

Euskadi digital segura: Un ecosistema referente en Europa



Libro Blanco de la Ciberseguridad en Euskadi

3ª edición 2024



Índice

01 *El Libro Blanco de la ciberseguridad en Euskadi*

02 *Metodología*

03 *Contextualización del sector*

- ✓ *Valor de Mercado*
- ✓ *Inversión*
- ✓ *Emprendimiento*
- ✓ *Empleo y Educación*
- ✓ *Entorno Regulatorio*

04 *Ciberseguridad Industrial*

05 *Ecosistema de Ciberseguridad en Euskadi*

El Libro Blanco de la Ciberseguridad en Euskadi

¿Qué es el Libro Blanco?

Objetivo principal:

- **Situación** del Sector de la Ciberseguridad (Internacional, nacional y Euskadi).
- **Identificar, clasificar y presentar** todos aquellos agentes que ofrecen productos o servicios de ciberseguridad en Euskadi.

¿A quién va dirigido?

- Empresas
- Instituciones Públicas
- Profesionales del Sector
- Estudiantes / Futuros profesionales

Fases:

- **Fase I: Elaboración del documento de Libro Blanco** de ciberseguridad en Euskadi y desarrollo del observatorio interactivo.
- **Fase II: Revisión y actualización** de datos, con la incorporación de nuevos agentes.

Áreas de estudio / Apartados

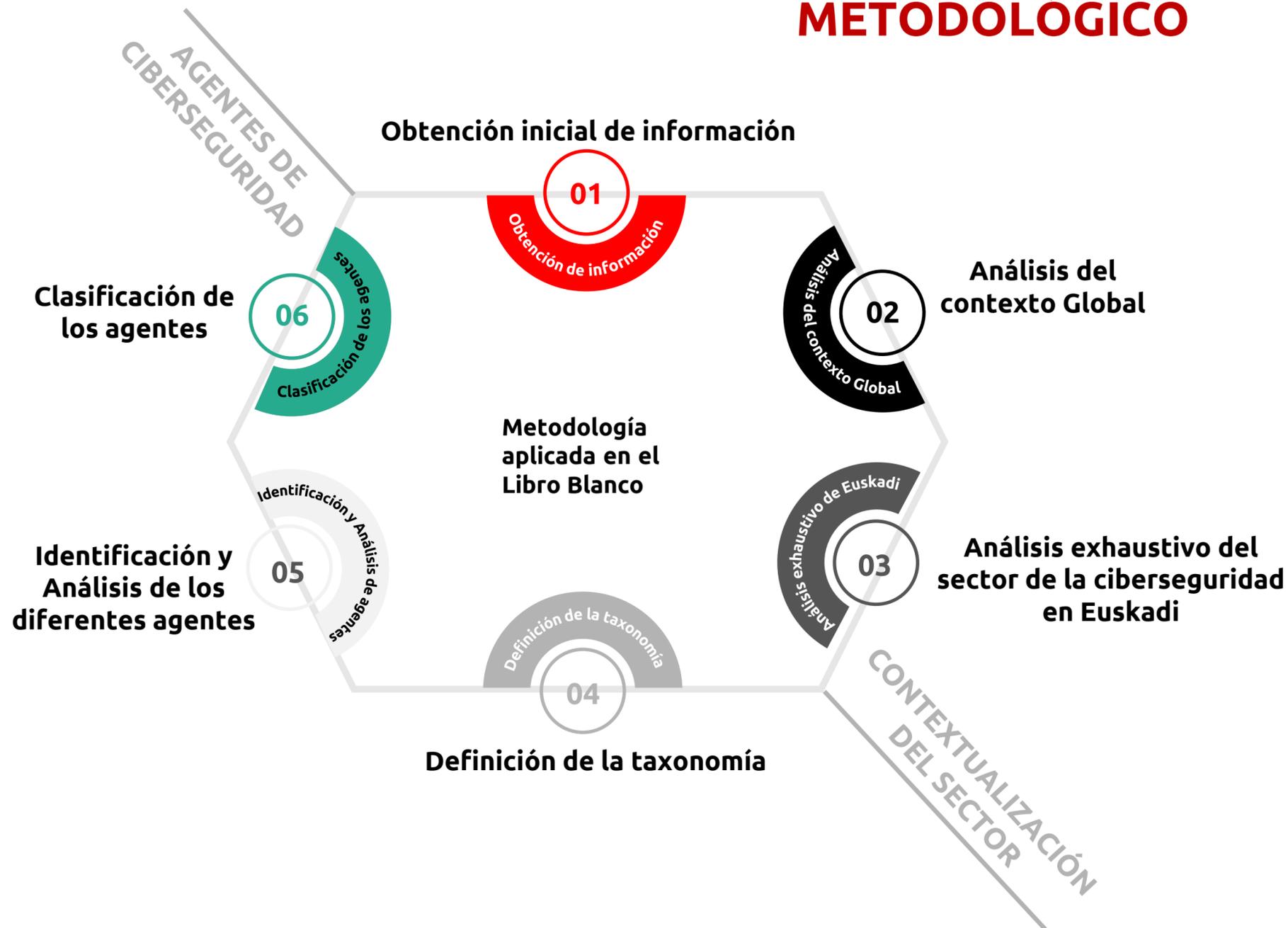
- Contextualización del sector (9):
 - Valor de mercado.
 - Inversión.
 - Empleo y educación.
 - Emprendimiento.
 - Cibercrimen.
 - Tendencias .
 - Entorno regulatorio.
 - Sellos de ciberseguridad.
 - Agencias de ciberseguridad.
- Ciberseguridad Industrial.
- Instrumentos de apoyo.
- Ecosistema de Ciberseguridad de Euskadi:
 - Agentes del mercado.
 - Emprendimiento.
 - Red Vasca de Ciencia y Tecnología.
 - Red de Centros de Educación.
 - Administraciones Públicas.



El documento estará disponible en spri.eus

Metodología

ENFOQUE METODOLÓGICO

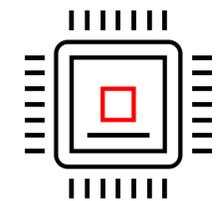


CATEGORIZACIÓN

Agentes



Productos o Servicios



Contacto con agentes



Formulario



Contacto telefónico



Contacto vía correo electrónico



Metodología – Categorización Agentes (Naturaleza)

Se ha llevado a cabo la categorización de los agentes en **función de su naturaleza** tomando como referencia el **modelo de clasificación propuesto por European Cyber Security Organisation (ECSO)**.



Administración Pública. Agentes formados para realizar las tareas de administrar y gestionar organismos, instituciones y entes del Estado.



Asociaciones. Agrupación de personas que desarrollan una actividad colectiva de forma estable, democrática y sin ánimo de lucro.



Centro de formación. Aquellos que siendo públicos o privados tengan como principal objetivo la impartición de formación de carácter no oficial.



Centro de Formación Profesional. centros educativos autorizados que imparten formación conducente para la obtención de títulos de Formación Profesional o Certificados de Profesionalidad.



RVCTI. Entidades de investigación, desarrollo e innovación que, trabajando en red, desarrollan un conjunto de actividades de I+D+i equilibrado.



Universidad. Institución destinada a la enseñanza superior, constituida por varias facultades y que concede los grados y másteres académicos correspondientes.



Fabricante. Proveedores que fabrican o desarrollan sus propias soluciones de ciberseguridad (hardware o software).



Integrador/Consultor. 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.



Distribuidor/Mayorista. Proveedores que adquieren grandes cantidades, o volúmenes de licencias, de soluciones de seguridad de diversos fabricantes, comercializándolas al por mayor.

Metodología – Categorización Productos/Servicios



La categorización de los productos y servicios existentes en Euskadi está **basada en el Framework for Improving Critical Infrastructure Cybersecurity** desarrollado por el National Institute of Standards and Technology (**NIST**)

MARCO DE CIBERSEGURIDAD DE NIST



Fuente: NIST Cybersecurity Framework (CSF)



CAPACIDAD	CATEGORÍA	GRUPO DE PRODUCTO / SERVICIO
IDENTIFICAR	Gestión de activos	Gestión del ciclo de vida de la seguridad y el software
		Gestión de servicios TI
	Entorno del negocio	Análisis de impacto en el negocio
	Gobernanza y gestión del riesgo	Certificación de seguridad
		Cumplimiento legal
Análisis del riesgo	Cumplimiento, riesgo y gobernanza	
		Herramientas de gestión de riesgos
		Análisis de riesgos

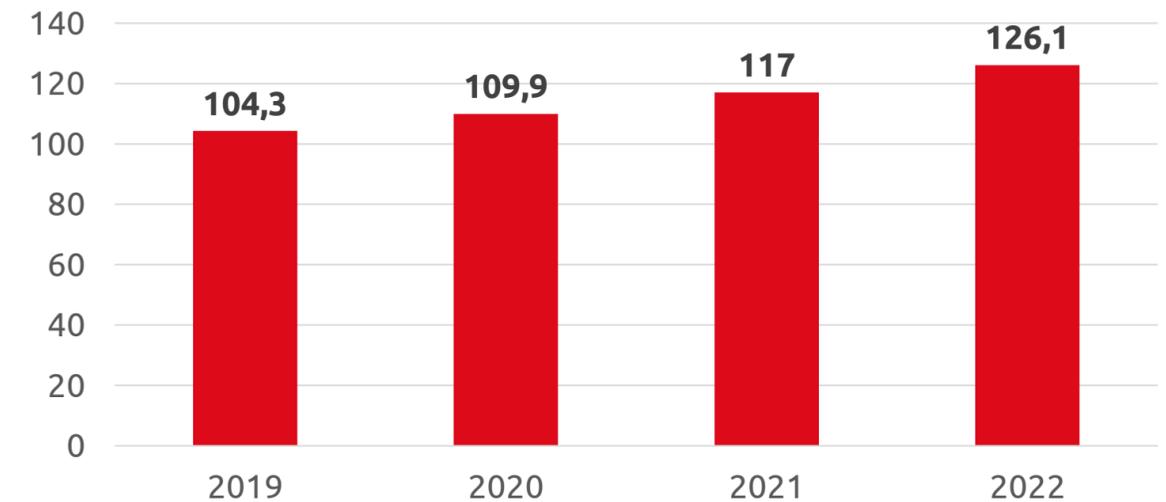
Fuente: Elaboración Propia

Contextualización del sector – Valor de mercado

El valor de mercado de la ciberseguridad se encuentra en **aumento a nivel global** en los últimos años.

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.

Valor mundial de la ciberseguridad en mil millones de \$

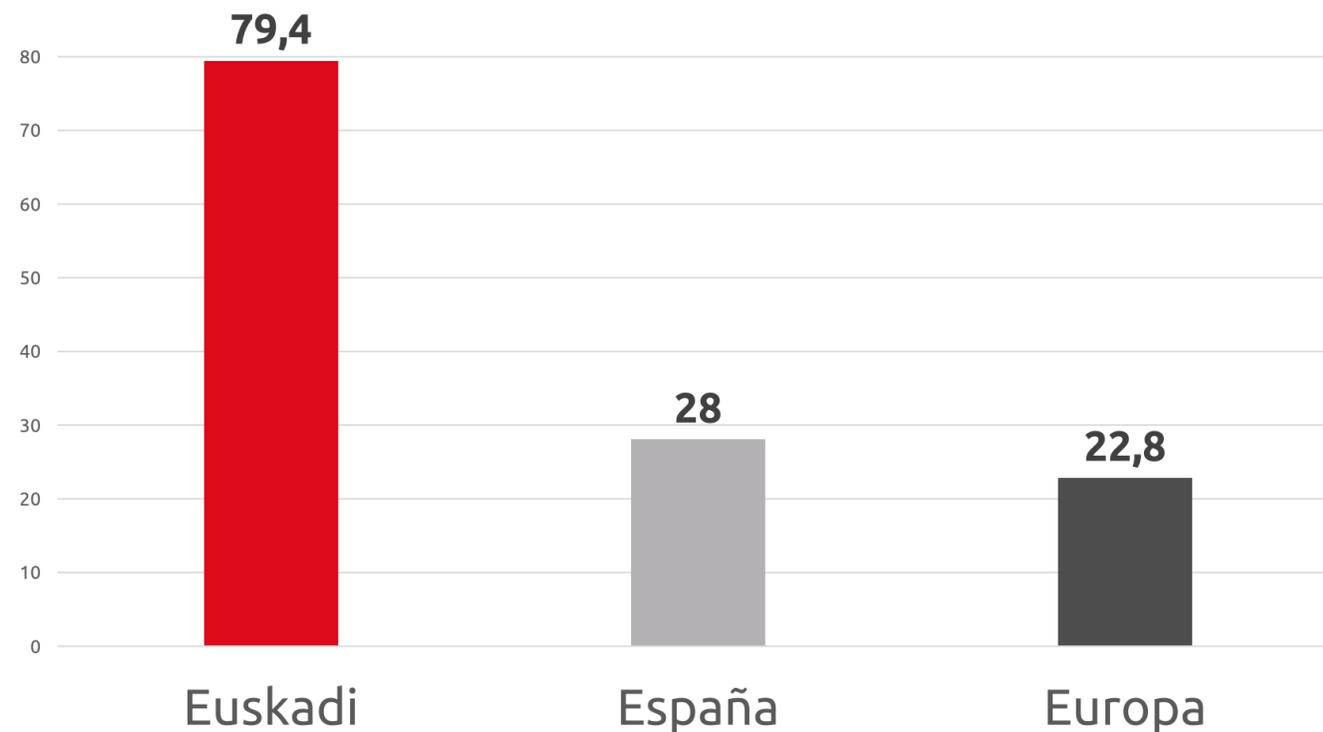


Fuente: Mordor Intelligence

Euskadi cuenta con una **destacada concentración de empresas especializadas en ciberseguridad**, sobrepasando significativamente el número de compañías por cada millón de habitantes en comparación tanto con España como Europa.

El número de empresas de ciberseguridad por millón de habitantes en Euskadi es de 79 frente a las 28 y 22 de España y Europa respectivamente.

Número de empresas de ciberseguridad por millón de habitantes



Fuente: European Cybersecurity Investment Platform

Contextualización del sector – 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.



Euskadi se presenta como **un territorio atractivo para la inversión en ciberseguridad**

- **Marco fiscal favorable** en Euskadi.
- **Entorno colaborativo fuerte y comprometido** con el **sector TEIC** en Euskadi que facilita la creación de empresas de ciberseguridad en el territorio. Algunas iniciativas: **Cybasque**, Robotekin, BcCAM, ADI, etc.
- Territorio con gran potencia en **innovación tecnológica e I+D**.
- **Red de Centros de Educación potente** en Euskadi con tendencia a especialización en el ámbito de la ciberseguridad.
- Apoyo **Institucional** diferencial.



Este escenario ha favorecido a la **atracción y a un incremento** en cuanto a la presencia de **agentes inversores en el territorio**.

Dos entidades referentes de inversión **pública**:



Inversión de naturaleza **privada**: VC y Private-Equity



Corporate Venturing, Empresas del sector, etc.



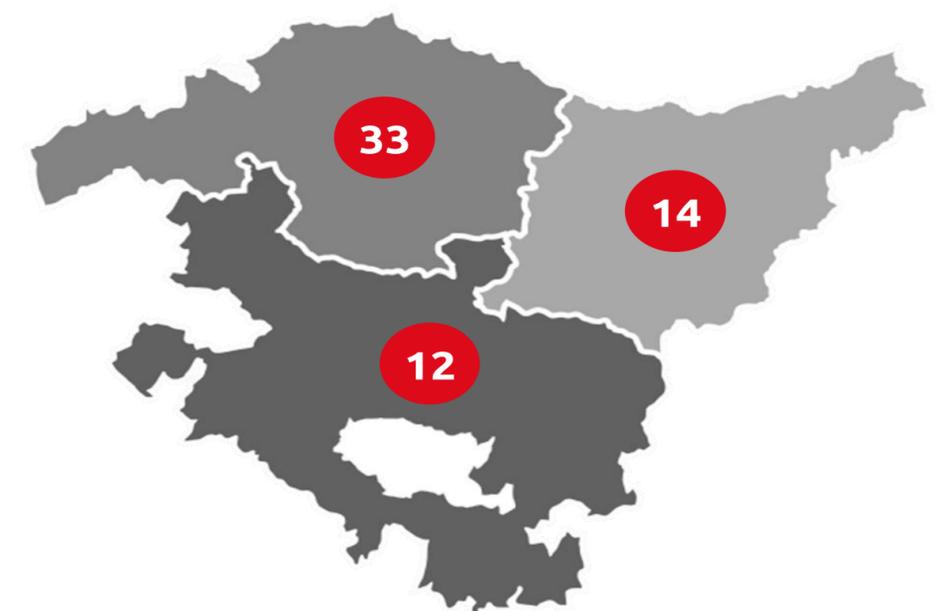
Contextualización del sector – Emprendimiento

En Euskadi, desde las diferentes instituciones públicas se ofrecen diversos programas y estrategias de apoyo al emprendimiento: **PIE 2023; BICs; BIND; Basque TEK Ventures, Up!Euskadi; BAT; Beaz Acceleration Program.**

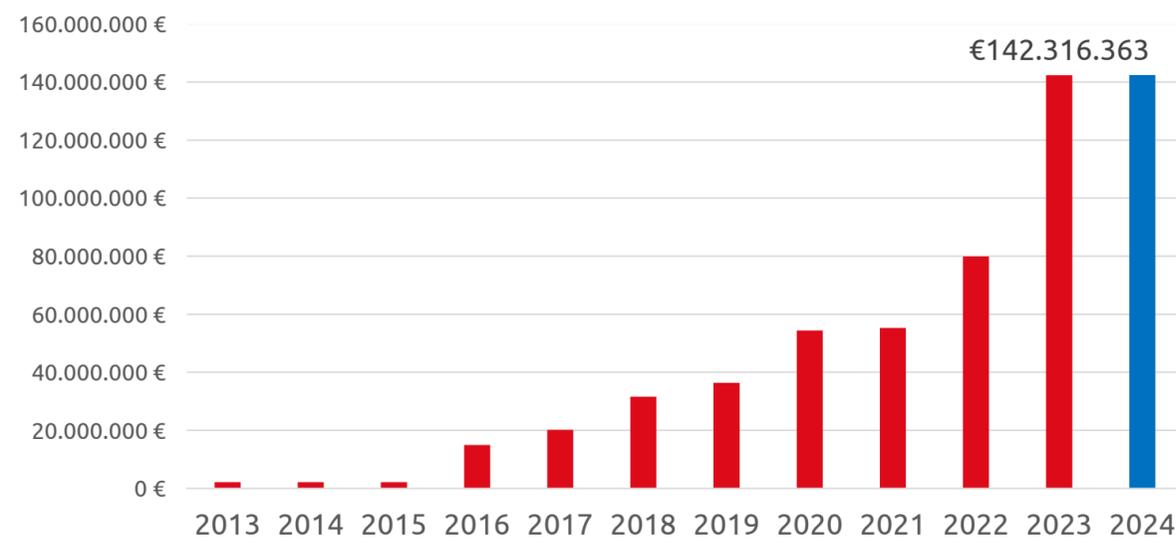
- La **actividad emprendedora** en Euskadi en materia de **ciberseguridad** destaca como **una de las más prominentes** a nivel estatal.
- Creación de un importante número de **startups** de ciberseguridad en Euskadi en los últimos tiempos, siendo **notable la presencia de aquellas que desarrollan su propia tecnología.**



Distribución de las startups de Euskadi



Valor de las startups en Euskadi



Fuente: UPIEuskadi

59 startups identificadas

Up!Euskadi
BASQUE COUNTRY

Fuente: Elaboración Propia.

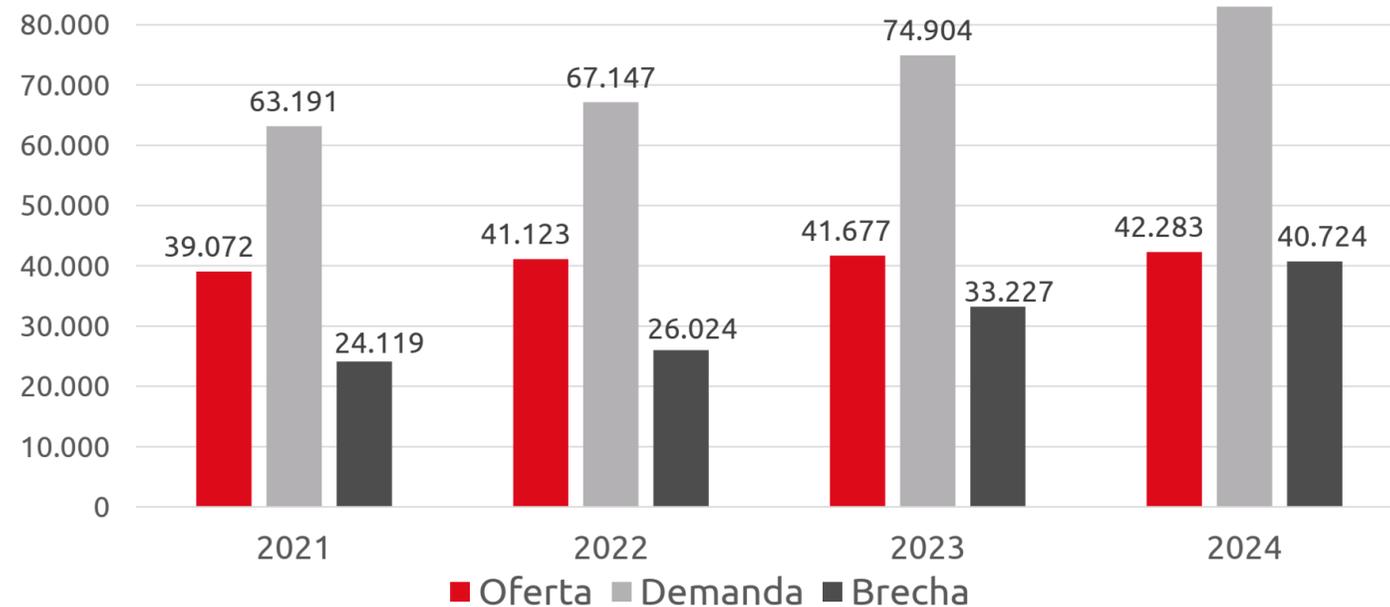
Contextualización del sector – Empleo y educación

Brecha de talento en la región de Euskadi.



Diferentes estrategias y mecanismos para combatir esta brecha.

Proyección de empleo en España



Fuente: ObservaCIBER

i) Red de Centros de Educación de Euskadi

Compromiso por parte de las Universidades y centros FP:
Adaptar, mejorar e incluir nueva oferta educativa en ciberseguridad.

EUNEIZ



5 Universidades.

15 Centros de Formación Profesional.

- 2 grados superiores.
- Cursos profesionales.
- Cybe-Range.
- Proyectos Internacionales.



ii) Ámbito Empresarial

Upskilling. Nuevas habilidades y competencias.
Reskilling. Reciclaje/Reorientación profesional.



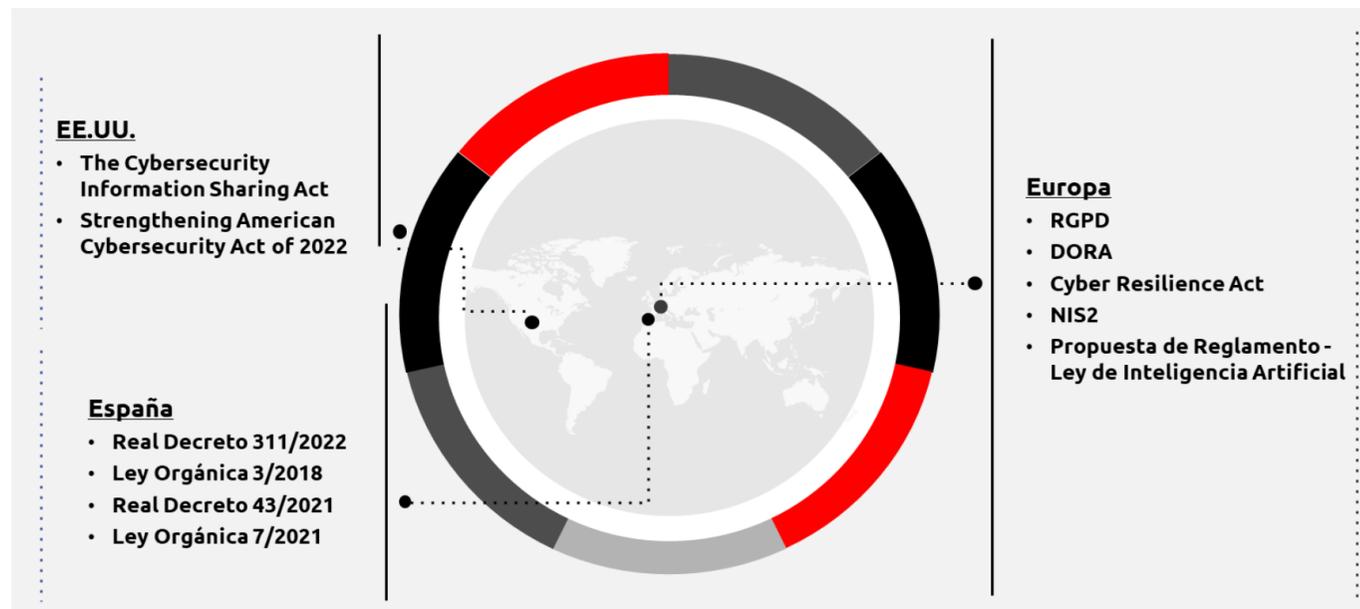
Atracción de Talento.



Contextualización del sector – Entorno Regulatorio

Contexto Global

Nuevas Leyes y Normativas de Ciberseguridad.



Fuente: Elaboración Propia

Certificación: Normas y Estándares de ciberseguridad.



Impacto

Desafíos y Oportunidades para las Empresas de Euskadi.

Tejido Empresarial de Euskadi

- ✓ Adaptaciones en poco tiempo.
- ✓ Establecer nuevas políticas y procedimientos.
- ✓ Inversiones en tecnología.
- ✓ Dedicación de recursos.
- ✓ Capacitación y Formación.



Agentes del Ecosistema de Ciberseguridad

- ✓ Mayor demanda productos y servicios.
- ✓ Necesidad de nuevos productos o servicios.
- ✓ Nuevas líneas de negocio / Diversificación.
- ✓ Nuevas empresas emergentes.



Ciberseguridad Industrial

Ámbito Industrial:

- La ciberseguridad en la industria cada vez algo más crítico, debido al **aumento de ataques cibernéticos** dirigidos a **sistemas de control industrial (ICS) y tecnologías operativas (OT)**.
- El **incremento de las vulnerabilidades y de los ataques** en el ámbito industrial ha motivado a las empresas a **dedicar recursos a la implementación de soluciones de ciberseguridad**.
- **Aumento** significativo del **mercado** y poco a poco a una **mejora o incremento de la ciberseguridad** de nuestra industria.

Desafíos:

- Falta de **conciencia y Capacitación**.
- **Recursos** limitados (Humanos y Económicos).
- **Falta de políticas y procedimientos** de seguridad.
- Vulnerabilidades en el **ámbito operacional (OT)**.
- **Actualizaciones y parches** de seguridad.
- **Regulaciones y cumplimiento**, necesidad de adaptación a las nuevas normas.

¿Cómo afronta Euskadi este escenario?

- Desde una **posición privilegiada**.

Todos los ingredientes:



- Ecosistema **tecnológico** potente (Activos tecnológicos y talento).
- **Madurez digital** del sector industrial.
- Mecanismos para el **desarrollo y atracción** de nuevos profesionales.
- **Ecosistema de ciberseguridad** potente (abundante, diverso, equilibrado y especializado).
- Apoyo **institucional** diferencial.

Programa de ayudas de Ciberseguridad Industrial

6 Convocatorias	1.700 Proyectos presentados	1.610 Proyectos aprobados	1.018 Empresas apoyadas
32.5 M€ Inversión / Gasto			
13.6 M€ Subvención concedida	8.450 € Subvención media	>155 Proveedores	

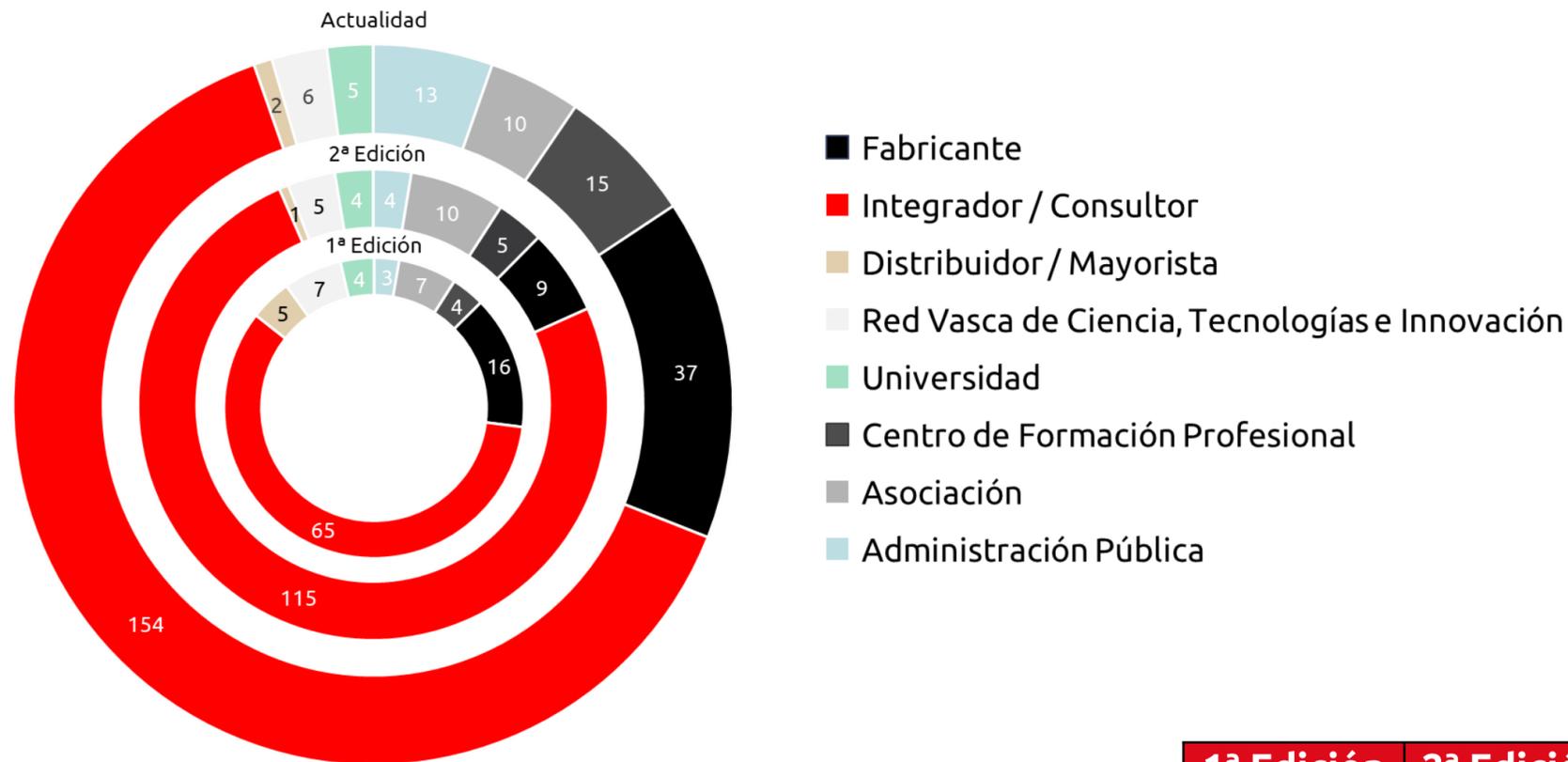
Ciberseguridad Industrial

basque
digital
innovation
hub



Ecosistema de ciberseguridad en Euskadi

Tras la segunda edición publicada en 2020, desde SPRI se publica una **tercera edición** en la que han sido catalogados **242 agentes, con 193 empresas privadas, de las cuales 59 son startups**, frente a las 125 empresas y 29 startups de la 2ª edición.



Fuente: elaboración propia



Fuente: elaboración propia

	1ª Edición (2018)	2ª Edición (2020)	Actualidad (2024)
Total	111	153	242

Fuente: elaboración propia

Informe Caracterización del Sector de la Ciberseguridad en Euskadi



Índice

01 *Metodología*

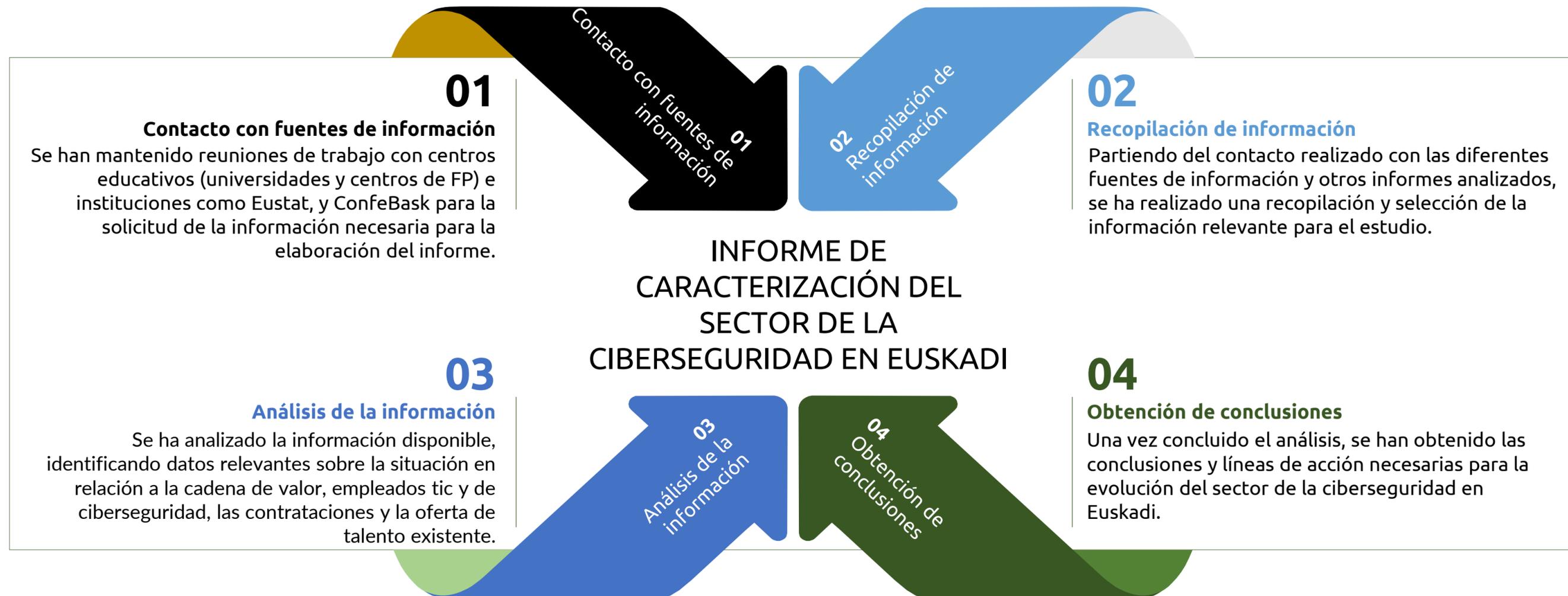
02 *Cadena del sector*

03 *Perspectiva y necesidades de profesionales*

- ✓ *Empleados TIC*
- ✓ *Contrataciones*
- ✓ *Oferta de talento*

04 *Conclusiones*

Metodología



Cadena de Valor del Sector

El ecosistema de ciberseguridad de Euskadi está compuesto principalmente por 4 protagonistas que componen la cadena de valor: La **Fabricación**, la **Distribución**, los **Servicios** y los **Clientes**.

Las **universidades** y los **centros de investigación** son elementos fundamentales por su impulso y por su labor de innovación. Asimismo, la **formación** y la **certificación** también cobran especial relevancia a lo largo de toda la cadena de valor del sector.

La mayoría de entidades se concentran en la prestación de servicios (Integrador/Consultor) lo que revela una **cadena de valor descompensada**.

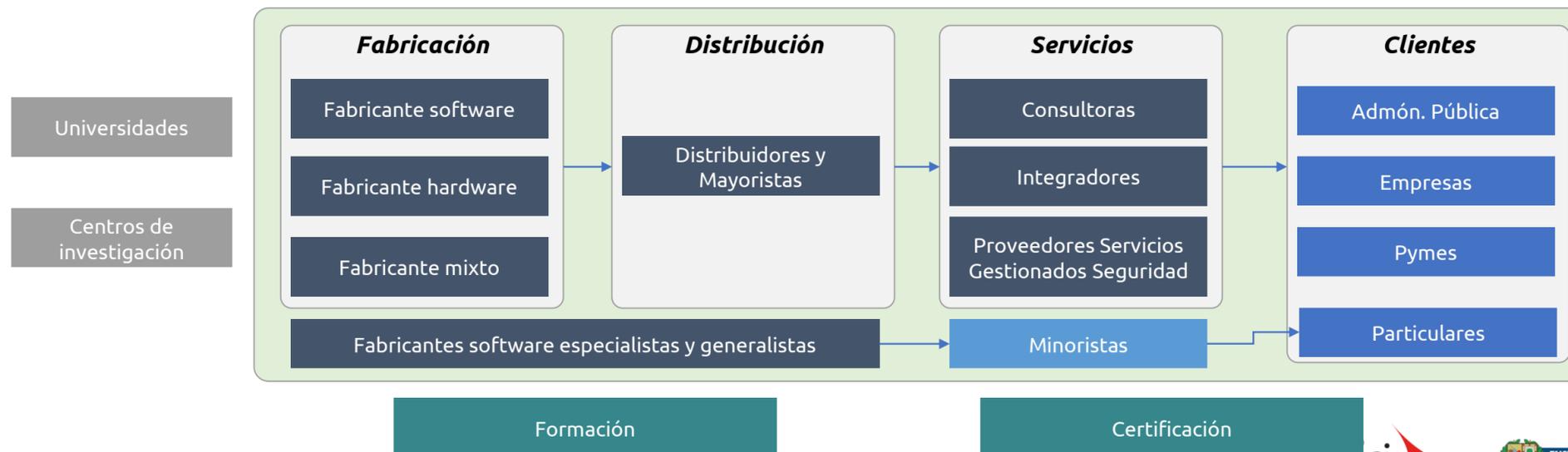


Tipos de agentes de ciberseguridad en Euskadi



Entidad	2018	2020	2023
Administración Pública	3	4	13
Asociación	7	10	10
Centro de Formación Profesional	4	5	15
Distribuidor/ Mayorista	5	1	2
Fabricante	16	9	37
Integrador/Consultor	65	115	154
Red Vasca de Ciencia, Tecnologías e Innovación	7	5	6
Universidad	4	4	5

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



Cadena de valor del sector de la ciberseguridad. Fuente: Elaboración propia

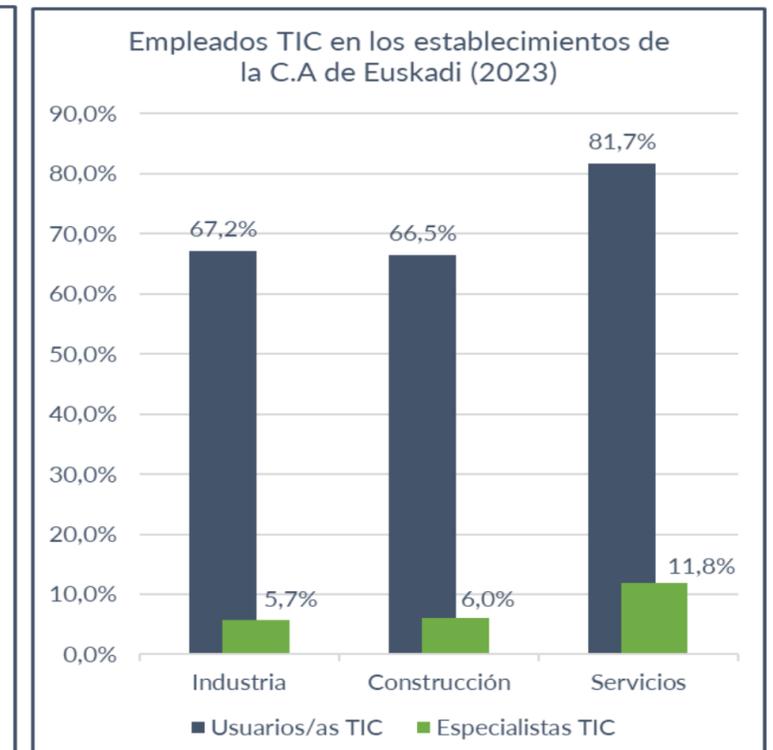
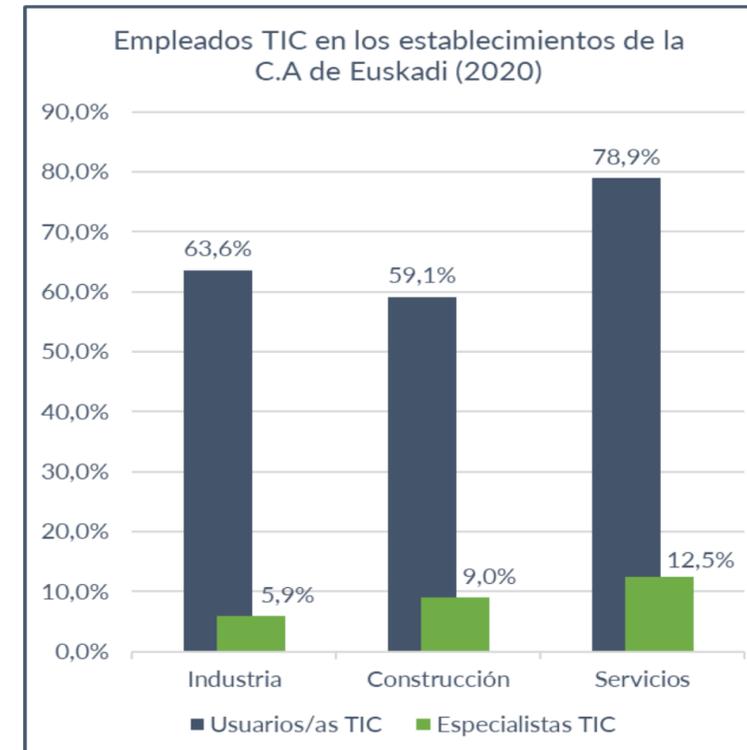
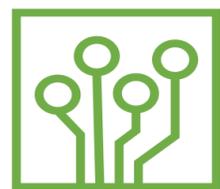


Empleados TIC y Ciberseguridad

Se debe poner el foco en la **escasez de expertos digitales avanzados**, ya que dificulta las perspectivas de crecimiento de la región.

En 2023 casi el 80% de las personas empleadas de **Euskadi** utilizaba sistemas TIC y se constata que **solo el 10,2% era personal especialista en TIC**.

Este desajuste entre el desarrollo de los profesionales del sector y el rápido avance de las nuevas tecnologías representa un desafío significativo para el territorio, en el que será necesario que las diferentes organizaciones del territorio promuevan acciones para reforzar el ecosistema de ciberseguridad de Euskadi.



Empleados TIC en los establecimientos de Euskadi. Fuente: Eustat

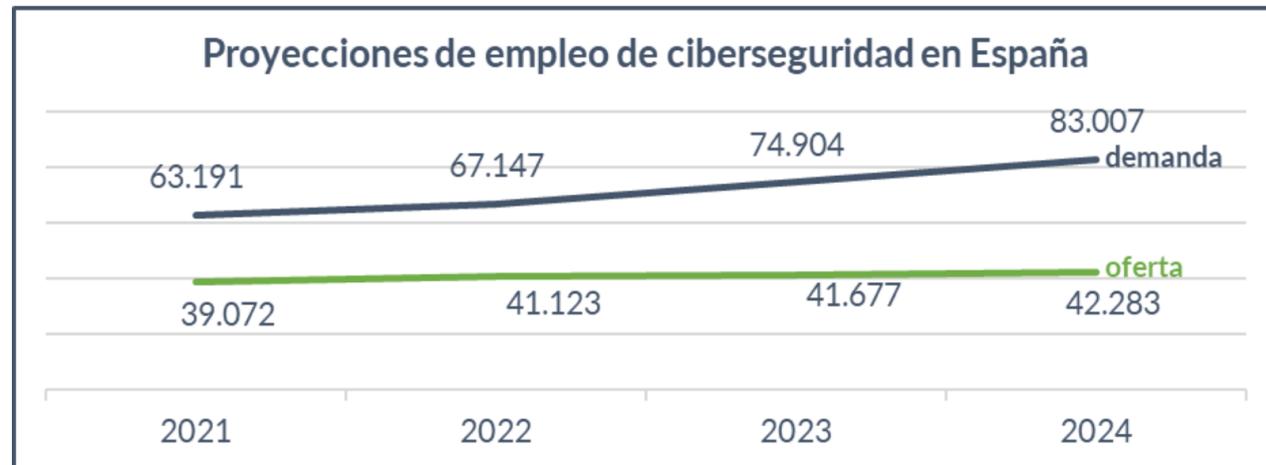
Mientras el número de usuarios TIC aumenta en las organizaciones de Euskadi, el porcentaje de especialistas se reduce.

Contrataciones

Según las previsiones de contrataciones para los próximos años en el sector privado de Euskadi, la demanda de **perfiles de educación superior** predomina sobre el resto de los perfiles.

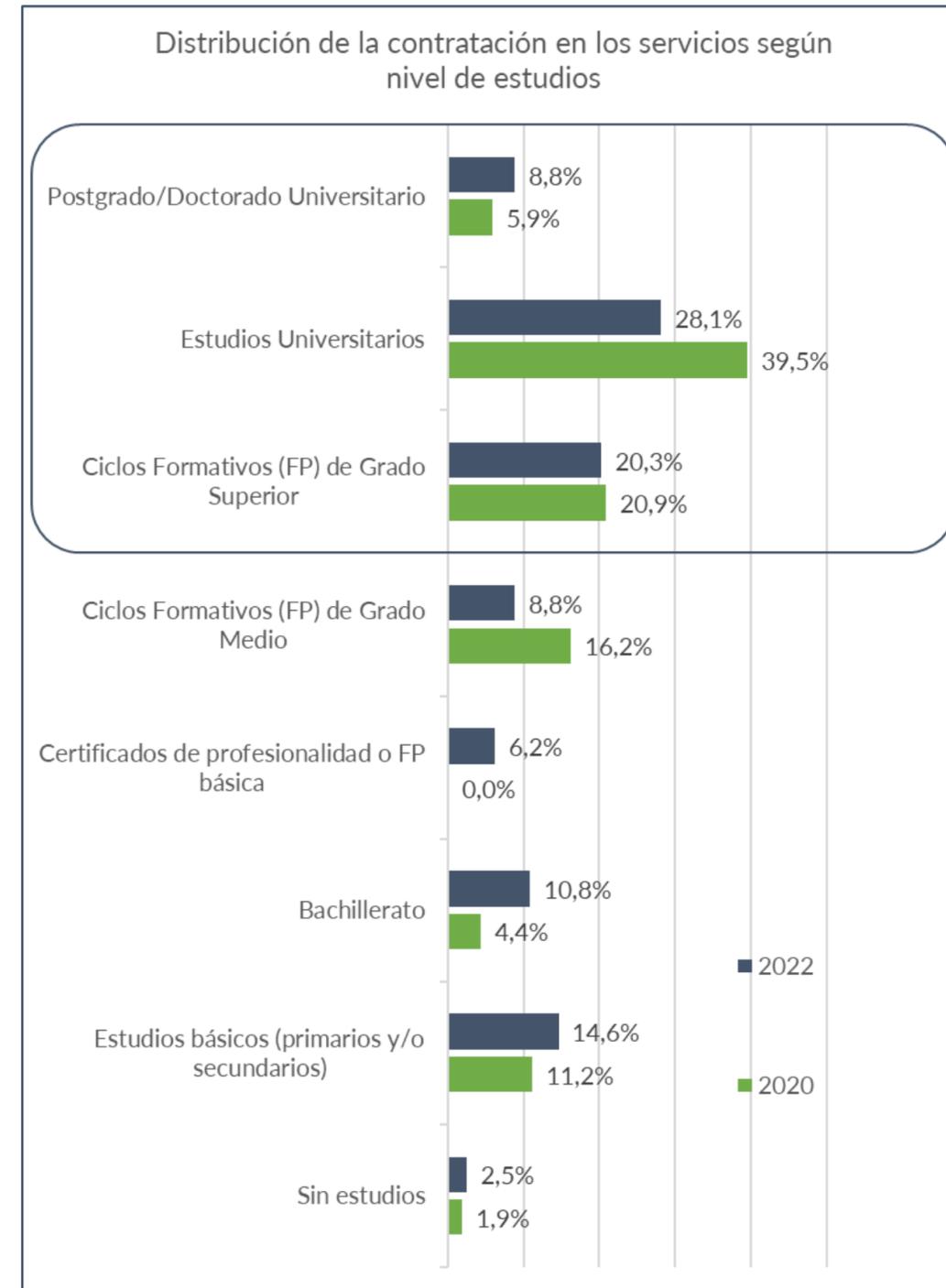
Los estudios dentro del ámbito de la **informática** son los más demandados en Euskadi tanto en grados universitarios como en grados de Formación Profesional.

Se prevé que continúe la brecha de talento en ciberseguridad en Euskadi.



Proyecciones de empleo de ciberseguridad en España. Fuente: ObservaCIBER

Para poder paliar esta brecha, se están promoviendo diversas acciones como la estrategia STEAM Euskadi y el impulso de nuevos grados superiores, grados universitarios y estudios de master en materia de ciberseguridad.



Distribución de la contratación según nivel de estudios. Fuente: ConfeBask

Oferta de Talento

Se busca un sector con **profesionales cualificados y expertos en la materia.**

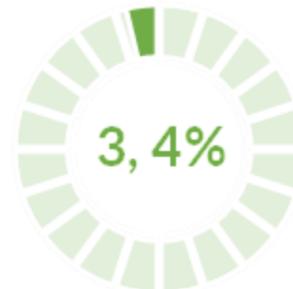
Es importante no solo tener en cuenta la oferta de nuevo talento, sino la **formación y certificación** de los mismos en ciberseguridad.

9.689

Alumnos universitarios graduados en 2021/21 en Euskadi



Egresados en Ingeniería

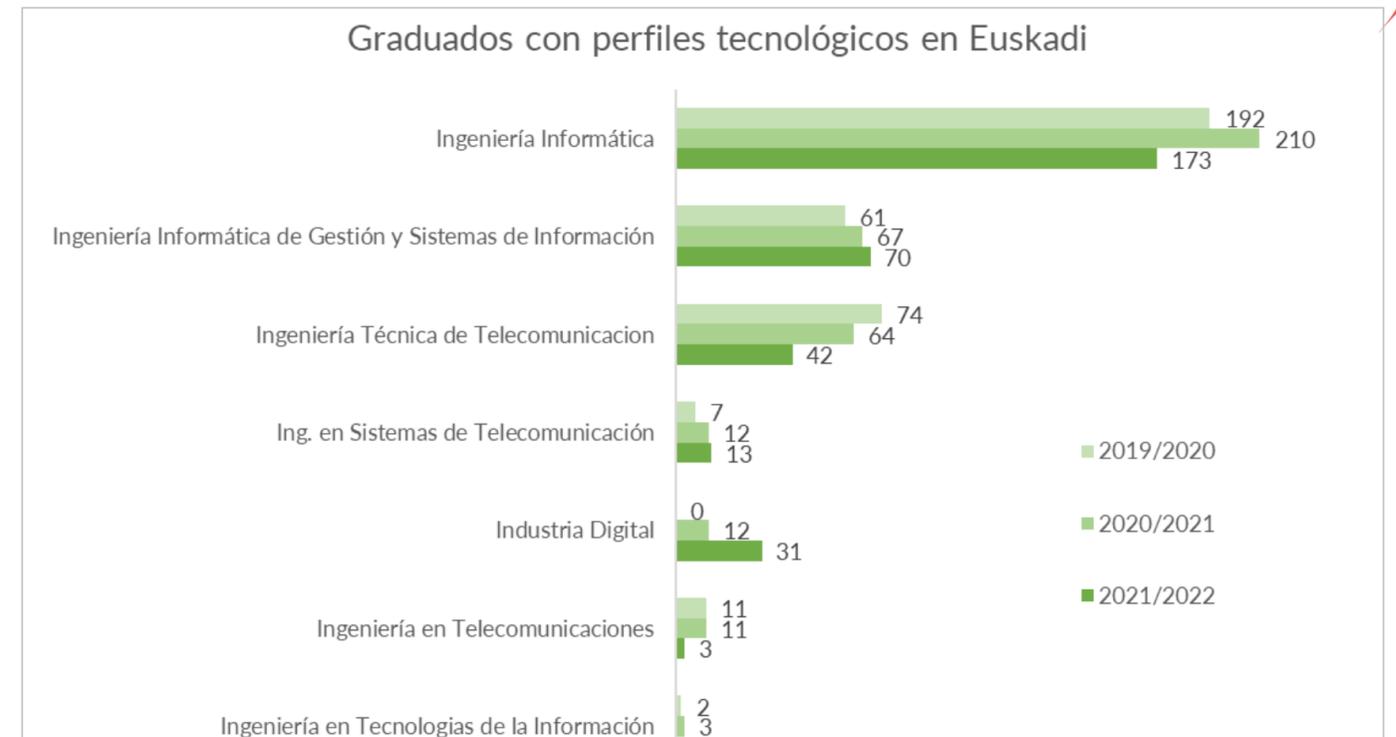


Graduados con perfiles tecnológicos en Euskadi

Egresados universitarios en Euskadi. Fuente: Eustat



Matriculados FP. Fuente: Eustat.



Graduados con perfiles tecnológicos en Euskadi. Fuente: Eustat

Adicionalmente, se pueden encontrar perfiles que encajen en grados como Matemáticas, con 72 graduados tanto en 2019/20 como en 2020/21 y 77 en 2021/22. Derecho cuenta con 621 graduados en 2019/20 y 611 en 2020/21 y 576 en 2021/22, donde aplicarían aquellos estudiantes que se forman en estudios del ámbito de la privacidad y ciberseguridad.



Conclusiones & Perspectivas Futuras



Conclusiones y Perspectivas Futuras



Conclusiones

Perspectivas Futuras

Ecosistema

Ecosistema Abundante, Diverso, Equilibrado y Especializado

- ✓ **Abundante.** Gran concentración de empresas en el territorio.
- ✓ **Diverso.** Agentes, así como productos y servicios de diferente tipología.
- ✓ **Equilibrado.** Presencia significativa y equilibrada de agentes en todas las categorías definidas (cadena de valor).
- ✓ **Especializado.** Tendencia hacia nichos de especialización (Robótica, IoT, Cumplimiento Normativo, Cloud, ICS, etc).

Punto de Estabilización y Especialización del sector

- ✓ Es posible que las empresas **no experimenten un aumento** significativo en número.
- ✓ Destacarán por un notable **incremento en su grado de especialización y valor añadido.** Vectores de Especialización: Vehículo Conectado, Computación Cuántica, 5G, etc.
- ✓ Compromiso **para mantener el equilibrio** en cuanto a agentes en el ecosistema.

Talento

Brecha Creciente + Herramientas

- ✓ La brecha entre la **demanda y oferta** de profesionales en el sector **sigue creciendo.**
- ✓ Las empresas buscan profesionales cualificados con perfiles **experimentados y certificaciones.**
- ✓ **Mecanismos** para combatirla (Ámbito Educativo y Empresarial).
- ✓ Necesidad de **Sensibilizar y Concienciar**
- ✓ **Riesgo de Pérdida** de talento.

Escenario Esperanzador

- ✓ **Tendencia alcista** en la región en cuanto a **salarios** se refiere (Factor de Competitividad).
- ✓ Adicionalmente, se pueden encontrar perfiles que encajen en **grados como Matemáticas**, con 72 graduados tanto en 2019/20 como en 2020/21 y 77 en 2021/22. **Derecho** cuenta con 621 graduados en 2019/20 y 611 en 2020/21 y 576 en 2021/22, donde aplicarían aquellos estudiantes que se forman en estudios del ámbito de la privacidad y ciberseguridad.

Conclusiones y Perspectivas Futuras



Conclusiones

Ciberseguridad como prioridad en la Industria

- ✓ **Aumento de amenazas cibernéticas**, así como las **vulnerabilidades** en el ámbito OT.
- ✓ **Mayor demanda** por parte del sector en cuanto a productos y servicios.
- ✓ **Incremento del valor del mercado** de la Ciberseguridad Industrial.
- ✓ Poco a poco **mejora o incremento del nivel de ciberseguridad** de nuestra industria.
- ✓ **Desafíos:** Concienciación y Capacitación, Recursos limitados, falta de políticas y procedimientos, etc.

Ciberseguridad Industrial

DESMA y SPRI: Fuerte compromiso con el sector

- ✓ **SPRI (DESMA)** como entidades **referentes** en todo lo relacionado con la ciberseguridad aplicada al **entorno empresarial** en Euskadi.
- ✓ Oferta **amplia y diversa** en cuanto a **instrumentos de apoyo** a las empresas del sector se refiere (I+D, Emprendimiento, Internacionalización, etc).

Apoyo Institucional

Perspectivas Futuras

Posición privilegiada (Afianzar y Potenciar)

- ✓ Ecosistema tecnológico potente.
- ✓ Madurez digital del sector industrial.
- ✓ Desarrollo y atracción de nuevos profesionales.
- ✓ Ecosistema de ciberseguridad potente (abundante, diverso, equilibrado y especializado)
- ✓ Apoyo institucional diferencial.

Futuro Prometedor:

- ✓ **Nivel** de ciberseguridad de **nuestro tejido industrial**.
- ✓ Explotar y potenciar la **especialización** en este ámbito.
- ✓ **Hub de referencia** internacional en ciberseguridad industrial.

Futuro: Dedicación intensiva en este ámbito

- ✓ **Mayor intensidad** (nivel Económico y nivel de instrumentos de apoyo).
- ✓ **Nuevas formas de apoyo** ante un entorno cambiante y en crecimiento.
- ✓ **SPRI (DESMA):** futuro prometedor, **dedicación y fuerte compromiso** con el sector de la ciberseguridad de Euskadi
- ✓ **Colaboración** estrecha, efectiva y coordinada entre instituciones públicas.

Servicios y Programas de Apoyo a la Ciberseguridad SPRI



Índice

01 *Instrumentos de apoyo*

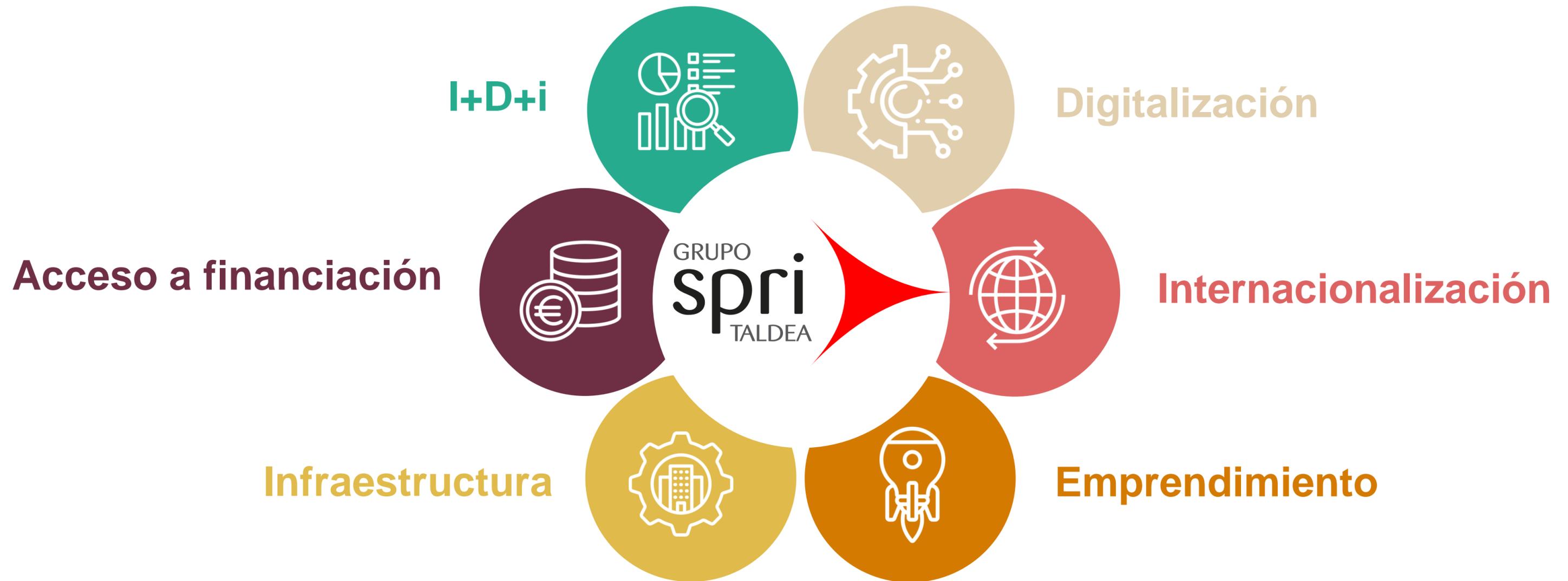
02 *Programas*

03 *Servicios*

Instrumentos de apoyo



Instrumentos de apoyo



Iniciativas RETECH



- 1 Servicio a las empresas del tipo CYBER-RANGE para la capacitación de profesionales
- 2 Servicio de SOC para PYMEs
- 3 Servicio de Pentesting y Certificación de Producto en Empresas (CRA - Cyber Resilience Act)
- 4 Simulacros de Incidentes de Ciberseguridad en Equipos Directivos/Responsables
- 5 Definición de Modelo de Referencia y Servicio de Diagnóstico en Competencias Digitales

Programas SPRI



Hazitek

Proyectos de investigación industrial o desarrollo experimental.
Presupuesto total de 90.000.000€ con dos líneas de apoyo:

- Proyectos I+D de carácter competitivo.
- Proyectos de carácter estratégico I+D.

ABIERTO



Mayo 2024



BDIH Konexio

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 entre otros.

Elkartek

- Proyectos de Investigación Fundamental Colaborativa
- Proyectos de Investigación con Alto Potencial Industrial
- Acciones Complementarias de Especial Interés

ABIERTO



Mayo 2024



Smart Industry

Respalda proyectos de Investigación Industrial y Desarrollo Experimental, ofreciendo hasta 300.000€ para proyectos que se centren en la transferencia de tecnología.

Azpitek

Apoyo a los agentes de la RVCTI para la adquisición e instalación de equipamiento científico-tecnológico.

Junio 2024



Julio 2024



Kloud

Apoyo a la migración de equipos presentes en las salas técnicas y CPDs a entornos cloud.

Programas SPRI



Hazitek

Proyectos de investigación industrial o desarrollo experimental.

- Empresas beneficiarias: Cualquier actividad.
- Presupuesto: 92,5M€
- Subvención máxima en competitivos: 500.000€

ABIERTO



Mayo 2024



BDIH Konexio

Integración de tecnologías digitales en la fabricación.

- Empresas beneficiarias: Industriales y conexas.
- Presupuesto: 900.000€
- Subvención máxima: 12.000-20.000€

Elkartek

Apoyo a la realización de proyectos RVCTI.

- Empresas beneficiarias: RVCTI
- Presupuesto: 44M€

ABIERTO



Mayo 2024

ETDE 25 EEDE

Smart Industry

Desarrollo experimental de Transferencia tecnológica.

- Empresas beneficiarias: Industriales y conexas.
- Presupuesto: 3,7M€
- Subvención máxima: 150.000€

Azpitek

Adquisición e instalación de equipamiento para la RVCTI.

- Empresas beneficiarias: RVCTI
- Presupuesto: 9M€

Junio 2024



Julio 2024

ETDE 25 EEDE

Kloud

Migración de CPDs a entornos cloud.

- Empresas beneficiarias: Cualquier actividad.
- Presupuesto: 1,6M€
- Subvención máxima: 30.000€

Programa Ciberseguridad Empresarial



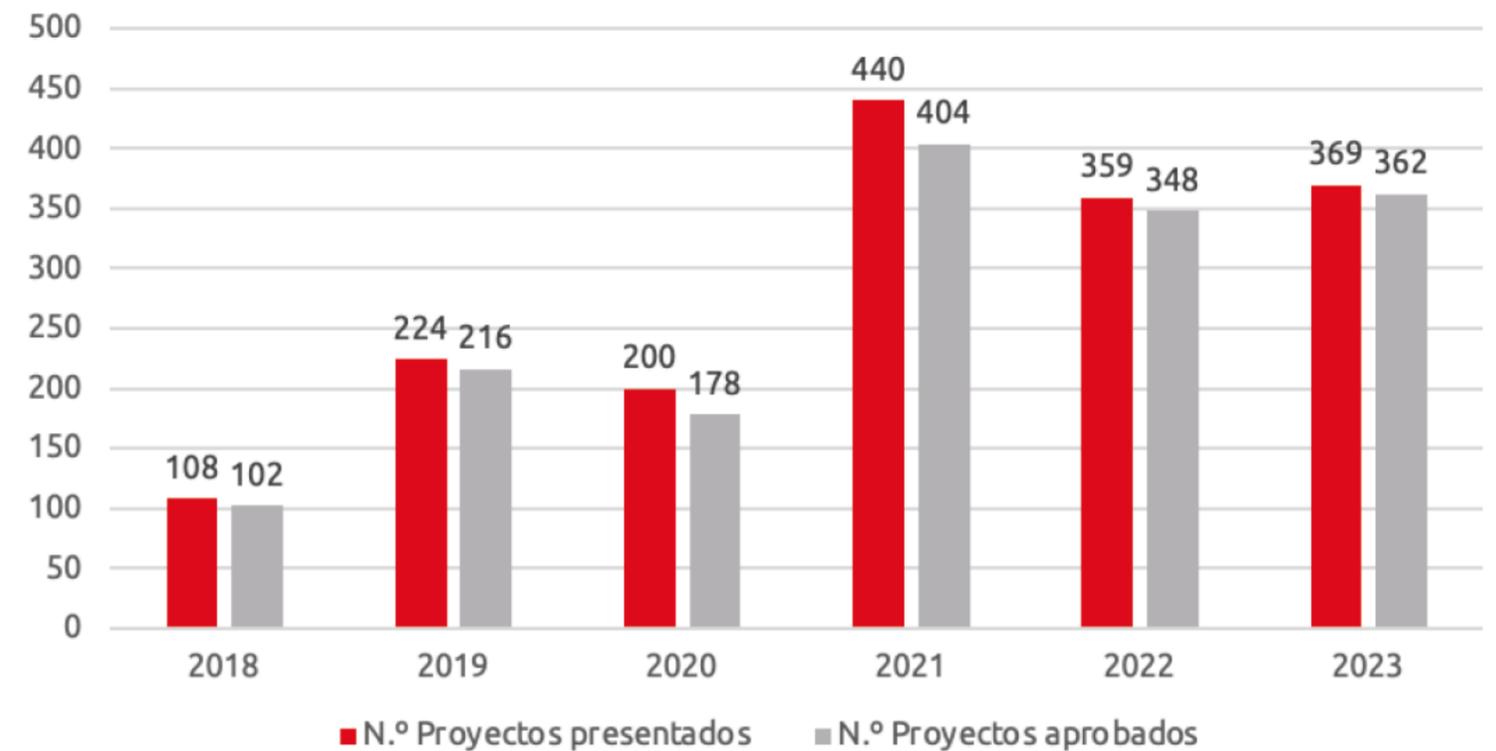
Convocatoria 2024

- **Ciberseguridad Industrial Empresarial**
- **Publicación BOPV mayo 2024**
- **3.500.000€** de presupuesto
- **23.000€** de Subvención máxima por empresa
- **Independientemente del tamaño** de la empresa **y la actividad empresarial**
- **Ejemplos de tipologías de proyectos:**
 - Diseño de **arquitecturas seguras** y **segmentación de redes**
 - Securización de **accesos remotos OT**
 - **Certificación** de dispositivos
 - **Diagnóstico** y **plan de acción** en ciberseguridad
 - Adopción de **buenas prácticas** y certificación
 - **Monitorización** de dispositivos

Programa Ciberseguridad Industrial



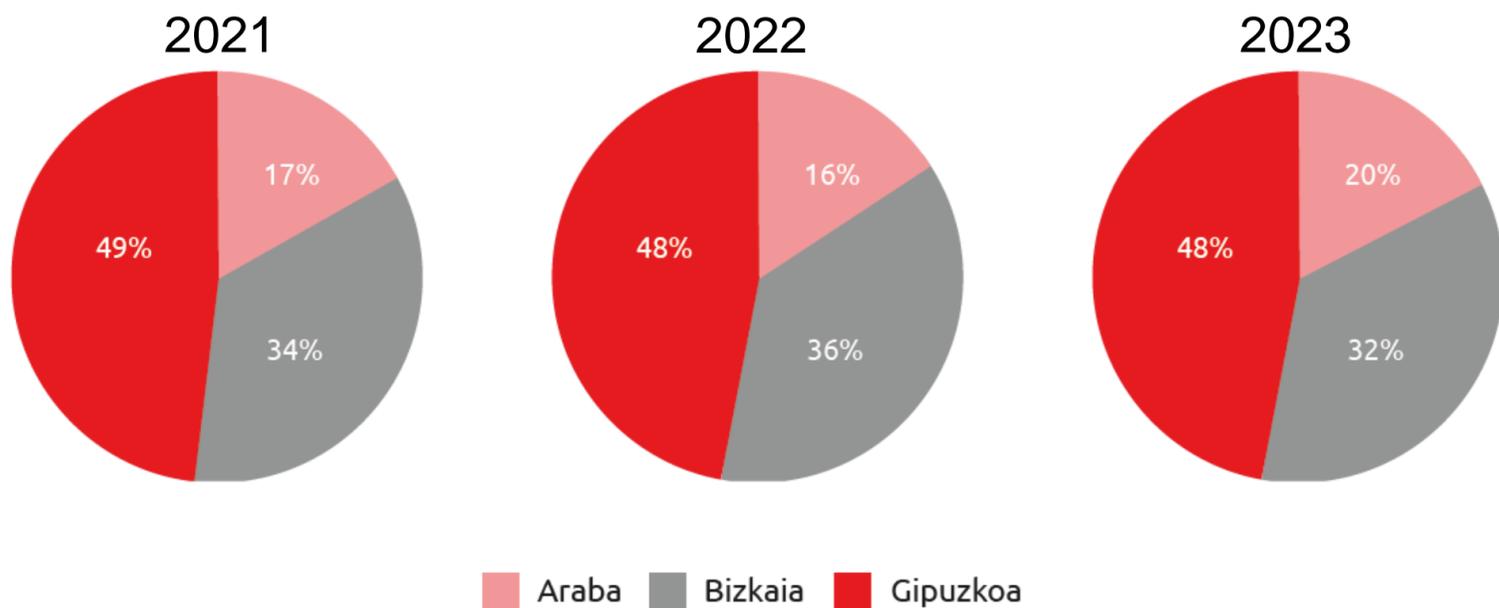
N.º Proyectos por convocatoria



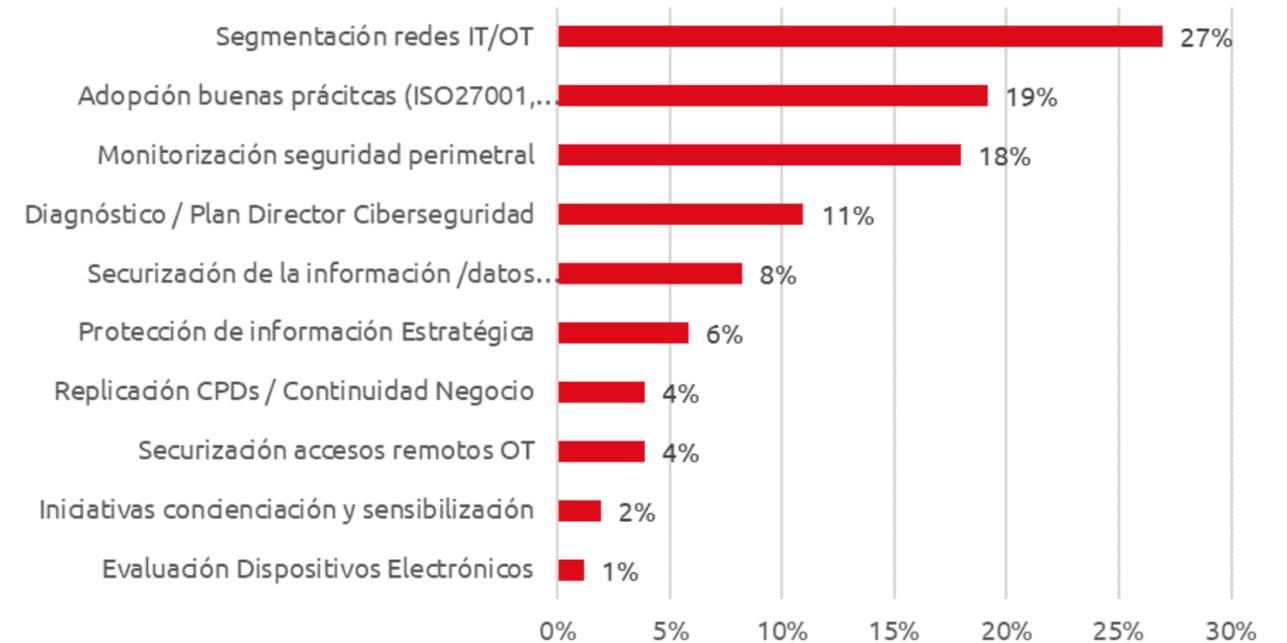
Programa Ciberseguridad Industrial

“El 58% de los proyectos aprobados en la convocatoria de 2023 fueron en empresas de entre 1 y 49 empleados”

Proyectos aprobados por Territorio Histórico



Tipologías de proyectos aprobados

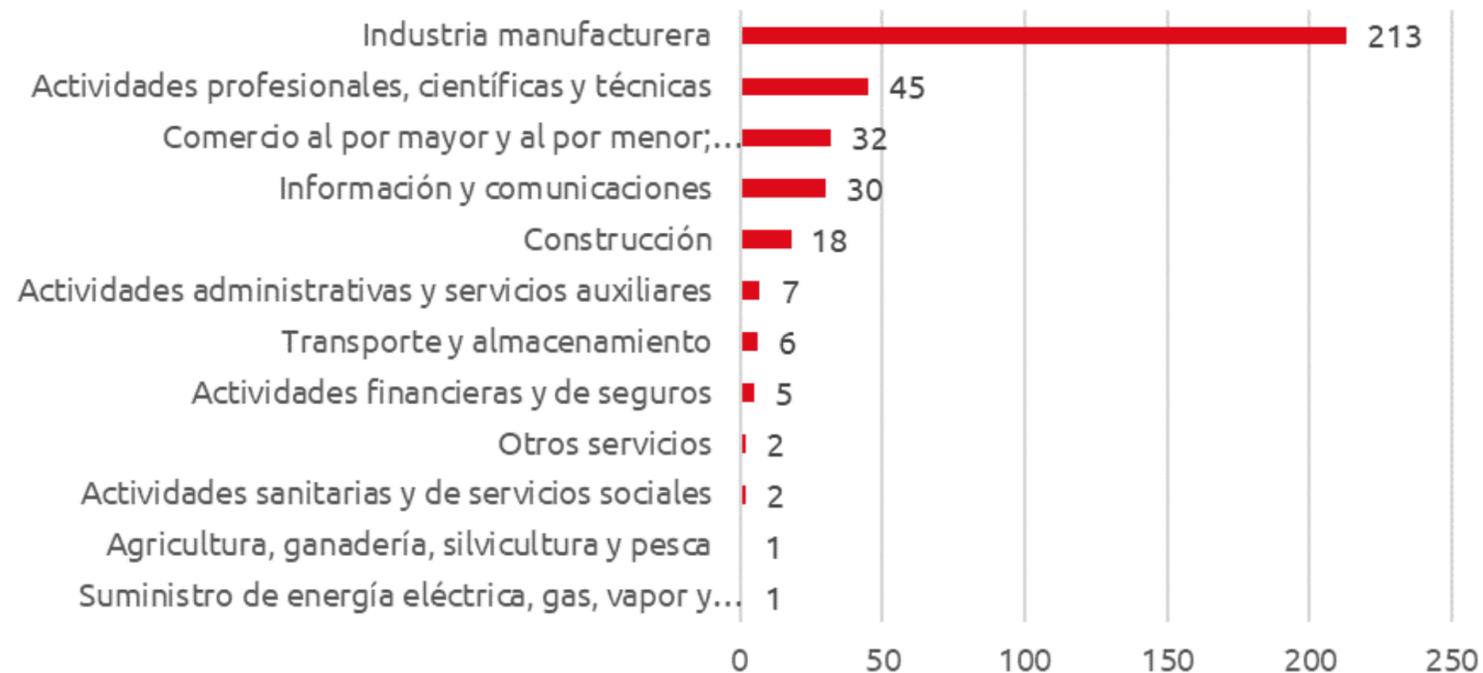


*“Incremento Sustancial: Proyectos relacionados con la **Adopción buenas prácticas** y **procesos de certificación** (IEC 62443, TISAX, ENS, ISO27001, etc)”*

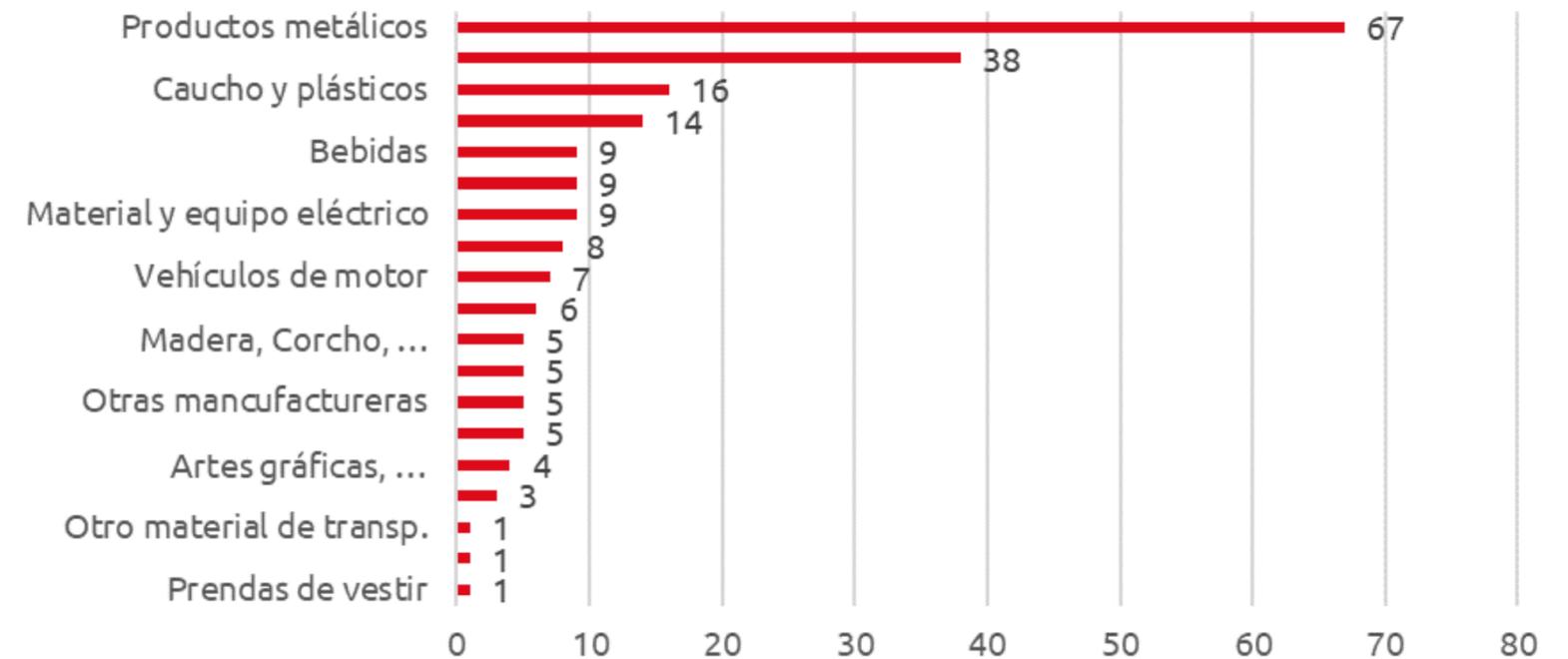
Programa Ciberseguridad Industrial

“Convocatoria 2023: Destacan las empresas **industriales** dedicadas a la **manufactura**”

Proyectos aprobados por sector de actividad



Industria Manufacturera



“Convocatoria 2024: Programa **abierto a cualquier sector de actividad**”

Enpresa digitala: Desarrollo Profesional en Competencias Digitales



¿Qué puede hacer un sistema de autenticación de usuarios por ti?

- **Formato:** Online
- **Fecha:** 13/03/2024
- **Horario:** 09:30-11:00 (1 h 30')
- **Precio:** Gratuito
- **Idioma:** Español

JORNADA



Pivoting en Redes

- **Formato:** Presencial
- **Fecha:** 11/03/2024 al 13/03/2024
- **Horario:** 09:00-13:30 (12 horas)
- **Precio:** 70€
- **Idioma:** Español

TALLER

Otros cursos

- Introducción al pentest sobre entornos de Directorio Activo I – Iniciación & Intermedio.
- Protección de datos personales aplicada a proyectos IoT, Big Data e Inteligencia Artificial.
- Reconocimiento de la ciberexposición de tu empresa.
- La ciberseguridad en sistemas robóticos.

Más información

944 536 262

enpresadigitala@spri.eus

<https://enpresadigitala.spri.eus/>

Servicio de Concienciación para Empresas

Dirigido a:

Agrupaciones Empresariales y Empresas, Futuros Profesionales, Organismos Públicos del Gobierno Vasco.

Sesiones Periódicas

Sesiones en Abierto

- **Formato:** Presencial / Online
- **Cuando:** Periódicas*
- **Duración:** 60 – 120 minutos
- **Precio:** Gratuito
- **Idioma:** Español / Euskera

JORNADA

Sesiones Privadas

- **Formato:** Presencial / Online
- **Cuando:** Bajo Demanda
- **Duración:** 60 – 120 minutos
- **Precio:** Gratuito
- **Idioma:** Español / Euskera

JORNADA

Sesiones Puntuales

Webinnars

- **Formato:** Online
- **Donde:** spri.eus
- **Duración:** 60 – 75 minutos
- **Precio:** Gratuito
- **Idioma:** Español / Euskera

WEBINNAR

*Al menos 8 sesiones al mes.

Servicio de Concienciación para Empresas

Algunas Temáticas:

- 1 ¿Estás conectad@? Necesitas Ciberseguridad / Konektatuta zaude? Zibersegurtasuna behar duzu
- 2 Normativa y Servicios de Ciberseguridad / Zibersegurtasun zerbitzu eta araudia
- 3 Ciberseguridad en el puesto de trabajo / Zibersegurtasuna lanpostuan
- 4 Ciberseguridad para perfiles de dirección / Zibersegurtasuna zuzendaritza profilentzat
- 5 Ciberseguridad para desarrolladores / Zibersegurtasuna garatzaileentzat
- 6 Ciberseguridad en la industria / Zibersegurtasuna industrian
- 7 Ciberseguridad en el teletrabajo / Zibersegurtasuna telelanean
- 8 Anticipándose a una crisis de ciberseguridad / Ziberkrisi bati aurrea hartuz
- 9 Ciberseguridad en la Empresa / Zibersegurtasuna enpresan

Mikroenpresa digitala = Formación + Asesoramiento



Ciberseguridad I: Buenas prácticas para proteger la información de tu negocio

- **Formato:** Online
- **Fecha:** 11/03/2024
- **Horario:** 12:00-14:00 (2 horas)
- **Precio:** Gratuito
- **Idioma:** Español



Ciberseguridad II: Ejemplos prácticos para proteger tu negocio

- **Formato:** Online
- **Fecha:** 14/03/2024
- **Horario:** 12:00-14:00 (2 horas)
- **Precio:** Gratuito
- **Idioma:** Español

Más información

690 922 752
mikroadigitala@spri.eus
<https://www.spri.eus/>

Eskerrik asko



Mesa Redonda 1: Ciberseguridad en la Industria



Moderadora:
Leyre Madariaga
Gobierno Vasco



Jorge Barroeta
MB Sistemas



Edorta Echave
Secure & IT

Mesa Redonda 2: Entorno regulatorio



Moderadora:
Leyre Madariaga
Gobierno Vasco



Iratxe Zuluaga
MERYTRONIC



Salva Trujillo
ORBIK
Cybersecurity

ESKERRIK ASKO

