trabajo.

A su vez, **Euskadi,** cuenta con un dilatado ecosistema de apoyo público distintivo al emprendimiento en el que, sin duda, las startups de ciberseguridad, vinculadas principalmente al emprendimiento digital, encuentran cabida [17].

Dispone de un ecosistema maduro compuesto por más de 100 agentes públicos y privados, una red de inversores activa y muy potente, y una red de centros tecnológicos capaces de proveer el talento y los activos tecnológicos necesarios. Además de un apoyo institucional diferencial a través del cual, a nivel regional, promueven y apoyan proyectos emprendedores en todas y cada una de las diferentes etapas de maduración [17].

> 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

El ecosistema ha experimentado un notable crecimiento y vitalidad, con la inclusión de diversos actores privados y entidades de naturaleza pública en áreas como las finanzas, la tecnología o el campo académico entre otros. Esta diversificación ha generado un entorno actual con capacidades multidisciplinarias que respaldan el espíritu emprendedor. Se ha creado un entramado de profesionales, recursos financieros, redes de apoyo, infraestructuras y programas de difusión, entre otros elementos, que se apoyan en un marco normativo, fiscal e institucional sólido y confiable. Todo eso se suma a la importancia crucial de tener un entramado empresarial, industrial y tecnológico robusto, junto con una sociedad altamente educada y cohesionada, que actúan como el origen y destino de múltiples iniciativas emprendedoras [17].

Todo este apoyo diferencial se rige por una **estrategia** que persigue unos objetivos concretos. Desde los años 80, el sector público del País Vasco ha hecho un esfuerzo importante por estar a la vanguardia a la hora de respaldar a nuevas empresas y emprendedores, generando condiciones fundamentales y ofreciendo una gama cada vez más amplia de apoyos y recursos adaptados a las necesidades de diversos tipos de colectivos emprendedores. Este esfuerzo ha equiparado al ecosistema vasco con otros sistemas de referencia tanto a nivel nacional como internacional. Este firme compromiso se refleja y se rige por el **Plan Interinstitucional de Emprendimiento (PIE) 2024** [54].

El plan PIE se centra en proporcionar a las empresas vascas herramientas, recursos y programas que les permitan desarrollar estrategias de emprendimiento exitosas. Estas herramientas incluyen asesoramiento personalizado, programas de formación, acceso a información sobre mercados exteriores, apoyo en la búsqueda de socios y distribuidores internacionales, o financiación específica para proyectos de emprendimiento, entre otros [54].

Con todo ello, su objetivo principal es apoyar el desarrollo de nuevas iniciativas empresariales a través de servicios a lo largo de toda la cadena de valor del emprendimiento. Esta estrategia se materializa en forma de diferentes iniciativas que se detalla a continuación, y que sin

duda favorecen a la eclosión de nuevas empresas emergentes vinculadas al sector de la ciberseguridad.

Entre estas iniciativas, destaca la red de **Business Innovation Centers (BICs)** que, promovidos por el Gobierno Vasco, SPRI, las diputaciones forales y ayuntamientos, constituyen el "brazo ejecutor" de estas políticas y programas de apoyo al emprendimiento avanzado. Fomentan el desarrollo de nuevos negocios innovadores proporcionando servicios de apoyo a lo largo de todo el proceso emprendedor. También pueden ofrecer un itinerario de "soft landing" con servicios personalizados de reubicación para emprendedores. Desde la red de BICs se persigue apoyar proyectos o iniciativas de emprendimiento dirigidas a la creación de nuevas empresas de base tecnológica y con un marcado carácter innovador [55][56][57][58].

BIC ARABA UP! EUSKADI
BIC BIZKAIA EZKERRALDEA UP! EUSKADI
BIC BIZKAIA UP! EUSKADI
BIC GIPUZKOA UP! EUSKADI

Los BICs cuentan con una filosofía de networking, trabajando a nivel regional en colaboración con diferentes agentes (centros tecnológicos, instituciones financieras públicas y privadas, universidades…) y a nivel global con actores clave en los principales centros de emprendimiento en todo el mundo.

Estos centros buscan empresas de base tecnológica, caracterizadas por su profundo componente innovador y que generalmente focalizan su actividad en alguno de los tres ámbitos de especialización inteligente del territorio: industria inteligente, las energías limpias y la salud personalizada. Estas áreas representan nichos estratégicos donde estas startups buscan desarrollar soluciones vanguardistas y disruptivas, aprovechando las oportunidades que ofrecen estos sectores emergentes y de gran potencial de crecimiento.

Actualmente, Euskadi cuenta con 4 BICs repartidos por territorio histórico, contando con dos en el territorio de Bizkaia: BIC ARABA, BIC BIZKAIA, BIC BIZKAIA EZKERRALDEA y, BIC GIPUZKOA. Son entidades consideradas como referentes indiscutibles dentro del campo del emprendimiento a nivel regional [55][56][57][58].

BIND 4.0 Basque Open Innovation Platform

En paralelo a la labor de los BICs, es digno de mención también la iniciativa **BIND 4.0 Basque Open Innovation Platform [59]**

Esta iniciativa, se establece como un espacio de innovación abierta a través del cual un conjunto diverso de entidades (que incluye desde empresas líderes en el mercado hasta pymes o entidades públicas), identifican desafíos o diferentes retos específicos que afectan a sus respectivos negocios, al mismo tiempo que se promueven convocatorias abiertas para que startups de todos los rincones del planeta presenten soluciones con el objetivo de resolver o dar respuesta a dichos desafíos concretos. Este proceso se traduce en un importante beneficio para ambas partes, ya que la entidad que identifica el desafío satisface o resuelve alguna necesidad en cuanto a su negocio, mientras

que la startup obtiene la oportunidad de trabajar en el desarrollo de un nuevo proyecto, al mismo tiempo que adquiere una referencia en cuanto a cliente que ayuda a fortalecer su posicionamiento en el mercado. Bajo este enfoque son unas cuantas las startups de ciberseguridad que han participado y se han visto beneficiadas en los últimos años por BIND 4.0 Basque Open Innovation Platform.

BIND 4.0, posee un importante reconocimiento a nivel europeo, destacándose el haberse erigido como ganador en la categoría "Improving the Business Environment" en la XIV Edición de los Premios Europeos a la Promoción Empresarial (EEPA), organizados por la Dirección General de Mercado Interior, Industria, Emprendimiento y pymes de la Comisión Europea.

Además, esta iniciativa se desglosa en tres líneas de actividad diferentes, con el objetivo de tratar de dar respuesta no solo a retos de empresas tractoras de Euskadi, sino también al tejido de pequeñas y medianas empresas de Euskadi, o incluso a entidades de naturaleza pública.

Por un lado, **BIND 4.0 Acceleration Program** lleva a cabo una convocatoria anual, ofreciendo aceleración a startups de alto impacto y la posibilidad de abordar proyectos colaborativos en el ámbito de Industria Inteligente fundamentalmente. Estos proyectos se ejecutan en entornos reales, con líderes del Ecosistema empresarial Vasco participando como Clientes de estas startups. El premio o recompensa final se erige en forma de proyecto llevado a cabo para algunas de estas importantes firmas, de manera que permite el escalado y continuar con el desarrollo de los productos o soluciones que ofrecen las startups que participan en el programa. Además, este programa que actúa como puente entre startups disruptivas y empresas destacadas en la industria, ofrece diferentes tipos de sesiones y talleres dirigidos a diversas áreas temáticas tales como networking, el asesoramiento empresarial o la formación específica a la hora de enfrentarse a oportunidades de negocio para clientes de estas características.

BIND 4.0: galardonado en la categoría "Improving the Business Environment" en la XIV Edición de los Premios Europeos a la Promoción Empresarial (EEPA) de la Comisión Europea

Conecta equipos dinámicos de startups con más de 70 empresas líderes en el País Vasco. Actualmente en su octava edición y, desde sus inicios, ha acelerado más de 130 startups y ha promovido el desarrollo de más de 200 proyectos, superando los 6,5 millones de euros de facturación. Y es que esta iniciativa público-privada del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco, se ha convertido en un referente de innovación abierta y aceleración de la Industria Inteligente a nivel mundial [60].

Otra de las líneas de actividad de esta plataforma es el **BIND 4.0 SME Connection**, donde las startups innovadoras descubren desafíos de diversas empresas de pequeño o mediano tamaño de Euskadi, y se sumergen en el ecosistema empresarial vasco, a través de la innovación abierta. Las startups participantes obtienen clientes de referencia en sectores estratégicos, mientras abordan proyectos dirigidos a implementar soluciones en entornos reales para resolver retos o desafíos de diferentes empresas de tipo PYME. El objetivo por lo tanto es dual, esto es, por un lado, conseguir resolver diferentes retos o problemáticas de negocio de estas pymes a través de la adopción de soluciones disruptivas ofrecidas por startups, y por otro lado, la posibilidad a estas últimas de ganar una referencia comercial en mercados importantes, además de la oportunidad de continuar evolucionando y desarrollando sus respectivos productos o soluciones. Para la identificación de estos clientes, el equipo BIND SME Connection se apoya en algunas de las ODCs (Organizaciones Dinamizadoras de Clusters) que cuentan con presencia y actividad en Euskadi [61].

Por último, es digno de mención también el **BIND 4.0 GovTech**. Lanzado por primera vez en 2022, busca abrir una nueva ventana de oportunidades de colaboración entre startups e instituciones públicas del **País Vasco**, fomentando la innovación y la transformación de los servicios y procesos que se ofrecen desde la Administración. Mediante esta iniciativa, nuevas empresas emergentes enfrentarán los desafíos tecnológicos de diferentes entidades de naturaleza pública mediante proyectos de innovación abierta. Las startups seleccionadas podrán implementar sus soluciones en entornos reales, colaborando con una o más empresas del sector público del País Vasco. Como instituciones públicas participantes en la primera edición se encuentran: SPRI, Ihobe, EJIE, Parke, EVE y HAZI [62].

Otra de las iniciativas llevadas a cabo en este ámbito en Euskadi es la nueva plataforma Up!Euskadi [63], 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.

Las startups, los inversores o diversos agentes del ecosistema, pueden añadir los detalles de su organización y poner en valor su perfil proporcionando un acceso abierto a los datos para toda la comunidad.

En Up!Euskadi se pueden encontrar también las principales startups 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. Son empresas dedicadas a ciberseguridad y orientadas a diferentes ámbitos como pueden ser Cloud, protección de datos, gestión de identidades y accesos, infraestructuras, entre otros.

De forma adicional, la iniciativa **BAT - B Accelerator Tower** [64] merece una mención especial también dentro del campo de emprendimiento en Euskadi. BAT es el pilar fundamental de un proyecto que busca situar a Bizkaia y Euskadi en el escenario global del emprendimiento. Con el respaldo de las principales instituciones vascas, BAT - B Accelerator Tower se posiciona como un centro singular a nivel mundial gracias a su capacidad para integrar herramientas públicas y privadas dedicadas al emprendimiento y la innovación. Representa la apuesta conjunta del Gobierno Vasco, la Diputación Foral de Bizkaia y el Ayuntamiento de Bilbao para posicionar a Euskadi como un referente destacado en emprendimiento e innovación. Esta iniciativa es clave para la proyección internacional del entorno empresarial regional y el fomento de nuevos sectores y empresas. Entre las cuales se pueden encontrar también empresas que focalizan su actividad dentro del campo de la ciberseguridad.

Se erige como un motor vital para el florecimiento empresarial en Euskadi, respaldado por una serie de valores distintivos que lo posicionan como un referente en el impulso del emprendimiento e innovación en la región. En su enfoque hacia el talento, destaca por su promoción activa y la facilitación en la búsqueda de habilidades excepcionales. Esta iniciativa está diseñada para atraer y retener talento creativo y emprendedor, fomentando así un ecosistema empresarial diverso y en constante evolución [64].

BAT-B Accelerator Tower se distingue por su enfoque personalizado. Ofrece un acompañamiento integral, desde la etapa inicial de establecer una empresa en el territorio hasta la búsqueda estratégica de colaboradores y aliados comerciales. Este apoyo adaptado a las necesidades individuales de cada proyecto refuerza el camino hacia el éxito empresarial.

La conjunción de estos valores diferenciales consolida a BAT - B Accelerator Tower como un entorno muy interesante para el emprendimiento e innovación en Euskadi. Su compromiso firme con el crecimiento empresarial regional y su proyección internacional establecen un camino claro hacia el éxito sostenible y el desarrollo empresarial continuo en la región [64].

A este respecto, es importante hablar también sobre **Beaz Acceleration Program**, por ser la primera aceleradora de startups público-privada en Bizkaia [65].

A través de este programa de alto rendimiento, con una duración de 6 meses, se implementa una dinámica de aceleración empresarial con el propósito de respaldar al ecosistema innovador mediante cuatro pilares fundamentales: capacitación exclusiva, asesoramiento experto, financiación adaptada a las necesidades y acceso a instalaciones que promueven conexiones globales.

El esquema de la nueva iniciativa foral de apoyo al ecosistema innovador se compone de tres fases distintivas que abordan el punto de partida, el progreso realizado y el logro de los objetivos acordados, o bien la posible necesidad de extensión del proceso.

En cada caso, el programa se ajusta a las necesidades específicas de las empresas, elaborando un plan de acción diseñado para alcanzar los objetivos establecidos, proceso durante el cual también se realiza la evaluación del impacto del proceso de aceleración y los resultados obtenidos.

Por otro lado y en cuanto a los beneficios que se obtienen al pertenecer a este programa, están el acceso a una escuela de negocios de primer nivel, donde se ofrece un programa exclusivo de capacitación para impulsar el crecimiento empresarial; la obtención de asesoramiento a través de un Consejo compuesto por 5 expertos especializados en áreas clave para el desarrollo de la empresa; financiación inicial de hasta 100.000 euros, facilitando la negociación para la ronda de inversión en esta fase de crecimiento; y, acceso al Centro Internacional de Emprendimiento de Bizkaia, que incluye participación en su programa completo de eventos y oportunidades de networking empresarial [65].

De forma complementaria a estas iniciativas singulares, desde el Departamento del Departamento del Desarrollo Económico, Sostenibilidad y Medioambiente de Gobierno Vasco, se llevan impulsando en los últimos años una serie de instrumentos de apoyo a las empresas con el objetivo primordial de favorecer al emprendimiento en la región.

A continuación, se muestran las principales ayudas tanto para el ámbito del emprendimiento, como para el ámbito intraemprendimiento publicadas en el año 2023 [66]:

Nombre	Descripción	País
Ekintzaile	Apoyar a nuevos proyectos empresariales innovadores y/o de base tecnológica, industriales y/o de servicios conexos ligados al producto proceso industrial, tutelados por un "Business Innovation Center" (BIC) de los existentes en la CAE, en las fases de maduración de la idea y de puesta en marcha de la empresa en la Comunidad Autónoma de Euskadi.	1.700.000 €
Ekintzaile +	Continuación del programa Ekintzaile. Nueva línea de ayudas destinada a respaldar proyectos con un alto potencial de desarrollo, aquellos que presentan un impacto significativo o una innovación tecnológica disruptiva. Esta iniciativa proporciona financiación para los costos inherentes a la operatividad empresarial, enfatizando los gastos relacionados con la adquisición de talento. Ayuda a fondo perdido de hasta el 70% de los gastos subvencionables, con un máximo de 100.000 euros por proyecto.	1.000.000 €
Barnekintzaile	Apoyo a la actividad intraemprendedora dentro de las empresas vascas, con el fin de promover nuevos proyectos empresariales innovadores y/o de base tecnológica, industriales y/o de servicios ligados al producto-proceso industrial, tutelados por un "Business Innovation Center" (BIC) de los existentes en la CAE, en las fases de maduración de la idea y de puesta en marcha de la empresa en la Comunidad Autónoma de Euskadi.	800.000 €
BIND	BIND es una plataforma de innovación abierta promovida por el Gobierno Vasco, a través de su Agencia de Desarrollo Empresarial SPRI, y en la que participan activamente empresas de diferente naturaleza (empresas tractoras, pymes e Instituciones Públicas) con presencia en el País Vasco. Esta plataforma cuenta con 3 líneas de actividad principales: 4.0 Acceleration Program, SME Connection y GovTech.	-
Basque Fondo	Apoyo a la maduración de una idea empresarial en un BIC (Business Innovation Centre). La nueva empresa puede acceder a préstamos en condiciones favorables.	Acceso a financiación convertible
Aurrera	Apoyo a la maduración de una idea empresarial en un BIC (Business Innovation Centre). La nueva empresa puede acceder a préstamos en condiciones favorables.	Acceso a la financiación
Reto 2030	Respalda proyectos destinados a impulsar y mejorar el entorno emprendedor del País Vasco, con el objetivo de dinamizar y armonizar las diversas iniciativas, involucrando y uniendo a los diferentes actores del ecosistema. Esto tiene como meta lograr una mayor sincronización y coordinación entre ellos. Se encuentra dirigida a residentes en Euskadi y entidades legales que tienen sede social o al menos un centro de operaciones establecido en Euskadi.	15.000 €

Tabla 2. Ayudas y servicios relacionados con el emprendimiento durante la anualidad 2023. Fuente: Gobierno Vasco/SPRI

Cabe hablar también de Basque Tek Ventures, una nueva iniciativa cuyo principal objetivo es promover y acelerar la creación de proyectos empresariales de alto impacto, basados en tecnología generada por los centros tecnológicos de Euskadi [67].

Liderada por SPRI, en colaboración con BRTA y la **red de BICs** de Euskadi, busca apoyar y fortalecer la labor de los investigadores y el entorno emprendedor, contribuyendo de manera positiva en los factores clave que influyen en la creación de Nuevas Empresas de Base Tecnológica (NEBTs), complementando así su trabajo [67].

En conjunto con diversos agentes, Basque Tek Ventures tiene como meta acelerar la introducción en el mercado de las tecnologías más prometedoras y la formación de nuevas empresas mediante un proceso de "Venture Building". Esto implica un recorrido guiado para iniciar y acelerar startups tecnológicas [67].

En la etapa inicial, se colabora con grupos de investigación de los centros afiliados a BRTA para valorar activos tecnológicos, identificar oportunidades, atraer talento y desarrollar casos de negocio como base para crear nuevas empresas de base tecnológica (NEBTs). Posteriormente, se trabaja con actores del ecosistema emprendedor e inversor para acelerar el crecimiento de estas NEBTs y garantizarles la financiación necesaria.

> Basque Tek Ventures identifica y prioriza los activos tecnológicos con mayor potencial, apoya la configuración de equipos de alto rendimiento y acompaña el lanzamiento de la empresa y su acceso al mercado

Los proyectos seleccionados recibirán apoyo integral para avanzar en su maduración, con énfasis en la configuración atractiva para el talento y la inversión. El equipo de Basque Tek Ventures, en colaboración con los Business Innovation Centers (BICs), acompañará a los equipos durante todo el proceso, estableciendo un plan de acción y facilitando servicios de alto impacto para alcanzar hitos clave, como definir la estrategia, transferir tecnología, estructurar la propiedad, reclutar al equipo fundador, obtener financiamiento, establecer y desarrollar prototipos, entre otros. Con ello, se busca identificar y atraer talento emprendedor para liderar este tipo de proyectos, proporcionándoles todo el apoyo necesario a lo largo del proceso de creación de la startup.

Para respaldar financieramente estos proyectos en etapas críticas, se establece un **nuevo fondo de transferencia tecnológica gestionado por Gestión de Capital Riesgo del País Vasco (Grupo SPRI)** que, invertirá en las nuevas empresas, proporcionando el capital necesario para superar el período de alta incertidumbre conocido como el "valle de la muerte" para las startups [28].

En definitiva, se trata de un enfoque adaptado al emprendimiento en alta tecnología, que busca reforzar y complementar iniciativas existentes, mejorar su integración y abordar los desafíos cruciales en la creación de NEBTs con nuevos servicios de alto impacto. Basque Tek Ventures tiene como objetivo alinear intereses, fomentar la colaboración entre sectores público y privado, impulsar la transferencia tecnológica y generar un impacto sostenido en el territorio a largo plazo. Su misión es contribuir a la formación de un nuevo tejido empresarial basado en tecnología avanzada y acelerar la transferencia de innovación disruptiva desde centros tecnológicos hacia los sectores industriales clave de Euskadi. Esta iniciativa de reciente creación ya cuenta con algún caso de éxito relacionado con startups que focalizan su actividad dentro del marco de la ciberseguridad.

Al hilo de lo anterior, es necesario resaltar que, 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 inno-

vación, mejorando y fortaleciendo sus servicios para potenciar el sector y enfrentar un futuro repleto de oportunidades [23]. 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.

Valor de las startups en Euskadi

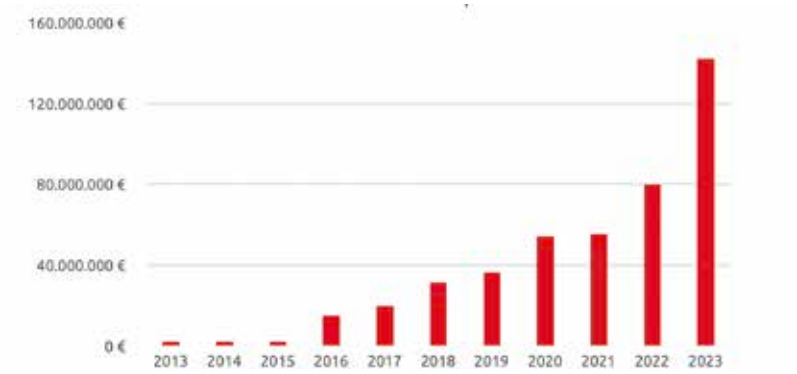


Figura 15. Valor de startups en Euskadi. Fuente: UP!Euskadi

Por otra parte, cabe destacar iniciativas como **b-venture**, que es el mayor **evento de emprendimiento** del norte de España [67]. En las cuatro ediciones han participado más de 400 startups de las cuales, 96 han sido seleccionadas a concurso. En una iniciativa promovida por el Diario El Correo, con el patrocinio del Gobierno Vasco y SPRI, junto a otras instituciones, entidades y empresas, su objetivo es la aceleración de proyectos "innovadores" e "invertibles", a los que se acompañará en su maduración, financiación y puesta en marcha. Se trata de un evento que cuenta con algunas de las mayores corporaciones, inversores y empresas de capital riesgo. Participan, entre otros, Indra, CAF Ventures, Acciona, Microsoft, Iberdrola, Metxa, BStartup, Laboral Kutxa, Plug & Play Spain, Lanzadera o Adara Ventures, entre otras.

Otro de los ámbitos para tener en cuenta dentro de nuestro ecosistema tecnológico vinculado a la ciberseguridad, es el apoyo técnico que se ofrece para startups y pymes. Como ejemplo de un caso de éxito, a continuación, se explica como un ecosistema tecnológicamente robusto como el que existe en Euskadi, puede contribuir a la mejora de capacidades, al mismo tiempo que a la adopción y transferencia de activos tecnológicos dentro del ámbito de la ciberseguridad que puedan ser explotados comercialmente por nuevas empresas emergentes.

La ciberseguridad es actualmente un elemento estratégico para la competitividad de la industria y un factor clave para la evolución de las tecnologías de Smart Industry. La Basque Research and Technology Alliance (BRTA) [68], formada por 4.000 profesionales de 17 centros tecnológicos y de investigación cooperativa, colabora con diversas organizaciones para garantizar la ciberseguridad en sus productos y servicios. La alianza BRTA asiste a las empresas para mantener altos estándares de ciberseguridad durante todo el ciclo de vida de sus productos, ya

que los ciberataques podrían llegar a interferir en las líneas de producción, generando graves problemas o incluso parando las mismas. Además, su papel resulta fundamental para dar soporte técnico a todas aquellas startups e iniciativas empresariales de emprendimiento que puedan surgir.

La ciberseguridad industrial es el área principal de desarrollo en el BRTA, el cual dispone de infraestructuras de investigación y laboratorios para evaluaciones de ciberseguridad, que forman parte del **Basque Digital Innovation Hub** (en adelante, BDIH) [69]. Se estructura como una red que brinda a las pymes la posibilidad de acceder a las competencias tecnológicas esenciales para afrontar los desafíos que plantean la Industria Inteligente, Energía y Salud. Esto no solo les permite crecer en un entorno digital y sostenible, sino también las capacita para adaptarse y sobresalir en sectores en constante evolución. Esta red está **conformada por varios nodos diseñados principalmente para abordar diferentes aspectos tecnológicos clave**.

En este sentido, cabe destacar el **nodo de ciberseguridad** del BDIH que, formado por cinco laboratorios de la Red Vasca de Ciencia, Tecnología e Innovación, proporciona a las empresas un entorno real para la realización de pruebas, simulaciones y entrenamientos.

En cuanto a las capacidades técnicas en asesoramiento y pruebas de concepto que ofrecen los laboratorios punteros del BRTA. Entre ellos, los más relevantes son:

- **Laboratorio para Cyber-Ranges** es un entorno virtual que se utiliza para el entrenamiento de personal y para la investigación y desarrollo de tecnología en ciberseguridad.
- **Laboratorio de Ciberseguridad en la Smart Grid** emula un entorno software-hardware de comunicaciones real.
- **Laboratorio de Ciberseguridad en Automoción** se representa el vehículo real escalado.
- **Laboratorio de evaluación de ciberseguridad** de producto está orientado a la verificación, validación y evaluación de componentes industriales y la pre-homologación y acompañamiento en la certificación de productos.
- **Laboratorio de industria segura 4.0** está orientado al concepto de fábrica inteligente o Smart Factory.

La consolidación de empresas y otros agentes de ciberseguridad, junto con el apoyo a nuevas empresas en este campo, requerirá contar con el conocimiento y las habilidades tecnológicas necesarias, permitiéndoles así competir en el mercado. En este sentido, es destacable el apoyo brindado por parte de los diferentes laboratorios del BRTA, ya que, las iniciativas de investigación, desarrollo e innovación se vuelven cada vez más fundamentales a la hora de incorporar los avances científico-tecnológicos en procesos y productos de empresas dentro del sector.

Cibercrimen

La transformación digital en la que se encuentran inmersas la gran mayoría de las empresas de todos los sectores ha supuesto el aumento de la superficie de ataque posible de las organizaciones, llegando a conseguir mediante dichos ataques sus datos más sensibles.

Estas circunstancias han sido las responsables de la creación del concepto conocido como cibercriminalidad, fenómeno que muestra desde hace años una tendencia ascendente a nivel global, convirtiéndose en uno de los principales problemas y preocupaciones de la sociedad hoy en día, **así como de las empresas**. Tanta es su fuerza que se ha llegado a generar un mercado propio, llegando a ser uno de lo más lucrativos a escala global.

En 2022, se superaron los 3.000.000 de ataques

A nivel global, se mantiene la tendencia ascendente en la comisión de ciberdelitos. En virtud de lo determinado por CS Cyber Security Hub en su Mid-year market report 2022, donde habla sobre los retos a los que se enfrentan los profesionales de la ciberseguridad, se destacan el phishing y el ataque de ingeniería social o ransomware como las mayores amenazas. En concreto, haciendo hincapié en lo dispuesto por el Anti Phising Working Group (APWG) en sus informes de tendencias, se conocieron un total de 3.394.662 ataques durante todo el 2022. Durante el segundo trimestre llegaron a conocer sobre un total de 1.097.811 ataques habiéndose configurado como un récord hasta ese momento. Sin embargo, en el tercer trimestre de ese mismo año, conocieron sobre un total de 1.270.883 ataques de phishing, el mayor récord alcanzado en un cuarto de año, quintuplicándose la cifra en comparación con el año 2020 [71].

Lo anterior, supuso un coste de 8 trillones de dólares a escala global, 4,35 millones de dólares por ciberataque sufrido en el año 2022 [1]. Entre los países que tienen una tasa mayor de cibercriminalidad se encuentran tal y como se muestra en el siguiente gráfico, Reino Unido, EE. UU., Canadá, Australia, Sudáfrica, Grecia, Francia, Alemania y España [72].

Países con mayor tasa de cibercriminalidad 2022

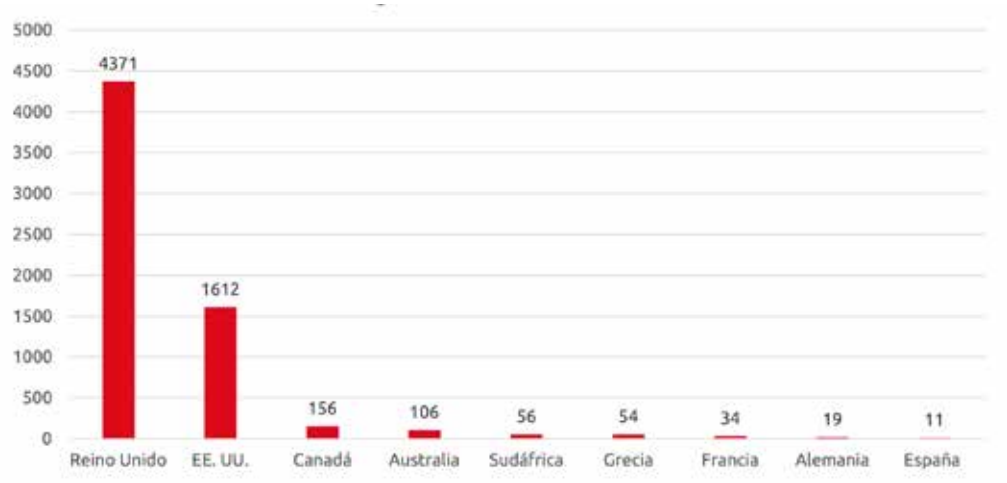


Figura 16. Ranking países con mayor tasa de cibercriminalidad. Fuente: Surfshark

Estos delitos derivaron en un coste medio para las empresas estatales de 105.655 €, el doble respecto al año anterior y muy por encima de la media mundial, de 78.409 € [73].

En lo que respecta al **ámbito estatal**, en virtud de lo mostrado en el informe sobre la tasa de criminalidad realizado por el Ministerio del Interior, el pasado año 2022 se registraron unos 375.506 delitos informáticos, aumento del 22,9% respecto al año anterior [74].

Si hablamos de **Euskadi** según los informes publicados por la **Ertzaintza**, se puede observar un crecimiento significativo en el número total de ciberdelitos cometidos durante 2022 con relación al año anterior:

Figura 17. Delitos informáticos en Euskadi 2021-2022. Fuente: Ertzaintza

En el año 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. Además, los delitos informáticos corresponden al 20,3% de los actos delictivos totales ocurridos en 2022 [75].

Esta tipología delictiva tiene como fin hacerse con activos económicos y bienes de la víctima mediante el uso de las nuevas tecnologías y cuenta con diferentes modalidades. Una de sus modalidades es el ransomware, que consiste en obligar a un tercero con violencia o intimidación a realizar u omitir un acto o negocio jurídico con contenido patrimonial. Tiene diversas variantes, como el bloqueo del acceso al dispositivo o cifrando archivos o el propio disco duro del ordenador para raptar su contenido, siendo posible su recuperación mediante el pago de una cantidad económica. Otra de sus modalidades se denomina phishing, que consiste en el envío de correos electrónicos suplantando la identidad de compañías u incluso, organismos públicos para solicitar información personal y bancaria al usuario con ánimo de defraudarles.

Por lo anterior, es necesario que tanto las organizaciones como los ciudadanos en general cuenten con los conocimientos fundamentales para no ser víctimas de delito informático, y, que conozcan el deber de denunciar dichos comportamientos evitando pagar las cantidades solicitadas por los ciberdelincuentes.

Con el objetivo de mantenerse actualizado en cuanto al análisis del entorno de la **ciberseguridad en Euskadi,** en los últimos años desde SPRI se han ido publicando diversos informes dirigidos a presentar la "Situación de la Ciberseguridad en Euskadi", en los que se realizan tanto el análisis de las diferentes vulnerabilidades encontradas, como la clasificación de las diferentes amenazas en base a su criticidad y se contemplan en virtud del sistema Common Vulnerability Scoring System (CVSS).

En el primer trimestre de 2022, se detectaron 5.800 vulnerabilidades, en el segundo semestre 6.653 (aumento del 15%), en el tercer trimestre 6.888 (aumento del 3,5%) y 6.751 (descenso del 2,03%) [76][77][78][79].

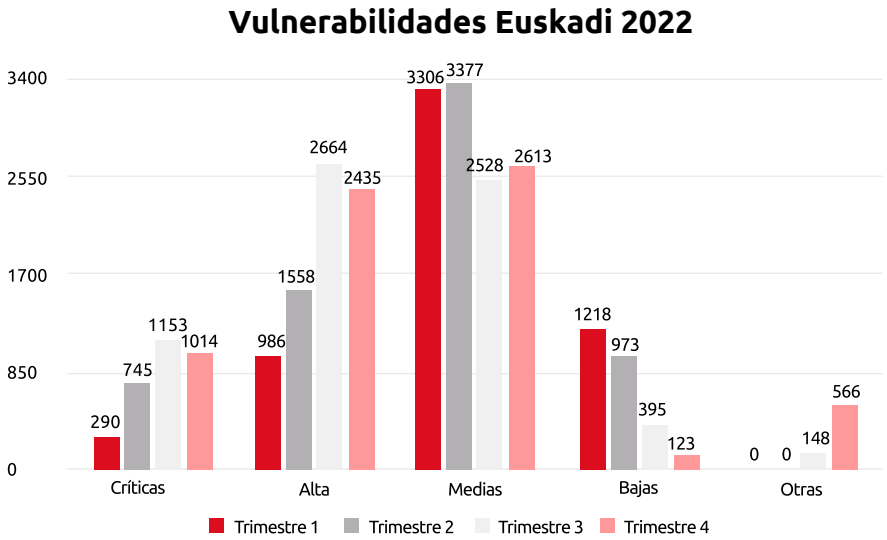


Figura 18. Vulnerabilidades detectadas en Euskadi en 2022. Fuente: SPRI

Durante los primeros seis meses del año 2023, se produjeron 12.878 ciberdelitos, incrementándose la cifra un 31% respecto al mismo periodo el año anterior, siendo la gran mayoría ciberestafas. El ranking de ciberdelitos en el primer semestre del 2023 se refleja de la siguiente manera [80]:

- 11.508 ciberestafas (30% más que en 2022).
- 505 ciberfalsificaciones (9% más que en 2022).
- 390 ciberamenazas y ciber coacciones (85 más que en 2022).
- 89 delitos de descubrimiento y revelación de secretos perpetrados a través de nuevas tecnologías (2% más que en 2022).
- 36 ciberdelitos sexuales (71% más que en 2022).
- 44 ciberataques (un 144% más que en 2022).
- 306 relacionados con otros delitos informáticos.

En relación con las amenazas que se han detectado durante todo el **año 2023**, la mayoría de los ataques han sido causados por infecciones de malware. Además, también es importante destacar que un alto porcentaje de estos ataques han sido ocasionados por vulnerabilidades que no han sido correctamente tratadas. Por ello, para prever **este tipo de ataques, es muy importante** seguir las siguientes recomendaciones:

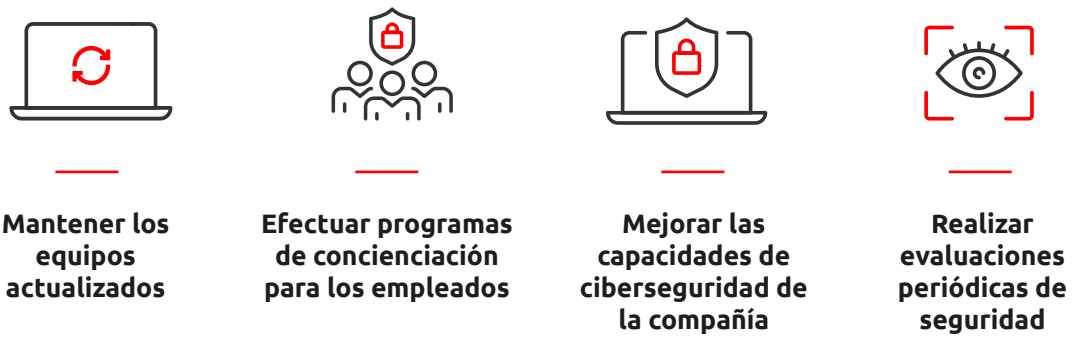


Figura 19. Recomendaciones. Fuente: elaboración propia

Estas recomendaciones en ciberseguridad se erigen como un pilar fundamental a nivel global, dado el constante y creciente aumento de amenazas y actividades delictivas en el mundo digital. En este contexto, resulta imperativo que regiones como **Euskadi** se adhieran **a estas mismas recomendaciones, ya que la naturaleza de las ciberamenazas no conoce fronteras ni límites geográficos.** Adoptar prácticas y medidas de seguridad alineadas con estándares internacionales 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.**

Tendencias ciberseguridad

La adopción de nuevas tecnologías, así como el incremento del uso de dispositivos electrónicos en el día a día está provocando un aumento en la superficie de ataque y fomenta la aparición de nuevas brechas de seguridad a explotar por los ciberdelincuentes.

En este 2023, los diferentes tipos de malware al igual que ocurría en ejercicios anteriores continuaron siendo las ciberamenazas más recurrentes. El informe semestral elaborado por SonicWall sobre las amenazas del 2023 afirma que los intentos de intrusión han aumentado en general, siendo el cryptojacking el que mayor volumen global ha registrado, creciendo a nivel mundial un 399% y un 799% a nivel Europa. El malware IoT y las amenazas de cifrado también aumentaron un 37% a nivel mundial en los primeros seis meses del año, alcanzando casi los 78 millones y 22% de visitas respectivamente a finales de junio [81].

No obstante, debido al repunte de más del 73% en el segundo trimestre, es probable que el ransomware **haya aumentado en la segunda mitad de 2023**. Esta ciberamenaza afecta especialmente a España, por ser el quinto país del mundo que sufre más ciberataques de ransomware después de EE. UU., Alemania, Reino Unido y Austria. Países como Alemania e India sufrieron aumentos del 52% y 133% respectivamente [81].

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

Debido al carácter cada vez más profesional de los atacantes, estos comienzan a tener como objetivo las infraestructuras críticas y cadenas de suministro [81]. Es previsible que se desarrollen y utilicen nuevas técnicas y cualidades tanto en los ataques de ransomware como los ataques de phishing, pudiendo llegar a anular en ciertos casos la protección que ofrece en estos momentos la autentificación multifactorial (MFA) [82][83].

Como se ha señalado, los ciberataques siguen siendo cada vez más sofisticados y se siguen utilizando vulnerabilidades de día cero como vector de entrada. Estas técnicas van a continuar sofisticándose en consonancia con su perfil progresivamente más profesional, centrándose en el cifrado de datos y hurto de información confidencial, para así después obtener una compensación económica [83].

Por todo ello, para poder hacer frente a estas amenazas, las empresas deben dar cumplimiento a las regulaciones de privacidad y ciberseguridad que se están desarrollando a nivel mundial, europeo y estatal. Además, debido a la alta demanda por parte de las empresas los servicios como Cyber Threat Intelligence (CTI) se espera que manifiesten un crecimiento importante durante los próximos años [84].

Adicionalmente, cabe destacar que la consideración y la importancia que está cobrando la ciberseguridad en las organizaciones va en aumento. La imagen del Chief Information Security Officer (CISO) va a estar cada vez más presente y se incrementarán las inversiones en ciberseguridad. Asimismo, con el objetivo de mejorar la madurez y preparación de las organizaciones, contra los ataques de ciberseguridad, las compañías están desarrollando y perfeccionando sus programas de concienciación y capacitación.

Figura 20. 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

A medida que el cibercrimen y su manera de ejecutarlo cambia y aumenta, surge la necesidad de actualizar y fortalecer la normativa en materia de ciberseguridad y protección de infraestructuras críticas con el objetivo de mejorar la resiliencia y la seguridad tanto de la ciudadanía como de las empresas.

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

Las regulaciones de ciberseguridad en todo el mundo consisten en una variedad que evoluciona en virtud de la trayectoria de la tecnología y varían según el espacio geográfico en el que se implementan. Si bien muchos aspectos de las normas actuales de ciberseguridad son resultado de orientaciones previas establecidas por otros países, muchos de ellos tienen características especiales que los distinguen [84].Dentro de estas nuevas regulaciones, se están incluyendo nuevos requisitos en referencia a la obligación de disponer de medidas y mecanismos de protección, así como, a la obligatoriedad de comunicar ante las autoridades los incidentes de seguridad sufridos por parte de las organizaciones.

EEUU

The Cibersecurity Information Sharing Act:
- Tiene como objetivo mejorar la ciberseguridad de EEUU
- Fomentar el intercambio de información

Strengthening American Cybersecurity Act of 2022:
- Objetivo de obligar a los operadores de infraestructuras críticas a notificar a la CISA

ESPAÑA

Real Decreto 311/2022
- Nueva actualización del Esquema Nacional de Seguridad

Ley Orgánica 3/2018:
- Protección de Datos Personales y garantía de los derechos digitales

Real Decreto 43/2021:
- Seguridad de las redes y sistemas de información

Ley Orgánica 7/2021:
- Materia de protección de datos

EUROPA

RGPD
- Garantizar la privacidad y seguridad de los datos de los ciudadanos y armonizar las leyes de privacidad en toda la UE

DORA:
- Desarrollar plan de respuesta de incidentes
- Programa de evaluación de riesgos
- Notificación de incidentes para evaluar vulnerabilidades.

Cyber Resilience Act:
- Obligar a los fabricantes a mejorar la seguridad de sus productos durante su ciclo de vida.
- Aumentar la transparencia de las propiedades de seguridad

NIS2:
- Cambiar la directiva actual.
- Objetivo de establecer la base para las medidas de gestión de riesgos de ciberseguridad y las obligaciones de notificación en todos los sectores.

Propuesta de Reglamento-Ley de Inteligencia Artificial:
- Impone diferentes obligaciones a todos los actores en la cadena de valor de la IA.
- Aplicable a todos los sistemas de IA que afecten a personas en la UE

Figura 20. Regulaciones de ciberseguridad. Fuente: CISA, Comisión Europea, Parlamento Europeo, BOE

Al hilo de lo anterior, dentro del panorama mundial, **Estados Unidos** es uno de los países líderes en el desarrollo de políticas y regulaciones de ciberseguridad. Las preocupaciones sobre ciberseguridad y la protección de las infraestructuras han estado presentes en todo el mundo durante décadas. Sin embargo, EE. UU. ha sido un actor influyente en este campo debido a varios factores, tales como, ser hogar de las principales empresas tecnológicas o ser objetivo principal de ciberataques por su posición como potencia mundial.

EE. UU. cuenta con The Cybersecurity Information Sharing Act (CISA), una ley federal cuyo objetivo principal es facilitar la colaboración y el intercambio de información sobre ciberamenazas entre el gobierno, las empresas y otras entidades.

Resulta destacable también la Strengthening American Cybersecurity Act of 2022 (SACA) [86]. Con su entrada en vigor en marzo de 2022, se trata de una ley de fortalecimiento de la ciberseguridad estadounidense, que exige legalmente que los operadores de infraestructuras críticas, como sistemas de agua o redes eléctricas alerten a la Cybersecurity and Infrastructure Security Agency (CISA) dentro de las 72 horas posteriores a cualquier brecha de seguridad. Además, las organizaciones que realicen el pago de un ransomware tienen 24h para reportar tales detalles a la Agencia. Debido a que las agencias regionales y estatales siguen siendo objetivo de determinados ciberdelincuentes, esta ley está diseñada para brindarle a CISA y otras agencias apropiadas la visibilidad de los ataques contra infraestructuras críticas para permitir la respuesta, la mitigación y las advertencias oportunas de ataques al público [87][87].

Si bien Estados Unidos ha desempeñado un papel influyente en el desarrollo de la ciberseguridad, otros países y regiones también han avanzado en la formulación de regulaciones y políticas de ciberseguridad, y la colaboración internacional es fundamental para abordar las ciberamenazas en el ámbito global.

En lo que concierne a la normativa **europea existente**, deben destacarse las siguientes:

Reglamento General de Protección de Datos (RGPD)

El RGPD de la UE, es la legislación que regula la protección de los datos de carácter personal en Europa. Sus principales objetivos son garantizar la privacidad y seguridad de los datos de los ciudadanos y armonizar las leyes de privacidad en toda la UE. Establece normas relativas a la recopilación, el procesamiento y la transferencia de los datos personales, los derechos de los individuos en relación con sus datos y la responsabilidad de las organizaciones que manejan los mismos. También impone sanciones por infracciones y busca promover una mayor transparencia en el manejo de los datos [88].

En lo relativo a la ciberseguridad, es una de las regulaciones principales en esta materia, puesto que, la creciente recopilación, almacenamiento y procesamiento de los datos personales en el entorno digital, ha generado preocupación con respecto a la protección de la privacidad de las personas.

En este sentido, es destacable que, junto con la ciberseguridad, este reglamento se centra en la protección de la información y la privacidad de los individuos, aunque abordan aspectos diferentes.

La prevención de las brechas de seguridad de las que se encarga la ciberseguridad es esencial para el correcto cumplimiento del RGPD que habla sobre la necesaria protección de la integridad de los datos personales.

En lo que respecta a los avisos de violaciones de seguridad, el RGPD requiere que las organizaciones notifiquen las violaciones de los datos a más tardar, 72h después de haber tenido conocimiento de la misma. Esta notificación, además, en virtud de lo dispuesto por el RGPD, debe ir acompañada de detalles sobre la naturaleza de la violación, la cantidad de los datos que hayan sido afectados, las posibles consecuencias y las medidas llevadas a cabo para hacer frente a la brecha sufrida.

Finalmente, el RGPD habla sobre la necesidad de llevar a cabo una Evaluación de Impacto relativa a la Protección de Datos (EIPD).

Digital Operational Resilience Act (DORA)

Habida cuenta del riesgo cada vez mayor de ciberataques dentro de la UE, el Consejo adoptó a finales de 2022 el Reglamento sobre resiliencia operativa digital, también conocido como DORA por sus siglas en inglés (Digital Operational Resilience Act), con el fin de reforzar la seguridad informática de las entidades financieras, que entró en vigor el 16 de enero del 2023 [89].

El objetivo de este reglamento es establecer unos requisitos homogéneos para todos los Estados miembros de la UE con el fin de prever y mitigar las ciberamenazas. Para ello, se ha creado un marco normativo sobre la resiliencia operativa digital, en virtud del cual todas las empresas deben asegurar su posibilidad de resistencia y respuesta de recuperación ante cualquier clase de trastorno y amenaza relacionada con las TIC.

De esta manera, se incorporan una serie de cambios en las prácticas de seguridad de datos de las empresas de servicios financieros, que son:

- Contar con un plan de respuesta a posibles incidentes.
- Mantener un programa de ciberseguridad que incluya una evaluación de los riesgos.
- Mantener controles de seguridad adecuados sobre su infraestructura digital.
- Notificar los incidentes cuando se produzcan para que los reguladores puedan evaluar sus vulnerabilidades y hacer recomendaciones para mejorar su postura de seguridad.
- Contar con un plan que garantice la continuidad del servicio durante las interrupciones que puedan producirse.

En definitiva, se trata de una regulación que forma parte del paquete de medidas para seguir construyendo y apoyando la fuerza de las finanzas digitales en el entorno financiero actual, mitigando los riesgos que se derivan de ella.

Antes de DORA, las instituciones financieras administraban las categorías principales de riesgo operativo principalmente a través de la asignación de capital, pero no administraban todas las características de la resiliencia operativa (la capacidad de la organización para continuar operando ante cualquier evento adverso).

Cyber Resilience Act

En vista de la ausencia de legislación en materia de ciberseguridad en los productos con elementos digitales (hardware y software), en septiembre de 2022, la Comisión Europea presentó el Cyber Resilience Act o conocida también como “Ley de ciber resiliencia” [89].

Es una propuesta de Reglamento que tiene como fin, reforzar las normas de seguridad de cara a que los productos hardware y software sean más seguros, puesto que con el tiempo se han vuelto objetivo indiscutible de diferentes tipos de ciberataques.

Se plantean dos cambios principales para garantizar el adecuado funcionamiento del mercado interior:

- Garantizar que los fabricantes de dichos productos tengan en consideración la necesidad de que los productos sean seguros durante todo su ciclo de vida y crear las condiciones necesarias para que dichos productos se introduzcan en el mercado con menos vulnerabilidades.
- Crear condiciones que permitan a los usuarios considerar la ciberseguridad al decidir y utilizar productos basados en la tecnología digital.

Además, se establecen cuatro finalidades concretas, siendo estas las siguientes:

- Asegurar que los fabricantes de los productos mejoren la seguridad de los mismos con elementos digitales desde sus fases más previas (diseño y desarrollo).
- Garantizar un marco acorde a la ciberseguridad, facilitando el cumplimiento por parte de los productores de hardware y software.
- Incrementar la transparencia de las características de seguridad de los productos con elementos digitales.
- Autorizar a las empresas y a los consumidores la utilización de productos con elementos digitales de manera segura.

En definitiva, se trata de la reglamentación que va a establecer los estándares mínimos necesarios de seguridad para los productos digitales comercializados en la UE.

NIS 2 Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo

La nueva versión de la Network and Information System Directive (NIS2), por la que se modifican el Reglamento (UE) N.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148, entró en vigor el pasado 16 de enero de 2023. El objetivo de esta directiva está en eliminar los desacuerdos entre los estados miembros a la hora de hablar de la aplicación de la directiva sobre la seguridad de las redes y sistemas de información (NIS) de 2016. El objetivo de la misma es definir unas normas mínimas relativas al funcionamiento de un marco normativo común, facilitando un mecanismo de cooperación entre las autoridades competentes de cada Estado miembro [91].

Esta trae consigo la actualización de sectores y actividades sujetos al cumplimiento de las obligaciones de ciberseguridad y la disponibilidad de remedios efectivos y medidas de ejecución necesarias para el cumplimiento de dichas obligaciones.

Con el fin de proporcionar una cobertura completa de los sectores y servicios cruciales para las actividades sociales y económicas fundamentales dentro del mercado interior, el ámbito de aplicación por sectores se amplía así a una mayor parte de la economía. Se establece un criterio uniforme para determinar qué entidades entran en el ámbito de aplicación de la Directiva con el fin de eliminar diferencias significativas entre los Estados miembros en este ámbito y garantizar la seguridad jurídica de todas las entidades pertinentes en relación con las prácticas de gestión de riesgos de ciberseguridad y las obligaciones de notificación.

Proporciona medidas legales para impulsar el nivel general de ciberseguridad en la UE garantizando:

- La preparación de los estados miembros exigiéndoles que estén equipados adecuadamente, como, por ejemplo, con un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés) y una autoridad nacional competente de sistemas de información y redes (NIS).
- La cooperación entre los diferentes estados miembros con la creación del "Cooperation Group" para apoyar y facilitar la estrategia de cooperación y el intercambio de información entre ellos.
- Cultura de seguridad en todos los sectores vitales para nuestra economía y sociedad y que dependen en gran medida de las TIC, como la energía, el transporte, el agua, la banca, las infraestructuras del mercado financiero, la sanidad y la infraestructura digital.

European Artificial Intelligence Act

El pasado 8 de diciembre de 2023, las Instituciones de la Unión Europea (UE) alcanzaron un acuerdo sobre los términos clave y componentes del Reglamento de Inteligencia Artificial (IA) tras meses de intensas negociaciones. El Reglamento de IA es un **hito en la regulación global de la IA**, reflejando 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. Este Reglamento se suma a otras legislaciones digitales importantes de la UE, como el RGPD, la Ley de Servicios Digitales, la Ley de Mercados Digitales, la Ley de Datos y la Ley de Ciberresiliencia.

El Reglamento de IA unificará la regulación de la IA en el mercado único de los 27 Estados miembros de la UE. también tiene importantes implicaciones extraterritoriales, ya que cubre todos los sistemas de IA que impactan a las personas en la UE, independientemente de dónde se desarrollen o implementen los sistemas.

Las obligaciones de cumplimiento son significativas y están determinadas en gran medida por el nivel de riesgo que el uso de un sistema de IA represente para la seguridad, la integridad o los derechos fundamentales de las personas. Las obligaciones se aplican a lo largo de la cadena de valor de la IA.

El acuerdo establece actualmente un **cronograma por fases para la aplicació**n, comenzando con la prohibición de sistemas de IA en 2025 y **extendiéndose progresivamente a todos los sistemas de IA para mediados o finales de 2026.** Hay importantes sanciones financieras por incumplimiento.

En lo correspondiente a **nivel estatal,** fue en 2004 cuando se comenzó a tener conciencia y a desarrollar una cultura en ámbito de ciberseguridad, a través del Real Decreto 421/2004, de 12 de marzo, donde se regula y define el ámbito y funciones del Centro Criptológico Nacional (CCN), como parte del Centro Nacional de Inteligencia (CNI) [91]. El CCN se convirtió a partir de esa fecha, en uno de los pilares fundamentales para la creación de una cultura de ciberseguridad nacional.

El desarrollo de diferentes leyes nacionales se demoró hasta el 2011, que surgió la primera ley sobre la regulación de las infraestructuras críticas, determinando, por un lado, las medidas que debían cumplir mediante la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Y, por otro lado, por el Real Decreto 704/2011 que definía el reglamento que tenían que cumplir este tipo de organizaciones.

Es preciso destacar el Código del Derecho de la Ciberseguridad, iniciativa conjunta del Instituto Nacional de Ciberseguridad (INCIBE) y el Boletín Oficial del Estado (BOE) que pone a disposición de todos los ciudadanos un compendio de normas relativas a la ciberseguridad [92]. El objetivo de este se encuentra en consolidar las directrices generales en el uso fehaciente del ciberespacio a través del impulso una visión inclusiva que asegure la seguridad y el progreso a nivel estatal.

Este código se encuentra dividido por capítulos que contienen toda la normativa nacional relacionada con la ciberseguridad, entre las que se encuentran a parte de las mencionadas, las siguientes:

- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional [93].
- Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana [94].
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico [95].
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones [96].
- Ley Orgánica 10/1995, de 23 de noviembre del Código Penal [97].
- Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal [98].
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información [99].
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información [100].
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales [101].

Tras la realización de este análisis sobre las regulaciones en materia de ciberseguridad es preciso mencionar el **Global Cybersecurity Index (GCI**) elaborado por la agencia de las Naciones Unidas, Unión Internacional de Telecomunicaciones (UIT, o ITU en inglés). El GCI tiene como objetivo evaluar y clasificar a los países en función de su preparación y capacidad en materia de ciberseguridad. Para ello, se basa en distintos indicadores estandarizados en una única matriz para poder monitorizar, medir y evaluar el nivel de compromiso de ciberseguridad, en base a los cinco pilares de la Agencia de Ciberseguridad Global (ACG), entre los cuales se encuentra la legislación de cada país. De esta manera, ayuda a los países a evaluar su situación en ciberseguridad y a realizar mejoras en esta materia [103].

En lo que respecta a **Euskadi**, se encuentra una reflexión positiva. El marco jurídico correspondiente a este territorio es el estatal, basado en Códigos, reglamentos y directivas de España y la UE. En este sentido, tal y como muestra el último GCI realizado, España, ocupa el cuarto lugar en el ranking, por ende, Euskadi cuenta con uno de los marcos legislativos más completos en esta materia. Además, se debe subrayar que este territorio obtuvo la mayor puntuación posible (20/20) en cuanto a la legislación refiere.

Para concluir, es preciso hablar de la sectorización en materia de regulación de ciberseguridad. Ello se refiere a la segmentación o división de diferentes áreas o sectores específicos para establecer regulaciones, estándares o directrices particulares en cada uno de ellos en relación con la ciberseguridad. Esto se hace para adaptar las políticas de seguridad a las necesidades y riesgos particulares que enfrenta cada sector.

En general, los marcos regulatorios y normativos en ciberseguridad están diseñados para abordar los desafíos específicos de sectores como la banca, la salud, la energía, el transporte, entre otros. Estos sectores tienen diferentes necesidades y riesgos en términos de ciberseguridad debido a la naturaleza de sus operaciones y la sensibilidad de los datos que manejan.

Así pues, en el ámbito financiero, las normativas se centran en resguardar las transacciones, prevenir el fraude y asegurar la integridad de los datos bancarios, garantizando así la continuidad de las operaciones. En el sector de la salud, las regulaciones se encuentran enfocadas a la protección de la información médica del paciente, velando por su confidencialidad e integridad, además de asegurar la disponibilidad de los sistemas para la atención médica constante. En industria, energía y servicios públicos, las regulaciones se orientan hacia la protección de infraestructuras críticas, como las redes eléctricas, para evitar interrupciones que puedan afectar a la población y la economía.

Son los organismos públicos o las entidades reguladoras las que establecen y actualizan la regulación en virtud del sector al que pertenezcan. Tal es así que, se vuelve notorio que cada sector tiene su marco regulatorio y normativo específico que a menudo incluye estándares de seguridad, directrices y requisitos de cumplimiento que las organizaciones dentro de ese sector deben seguir para protegerse contra ciberamenazas.

El Impacto de las regulaciones en ciberseguridad se convierte en un desafío y una oportunidad para las empresas de Euskadi

Las regulaciones tienen un impacto significativo **en el entorno empresarial de Euskadi**. En la Administración Pública, estas regulaciones están diseñadas para salvaguardar los datos sensibles y asegurar la integridad de los sistemas. Esto conlleva la implementación de estándares más altos de seguridad y protocolos más rigurosos, lo que puede afectar a las empresas de la región de varias maneras.

En cambio, en el sector privado, estas regulaciones pueden representar 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 ciberseguridad también podrían generar oportunidades para empresas especializadas en ofrecer soluciones de seguridad, consultoría o servicios relacionados, erigiéndose como nuevos nichos o áreas de negocio para estas. No obstante, para las empresas más pequeñas o con recursos limitados, el cumplimiento de estos estándares puede representar un desafío a nivel financiero y operativo.

En este contexto, resulta relevante mencionar que en Euskadi el tejido empresarial industrial posee un peso importante en la economía, lo que los obliga a estar al tanto de regulaciones como el Cyber Resilience Act o la NIS2 entre otras.

Por otro lado, el cumplimiento de estas normativas puede generar confianza entre los clientes y socios comerciales, fortaleciendo la reputación y la credibilidad de las empresas en el mercado.

En general, estas regulaciones impulsan a las organizaciones a mejorar sus prácticas de ciberseguridad y a adoptar medidas proactivas para proteger la información, lo que contribuye a un ecosistema empresarial más robusto y seguro en Euskadi.

Sellos de ciberseguridad

Como consecuencia de la aparición de nuevos servicios, productos y tecnologías en el área de la ciberseguridad, surge la necesidad de crear diferentes sellos con el objetivo de proporcionar a los usuarios información sobre el cumplimiento de los requisitos relacionados con la ciberseguridad establecidos en el sistema en el que se basa dicho sello.

Esta clasificación debe ser establecida mediante mecanismos robustos y solidos con el objetivo de verificar e identificar a las empresas y los productos/servicios. Para poder obtener dichos sellos, se deben cumplir una serie de requisitos que son propuestos por cada una de las organizaciones emisoras. Además, estos sellos ayudan a dar visibilidad y otorgan reconocimiento a las empresas que los consiguen.

Si bien existe una diversidad más extensa disponible, a continuación, se exponen algunos ejemplos representativos de sellos emitidos a nivel mundial:

- Cybersecurity made in Europe (ECSO) [104].
- Cybersecurity Label (The European watch on cybersecurity & privacy) [105].
- Cybersecurity Labelling Scheme (Cyber Security Agency Singapore) [106].

Figura 22. Sellos de ciberseguridad. Fuente: elaboración propia

Por otro lado, se están creando sellos y estándares para productos como:

- The ISASecure Certifications para la automatización y ciberseguridad de los sistemas de control [110].
- Tisax para la gestión de la seguridad de la información en automóviles [111].
- El estándar IEC 62443 que tiene como objetivo el de proveer un marco que facilite la identificación de vulnerabilidades en los sistemas de automatización industrial (ICS) ofreciendo una guía para el funcionamiento seguro de los ICS [112].

Adicionalmente, uno de los sellos que está cobrando cada vez más importancia es el "Cybersecurity made in Europe", solamente emitido por ECSO y sus socios autorizados. Este sello es una herramienta impulsada por la industria, diseñada para ayudar a promover las empresas europeas de ciberseguridad y aumentar su visibilidad en el mercado europeo y mundial.

Para obtener el sello las empresas deben cumplir con una serie de criterios:

- **Debe ser una empresa europea.** En el caso de formar parte de un grupo, la sede debe estar registrada en Europa.
- **Debe ser propiedad europea.** La empresa tiene que proporcionar la garantía de la inexistencia de propiedad/control de fuera de Europa.
- **Europa tiene que ser su lugar principal de negocios.** La empresa debe demostrar que tiene más de un 50% de las actividades de I+D en ciberseguridad y más de un 50% del personal en Europa.
- La empresa declara **cumplir con los "Requisitos básicos** de seguridad indispensables para los productos y servicios TIC seguros" de **ENISA.**
- La empresa debe declarar **cumplir con el RGPD.**

En Euskadi, cabe destacar 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 o los diferentes inversores en el sector de la ciberseguridad. Al obtener este distintivo, las empresas no solo validan su cumplimiento con las exigentes normativas y medidas de seguridad europeas, sino que también proyectan una imagen de confianza y compromiso con la protección de datos y sistemas en el ámbito digital.

Este tipo de sellos, alineados con estándares de primer nivel en seguridad digital, no solo impulsan la competitividad de las organizaciones, sino que también ofrecen a sus clientes y colaboradores la certeza de que están trabajando con entidades comprometidas con la protección y la integridad de la información en un contexto europeo de confianza y seguridad digital

Agencias de ciberseguridad

Como se analiza durante todo el documento, el avance de las tecnologías de la información y la comunicación (TIC) ha supuesto la dependencia del desarrollo económico y progreso de la sociedad en las mismas, convirtiéndose en elementos esenciales para el correcto desarrollo de la sociedad hoy en día. Todo ello provoca la necesidad de desplegar mecanismos para identificar y reducir los riesgos que traen consigo la utilización de las TIC.

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

Debido al progreso de las nuevas tecnologías, ha habido un aumento en las comunicaciones electrónicas entre ciudadanos, empresas y las diversas Administraciones Públicas, llevado ello a una mayor exposición de las ciberamenazas. Por ello, es esencial 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.

Además, la constante digitalización de las relaciones personales y de las transacciones económicas, suponen la exposición de un gran volumen de datos en la red, lo que conlleva la necesidad de ajustar la protección de las infraestructuras y servicios de comunicación contra amenazas en el ámbito de la ciberseguridad volviéndose un pilar fundamental para los diferentes sectores y administraciones hoy en día.

Una de las agencias de referencia a nivel global es **Cybersecurity and Infraestructure Security Agency (CISA).** Es una agencia federal encargada de fortalecer la ciberseguridad de EE. UU. y de proteger su infraestructura crítica contra las ciberamenazas. Trabaja con sus socios para defenderse contra las amenazas actuales y colaborar para construir una infraestructura más segura y resiliente para el futuro. Su trabajo se extiende en tres áreas principales: ciberseguridad, seguridad de la infraestructura y comunicaciones de emergencia.

A nivel europeo, debe hablarse de La **Agencia de la Unión Europea para la Ciberseguridad (ENISA,** por sus siglas en inglés). Fundada en 2004 y reforzada por el Reglamento sobre la Ciberseguridad de la UE, un papel fundamental en la política de ciberseguridad de Europa. Su labor se concentra en potenciar la confiabilidad de los productos, servicios y procesos de las TIC a través de programas de certificación de ciberseguridad. Su función es proporcionar asesoramiento experto, colaborar en la creación de políticas y fomentar la cooperación entre los Estados miembros de la UE en temas relacionados con la ciberseguridad. ENISA trabaja en la identificación de amenazas, el intercambio de información, la investigación y el desarrollo de buenas prácticas para fortalecer la ciberseguridad en Europa.

En este contexto, las instituciones públicas a nivel estatal han desempeñado un papel activo y determinante al impulsar y promover iniciativas enfocadas en salvaguardar la integridad y confidencialidad de la información digital.

El Instituto Nacional de Ciberseguridad (INCIBE) destaca como un referente clave en este ámbito. Fundado con el propósito de consolidar la ciberseguridad en España, INCIBE se ha dedicado a la promoción de la conciencia digital, la formación especializada, el análisis y respuesta ante incidentes, así como el impulso de proyectos innovadores en el campo de la seguridad digital. Su labor, ha sido fundamental en la creación de un entorno más seguro para los ciudadanos, las empresas y las administraciones públicas.

Además de INCIBE, a nivel estatal, se cuenta con otras agencias de ciberseguridad que colaboran en el fortalecimiento de la protección digital. Entre ellas se encuentra el CCN-CERT, adscrito al Centro Criptológico Nacional del Centro Nacional de Inteligencia, que tiene competencia en el Sector Público en general, a nivel autonómico, regional, así como en sistemas que gestionan información clasificada. Asimismo, el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), cuya labor se centra en proteger las infraestructuras críticas del país contra ciberamenazas. De otro lado, la Agencia Española de Protección de Datos (AEPD) que desempeña un papel crucial en la garantía de la privacidad y la correcta gestión de la información personal en entornos digitales.

> Euskadi ha decidido desarrollar un proyecto común con el objetivo de fortalecer y dirigir la coordinación de los recursos disponibles a través de la creación de “Cyberzaintza”

Estas agencias, junto con otros organismos públicos, desarrollan programas de concienciación, investigaciones, capacitaciones y servicios de respuesta ante incidentes que fortalecen la resiliencia y la protección contra las crecientes ciberamenazas.

Al hilo de lo anterior, cabe destacar que la CAE, lleva varios años implicada 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.

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.

Desde SPRI, se vislumbra un futuro prometedor, cargado de entusiasmo y compromiso, que se traducirá en forma de nuevas iniciativas de apoyo para las empresas con el objetivo de seguir fomentando y favoreciendo al crecimiento del sector de la ciberseguridad de Euskadi, haciéndolo cada vez más competitivo.

Por otro lado, es preciso también destacar ZIUR, el **Centro de Ciberseguridad Industrial de Gipuzkoa.** Creado por la Diputación Foral de Gipuzkoa para ayudar a las empresas industriales a reforzar su protección y la de sus productos o servicios a los ciberataques. Se centra en mejorar la capacidad de ciberseguridad de las empresas industriales de Gipuzkoa, ayudando a las empresas a identificar sus necesidades en ciberseguridad y encontrar las soluciones más adecuadas para las mismas.

Cuenta con **4 objetivos** principales:

- **Difusión**: fomentar el desarrollo de conocimiento en el campo de la ciberseguridad.
- **Concienciación y formación:** crear conciencia y brindar capacitación a las empresas.
- **Investigación y exploración:** realizar vigilancia tecnológica, operar un observatorio de ciberseguridad y establecer un laboratorio de investigación
- **Prevención**: ofrecer herramientas preventivas en el ámbito de la ciberseguridad.

En definitiva, generan y comparten conocimiento para mejorar las capacidades de ciberseguridad de las empresas del territorio.

Debido a las tendencias existentes la ciberseguridad se configura como materia transversal para las iniciativas llevadas a cabo por los organismos públicos. En este sentido, 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".**

Fue el pasado mes de junio de 2023 cuando fue aprobado por el Consejo de Gobierno el anteproyecto de ley de creación de la Agencia Vasca de Ciberseguridad, la cual se puso en marcha el pasado 13 de septiembre, con la primera reunión del Consejo de Administración. Presidida por el, Vicelehendakari Primero y Consejero de Seguridad, a quien acompañaba la Consejera de Desarrollo Económico, Industria y Medio Ambiente se dio el visto bueno a los estatutos definitorios de los objetivos, funciones, estructura y bases legales y operativas de la nueva agencia [110].

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 síntesis, 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 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 de 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.** Por ello, este apartado explora el impacto y la evolución de este campo, desde el auge del mercado global de la ciberseguridad industrial hasta las tendencias de ciberataques, evidenciando la necesidad de medidas preventivas tanto para las grandes empresas como para las pymes. Además, se analiza el rol clave de instituciones públicas, delineando su labor en la detención temprana de las amenazas y su contribución a la seguridad de los sistemas industriales.

El mercado de ciberseguridad industrial a nivel global se prevé que alcance los 15.000 millones en 2023 y los más de 23.000 mil millones en 2032, presentando una CAGR de 5,1% durante el periodo 2023-2032

La ciberseguridad industrial puede ser definida como la aplicación de controles sobre los activos de valor de las infraestructuras industriales a partir de los resultados de un análisis de riesgos, y con el objetivo de mitigar los riesgos que ese análisis ha encontrado.

La tendencia creciente en la comisión de ciberdelitos en el entorno industrial ha supuesto el crecimiento del valor de mercado de la ciberseguridad industrial a nivel mundial.

El tamaño del mercado de ciberseguridad industrial a nivel global se prevé que alcance los 15.000 millones en 2023 y los más de 23.000 mil millones en 2032, presentando una CAGR de 5,1% durante el periodo 2023-2032 [111]. Siguiendo lo mostrado por Fortune Business Insights, la integración de soluciones de ciberseguridad y servicios avanzados en la nube por parte de varias industrias generará oportunidades para el mercado global durante dicho periodo [112].

En el ámbito industrial, son las pymes las dominantes en el mercado, que, a su vez, se muestran como las más vulnerables ante los ciberataques debido a sus limitaciones financieras y de recursos disponibles. De cara a cambiar esta situación, se espera que las pymes adopten medidas para mejorar la seguridad. Se entiende que dichas medidas serán adoptadas por la creciente necesidad de reducir costes operativos y de filtración de datos y proteger los activos TI.

Tal y como se ha mencionado previamente, son las pymes las que predominan en el mercado de la ciberseguridad industrial, sin embargo, por sus limitaciones financieras y la falta de recursos que ello provoca, al mismo tiempo, se configuran como las más vulnerables.

Por otro lado, gracias a su amplio almacenamiento de datos, las grandes empresas disponen de una variedad de redes, servidores, dispositivos de almacenamiento y terminales, lo que las sitúa en alto riesgo de sufrir pérdidas financieras considerables en caso de un ciberataque. Otro factor que se prevé que impulsará la demanda en este segmento del mercado es que muchas empresas están adoptando modelos de trabajo híbridos, lo que aumenta el riesgo de seguridad para las **grandes empresas** cuando utilizan redes anónimas y dispositivos personales [111].

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 [113].

En este sentido, **España** cuenta con el **INCIBE-CERT** que es quien **ha trabajado en los últimos años** en los servicios de alerta temprana y avisos en materia de ciberseguridad, sobre todo en la sección de avisos SCI, relacionados con los Sistemas de Control Industrial y el mundo del IoT en entornos industriales [113].

Siguiendo lo indicado por INCIBE, y como se muestra en el siguiente gráfico, a nivel estatal se registraron alrededor 338 avisos relacionados con el sector industrial **en el año 2022,** desde dispositivos IoT hasta los más tradicionales como los relacionados con web, escritorio, aplicaciones para móviles, etc. [113].

En relación con los sectores, según los datos obtenidos, se han producido avisos que han afectado a casi todos los sectores estratégicos definidos como Infraestructuras Críticas por la Ley 8/2011. Respecto a las **vulnerabilidades,** la validación incorrecta del parámetro de entrada, el Cross-Site Scripting (XSS) y el desbordamiento de búfer basado en pila, se han presentado como las más comunes, 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 [113].

Avisos por mes en 2022

Figura 23. Número de avisos publicados por mes durante 2022. Fuente: INCIBE

Asimismo, como ha ocurrido en años anteriores, las vulnerabilidades relacionadas con las lecturas fuera de los límites y el control de acceso inadecuado siguen siendo frecuentes, lo que permite que el atacante obtenga información confidencial de forma remota o incluso llegue a tomar el control **de los dispositivos**.

Además, cabe prestar especial atención a las vulnerabilidades relacionadas con los servicios web. En la actualidad, muchos de los dispositivos industriales integrados en las redes, tienen un servidor web que ofrece una interfaz más intuitiva para el operador y habilitando acciones que pueden ser cruciales para que el proceso en el que está involucrado el dispositivo funcione sin problemas.

En definitiva, en el año 2022 se siguió con la tendencia ascendente en cuanto a los avisos y vulnerabilidades se refiere, ya que el número de ambas creció considerablemente, previendo una tendencia similar para 2023.

Los problemas principales a la hora de implantar la ciberseguridad en la industria derivan de la falta de presupuestos y recursos económicos que dedican para este fin. A fin de solucionar dicho problema, la UE decidió impulsar una serie de normativas que ayudarían a las empresas a tomar conciencia gradual de la importancia de la ciberseguridad en la industria, incentivando así una mayor inversión en este ámbito. En el caso concreto de las empresas definidas como infraestructuras críticas, una vez consideradas como tal, pasaban a tener la obligación legal de contar con medidas adecuadas de ciberseguridad tras haberse realizado el análisis de riesgos correspondiente. Por ello, a nivel europeo se encuentra la **Directiva 2008/114/CE del Consejo, sobre Identificación y Designación de las Infraestructuras Críticas Europeas y la Evaluación de la Necesidad de Mejorar su Protección,** lo que supuso el primer paso en regulación de ciberseguridad industrial.

Además, la utilización de guías y estándares de buenas prácticas permitirá la mejora en la gestión de la ciberseguridad industrial para mitigar los riesgos. 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 [114].

Asimismo, la Guía NIST SP 800-82 [115] 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.

Por su parte, cabe hablar de los diferentes nodos (hubs, en inglés) en materia de ciberseguridad industrial. A la hora de realizar un análisis sobre los mismos, llegamos a la conclusión de que nos encontramos ante un panorama escaso, ya que, los hubs a diferencia de los llamados clusters, se configuran como centros multisectoriales, no especializados en un único sector. Por ello, resulta habitual encontrarnos con hubs dedicados a innovación o transformación digital de empresas, en las que se encuentran las dedicadas a la industria.

Antes de realizar el análisis de los diferentes hubs, es necesario hablar de los European Digital Innovation Hubs (EDIH), que son aquellos hubs definidos por la Comisión Europea como las ventanillas que apoyan a las empresas y la administración pública para responder a los retos digitales y ser más competitivos. Esta red EDIH está cofinanciada por la Comisión Europea y por los Estados miembros de la UE [116]. En aras de lo anterior, es la propia comisión quien ofrece un catálogo de estos EDIH facilitando la búsqueda por tipo, países, servicios, tecnologías y sectores. Además, el análisis de cada una de estas características se encuentra regulado por niveles del 1 al 5.

En este sentido, realizado el filtrado por tecnología de ciberseguridad (5/5) y en sector industrial (5/5), se encuentra con un ecosistema escaso y sin hubs específicos o concretos de ciberseguridad industrial. No obstante, tienen como fin la digitalización de las empresas industriales, lo que supone que prestan servicios también en el ámbito de la ciberseguridad industrial. Estos hubs no se encuentran dedicados únicamente al ámbito industrial, pero entre las diferentes tecnologías que abarcan, se encuentra la ciberseguridad industrial.

Ampliando el área de enfoque, y centrándonos en los países con más potencia europea pueden tener en el sector de la industria, se presenta un panorama parecido en el que no se encuentran hubs dedicados únicamente a ciberseguridad industrial, no obstante, encontramos varios hubs dedicados a la digitalización e innovación en el entorno industrial. Ejemplo de ello son:

- **FactoryXChange,** hub irlandés dedicado a extender las competencias digitales y habilidades avanzadas en tecnologías digitales a las partes interesadas. Se configura como un hub de la industria 5.0.
- Otro claro ejemplo es el **AI5production hub** de Austria, que tiene como objetivo principal transformar las empresas industriales en 5.0, esto es, se dedica a la transformación digital de los procesos de producción de pymes.
- **DIH4AISec**, hub europeo de Inteligencia Artificial y Ciberseguridad, que se dedica a apoyar a las empresas de los sectores de la producción, la movilidad y la artesanía especializada, así como al sector público de Baja Sajonia, en la aplicación y el desarrollo de la Inteligencia Artificial y la Ciberseguridad.

A **nivel estatal,** son distintas las regiones que han optado por formar un hub de ciberseguridad que tenga tecnologías de ciberseguridad industrial. Ejemplo de ello, tenemos ello los siguientes:

- **Digital Impulse hub:** con sede principal en Cataluña y con alcance a nivel europeo, se configura como un hub cuyo objetivo principal es llevar la tecnología de los laboratorios a la fabricación. Esto es, trata sobre la digitalización de empresas a través de tecnologías avanzadas.
- **Agora DIH:** se configura como la iniciativa de la Región de Murcia con el objetivo principal de habilitar tecnología avanzada para la transformación digital de las empresas pymes y Administraciones Púbicas.
- **EDIH Madrid Region:** un hub de innovación, a través del cual se coordinan las políticas de transformación digital de empresas y administraciones públicas a nivel regional, nacional y del resto de países de la UE. En materia industrial, acompañan a pymes industriales en sus procesos de transformación digital en áreas como la ciberseguridad, la robótica, el blockchain, etc.
- **InnDIH:** perteneciente a la Comunidad Valenciana, tiene como fin impulsar la digitalización de las pymes y de la Administración Pública y el desarrollo económico. En materia de ciberseguridad abarca tecnologías con las que asegurar la protección completa de los datos, proteger las comunicaciones y las transacciones digitales. En materia industrial, ofertan apoyo para proteger las tecnologías de Fabricación Avanzada, para la protección y buen funcionamiento de las de las infraestructuras y procesos industriales, así como de la propiedad industrial.

Euskadi, a través del BDIH, cuenta con un nodo específico en ciberseguridad compuesto por 5 laboratorios mediante los que responde a la especialización inteligente

A nivel de **Euskadi**, debemos hablar del previamente mencionado **BDIH,** que se configura como una iniciativa que responde a la especialización inteligente **RIS3** para apoyar al tejido empresarial en la experimentación de innovaciones digitales y sostenibles. Se trata de una red de activos y servicios para la formación, investigación, testeo y validación de tecnologías a disposición de las empresas. Este mismo 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 fomentar el emprendimiento y la innovación en el sector industrial.

Las empresas e instituciones en Euskadi reconocen la importancia de mantenerse a la vanguardia en ciberseguridad, no solo para proteger sus propias operaciones, sino también para salvaguardar la estabilidad y la confiabilidad de las infraestructuras críticas que sustentan la economía local. Esta conciencia se ha traducido en esfuerzos continuos para fortalecer sistemas, promover una cultura de ciberseguridad y estar atentos a las innovaciones y tendencias que puedan influir en la seguridad de las operaciones industriales en la región

Finalmente, es preciso hablar de las posibles tendencias futuras en materia de ciberseguridad industrial, siendo la principal, la integración de soluciones de seguridad con la nube, que está impulsando el crecimiento del mercado [111].

En el 2023, se estima que se produzca un incremento global en el número de ciberataques en el sector industrial, enumerándose como las más importantes las siguientes [117]:

- Se prevé que a lo largo de 2023 se produzca **un cambio en las amenazas persistentes avanzadas** (APT) contra varias organizaciones del sector industrial. La posibilidad de ataque se ha incrementado como consecuencia de la digitalización en sectores como IoT y Smart, y la aparición de gemelos digitales y sistemas predictivos en la industria ha aumentado aún más la superficie expuesta a ataques.
- Los **aumentos de precios del hardware y la energía** son inevitables debido a la tensión geopolítica y claramente representan una amenaza para la ciberseguridad. Como resultado, es posible que no se pueda actualizar, implementar o mejorar los sistemas de seguridad industrial debido a los altos costos. Los sistemas de gestión de mantenimiento computarizados (CMMS), por ejemplo, fueron objeto de numerosos ataques en 2022.
- En los últimos años, las empresas se han **migrado rápidamente a la nube** en un esfuerzo por incorporar nuevas prácticas de trabajo en los sistemas que ya han sido integrados por empresas del sector industrial. El uso de varios proveedores de servicios en la nube da como resultado una inconsistencia sistemática, lo que, a su vez, causa varios problemas de seguridad. Dado que el objetivo principal es adoptar el sistema en lugar de defenderlo de posibles ataques, tanto la gestión de estos procesos como la configuración por parte de desarrolladores y usuarios de aplicaciones industriales en la nube pueden presentar un riesgo de seguridad. **desarrollo de sistemas y aplicaciones locales a gran escala.**

• El aumento del método de trabajo híbrido **aumenta el perímetro de la empresa**, lo que puede generar importantes problemas de seguridad.

• Se prevé un **aumento de los ataques de ingeniería social,** siendo el eje central el ataque por correo electrónico, obteniendo un incremento considerable en los ataques de vishing.

• **Los ataques dirigidos contra los usuarios de autenticación multifactor (MFA) serán el objetivo principal.** En el caso de los sistemas de control industrial, gran parte d ellos accesos de importancia requieren de este método de acceso para garantizar la seguridad y el acceso. Se prevé que se den nuevas vulnerabilidades MFA y técnicas de evasión.

• Con el riesgo y aumento de los ataques a la cadena de suministro, los sistemas industriales **elevarán las exigencias** mínimas a la hora de realizar la selección de proveedores.

• La mayor parte de los ataques se centrarán en las infraestructuras industriales productoras de energía.

• Actualización de normativa:

- El Reglamento Delegado de la UE 2022/30 de 20 de octubre de 2021 que complementa la Directiva 2014/53/EU sobre Equipos Radioeléctricos (RED) que hará obligatoria la ciberseguridad para todos los equipos inalámbricos. Establece un marco regulatorio para los equipos de radio, entendiéndose así todos los dispositivos conectados a Internet o aquellos que procesan datos de conectividad, entre los que se pueden encontrar los equipos utilizados para transferir dinero o moneda virtual. Los requisitos esenciales relativos a la ciberseguridad se encuentran recogidos en el artículo 3.3 (d), (e) y (f). Este artículo, especifica los requisitos mínimos que se deben cumplir para una correcta protección de redes, datos personales, privacidad y para la protección contra el fraude de transacciones de dinero no efectivo. Esta norma entrará en vigor a partir del 1 de agosto de 2024, con un periodo de transición de 30 meses que comenzó a fecha de 1 de febrero de 2022. Mientras tanto, los organismos europeos se encuentran trabajando en su estandarización [118].

- NIST IR 8270. Se prevé un aumento de los ataques al entorno satelital, por lo que se ha realizado a actualizar la presente norma durante el año 2023. Se trata de un documento de referencia de información para gestionar los riesgos de ciberseguridad y considerar cómo los requisitos de ciberseguridad pueden coexistir dentro de los requisitos del sistema de vehículos espaciales [119].

En definitiva, habrá un aumento exponencial de los ciberataques siendo tanto los sistemas industriales, como los equipos de nueva generación los objetivos principales. Además, las actualizaciones en la normativa cobrarán especial importancia por ser el cumplimiento básico para cualquier empresa del sector industrial, evitando así posibles sanciones por incumplimiento.

En lo que respecta al ámbito regional, en **Euskadi,** la ciberseguridad industrial ha emergido como una prioridad clave para proteger las infraestructuras. La historia industrial de Euskadi ha influenciado significativamente la atención hacia la ciberseguridad en la región. Dada su sólida base industrial, Euskadi ha sido consciente de la importancia de salvaguardar sus activos críticos contra ciberamenazas emergentes. Esta tradición industrial ha generado una mentalidad proactiva y un importante grado de especialización en la implementación de medidas de ciberseguridad, ya que las empresas en la región entienden la relevancia de proteger sus procesos de producción, la infraestructura y los datos sensibles.

Euskadi busca posicionarse como hub en ciberseguridad industrial, 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

La rica historia industrial de Euskadi ha actuado como un impulsor para la adopción de estándares de seguridad y la promoción de la colaboración entre sectores, reconociendo que la ciberseguridad es un componente vital para la continuidad y la competitividad en la industria. Esta interconexión entre la herencia industrial y la atención actual en ciberseguridad demuestra cómo **Euskadi** no solo abraza su legado industrial, sino que también **busca adaptarse y protegerse en un entorno cada vez más digitalizado y propenso a ciberamenazas.**

La colaboración entre sectores ha sido fundamental, promoviendo alianzas entre el sector público y privado para compartir información y fortalecer las defensas contra amenazas como ramsomware e intrusiones en sistemas industriales. La implementación de estándares de seguridad, la investigación y la innovación continúan siendo áreas destacadas, enfocadas en desarrollar y aplicar estrategias adaptadas a las necesidades específicas de la industria regional.

Euskadi, con la firme aspiración de consolidarse como un **hub destacado en ciberseguridad industrial,** ha sentado las bases para alcanzar este ambicioso objetivo. El tejido industrial de la región necesita que siga aumentando la madurez digital, lo que significa que las empresas tienen que seguir adaptándose a estas tecnologías avanzadas para optimizar sus procesos cada vez más interconectados. Esta predisposición hacia la innovación y la digitalización proporciona un entorno para el desarrollo de capacidades en ciberseguridad.

Adicionalmente, el ecosistema tecnológico en Euskadi se destaca por su robustez, actuando como un catalizador para convertirse en un hub de referencia en ciberseguridad industrial. 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 en ciberseguridad industrial se ve respaldada 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. Esta combinación única de factores no solo va a impulsar 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 escenario, Euskadi dispone de todos los elementos necesarios para concretar su visión de liderazgo en los próximos años dentro del ámbito de la ciberseguridad industrial.**

Instrumentos de apoyo a la ciberseguridad

En cuanto a los instrumentos de apoyo a la ciberseguridad con impacto en Euskadi, destaca la Agenda Digital de España como un componente esencial de la transformación digital a nivel nacional.

Se enfoca en promover la transformación digital del país, estableciendo estrategias para fortalecer la infraestructura digital, la conectividad, la ciberseguridad, la digitalización de las empresas y la capacitación digital de la ciudadanía.

El objetivo marcado por la Agenda España Digital 2026 es mejorar las capacidades de ciberseguridad en España, impulsar el desarrollo empresarial en el sector (industria, investigación, desarrollo e innovación, y talento) y consolidar el liderazgo internacional en seguridad digital.

Para lograr estos objetivos y fortalecer la confianza digital, es necesario implementar una cultura de ciberseguridad. Esto implica concienciar sobre los riesgos digitales y formar en competencias de seguridad. Por ello, el Instituto Nacional de Ciberseguridad (INCIBE) está llevando a cabo diversas iniciativas alineadas con estos objetivos [122]:

• **Fortalecimiento de la ciberseguridad para ciudadanos, pymes y profesionales (Confía):** desarrollando mecanismos de información, concienciación y formación en ciberseguridad, ampliando los servicios disponibles y colaborando con actores públicos y privados para mejorar las capacidades digitales y la defensa conjunta ante amenazas.

• Impulso de España como **nodo internacional en ciberseguridad:** mediante la creación del Centro Nacional de Competencias en Ciberseguridad (NCC-ES), en consonancia con el Centro Europeo de Competencias (ECCC), y fomentando la participación en la Red europea de centros.

• **Impulso del ecosistema empresarial de la ciberseguridad:** acciones para expandir la industria nacional, fomentar la investigación y el desarrollo, e identificar y desarrollar talento en este campo.

- **INCIBE Emprende:** iniciativas de ideación, incubación y aceleración para nuevas startups y el crecimiento de las ya existentes en ciberseguridad.
- **Talento Hacker:** programa para captar, formar y emplear trabajadores en este ámbito.
- **Ciberinnova:** iniciativas para impulsar la industria nacional y la competitividad a través de la innovación en seguridad.
- **Internacionalización:** fomento del crecimiento e internacionalización del ecosistema empresarial de ciberseguridad.

• **Redes Territoriales de Especialización Tecnológica (RETECH):** proyectos regionales orientados a la transformación digital, asegurando la coordinación y colaboración entre ellos.

Por otro lado, se encuentra el **Plan de Recuperación, Transformación y Resiliencia**, uno de los ejes transversales de España Digital, es un plan integral que busca la recuperación económica tras la crisis generada por la pandemia, para modernizar el tejido productivo, fomentar la innovación y fortalecer la resiliencia del país [121].

Es destacable que 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.

En la primera fase de la transformación digital, se contemplan inversiones públicas de 20.000 millones de euros hasta 2023 o 2025, dependiendo de los proyectos. Esta inyección de fondos europeos representa aproximadamente el 30% de las inversiones planificadas en el marco del Plan de Recuperación. Estas inversiones tienen un alcance y magnitud que prometen un impacto genuinamente transformador.

La **"Adenda**", segunda fase del Plan de Recuperación, busca seguir **impulsando inversiones alineadas** a la estrategia digital europea. Se enfoca en tres **áreas clave**: infraestructuras **y/o tecnología,** economía y personas. 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. Esta iniciativa está enmarcada dentro del Plan de Recuperación, Transformación y Resiliencia, que cuenta con un presupuesto de 3.067 millones de euros financiados por la Unión Europea a través de los fondos Next Generation EU.

Además de estas tres áreas, se incorporan **dos ejes transversales** destinados a **potenciar proyectos estratégicos** de gran alcance mediante la colaboración entre el sector público y privado, así como la **colaboración entre el Estado y las Comunidades Autónomas en una gobernanza conjunta.**

En este punto es preciso hablar también de las **Redes Territoriales de Especialización Tecnológica (RETECH)** [123][124]. Propiciada por el Plan de Recuperación, Transformación y Resiliencia, se configura como una herramienta para hacer realidad la transformación digital a nivel estatal, siendo su propósito instaurar iniciativas territoriales que impulsen la transformación digital de manera conjunta y colaborativa entre diversas regiones.

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.** Tras una convocatoria pública, los proyectos fueron aprobados en diciembre de 2022 y recibirán financiación a través de los fondos del Plan de Recuperación (Next Generation) [123].

Los proyectos integrados en RETECH abarcan diversos sectores de acción estratégica, fundamentados en las prioridades definidas en el Plan de Recuperación, así como en las necesidades, requerimientos y potencialidades específicas manifestadas por las distintas regiones, entre los que se encuentra la **ciberseguridad**.

La iniciativa RETECH Ciberseguridad es un **componente estratégico en el impulso del ecosistema de ciberseguridad en el estado,** abarcando capacidades, la industria, la investigación y el desarrollo, así como el talento en este ámbito. Con la coordinación de INCIBE, perteneciente al Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, se ha congregado en su primera etapa a 15 comunidades autónomas, con un presupuesto inicial de 149 millones de euros. Se encuentra estructurado en 3 nodos, **formando parte Euskadi 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 **otros** sectores considerados 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 **modelada** 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 enfrenta obstáculos **significativos** [123][124]. **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.

En esta línea, cabe mencionar también 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**. Esto incluye la creación de estrategias específicas para mejorar la seguridad en línea, diseñada a medida para la organización [125]. Asimismo, la Agenda **España Digital 2026** contempla inversiones destinadas a reforzar la **industria de la ciberseguridad** y la formación de talento por un valor de 450 millones de euros [126].

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 las 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.** Abarca una triple transición: tecnológica y digital, energética y climática, así como social y sanitaria. Estas transiciones son el resultado del impacto que las tendencias globales dominantes tienen en Euskadi [127].

Dentro de este Plan, se delinean tres pilares estratégicos fundamentales y un elemento central:

- **Excelencia Científica:** este pilar se enfoca en promover la investigación de calidad y el avance en el conocimiento, impulsando la excelencia en todos los ámbitos científicos.
- **Liderazgo Tecnológico e Industrial:** aquí se prioriza el impulso a la innovación tecnológica y el desarrollo industrial, buscando posicionar a Euskadi como líder en estos campos a nivel nacional e internacional.
- **Innovación Abierta:** este pilar se centra en la promoción de la innovación a través de la colaboración y la apertura, fomentando la cooperación entre diferentes actores y sectores para potenciar el desarrollo de soluciones innovadoras.

Y como elemento central, se destaca el **talento**, reconociéndose como el motor fundamental que impulsa el progreso en cada uno de estos pilares estratégicos. El desarrollo y la retención del talento se consideran aspectos vitales para el éxito y la sostenibilidad de las iniciativas contempladas en el Plan.

El éxito de la visión trazada en el **PCTI 2030** depende de la sinergia equilibrada de cuatro elementos fundamentales. Estos elementos deben trabajar en conjunto para convertir los avances en investigación en logros tangibles tanto a nivel económico como social. Esta perspectiva abarca la investigación básica, que busca generar nuevo conocimiento vanguardista, así como la investigación aplicada y la innovación, orientadas a fortalecer la competitividad internacional del entramado empresarial vasco y a impulsar mejoras en áreas como la salud, el transporte y el medio ambiente. Este enfoque contempla todos los niveles de desarrollo tecnológico, desde conceptos incipientes hasta soluciones completamente implementables (Technology Readiness Levels - TRLs) [127].

El PCTI 2030 se enfoca en estimular la innovación en todas sus formas, desde aquella que representa una disrupción hasta la que tiene un carácter más incremental, aplicándose ello tanto en las grandes empresas como, especialmente, en las más pequeñas. Además, también se extiende a entidades como las administraciones públicas, instituciones sanitarias y la colaboración con diversos actores de la Red Vasca de Ciencia, Tecnología e Innovación.

Por otro lado, cabe destacar la **Estrategia para la Transformación Digital de Euskadi 2025 (ETDE2025)** que 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). Estos elementos no operan de manera independiente, sino como un sistema interconectado, con el objetivo primordial de generar valor para Euskadi [128].

La selección de las palancas tecnológicas se ha realizado considerando su potencial disruptivo a corto, mediano y largo plazo en relación con los desafíos planteados en las tres transiciones principales. Una de estas palancas tecnológicas es la ciberseguridad al considerarse como habilitadora y estratégica de cara a la digitalización y evolución de nuestra economía. Por otro lado, los habilitadores se definen como los recursos, canales o capacidades que facilitan y aceleran la implementación de las tecnologías digitales.

Euskadi cuenta con un ecosistema robusto en lo que a instrumentos de apoyo se refiere. La ciberseguridad cuenta con un papel protagonista.

En línea con estas dimensiones, el objetivo general de la estrategia se centra en acelerar la adopción de las tecnologías emergentes, fortalecer el desarrollo y aprovechar el potencial comprobado de los habilitadores. Esto se lleva a cabo activando e impulsando su rápida integración en áreas esenciales de aplicación. Esta iniciativa está diseñada para contribuir a las transiciones fundamentales que enfrenta Euskadi para 2025: la transición tecnológico-digital, la energética-medioambiental y la social y sanitaria.

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 [132][133][134][135]. 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 RVCTI, (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 2023

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 2023

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 fabricación avanzada. 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 [133].

Ciberseguridad Industrial 2023

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.

De esta manera, el programa que ya va por su sexta edición, y que 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 [137]. Los proyectos objeto del programa deben de ser realizados por empresas externas y expertas en el campo de la ciberseguridad.

Este sencillo, a la par que eficaz enfoque, ha suscitado el interés a lo largo de estos años de infinidad de empresas, las cuales se han visto beneficiadas por el programa, abordando proyectos de ciberseguridad, que, de otra forma, dado a la fuerte inversión que suponen, quizás no se hubieran materializado. A continuación, se presenta una foto general con los datos más significativos de estas seis convocatorias del programa.

6 **Convocatorias**	**1.700** **Proyectos presentados**	**1.610** **Proyectos aprobados**	**1.018** **Empresas apoyadas**

31.5 M€
Inversión / Gasto

13.6 M€ **Subvención concedida**	**8.450 €** **Subvención concedida**	**>155 €** **Subvención concedida**

Como se puede apreciar 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 del 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.

Presupuesto Asignado al programa de Ciberseguridad Industrial

Figura 25. Presupuesto asignado al programa Ciberseguridad Industrial. Fuente: SPRI

A nivel de proyectos, en las últimas 3 convocatorias, la cifra de proyectos aprobados ha experimentado un crecimiento significativo, hasta al punto que se empieza a consolidar la cifra de en torno a 350 proyectos apoyados al año. Esta notable demanda suscitada en las últimas convocatorias del programa (véase la figura siguiente), ayuda a entender la realidad y permite apuntalar cierta tendencia en lo que al tejido empresarial de Euskadi se refiere, donde cada vez resulta mayor el número de empresas que consideran prioritario el abordar proyectos de ciberseguridad en el corto-medio plazo. Adicionalmente, se observa cierta tendencia en cuanto a empresas que deciden abordar proyectos de ciberseguridad de forma sistemática y recurrente año tras año. Actuaciones, que, en muchos casos, forman parte de un plan director de Ciberseguridad perfectamente definido para cada una de estas organizaciones.

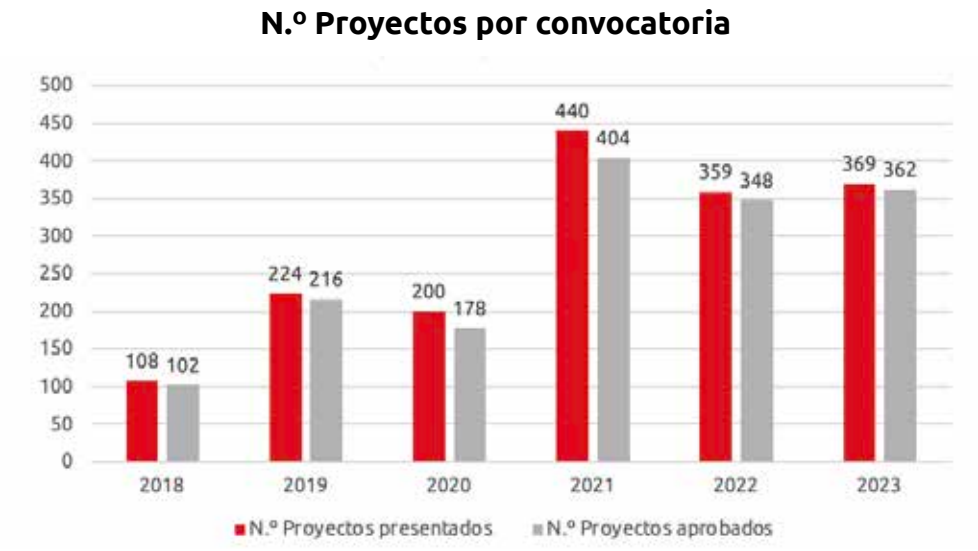


Figura 26. N.º Proyectos por convocatoria del programa Ciberseguridad Industrial. Fuente: SPRI

La subvención concedida por anualidad a lo largo de estas convocatorias va intrínsecamente relacionada con el número de proyectos aprobados, con lo que ésta ha sufrido una evolución similar a lo largo de estos años, tal y como se puede apreciar en la gráfica a continuación. Siendo el 2021 también un año trascendental a nivel de cifras tanto para las empresas que se pudieron beneficiar del programa, como para el sector de la ciberseguridad de Euskadi. Se conoce que este fuerte incremento pudo venir derivado fundamentalmente, de la crisis sanitaria ocasionada por la COVID19, donde el auge del teletrabajo, la falta de concienciación entre la ciudadanía y empleados, así como la instalación y el despliegue de nuevas infraestructuras y mecanismos de comunicación en tiempo récord, propiciaron el escenario perfecto para que el número de incidentes de ciberseguridad se multiplicara. De esta manera, y con el objetivo de mitigar y securizar estos nuevos entornos, en 2021 se vio un fuerte incremento de actividad en el sector de la ciberseguridad en Euskadi, que quedó reflejada también en las cifras programa.

A continuación, se puede observar la distribución en cuanto a subvención concedida en cada convocatoria:

Figura 27. Subvención por convocatoria del programa Ciberseguridad Industrial. Fuente: SPRI

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 del territorio histórico 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.

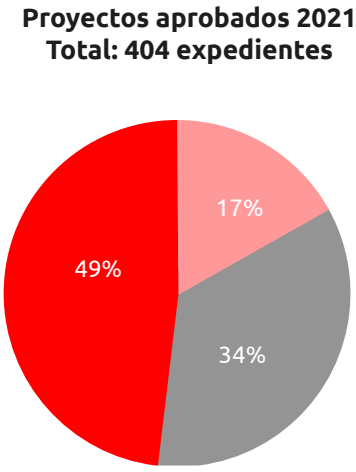


Figura 27. N.º de proyectos aprobados por territorio histórico 2021. Fuente: SPRI

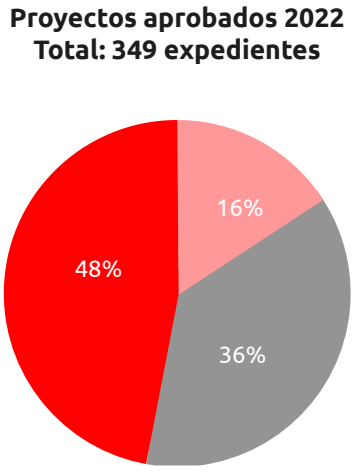


Figura 28. N.º de proyectos aprobados por territorio histórico 2022. Fuente: SPRI

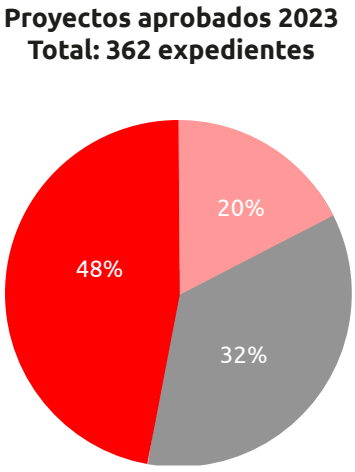


Figura 29. N.º de proyectos aprobados por territorio histórico 2023. Fuente: SPRI

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.

Proyectos aprobados 2021
Total: 404 expedientes

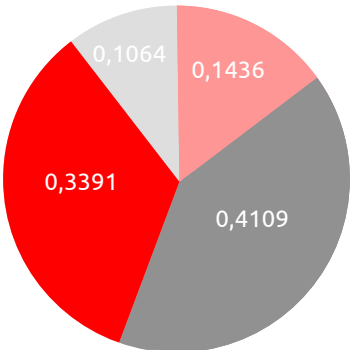


Figura 30. N.º de proyectos aprobados por N.º Empleados 2021. Fuente: SPRI

Proyectos aprobados 2022
Total: 349 expedientes

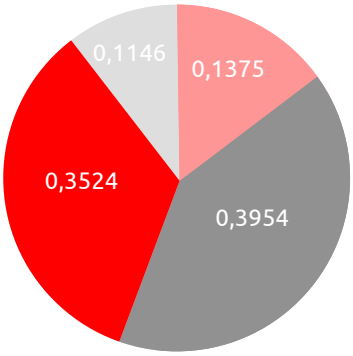


Figura 31. N.º de proyectos aprobados por N.º Empleados 2022. Fuente: SPRI

Proyectos aprobados 2023
Total: 362 expedientes

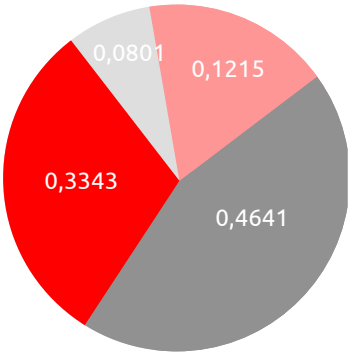


Figura 32. N.º de proyectos aprobados por N.º Empleados 2023. Fuente: SPRI

1-9 empleados 10-49 empleados 50-249 empleados 250 o más

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 implantación 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. Adicionalmente, se puede observar cierta masa crítica en otros sectores que, sin ser necesariamente industriales, las empresas que focalizan su actividad dentro de estos segmentos, y que se han beneficiado del programa, 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". Para el resto de los sectores el número de proyectos aprobados a lo largo de estas 6 convocatorias del programa resulta prácticamente residual.

Proyectos Aprobados por Sector de Actividad

Figura 34. N.º de proyectos aprobados por Sector de Actividad. Fuente: SPRI

Del mismo modo, dentro del sector de actividad de industria manufacturera, destacan los proyectos aprobados a empresas que enmarcan su actividad dentro de los subsectores de "Productos Metálicos" y "Maquinaria y equipo n.c.o.p.". Con carácter general, estos subsectores congregan a empresas tales como talleres de mecanizados o del campo de la máquina-herramienta.

Proyectos Aprobados - Industria Manufacturera

Figura 35. N.º de proyectos aprobados dentro de Industria Manufacturera. Fuente: SPRI

Como resultado de este análisis, se podría concluir con que el tipo de perfil de empresa que presenta proyectos y se beneficia del programa Ciberseguridad Industrial en mayor medida, son empresas de entre 10 y 49 trabajadores, del territorio histórico de Gipuzkoa, y del sector de industria manufacturera, destacando aquellas que se dedican a la fabricación de productos metálicos.

Otra cuestión importante a tener en cuenta y que resulta indicativo del tipo de inversiones que están realizando las empresas de Euskadi en esta materia, es la tipología de proyectos aprobados a lo largo de las diferentes convocatorias del programa. Entre los proyectos o actuaciones subvencionables dentro del programa, se encuentran los proyectos dirigidos a la [134]:

- Convergencia e integración de los sistemas de protección ante ciberataques para entornos IT/OT (Information Technology / Operational Technology). Diseño y ejecución de arquitecturas seguras y en su caso materialización de la segmentación de redes industriales.

- Securización de los accesos remotos OT a los equipos industriales de la planta productiva requeridos para el mantenimiento de equipo, control y operación de los mismos, tareas realizadas cada vez con más frecuencia de manera remota.

- Securización de la información/datos industriales. Auditorías y simulaciones de ataques por personas externas a la organización y auditorias sobre perfiles internos con diferentes niveles de accesos a datos de la compañía.

- Evaluación de la ciberseguridad de dispositivos electrónicos, así como su certificación.

- Iniciativas para la concienciación y/o capacitación de la plantilla de la empresa industrial en el ámbito de ciberseguridad.

- Diagnóstico de situación actual de la industria en materia de ciberseguridad industrial y elaboración de su plan de acción para la mejora de la Ciberseguridad. Análisis de riesgo industrial y de vulnerabilidad industrial. Inventario de los diferentes elementos en un sistema crítico industrial. Realización de un test de intrusión industrial. Análisis de vulnerabilidades en aplicaciones web. Auditorias de las comunicaciones inalámbricas industriales.

- Replicación de CPDs dirigidos a la adopción de políticas de ciberseguridad relacionadas con Planes de Recuperación ante Desastres o de contingencia, así como a escenarios de alta disponibilidad dirigidos a garantizar la continuidad de negocio en cualquier empresa.

- Adopción de buenas prácticas y procesos de certificación relativos a la obtención y cumplimiento de diversos estándares 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) ampliamente reconocidos, así como reglamento o leyes en vigor de obligado cumplimiento. Adaptación al cumplimiento del Esquema Nacional de Seguridad (Real Decreto 3/2010), Reglamento PIC (Real Decreto 704/2011). Mejora continua del proceso de gestión de ciberseguridad mediante el despliegue de medidas específicas o evolución de las mismas a niveles de madurez superiores a los preexistentes.

• Medidas de protección de información estratégica o sensible como puedan ser la propiedad intelectual, estrategias de I+D+i, planos de edificios o de diseño de productos, información afectada por el RGPD o cualquiera otra directamente relacionada con la competitividad y sostenibilidad del negocio. (ejemplo de medidas: cifrado del almacenamiento, control de acceso, control de distribución de copias, borrado seguro, etc.).

• Monitorización de dispositivos de seguridad perimetral y de otros dispositivos industriales (Switches, sondas, Appliances, firewalls industriales, PLCs, EDRs, etc.).

• Otros proyectos que incrementen de manera significativa el nivel de ciberseguridad de las empresas industriales y reduzcan el riesgo y la vulnerabilidad ante los diferentes tipos de ataques existentes.

En este sentido, analizando la información de las diferentes convocatorias del programa, se extrae que la tipología de proyectos más repetida sería la relacionada con el Diseño y Ejecución de nuevas arquitecturas de red con el objetivo de garantizar la segmentación entre entornos IT y OT. Adicionalmente, otra de las tipologías de proyectos que han tenido un peso importante a lo largo de estas 6 convocatorias del programa, sería la relativa a la monitorización de dispositivos de seguridad perimetral y de otros dispositivos industriales tales como switches o firewalls, entre otros.

Incremento Sustancial: Proyectos relacionados con la Adopción buenas prácticas y procesos de certificación (IEC 62445, TISAX, ENS, ISO27001, etc)

Por último, 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 **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.

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.

Tipología	2021	2022	2023
Convergencia e integración de los sistemas de protección ante ciberataques para entornos IT/OT (Information Technology / Operational Technology). Diseño y ejecución de arquitecturas seguras y en su caso materialización de la segmentación de redes industriales.	18%	14%	27%
Adopción de buenas prácticas y procesos de certificación relativos a la obtención y cumplimiento de diversos estándares 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)	10%	8%	19%
Monitorización de dispositivos de seguridad perimetral y de otros dispositivos industriales (Switches, sondas, Appliances, firewalls industriales, PLCs, EDRs, etc.).	13%	12%	18%
Diagnóstico de situación actual de la industria en materia de ciberseguridad industrial y elaboración de su plan de acción para la mejora de la Ciberseguridad. Análisis de riesgo industrial y de vulnerabilidad industrial. Inventario de los diferentes elementos en un sistema crítico industrial. Realización de un test de intrusión industrial. Análisis de vulnerabilidades en aplicaciones web. Auditorias de las comunicaciones inalámbricas industriales.	12%	9%	11%
Securización de la información/datos industriales. Auditorías y simulaciones de ataques por personas externas a la organización y auditorias sobre perfiles internos con diferentes niveles de accesos a datos de la compañía.	12%	9%	8%
Medidas de protección de información estratégica o sensible como puedan ser la propiedad intelectual, estrategias de I+D+i, planos de edificios o de diseño de productos, información afectada por el RGPD o cualquiera otra directamente relacionada con la competitividad y sostenibilidad del negocio.	10%	8%	6%
Securización de los accesos remotos OT a los equipos industriales de la planta productiva requeridos para el mantenimiento de equipo, control y operación de los mismos, tareas realizadas cada vez con más frecuencia de manera remota.	11%	7%	4%
Replicación de CPDs dirigidos a la adopción de políticas de ciberseguridad relacionadas con Planes de Recuperación ante Desastres o de contingencia, así como a escenarios de alta disponibilidad dirigidos a garantizar la continuidad de negocio en cualquier empresa.	-	-	4%
Iniciativas para la concienciación y/o capacitación de la plantilla de la empresa industrial en el ámbito de ciberseguridad.	8%	8%	2%
Evaluación de la ciberseguridad de dispositivos electrónicos, así como su certificación.	-	-	1%
Evaluación del software industrial	6%	6%	-

Tabla 3. Porcentaje de proyectos aprobados por tipología de proyecto. Convocatoria 2021, 2022 y 2023. Fuente: SPR

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 [135]:

- **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.

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

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 [136].

Hay **cuatro líneas de subvención**, cada una dirigida a distintos aspectos de la **transformación digital** y la sostenibilidad ambiental, así como a diversos tipos de empresas y sectores entre los que se encuentra la ciberseguridad.

- **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, sistemas 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 algunas de las siguientes actividades innovadoras:

• La introducción del **uso intensivo de tecnologías digitales** en todos los procesos de las empresas, tales como, 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 **distinta naturaleza,** 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 agentes 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 **categorías**, 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 mayoristas/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 e ingeniería 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:

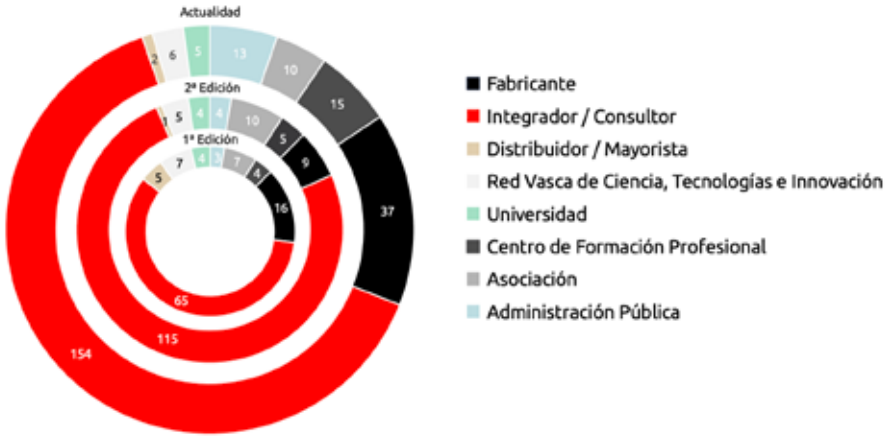


Figura 36. Agentes listados en diferentes ediciones del Libro Blanco. Fuente: SPRI

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.

	1ª Edición	2ª Edición	3ª Edición
Total	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.

193	20	10	6	13
Empresas de las cuales 59 startups	Red de Centros de Educación	Asociaciones	RVCTI	Administración Pública

Figura 37. Agentes del mercado de ciberseguridad en Euskadi. Fuente: SPRI

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

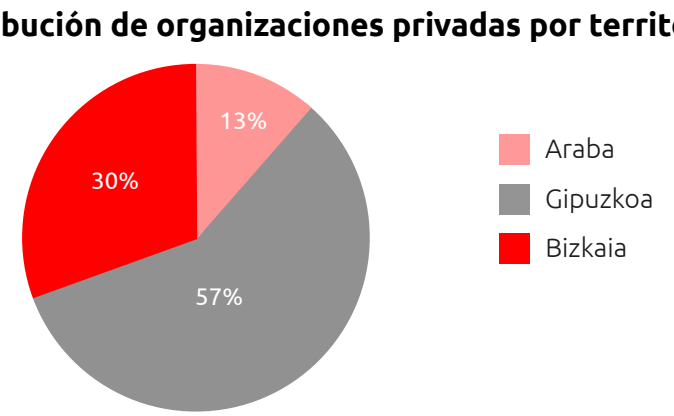


Figura 38. Distribución de agentes privados por territorio histórico. Fuente: SPRI

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.

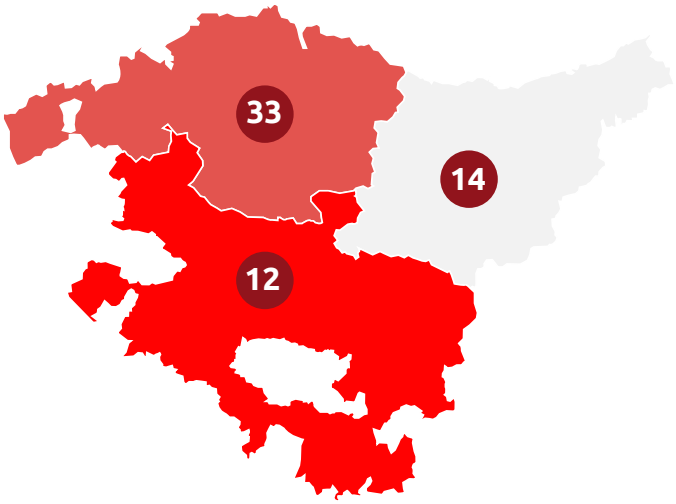


Figura 41. Startups de ciberseguridad en Euskadi. Fuente: SPRI

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

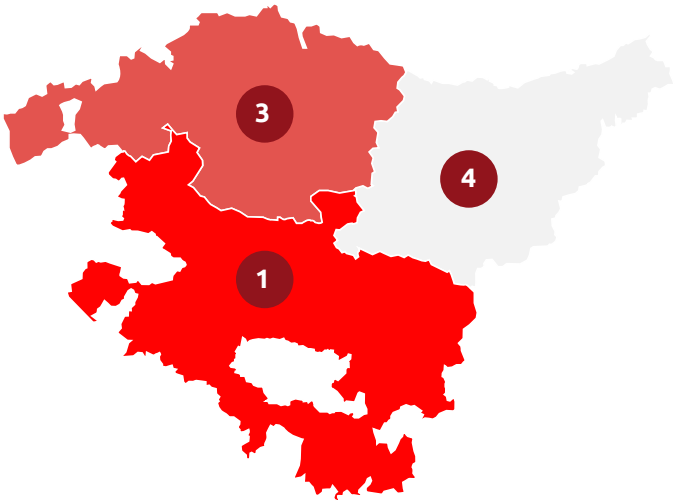


Figura 40. Distribución de centros de actividad de agentes RVCTI de ciberseguridad en Euskadi. Fuente: SPRI

Vicomtech	Tecnalia	Innovalia
Ikerlan	Ceit	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 - 10.3 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.

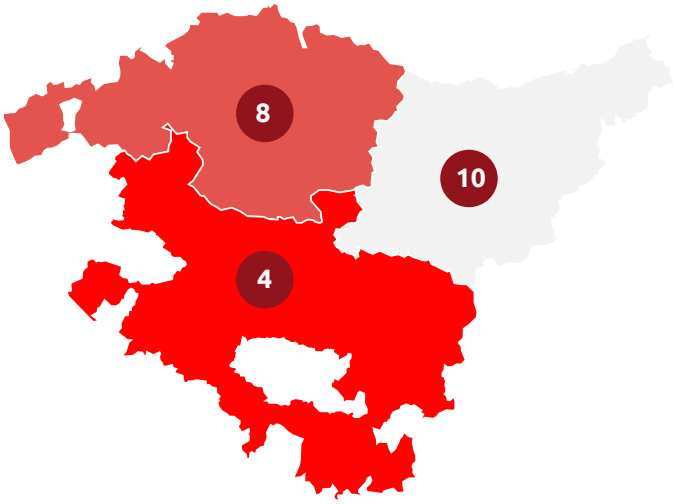


Figura 41. Distribución en cuanto a sedes de centros de educación en materia de ciberseguridad. Fuente: SPRI

Centro de Formación Profesional:

Centro SEIM
CIFP Tartanga LHII
CIFP Txurdinaga
EASO Politeknikoa
Egibide Vitoria-Gasteiz Alava
FP Andra Mari
IES Zubiri-Manteo
Izarraitz Lanbide Heziketa Laudioalde Lanbide Eskola
Lea-Artibai Ikastetxea
Maristak Durango Ikastetxea
Politeknika Txorierri
Tknika
Uni Eibar-Ermua
Urola Garaiko Lanbide Eskola

Universidad:

Mondragon Unibertsitatea
Tecnun - Universidad de Navarra
Universidad de Deusto
Universidad de Vitoria-Gasteiz EUNEIZ
UPV/EHU

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 Cyberzaintza en Euskadi representa un claro esfuerzo de estas instituciones por fortalecer la seguridad digital, abordar desafíos específicos y salvaguardar los intereses en el ámbito digital.**

Se destacan también las iniciativas llevadas a cabo en el ámbito de la ciberseguridad por el **Departamento de Desarrollo Económico, Sostenibilidad y Medioambiente del Gobierno Vasco, a través de SPRI,** organismos que se erigen como referentes en todo lo relacionado con la ciberseguridad aplicada al entorno empresarial, y más concretamente al industrial. Un apoyo institucional sin duda diferencial que ha contribuido en los últimos años al fortalecimiento y crecimiento tan vertiginoso que ha experimentado el sector de la ciberseguridad en Euskadi.

- Agencia Vasca de Protección de Datos
- Ayuntamiento de Vitoria-Gasteiz
- BilbaoTIK
- BiscayTIK
- CCASA
- Cyberzaintza
- DonostiaTIK
- EJIE
- Izenpe
- IZFE
- Lantik
- SPRI
- Ziur

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.

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

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 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.

Euskadi como centro líder y hub de referencia en ciberseguridad Industrial

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 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.

Bibliografía

Bibliografía de las diferentes fuentes para el desarrollo del documento.

1.ESENTIRE (2022). 2022 Official Cybercrime Report. Disponible en: https://www.esentire.com/resources/library/2022-official-cybercrime-report

2.Comisión Europea (2022). European Cybersecurity Investment Platform. Disponible en: https://www.eib.org/attachments/lucalli/20220206-european-cybersecurity-investment-platform-en.pdf

3.Renub Research (2023). Europe Cyber Security Market, Size, Forecast 2023-2028, Industry Trends, Growth, Impact of Inflation, Opportunity Company Analysis. Disponible en: https://www.renub.com/europe-cyber-security-market-p.php

4.DBK (2023). Informe Especial DBK: Ciberseguridad.

Disponible en: https://www.dbk.es/es/estudios/17541/summary

5.Global Data (2022). Cybersecurity Market Size, Share, Growth & Forecast. Disponible en: https://www.globaldata.com/store/report/cybersecurity-market-analysis/

6.FORBES (2023). Cybersecurity As A Strategic Investment: How ROI Optimization Can Lead To A More Secure Future. Disponible en: https://www.forbes.com/sites/forbestechcouncil/2023/08/16/cybersecurity-as-a-strategic-investment-how-roi-optimization-can-lead-to-a-more-secure-future/?sh=d9e61c34cf7f

7.Venture in Security (2023). Generalist VC firms in cybersecurity. Disponible en: https://ventureinsecurity.net/p/generalist-vc-firms-in-cybersecurity

8.News & Analysis driven by the PitchBook Platform (2023). PE cybersecurity investment relatively robust in Europe, plummets in US. Disponible en: https://pitchbook.com/news/articles/Cybersecurity-private-equity-deals-US-Europe

9.Comisión Europea (2022). European Cybersecurity Investment Platform. Disponible en: https://www.eib.org/attachments/lucalli/20220206-european-cybersecurity-investment-platform-en.pdf

10.Comisión Europea (2021). Programa Europa Digital. Disponible en: https://ec.europa.eu/info/funding-tenders/find-funding/eu-funding-programmes/digital-europe-programme_es

11.ElReferente (2023). Adara Ventures. Disponible en: https://elreferente.es/directorio/adara-ventures/

12.StartechUP (2021). 10 empresas de Capital Riesgo que invierten en compañías de SaaS en este momento. Disponible en: https://www.startechup.com/es/blog/venture-capital-firms-investing-saas-companies/#3_Accel_Partners

13.WebCapitalRiesgo (2022). Alantra lanza la gestora 33N Ventures para invertir en ciberseguridad en Europa, Israel y EE.UU. Disponible en: https://www.webcapitalriesgo.com/alantra-lanza-la-gestora-33n-ventures-para-invertir-en-ciberseguridad-en-europa-israel-y-eeuu/

14.33N Ventures. Disponible en: https://33n.vc/

15. SANTANDER (2022). Santander y Forgepoint Capital anuncian una alianza estratégica para impulsar la inversión y la innovación en ciberseguridad. https://www.santander.com/es/sala-de-comunicacion/notas-de-prensa/2022/10/santander-y-forgepoint-capital-anuncian-una-alianza-estrategica-para-impulsar-la-inversion-y-la-innovacion-en-ciberseguridad

16. IBERDROLA (2023). Portfolio de inversiones. Más de 125 millones de inversión en innovación a través de nuestra cartera de startups. Disponible en: https://www.iberdrola.com/innovacion/programa-internacional-startups-perseo/porfolio-inversiones

17. Up!Euskadi (2023). Explore the Basque Country ecosystem. Disponible en: https://startup.spri.eus/intro-curated-content?applyDefaultFilters=true

18. LeadersLeague (2023). Inversión en capital. Operaciones de capital de riesgo. Disponible en: https://www.leadersleague.com/es/rankings/inversion-en-capital-operaciones-de-capital-de-riesgo-clasificacion-2023-fondos-de-inversion-espana

19. ElReferente (2023). JME Ventures. Disponible en: https://elreferente.es/directorio/jme-venture-capital/

20. JME Ventures (2023). Investing in Spain's next success stories. Disponible en: https://www.jme.vc/

21. Kibo Ventures (2023). European venture capital empowering outliers to solve bog problems. Disponible en: https://kiboventures.com/

22. Caixa Capital Risc (2023). Disponible en: https://www.caixacapitalrisc.es

23. SPRI (2023). Up!Euskadi. Ecosistema vasco de emprendimiento. Disponible en: https://upeuskadi.spri.eus/es/startups-de-euskadi/

24. Comisión Europea (2022). European innovation scoreboard. Disponible en: https://research-and-innovation.ec.europa.eu/statistics/performance-indicators/european-innovation-scoreboard_en

25. ICEX (2020). Investin Spain. País Vasco: Razones para invertir. Disponible en: https://www.investinspain.org/content/icex-invest/es/regions/pais-vasco/razones-para-invertir.html

26. Bizkaia. Foru Aldundia. Diputación Foral. Impuestos directos. Impuesto sobre Sociedades (IS). Disponible en: https://www.bizkaia.eus/es/web/educacion-tributaria/impuesto-sobre-sociedades-is-

27. Gipuzkoa. Foru Aldundia. Diputación Foral. Impuestos directos. Impuesto sobre Sociedades (IS). Disponible en: https://www.gipuzkoa.eus/es/web/ekonomiaetazergak/impuesto-sobre-sociedades

28. Araba. Foru Aldundia. Diputación Foral. Impuesto sobre sociedades (IS). Disponible en: https://web.araba.eus/es/hacienda/sociedades/informacion

29. Grupo SPRI (2023). Acelerando el crecimiento de las empresas vascas. Disponible en: https://www.spri.eus/es/capital-riesgo/

30. Bizkaia seed capital (2023). Seed capital Bizkaia. Disponible en: https://www.seedcapitalbizkaia.eus/seed-capital-bizkaia/

31. Inveready (2023). Strategy. Disponible en: https://inveready.com/investment-vehicles/

32. Crunchbase (2023). Orza Investments. Disponible en: https://www.crunchbase.com/organization/orza-investments

33.All Iron Ventures (2023). Scaling your company is a though journey. Disponible en: https://www.alliron.vc/

34.Easo Ventures (2023). Política de inversión. Disponible en: https://www.easoventures.com/politica-de-inversion/

35.Talde (2023). Capital Privado. Disponible en: https://www.talde.com/es/gestion-de-activos/capital-privado

36.(ISC)2 (2022). Cybersecurity Workforce Study. Disponible en: https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

37.ENISA (2023). European Cybersecurity Skills Framework (ECSF). Disponible en: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

38.ObservaCIBER (2022). Análisis y diagnóstico del talento de ciberseguridad en España. Disponible en: https://files.incibe.es/incibe/talento/INCIBE_Resumen_DIAG.pdf

39.ConfeBask (2022). Necesidades de empleo y cualificaciones de las empresas vascas para 2022. Disponible en: https://www.confebask.eus/sites/default/files/2022-05/Necesidades%20Empleo%20y%20Cualificaciones%202022_0.pdf

40.STEAM Euskadi (2022). Disponible en: https://steam.eus/es/

41.STEAM Euskadi (2018). I Estrategia de Educación STEAM Euskadi. Disponible en: https://steam.eus/es/i-estrategia-de-educacion-steam-euskadi/

42.Euskadi (2023). Ikastetxe publikoen edo itunpeko pribatuen Lanbide Heziketako Eskaintza. Oferta de Formación Profesional en centros públicos o en privados concertados. Disponible en: https://www.euskadi.eus/contenidos/informacion/lheskaintza/es_def/adjuntos/PorCiclosOsoa_2023_2024ab.pdf

43.Politeknika Txorierri (2023). Ciberseguridad. Entornos ubicuos y móviles. Disponible en: https://politeknikatxorierri.eus/formacion/ciberseguridad-entornos-ubicuos-y-moviles/

44.Politeknika Txorierri (2023). Proyectos Internacionales sobre Ciberseguridad en Ámbitos Industriales. Disponible en: https://politeknikatxorierri.eus/proyecto-dicystech/

45.Tknika (2023). Cursos. Disponible en: https://tknika.eus/cursos/

46.EUNEIZ (2022). Grado en Ciberseguridad. Disponible en: https://www.euneiz.com/grados-universitarios/grado-ciberseguridad/

47.Boletín Oficial del Estado (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

48.Comisión Europea (2023). Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Disponible en: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

49.Indeed (2023). ¿Qué sueldo tiene un profesional de la ciberseguridad en España? Disponible en: https://es.indeed.com/orientacion-laboral/buscar-trabajo/sueldo-ingeniero-ciberseguridad-espana

50.Sifted - Financial Times (2023). Cybersecurity startups to watch, according to VCs. Disponible en: https://sifted.eu/articles/cybersecurity-startups-to-watch

51.INCIBE (2023). INCIBE Emprende. Disponible en: https://www.incibe.es/emprendimiento

52.Gobierno de España. Plan de Recuperación, Transformación y Resiliencia, y la Agenda Digital 2026. Disponible en: https://planderecuperacion.gob.es/

53.Gobierno Vasco (2023). Plan Interinstitucional de Emprendimiento de Euskadi - PIE 2024. Disponible en: https://www.spri.eus/archivos/2021/04/pdf/pie-2024_cas.pdf

54.Gipuzkoa (2023). BIC Gipuzkoa, motor del sistema de innovación. Disponible en: BIC Gipuzkoa, motor del sistema de innovación - gipuzkoa

55.BIC Bizkaia (2023). Disponible en: https://bicbizkaia.eus/

56.BIC Bizkaia Ezkerraldea (2023). Disponible en: https://bicezkerraldea.eus/

57.BIC Araba (2023). Disponible en: https://www.bicaraba.eus/en/

58.Gobierno Vasco (2023). BIND 4.0. Disponible en: https://bind40.com/

59.BIND 4.0. Basque Open Innovation Platform (2023). Startup Acceleration Program. Disponible en: https://bind40.com/open-innovation-acceleration-program/

60.BIND 4.0. Basque Open Innovation Platform (2023). BIND SME Connection. Disponible en: https://bind40.com/startup-sme-connection/

61.BIND 4.0. Basque Open Innovation Platform (2023). BIND GovTech. Disponible en: https://bind40.com/startup-govtech/

62.Gobierno Vasco (2023). UP!Euskadi. Disponible en: https://upeuskadi.spri.eus/es/aceleradoras-de-startups/

63.BAT B Accelerator Tower (2023). Disponible en: https://bacceleratortower.com/en/

64.Bizkaia BEAZ (2023). Beaz Acceleration Program. Disponible en: https://beazaccelerationprogram.eus/es/

65.Gobierno Vasco (2023). Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente. Disponible en: https://www.euskadi.eus/catalogo-ayudas-servicios-empresas-2023/web01-s2ekono/es/

66.Grupo SPRI (2023). Basque Tek Ventures. Disponible en: https://www.spri.eus/es/ayudas/basque-tek-ventures/

67.B-VENTURE (2023). ¿Qué es? Disponible en: https://www.b-venture.com/que-es/

68.Gobierno Vasco (2023). BRTA. Disponible en: https://www.brta.eus/en/home

69.Gobierno Vasco (2023). Basque Digital Innovation Hub. Disponible en: https://bdih.spri.eus/es/basque-digital-innovation-hub/

70.CS Cybersecurity Hub (2023). CS Hub mid-year market report 2022. Disponible en: https://www.cshub.com/executive-decisions/reports/cs-hub-mid-year-market-report-2022

71.Surfshark. Cybercrime statistics. Disponible en: https://surfshark.com/research/data-breach-impact/statistics

72.Hiscox (2022). El coste de los ciberataques se duplica en el último año para las empresas españolas. Disponible en: https://www.hiscox.es/el-coste-de-los-ciberataques-se-duplica-en-el-ultimo-ano-para-las-empresas-espanolas

73.Ministerio del Interior (2023). La tasa de criminalidad se sitúa en el 48,8 al cierre de 2022. Disponible en: https://www.interior.gob.es/opencms/en/detail-pages/article/La-tasa-de-criminalidad-se-situa-en-el-488-al-cierre-de-2022/

74. Ertzaintza (2023). Memoria Delincuencial 2022 de la Euskal Polizia. Disponible en: https://www.ertzaintza.euskadi.eus/lfr/documents/62347/7614212/Memoria_Delicuencial_2022_de_la_Euskal_Polizia.pdf/92da3d71-e776-368b-2726-777c8eb5c-00b?t=1679998701819

75. SPRI (2023). Estado de la ciberseguridad en Euskadi 1er trimestre 2022 Disponible en: https://www.ciberseguridad.eus/sites/default/files/2022-08/bcsc-estado-de-la-ciberseguridad-en-euskadi.pdf

76. SPRI (2023). Situación de la ciberseguridad en Euskadi 2º trimestre 2022. Disponible en: https://www.ciberseguridad.eus/sites/default/files/2022-09/BCSC_Informe-estado-2022.pdf

77. SPRI (2023). Situación de la ciberseguridad en Euskadi 3e trimestre 2022. Disponible en: https://www.ciberseguridad.eus/sites/default/files/2022-11/BCSC%20-%20Informe%20Estado%20Tercer%20Trimestre%20-%20Castellano%20v2.0.pdf

78. SPRI (2023). Estado de la ciberseguridad en Euskadi 4º trimestre 2022 Disponible en: https://www.ciberseguridad.eus/sites/default/files/2023-02/BCSC%20-%20Informe%20Estado%20Cuarto%20Trimestre%20-%20Castellano%20v2.pdf

79. Ertzaintza (2023). Infracciones penales conocidas por la Ertzaintza en la C.A.E. por tipos según territorio. Enero-Junio 2022-2023. Disponible en: https://www.ertzaintza.euskadi.eus/lfr/documents/62347/7803388/01+Delitos+por+territorios+23+06+c.jpg/b3eebd06-59ab-f736-ab36-2211124eb868?t=1691567777997

80. SonicWall (2023). Sonicwall cyber threat report. Tracking cybercriminals into the shadows. Disponible en: https://www.sonicwall.com/es-mx/2023-mid-year-cyber-threat-report/

81. Sealpath (2021). Predicciones en el ámbito de la Seguridad Centrada en los Datos para 2022. Disponible en: https://www.sealpath.com/es/blog/predicciones-seguridad-datos-2022/

82. CCN-CERT (2023). Ciberamenazas y tendencias - Edición 2023. Disponible en: https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7188-ccn-cert-ia-35-23-ciberamenazas-y-tendencias-edicion-2023/file.html

83. TÜV SÜD (2022). TÜV SÜD: Tendencias de ciberseguridad para 2023. Disponible en: https://www.tuvsud.com/es-es/noticias/2022/diciembre/tuev-sued-cybersecurity-trends-in-2023

84. IRSHAD (2023). Cyber Law: Addresing Legal Challenges in the Digital Age. Disponible en: https://irshadjournals.com/index.php/ujldp/article/view/92/86

85. Government Technology (2022). The Strengthening American Cybersecurity Act: What to know and how to comply. Disponible en: https://papers.govtech.com/The-Strengthening-American-Cybersecurity-Act-What-to-Know-and-How-to-Comply-141446.html#:~:text=Signed%20into%20law%20in%20March,hours%20of%20any%20data%20breach.

86. Congress.gov (2022). Strengthening American Cybersecurity Act of 2022. Disponible en: https://www.congress.gov/bill/117th-congress/senate-bill/3600/text

87. Boletín Oficial del Estado (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

88.Consejo de la Unión Europea (2022). Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (DORA). Disponible en: https://data.consilium.europa.eu/doc/document/ST-10581-2022-INIT/en/pdf

89.Comisión Europea (2022). Cyber Resilience Act. Disponible en: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

90.Comisión Europea (2023). Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Disponible en: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

91.Boletín Oficial del Estado (2004). Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2004-5051

92.Boletín Oficial del Estado (2023). Código de Derecho de la Ciberseguridad. Disponible en: https://www.boe.es/biblioteca_juridica/codigos/codigo.php?modo=2&id=173_Codigo_de_Derecho_de_la_Ciberseguridad

93.Boletín Oficial del Estado (2015). Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2015-10389

94.Boletín Oficial del Estado (2015). Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. Disponible en: https://www.boe.es/buscar/act.php?id=-BOE-A-2015-3442

95.Boletín Oficial del Estado (2002). Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

96.Boletín Oficial del Estado (2007). Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243

97.Boletín Oficial del Estado (1995). Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

98.Boletín Oficial del Estado (1883). Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036

99.Boletín Oficial del Estado (2022). Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2018-2257#:~:text=El%20presente%20real%20decreto%2D-ley,sistema%20de%20notificaci%C3%B3n%20de%20incidentes

100.Boletín Oficial del Estado (2021). Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información Disponible en: https://www.boe.es/diario_boe/txt.php?id=-BOE-A-2021-1192

101.Boletín Oficial del Estado (2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

102.Boletín Oficial del Estado (2022). Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

103.Boletín Oficial del Estado (2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

104.Boletín Oficial del Estado (2011). Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630

105.Boletín Oficial del Estado (2022). Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2022-4973

106.ITU (2020). Global Cybersecurity Index. Disponible en: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

107.ECSO (2020). Cybersecurity made in Europe. Disponible en: https://securitydelta.nl/images/2._LABEL-Terms-Conditions-of-Usage-v2.pdf

108.The European watch on cybersecurity & privacy. THE NEW CYBERSECURITY LABEL CREATING A CLEARER PATH TO BETTER CYBERSECURITY FOR EUROPEAN SMES. Disponible en: https://www.cyberwatching.eu/news-events/news/new-cybersecurity-label-creating-clearer-path-better-cybersecurity-european-smes

109.Cyber Security Agency Singapore (2022). Cybersecurity Labelling Scheme (CLS). Disponible en: https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls

110.ISASecure. Disponible en: https://www.isasecure.org/en-US/

111.ENX. TRUSTED INFORMATION SECURITY ASSESSMENT EXCHANGE. Disponible en: https://portal.enx.com/en-us/TISAX/

112.International Society of Automation. The World's Only Consensus-Based Automation and Control Systems Cybersecurity Standards. Disponible en: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

113.Euskadi (2023). Nace Cyberzaintza, la nueva Agencia Vasca de Ciberseguridad. Disponible en: https://www.euskadi.eus/gobierno-vasco/-/noticia/2023/nace-cyberzaintza-nueva-agencia-vasca-ciberseguridad/

114.Shubham Munde (2023). Industrial Cyber Security Market Research Report Information by Product (Gateway, Routers ans Ethernet Switches), By Solutions (Antivirus, Firewall, DDOS, Data Loss Prevention (DLP) and SCADA), By Organization Size (Large & SME's), By Industries (Manufacturing, Transportation, Poer Grid, Oil &Gas) And By Region (North America, Europe, Asia-Pacific, And Rest Of The World) – Market Forecast Till 2032. Disponible en: https://www.marketresearchfuture.com/reports/industrial-cyber-security-market-4408#author

115.Markets and markets (2023). Industrial Cybersecurity Market by Security Type (Network, Endpoint, Application, Cloud Wireless), Offering (Products and Services), End-user (Power, Utilities, Transportation, Chemicals & Manufacturing) and Region (2022-2027). Disponible en: https://www.marketsandmarkets.com/Market-Reports/industrial-cybersecurity-market-37646764.html?gclid=CjwKCAjwvJyjBhApEiwAWz2nLf-8b0AZ_-roGe14te-x3gpd38P55NgWkR2r1r-Ek1m5GN154yTeqDhoCm5AQAvD_BwE

116.INCIBE (2023). La seguridad industrial de 2022 en cifras. Disponible en: https://www.incibe.es/incibe-cert/blog/seguridad-industrial-2022-cifras

117.The International Society of Automation (ISA) (2023). Disponible en: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

118.Gobierno de España. Ministerio del Interior (2023). Guía sobre controles de seguridad en sistemas OT. Disponible en: https://www.ismsforum.es/ficheros/descargas/maqueta-guiaotv101621955967.pdf

119.Comisión Europea (2021) EDIH Catalogue. Disponible en: https://european-digital-innovation-hubs.ec.europa.eu/edih-catalogue

120.INCIBE (2023). Top predicciones en ciberseguridad industrial para el 2023. Disponible en: https://www.incibe.es/incibe-cert/blog/que-esperar-de-la-ciberseguridad-industrial-en-2023

121.EUR-Lex (2022). Commission delegated regulation (EU) 2022/30 of October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.007.01.0006.01.ENG

122.NIST (2023). NIST IR 8270. Introduction to Cybersecurity for Commercial Satellite Operations. Disponible en: https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8270.pdf

123.España Digital 2026 (2023). España Digital: una transformación digital humanista. Disponible en: https://espanadigital.gob.es/#:~:text=Espa%C3%B1a%20Digital%3A%20una%20transformaci%C3%B3n%20digital,alcanzando%20a%20todos%20los%20territorios ´

124.La Moncloa (2021). Plan de Recuperación, Transformación y resiliencia. Disponible en: 30042021-Plan_Recuperacion_ Transformacion_ Resiliencia.pdf (lamoncloa.gob.es)

125.INCIBE (2023). España Digital 2026. Disponible en: https://www.incibe.es/ed2026

126.INCIBE (2023). Redes Territoriales de Especialización Tecnológica (RETECH). Disponible en: https://www.incibe.es/retech

127.Gobierno de España. Plan de Recuperación, Transformación y Resiliencia de España (2023). Conoce el programa RETECH: Redes Territoriales de Especialización Tecnológica. Disponible en: Conoce el programa RETECH: Redes Territoriales de Especialización Tecnológica | Plan de Recuperación, Transformación y Resiliencia Gobierno de España. (planderecuperacion.gob.es)

128.Ministerio de Industria, Comercio y Turismo (2021). ACTIVA Ciberseguridad. Disponible en: Industria Conectada 4.0 - ACTIVA Ciberseguridad (industriaconectada40.gob.es)

129.Ministerio de Asuntos Económicos y Transformación Digital (2021). El Gobierno lanza el programa Kit Digital para invertir más de 3.000 millones de euros en la digitalización de las pymes y autónomos. Disponible en: 211125_np_kit.pdf (mineco.gob.es)

130.Euskadi (2023). PCTI 2030. Plan de Ciencia, Tecnología e Innovación Euskadi 2030. Disponible en: https://www.euskadi.eus/pcti-2030/web01-a2pcti30/es/#:~:text=El%20Plan%20de%20Ciencia%2C%20Tecnolog%C3%ADa,y%20la%20calidad%20del%20empleo.

131.Grupo SPRI (2021). Estrategia para la transformación digital de Euskadi 2025. Disponible en: https://www.spri.eus/es/teics-comunicacion/estrategia-para-la-transformacion-digital-de-euskadi-2025/

132.Grupo SPRI (2022). Basque Industry 4.0. Disponible en: https://www.spri.eus/es/ayudas/basque-industry-4-0/

133.Grupo SPRI (2022). El Gobierno vasco ofrece 3,5 millones para ayudas en ciberseguridad industrial. Disponible en: https://www.spri.eus/es/ciberseguridad/el-gobierno-vasco-ofrece-35-millones-para-ayudas-en-ciberseguridad-industrial/

134.Diputación Foral de Gipuzkoa(2022). Gipuzkoa Digitala - producto 4.0. Disponible en: Gipuzkoa Digitala - producto 4.0 - Sede - Sede

135.Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente (2023) Catálogo de Ayudas y Servicios a las empresas para el año 2023. Disponible en: https://www.euskadi.eus/catalogo-ayudas-servicios-empresas-2023/web01-s2ekono/es/

136.SPRI (2023). Smart Industry 2023. Impulsamos la transferencia tecnológica desde agentes I+D hacia empresas industriales. Disponible en: https://www.spri.eus/es/ayudas/smart-industry/

137.SPRI (2023). Ciberseguridad Industrial 2023. El futuro de la Industria requiere unas empresas seguras. Disponible en: https://www.spri.eus/es/ayudas/ciberseguridad-industrial/

138.Diputación Foral de Gipuzkoa (2023). Programa GIPUZKOA DIGITALA: CIBERSEGURIDAD. Disponible en: https://www.gipuzkoa.eus/es/web/ekonomia/programas-y-ayudas/proyectos-estrategicos/zibersegurtasuna

139.Bizkaia Foru Aldundia Diputación Foral (2023). Programa Transición Digital y Verde. Disponible en: https://www.bizkaia.eus/es/tema-detalle/-/edukia/dt/11909

140.Diputación Foral de Álava (2023). Álava Innova – Digitaliza. Disponible en: https://egoitza.araba.eus/es/-/alava-innova

141.National Institute of Standards and Technology (2018). Framework for Improving Critical Infrastructure Cybersecurity. Disponible en: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

142.European Cyber Security Organisation (2023). Membership. Disponible en: https://ecs-org.eu/membership/

Anexos

Grupo Spri,
Agencia vasca de
Desarrollo empresarial

spri.eus

GRUPO spri TALDEA

EUSKO JAURLARITZA
GOBIERNO VASCO

EKONOMIAREN GARAPEN, JASANGARRITASUN ETA INGURUMEN SAILA

DEPARTAMENTO DE DESARROLLO ECONÓMICO, SOSTENIBILIDAD Y MEDIO AMBIENTE