Caracterización del sector de la ciberseguridad en Euskadi

CYBASQUE

2023

Índice de contenidos

Prólogo 2
Perspectivas y necesidades de profesionales 4
Agentes del sector de la ciberseguridad en Euskadi 6
Empleados TIC y de ciberseguridad 9
Contrataciones 11
Oferta de talento 14
Conclusiones 19
Bibliografía 20

Índice de figuras

Figura 1. Número total de agentes de ciberseguridad en Euskadi. Fuente: SPRI 6
Figura 2. Cadena de valor del sector de la ciberseguridad. Fuente: Elaboración propia 6
Figura 3. Agentes listados en diferentes ediciones del Libro Blanco. Fuente: SPRI 7
Figura 4. Líneas de investigación en Euskadi. Fuente: RENIC 8
Figura 5. Experiencia requerida en base a pliegos de licitación pública de Euskadi. Fuente: Elaboración propia 9
Figura 6. Empleados TIC en los establecimientos de Euskadi. Fuente: Eustat 10
Figura 7. Distribución de la contratación prevista según nivel de estudios. Fuente: ConfeBask 11
Figura 8. Distribución de la contratación prevista por familias de Estudios Universitarios y FP. Fuente: ConfeBask 12
Figura 9. Proyecciones de empleo en España. Fuente: ObservaCIBER 12
Figura 10. Egresados universitarios por área de estudio en Euskadi. Fuente: Eustat 14
Figura 11. Graduados con posible interés en ciberseguridad en Euskadi. Fuente: Eustat 15
Figura 12. Egresados universitarios en Euskadi. Fuente: Eustat 15
Figura 13. Matriculados FP. Fuente: Eustat 15

PRÓLOGO

Prólogo

En los últimos tiempos, el ámbito empresarial ha apreciado una transformación destacable como consecuencia de la evolución de las nuevas tecnologías y la profunda digitalización que está aconteciendo en la economía y en la sociedad. Esta transformación ha resultado en el desarrollo y mejora notable de los procesos y servicios en las organizaciones, implicando no solo una revolución en las prácticas comerciales, sino también un incremento sustancial en la dependencia de la tecnología por parte de las diferentes organizaciones.

La interconexión intensificada como resultado de esta mayor dependencia, se posiciona como una de las principales causas del aumento de la ciberdelincuencia, incrementando así los riesgos asociados a la ciberseguridad y afectando tanto a la integridad, confidencialidad y disponibilidad de la información manejada como a los servicios ofrecidos por estas entidades. Además, el continuo avance en la sofisticación de las técnicas delictivas ha creado demandas adicionales en diversas organizaciones, lo que las obliga a destinar mayores recursos hacia la adquisición de servicios y herramientas de ciberseguridad.

Asimismo, se suscita la imperiosa necesidad de reconsiderar los parámetros de seguridad en el entorno industrial, lo que implica un incremento en el interés por la implementación de medidas de ciberseguridad en dicho ámbito.

Todo lo anterior, ha supuesto el crecimiento exponencial en la demanda de profesionales especializados en ciberseguridad. Esta demanda ha ido en aumento de manera paralela a los avances tecnológicos y la digitalización de la sociedad, observándose un incremento significativo en la demanda de graduados universitarios o de formación profesional en el campo de las Tecnologías de la Información y la Comunicación (TIC). Aunque tradicionalmente se ha considerado que la ciberseguridad está estrechamente relacionada con las ciencias de la informática, la complejidad y diversificación de las amenazas cibernéticas y la necesidad de cumplir con nuevas regulaciones existentes, han generado una demanda cada vez mayor de profesionales provenientes de diversas disciplinas. Específicamente, se ha evidenciado un interés creciente en profesionales que posean conocimientos en el ámbito normativo y legal relacionado con la ciberseguridad. Esto se debe a la necesidad de comprender y cumplir con las regulaciones y estándares en un entorno digital cada vez más complejo y regulado.

Al hilo de lo anterior, Euskadi presenta un desafío claro en este ámbito, hacer frente a la brecha de talento existente en el ámbito de la ciberseguridad, siendo la necesidad de captación, capacitación e inserción laboral de profesionales, una de las necesidades principales del sector.

El estudio se erige como una herramienta fundamental para comprender mejor el panorama laboral en el ámbito de la ciberseguridad en la región vasca. Proporcionando información valiosa que puede ser utilizada para diseñar estrategias y políticas que impulsen el desarrollo sostenible y la competitividad de todos los eslabones de la cadena de valor del sector de la ciberseguridad en el futuro.

PERSPECTIVAS Y NECESIDADES DE PROFESIONALES

Perspectivas y necesidades de profesionales

La evolución del mundo digital ha generado la necesidad de una transformación digital, integrando nuevas tecnologías, procesos de innovación, adaptación y protección. Las ciberamenazas siguen desarrollándose a un ritmo rápido, y aunque las inversiones continúan llegando a la ciberseguridad, queda mucho trabajo por hacer en un entorno en constante evolución.

Euskadi fue la quinta Comunidad Autónoma en la que más se invirtió por parte de las Administraciones Públicas en materia de ciberseguridad en el primer trimestre de 2023.

En el primer trimestre de 2023 la inversión en ciberseguridad por parte de las Administraciones Públicas estatales alcanzó los 81,04 millones de euros [1]. Gracias a las inversiones realizadas y a la estrecha colaboración de alto nivel dentro de las compañías, más del 70% de los ejecutivos perciben una mejora en las iniciativas de ciberseguridad de sus empresas en el último año [2].

En este entorno de rápida extensión de la digitalización, el Gobierno Vasco ha definido la "Estrategia para la Transformación Digital de Euskadi 2025 (ETDE2025)" dotada de 1.400 millones de euros, representa un nuevo enfoque en la interacción entre la Administración Pública de Euskadi y los sectores económicos y sociales, orientado a abordar de manera colaborativa los desafíos globales a través de la transformación digital [3].

El objetivo primordial de esta estrategia es acelerar la adopción de sectores tecnológicos emergentes, fortalecer su desarrollo y aprovechar el potencial de los diversos facilitadores disponibles, promoviendo su rápida integración en áreas esenciales. Esto contribuirá a la transición de Euskadi hacia un futuro tecnológico-digital, energético-ambiental y social-sanitario para el año 2025.

En el ámbito tecnológico-digital, se establece el objetivo de la creación de 300 nuevas empresas especializadas en diversos campos tecnológicos, tales como ciberseguridad, inteligencia artificial, computación cuántica, visión artificial, *blockchain*, internet de las cosas (IoT), realidad aumentada, *big data* y robótica para el año 2025 [3].

Además, a nivel estatal se aprueba el "Plan de España Digital 2026" donde se espera reforzar la capacidad estatal en ciberseguridad y se busca disponer de 20.000 especialistas en ciberseguridad, Inteligencia Artificial y datos en 2025 [4]. Las estrategias que actualmente se encuentran disponibles buscan adaptarse con éxito a la Transformación Digital existente en todos los ámbitos de la sociedad. Para ello, Euskadi apuesta por un nuevo modelo de Transformación Digital que supone una forma diferente de entender y ejercer la relación entre la Administración Pública Vasca y los agentes económicos y sociales, de forma que se puedan afrontar conjuntamente los retos globales.

Como uno de los desafíos principales del ecosistema de la ciberseguridad en Euskadi, se presenta la necesidad de paliar la brecha de talento existente en el territorio vasco. En este sentido, con el fin de conseguir los niveles de capacitación profesional requeridos, se detectan 2 vías de actuación principales: la contratación de nuevos profesionales, provenientes tanto de grados universitarios como de Formación Profesional y el aprovechamiento de las

competencias profesionales experimentados a través de capacitación adicional por medio de formaciones y cursos que les permitan reconducir su actividad hacia este campo.

Aunque estas medidas permitirán dotar a la actividad económica y los servicios públicos de una mayor capacidad profesional, en el futuro más inmediato seguirá habiendo una demanda de puestos de trabajo sin cubrir. En este contexto, tener un conocimiento del estado del sector se convierte en imprescindible para tomar las medidas necesarias que permitan revertir la situación y mitigar los riesgos asociados a la ciberseguridad. Entre estas medidas se identifican claves la inversión, la innovación y el cambio cultural.

Agentes del sector de la ciberseguridad en Euskadi

La creciente demanda de productos y soluciones para mejorar la protección de las infraestructuras TIC ha potenciado también el crecimiento del sector de la ciberseguridad, creando nuevas oportunidades de negocio. Euskadi cuenta con una amplia gama de agentes que ofrecen productos y servicios de ciberseguridad en Euskadi. Actualmente, Grupo SPRI tiene registrados en su catálogo de ciberseguridad 242 agentes, frente a los 111 registrados en 2018, lo que demuestra la tendencia alcista en lo que a agentes en el sector de la ciberseguridad en Euskadi se refiere [5].

Figura 1. Número total de agentes de ciberseguridad en Euskadi. Fuente: SPRI

Al hilo de lo anterior, el ecosistema de ciberseguridad de Euskadi está compuesto por 4 eslabones dentro de la cadena de valor definida en el sector:

- Fabricación: empresas que proveen soluciones, aplicaciones y herramientas que garantizan la seguridad.
- Distribución: recoge las empresas dedicadas a distribuir los productos fabricados, ejerciendo como intermediario entre el fabricante y los prestadores de servicios.
- Servicios: agentes prestadores de servicios de ciberseguridad.
- Clientes: Administraciones Públicas, empresas y particulares destinatarios de los diferentes productos y servicios de ciberseguridad.

A través de la revisión de las diferentes versiones del Libro Blanco de ciberseguridad en Euskadi publicado por SPRI, se observa una tendencia continua al alza en el número de agentes identificados.

Además, las universidades y los centros de investigación son elementos fundamentales por su impulso y por su labor de innovación. Asimismo, cobran especial relevancia la formación y la acreditación de las capacidades de los profesionales mediante certificaciones del sector de la ciberseguridad.

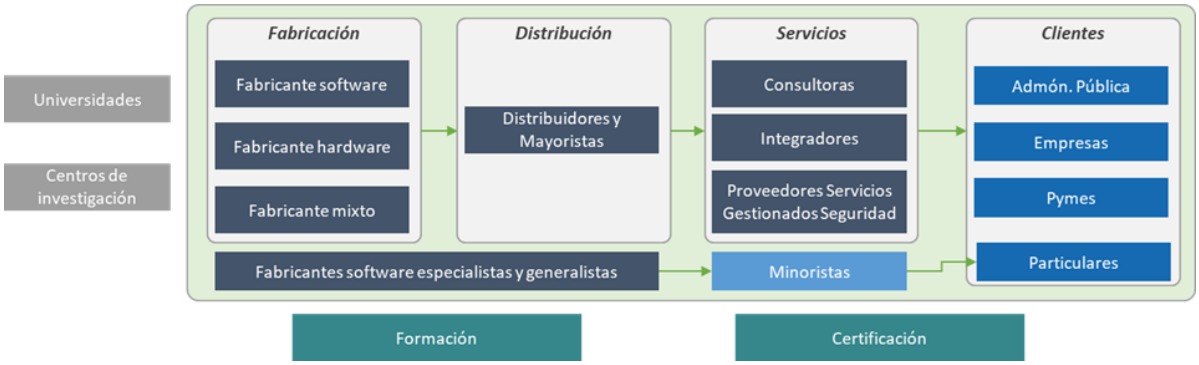


Figura 2. Cadena de valor del sector de la ciberseguridad. Fuente: Elaboración propia

En lo que respecta a los diversos agentes que componen el ecosistema de ciberseguridad en Euskadi, tal y como se muestra en el siguiente gráfico, existe una amplia variedad y heterogeneidad en el territorio. Es importante destacar aquellos agentes enfocados en la prestación de servicios (Integrador/Consultor) o en la fabricación (Fabricante) y distribución de productos (Distribuidor/Mayorista), donde se observa una disparidad en la región. La mayoría de los agentes de ciberseguridad en Euskadi se centran en la oferta de servicios en este ámbito, mientras que existe una notable escasez de aquellos dedicados a la fabricación y distribución de productos de ciberseguridad. Esto revela la existencia de una cadena de valor descompensada en la oferta de productos/servicios en materia de ciberseguridad.

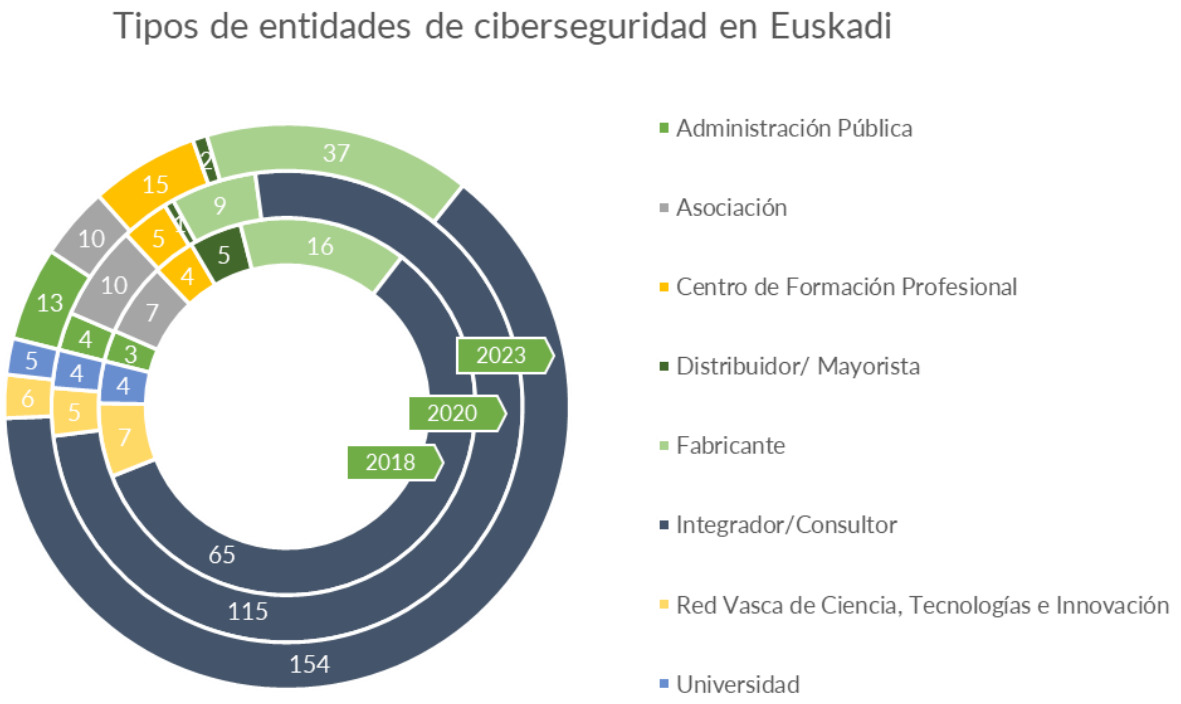


Figura 3. Agentes listados en diferentes ediciones del Libro Blanco. Fuente: SPRI

En lo que respecta a la investigación, Euskadi cuenta con diferentes centros de investigación y desarrollo que ejercen un fuerte magnetismo sobre una amplia red de profesionales. Estas instituciones tienen como propósito impulsar el avance económico y social, así como fortalecer la competitividad empresarial de la zona. Adicionalmente, actúan como verdaderos motores de difusión de la ciencia, la tecnología y la innovación, desempeñando un papel crucial en la transferencia de conocimientos hacia la sociedad y facilitando la colaboración entre diversos actores del ecosistema de Euskadi de investigación y desarrollo. Su contribución abarca desde la generación de nuevos conocimientos hasta la creación de oportunidades de aplicación práctica, promoviendo así un entorno propicio para el progreso sostenible en la región.

Es importante destacar el Basque Digital Innovation Hub de Euskadi, una red integrada de recursos y servicios especializados en fabricación avanzada que ofrece infraestructuras destinadas a la formación, investigación, pruebas y validación, brindando a las empresas acceso, conocimientos y servicios específicos en campos como la fabricación aditiva, la robótica flexible y la ciberseguridad. Su objetivo principal es proporcionar a las empresas industriales, especialmente a las pymes, las capacidades tecnológicas necesarias para enfrentar los desafíos

de la industria inteligente. En el ámbito de la ciberseguridad concretamente, cuenta con el nodo de ciberseguridad, que, compuesto por 5 laboratorios, tiene como objetivo impulsar la iniciativa empresarial y la innovación, centrándose particularmente en proyectos vinculados a s*mart-grid*, automoción, *blockchain* y certificación de productos.

En la siguiente imagen se muestran las líneas de investigación que actualmente tienen mayor presencia en las entidades de Euskadi [6]:

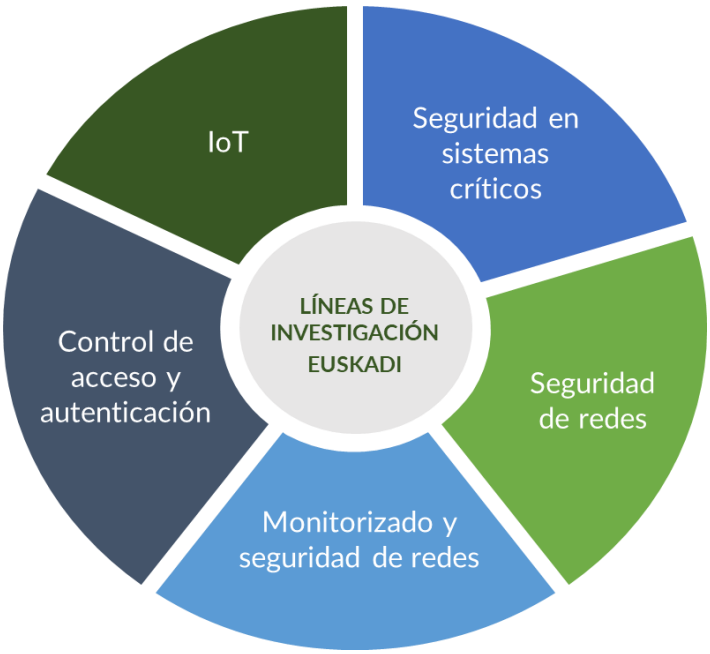


Figura 4. Líneas de investigación en Euskadi. Fuente: RENIC

Empleados TIC y de ciberseguridad

Según el análisis realizado por Cybasque sobre los diversos pliegos de licitación disponibles en el campo de la ciberseguridad en Euskadi, se observa que, al llevar a cabo proyectos en este ámbito, se requiere, entre otros aspectos, que los profesionales cuenten con experiencia previa en actividades similares y que cuenten con certificaciones que acrediten las capacidades de los diferentes profesionales del sector.

De la misma manera, se destaca la importancia de crear equipos distribuidos donde se encuentren profesionales con conocimientos y experiencias variadas. Esto ayudará también a equilibrar las necesidades de profesionales con mucha experiencia.

En definitiva, se busca un sector con una oferta de servicios de calidad y profesionales experimentados [7].

Jefe/Director de proyecto	3-8 años de experiencia
Perfil consultor	5 años o que parte del equipo tenga 5 años de experiencia (equipos distribuidos)
Analista-Programador	3 años de experiencia
Programador	2 años de experiencia
Otros perfiles (diseñador web, técnico...)	2-3 años de experiencia

Figura 5. Experiencia requerida en base a pliegos de licitación pública de Euskadi. Fuente: Elaboración propia

De acuerdo con datos de Eustat, mientras el número de usuarios TIC aumenta en las organizaciones de Euskadi, el porcentaje de especialistas se reduce.

La carencia de profesionales en el campo de las TIC es evidente, especialmente en lo que respecta al personal altamente especializado. En el año 2023, cerca del 80% de los empleados en Euskadi utilizaba sistemas TIC, sin embargo, solo el 10,2% de este contingente se constituía como personal especializado en dicho ámbito. En comparación con el año 2020, se aprecia un incremento en el número de usuarios de TIC, aunque este crecimiento no se refleja de manera equivalente en la expansión del cuerpo profesional dedicado a las TIC. En el sector de servicios, donde se concentra la mayor actividad empresarial en ciberseguridad, se evidencia un aumento en el número de usuarios de TIC (2,8%), mientras que la cantidad de especialistas experimenta un decremento del 0,7%. Por consiguiente, es imprescindible dirigir la atención hacia la escasez de expertos digitales avanzados, ya que esta situación obstaculiza las perspectivas de crecimiento del país [8].

A modo de conclusión, se observa que el uso de las nuevas tecnologías ha experimentado un notable incremento en todos los ámbitos de la sociedad, desde la comunicación hasta la educación y el trabajo. Sin embargo, este rápido avance no ha sido acompañado por un aumento proporcional en el número de expertos en estas tecnologías. A pesar de la creciente demanda de profesionales con habilidades digitales, la brecha entre la oferta y la demanda de expertos en tecnología sigue siendo significativa. Esta disparidad plantea desafíos importantes en términos de capacitación y desarrollo de talento, así como en la garantía de que la sociedad pueda aprovechar plenamente el potencial de estas innovaciones en beneficio de todos.

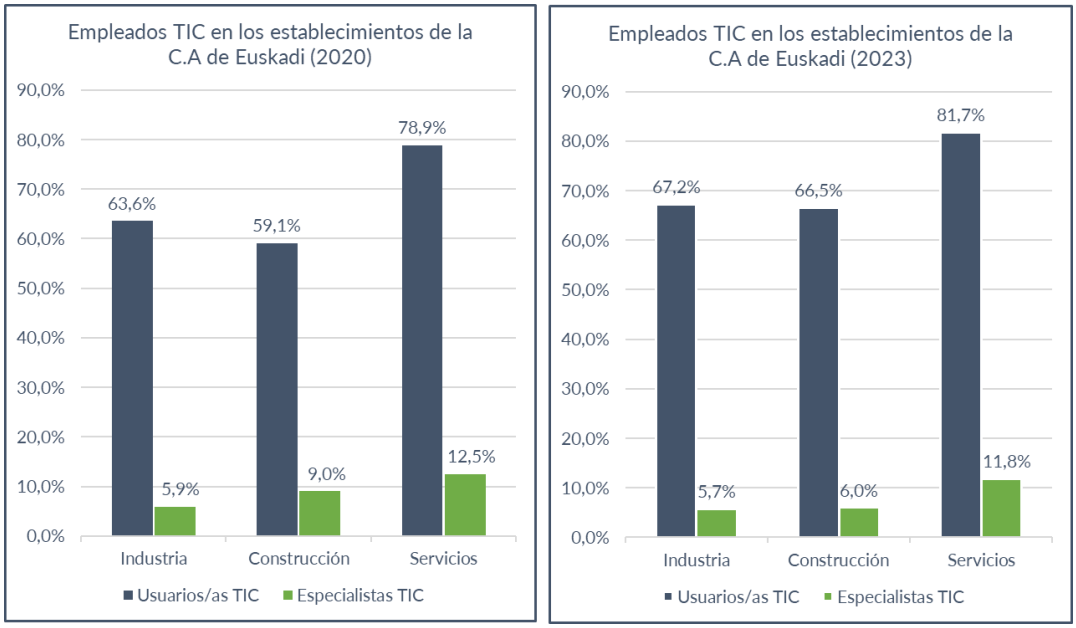


Figura 6. Empleados TIC en los establecimientos de Euskadi. Fuente: Eustat

Contrataciones

En Euskadi emergen continuamente nuevas necesidades y con ello también nuevos profesionales para llevar a cabo estos servicios y productos. Si bien es cierto que existe la posibilidad de reciclar el talento interno hacia posiciones de ciberseguridad, es necesario conocer la demanda de contratación que se espera en los próximos años para poder disponer de profesionales formados en la materia.

En virtud de los datos obtenidos por parte de ConfeBask, se prevé que la demanda de perfiles de educación superior predomine frente al resto. Además, teniendo en cuenta que las empresas del sector de la ciberseguridad están dirigidas mayormente a servicios, se estima que las contrataciones se den en su gran mayoría también en este sector [9].

Los perfiles con educación superior predominan en la demanda prevista dentro del ámbito de ciberseguridad.

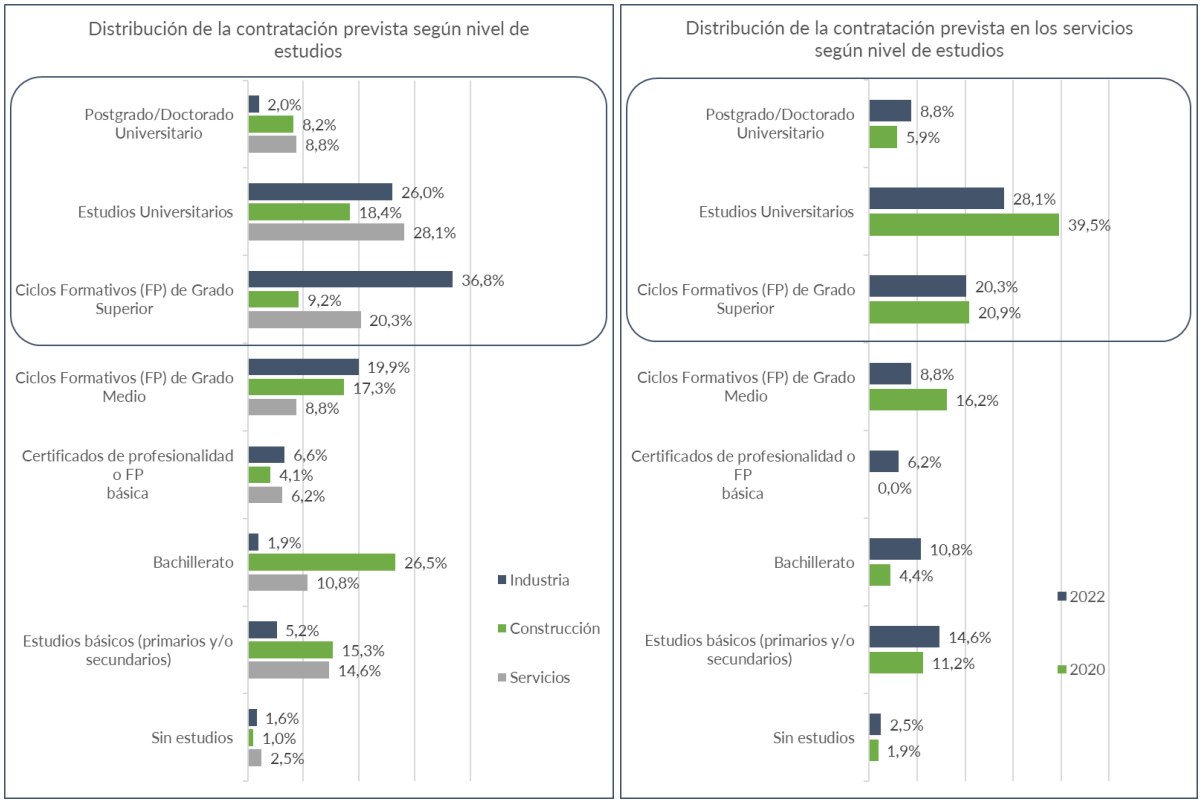


Figura 7. Distribución de la contratación prevista según nivel de estudios. Fuente: ConfeBask

Si observamos las previsiones de contratación realizadas, los estudios dentro del ámbito de la informática son los más demandados en Euskadi tanto en grados universitarios como en grados de Formación Profesional, seguido por otras ingenierías, y así seguirá siendo al menos en el futuro más inmediato [9].

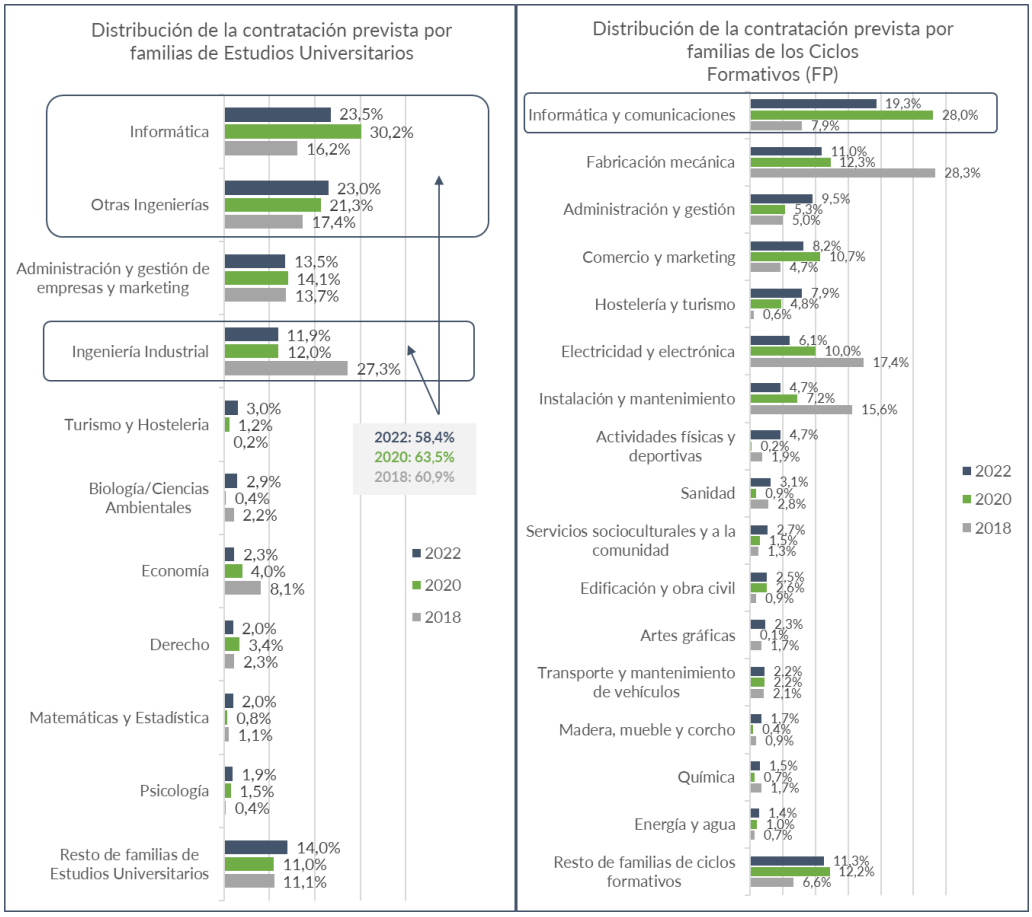


Figura 8. Distribución de la contratación prevista por familias de Estudios Universitarios y FP. Fuente: ConfeBask

El siguiente gráfico recoge las proyecciones de la oferta y demanda de profesionales de ciberseguridad en España, donde se observa la existencia de la brecha de talento en el sector en España, previéndose un futuro similar en Euskadi el próximo año [10]. 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.

De acuerdo a las proyecciones, la brecha entre oferta y demanda de empleo en el ámbito de ciberseguridad tiene una tendencia creciente que continuará en 2024.

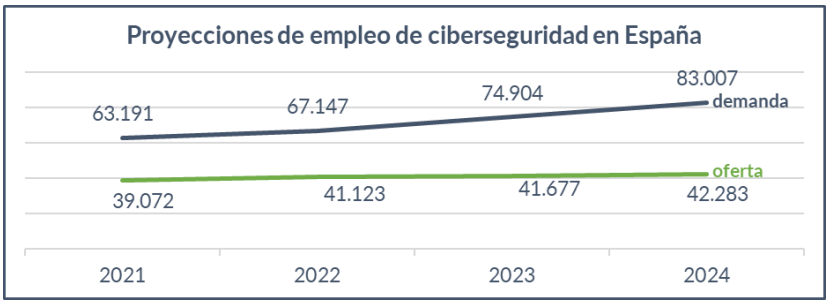


Figura 9. Proyecciones de empleo de ciberseguridad en España. Fuente: ObservaCIBER

Ante esta evidente brecha de talento que se vislumbra en el sector de la ciberseguridad, las empresas se verán obligadas a reconsiderar sus estrategias de contratación. En lugar de depender exclusivamente de profesionales con títulos universitarios o de educación superior, será necesario buscar talento fuera de este ámbito académico tradicional. Esto implicará tanto la búsqueda de individuos con habilidades y experiencia relevantes, como también la inversión en programas de formación y reciclaje para aquellos empleados que no provengan de este trasfondo educativo. La prioridad será formar equipos equilibrados en cuanto a experiencia y habilidades, con el objetivo de mitigar la brecha de talento de la manera más efectiva posible en el futuro cercano.

Oferta de talento

Cuando evaluamos el talento disponible en una región, es esencial abordar la conversación sobre la oferta educativa, ya que está estrechamente ligada a la disponibilidad de talento en dicho lugar. La calidad y diversidad de los programas educativos no solo influyen en el desarrollo personal de los estudiantes, sino que también tienen un impacto considerable en la capacidad de la zona para cultivar y aprovechar el talento local. Por ende, al centrarnos en mejorar y expandir la oferta educativa, podemos potenciar el crecimiento y la competitividad del territorio, garantizando un flujo constante de habilidades y conocimientos que impulsan tanto el progreso económico como el social.

Para conocer la diversidad de perfiles dedicados a la ciberseguridad, se plantea un análisis del talento emergente, abarcando tanto a los graduados universitarios como a los titulados en programas de Formación Profesional (FP). Es importante tener en consideración que no todos los egresados con aptitudes para el sector de la ciberseguridad se incorporan necesariamente en roles específicos dentro de esta disciplina.

Según las estadísticas de 2021/22, 9.689 alumnos terminaron sus estudios de grado en las universidades de Euskadi, siendo un 20,5% los egresados dentro del área de estudio de Ingeniería y Arquitectura [11].

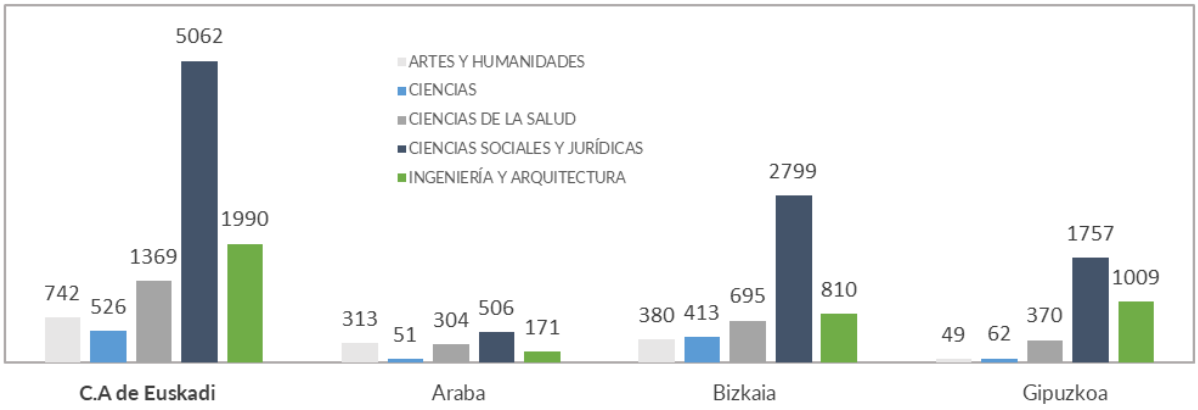


Figura 10. Egresados universitarios por área de estudio en Euskadi. Fuente: Eustat

Considerando los ámbitos de estudio inherentes a cada grado y con el propósito de identificar aquellos con mayor aptitud para desempeñar labores en el campo de la ciberseguridad, se tomarán en consideración los grados de Informática, Telecomunicaciones y otros programas que incorporen el estudio de tecnologías emergentes. Un total de 332 graduados (equivalente al 3,4% del total) podrían demostrar interés o haber cursado materias de relevancia en ciberseguridad, destacando un mayor número de titulados en Ingeniería Informática (173 graduados), Ingeniería Informática de Gestión y Sistemas de la Información (70 graduados), así como en Ingeniería Técnica de Telecomunicación (42 graduados).

Al examinar el siguiente gráfico, se evidencia que los programas de estudio con mayor cantidad de graduados son aquellos pertenecientes al ámbito de la Informática, tales como Ingeniería Informática e Ingeniería Informática de Gestión y Sistemas de la Información.

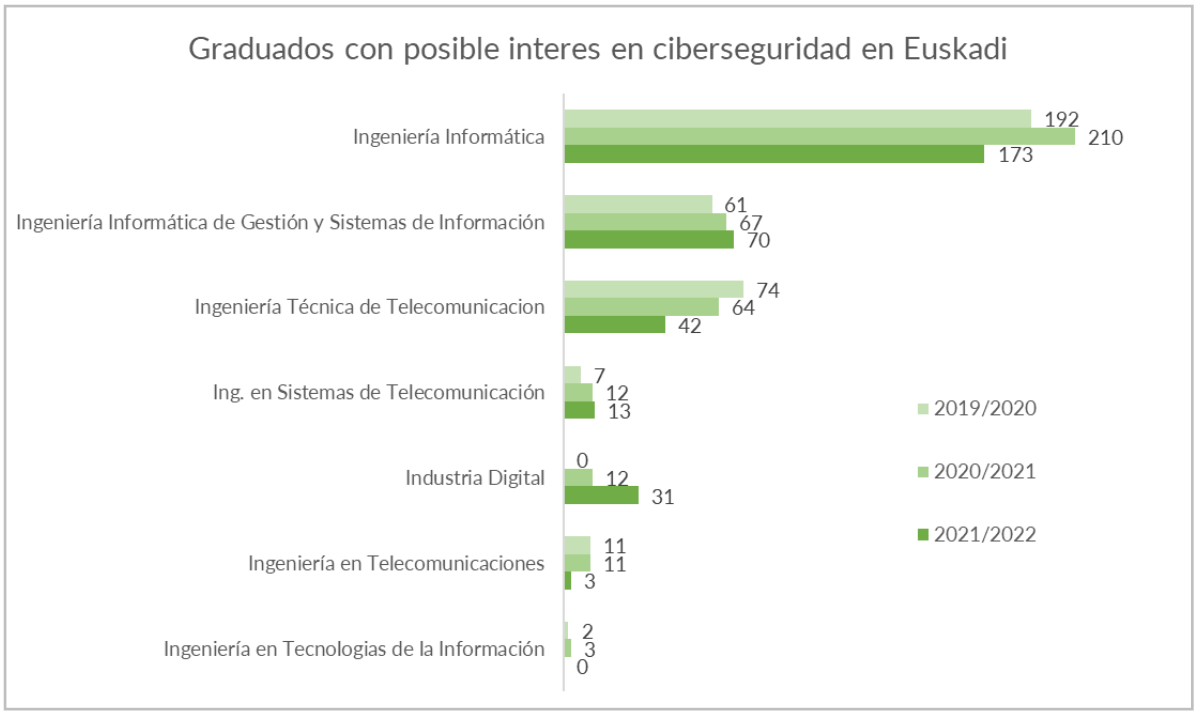


Figura 11. Graduados con posible interés en ciberseguridad en Euskadi. Fuente: Eustat

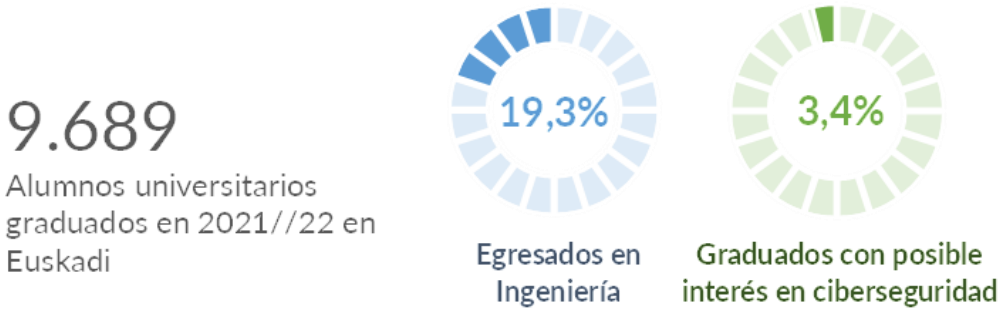


Figura 12. Egresados universitarios en Euskadi. Fuente: Eustat

Además, es posible identificar perfiles que se alinean con distintos grados, por ejemplo, en el caso de Matemáticas, se observa que hubo 72 graduados tanto en el periodo 2019/20 como en 2020/21, y 77 graduados en 2021/22. Por otro lado, en el campo de Derecho, se registraron 621 graduados en 2019/20, 611 en 2020/21 y 576 en 2021/22, lo que incluiría a los estudiantes especializados en áreas como la privacidad y la ciberseguridad.

Figura 13. Matriculados FP. Fuente: Eustat

En cuanto a los estudios de formación profesional, para este sector interesan sobre todo aquellos de formación profesional de grado superior en estudios como los de IT y comunicaciones, y electricidad y electrónica, donde se puede observar un crecimiento del interés por medio del crecimiento de las matriculaciones cada año [12].

En el ámbito educativo de la región, diversas organizaciones e instituciones están concentradas en mejorar y especializarse en ciberseguridad. Con el propósito de abordar la brecha de talento existente en esta área, los miembros que conforman la Red de Centros de Educación de Euskadi, están implementando una serie de iniciativas destinadas a fortalecer y profundizar sus conocimientos en ciberseguridad, entre las que se encuentra el lanzamiento de nuevos planes de estudios dirigidos a ciberseguridad.

Ahondando en la oferta en cuanto a estudios de formación profesional, en Euskadi se diferencian dos grados superiores principales, los cuales se imparten en 12 centros de Formación Profesional diferentes:

- Curso de Especialización en Ciberseguridad en entornos de las Tecnologías de la Información.
- Ciberseguridad en Entornos de las Tecnologías de Operación.

Como se ha mostrado previamente, en Euskadi se encuentran establecidos 15 Centros de Formación Profesional, los cuales ofrecen una amplia gama de programas educativos, tanto reglados como no reglados, demostrando así su compromiso con el fortalecimiento del territorio en esta área.

Además, diversas organizaciones complementan esta oferta mediante la provisión de programas de formación no reglada. Un ejemplo destacado es el bootcamp de ciberseguridad, que se realizó por segundo año consecutivo en el centro 42 Urduliz en 2023. Este bootcamp, de modalidad presencial y sin costo alguno, constituye una iniciativa dirigida a satisfacer la demanda laboral y se lleva a cabo en colaboración con expertos de Telefónica Tech. Su objetivo es capacitar a los participantes en habilidades prácticas necesarias para ingresar en una de las industrias de mayor crecimiento en el mercado digital [14].

En el ámbito universitario en Euskadi, las instituciones educativas están realizando esfuerzos significativos para adaptar, mejorar e incorporar nuevos programas relacionados con la ciberseguridad. Euskadi cuenta con 5 universidades, Tecnun, Universidad de Deusto, Universidad EUNEIZ, Universidad de Mondragón y la Universidad del País Vasco (UPV/EHU), quienes están llevando a cabo diferentes iniciativas para fortalecer el entorno profesional del ámbito de la ciberseguridad del territorio, proporcionando estudios relacionados con el sector, dirigidos al ámbito de la ciberseguridad, análisis de datos, computación en la nube y protección de datos.

Asimismo, la recientemente creada Universidad EUNEIZ, lanzó el primer Grado en Ciberseguridad a nivel territorial, evidenciando su compromiso con este campo y la necesidad de desarrollar itinerarios educativos específicos para especializar a los estudiantes de la región y abastecer las necesidades del sector con profesionales capacitados.

Adicionalmente, es relevante destacar que la oferta educativa universitaria en la región de Euskadi exhibe una notable diversidad. Esta variedad no solo refleja el compromiso de diversas entidades académicas por mejorar y adaptarse a las demandas emergentes del sector, especialmente mediante la implementación de nuevos programas en el campo de la ciberseguridad, sino que también resalta la amplia gama de programas de grado en el ámbito STEM disponibles en la región.

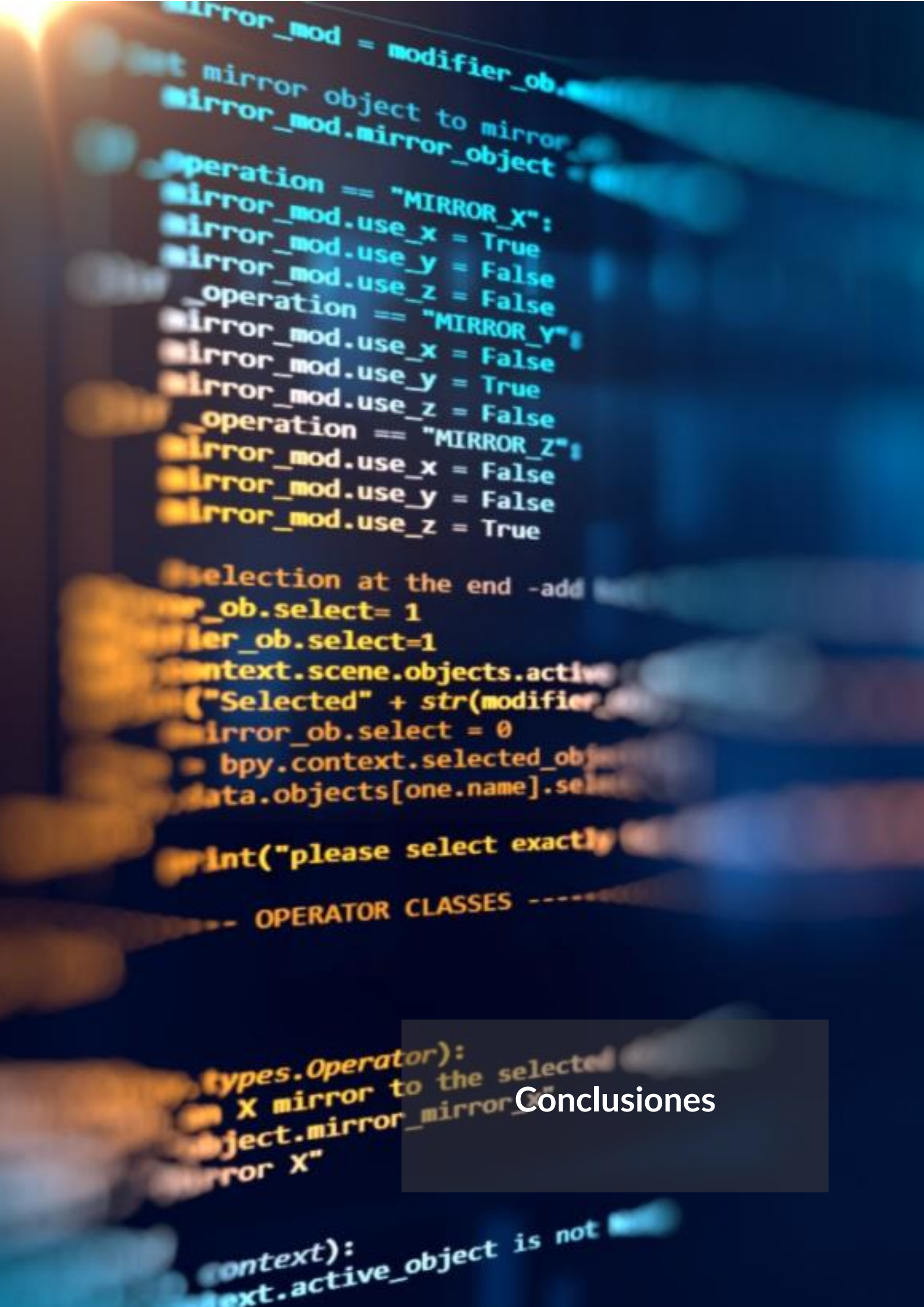
En este sentido, es preciso hablar de la estrategia STEAM Euskadi cuyo objetivo es impulsar la educación y formación científico-técnica en todas las etapas educativas, buscando promover la educación en ciencia y tecnología en todos los niveles educativos [15][16]. Esta estrategia

adquiere especial importancia para la región debido a su estrecha relación con la ciberseguridad.

A parte de la oferta de talento resultante de los egresados, las diferentes organizaciones están valorando el uso de medidas adicionales a la contratación de nuevos talentos, considerando a los empleados existentes mediante técnicas de *reskilling* y de *upskilling*. Medidas de *reskilling* son aquellas utilizadas para formar a los profesionales en el ámbito de la ciberseguridad pese a no estar directamente relacionados con la materia. Por otro lado, las medidas de *upskilling* son aquellas que se dirigen a potenciar la productividad y competitividad de los empleados en sus áreas de trabajo, como en este caso, el campo de la ciberseguridad.

A modo de conclusión, a pesar de la limitada disponibilidad de talento en el territorio de Euskadi hasta la fecha, se anticipa una transformación significativa en los próximos años. Este cambio se encuentra respaldado por el progresivo incremento en la oferta de grados educativos y programas establecidos por diversas entidades educativas.

Asimismo, el compromiso creciente con la formación y el desarrollo de habilidades en la región es evidente, lo que augura un aumento en la disponibilidad de talento local en un horizonte temporal próximo. Es importante destacar que las medidas de *upskilling* y *reskilling*, que están siendo implementadas con mayor fuerza en la región, también contribuirán significativamente a este proceso de transformación. Esta evolución refleja un renovado compromiso con la educación y la capacitación, sentando así las bases para un ecosistema más próspero y competitivo en el contexto de Euskadi.



Conclusiones

Conclusiones

Aumento de agentes de ciberseguridad

Se puede afirmar que en Euskadi existe una amplia diversidad de agentes en el ámbito de la ciberseguridad. Sin embargo, al analizar la cadena de valor, se evidencia una mayor concentración en el sector de servicios en comparación con la fabricación y distribución de productos. A pesar de esta disparidad, se observa una tendencia al alza en la disponibilidad de agentes de ciberseguridad a lo largo del tiempo, lo que subraya la creciente necesidad de expertos en la materia, recalcando la importancia estratégica de fortalecer el ecosistema de ciberseguridad en la región para hacer frente a los desafíos emergentes en este campo crucial.

Brecha de talento

El aumento del uso y la dependencia de las nuevas tecnologías en diversos ámbitos de la sociedad contrasta con la insuficiente cantidad de profesionales especializados en ciberseguridad. Esta disparidad plantea un desafío significativo en términos de protección de datos y seguridad digital. Sin embargo, ante esta creciente demanda, es alentador ver cómo los diferentes centros educativos están tomando medidas proactivas. La introducción de nuevos programas de estudio dirigidos a la ciberseguridad es un paso crucial para enfrentar esta brecha de talento y asegurar que haya profesionales capacitados para abordar los desafíos emergentes en el ámbito de la seguridad informática. Estas iniciativas son fundamentales para garantizar la protección adecuada de la información y los sistemas en un mundo cada vez más digitalizado y conectado.

Necesidad de profesionales cualificados

En un sector cada vez más especializado, se observa la necesidad de perfiles que dispongan de experiencia y certificaciones profesionales que acrediten sus capacidades en materia de ciberseguridad. Por ello, las diferentes organizaciones deben fomentar la formación de sus profesionales y realizar acciones de retención de talento.

Capacitación de los empleados existentes

Ante la falta de nuevos profesionales, las diferentes organizaciones están valorando el uso de medidas adicionales a la contratación, considerando a los empleados existentes mediante por un lado, técnicas de *reskilling* basadas en el reciclaje profesional, en la capacitación de los trabajadores para otro puesto, dotándoles de nuevas habilidades de competencias. Y por otro lado, en técnicas de *upskilling* que se basan en brindar formación a un profesional en nuevas habilidades y competencias que le permiten crecer en su rol actual, mejorando su productividad en el propio puesto.

Bibliografía

[1] Portal de Adjudicaciones TIC (2023). *Inversión TIC de las Administraciones Públicas en Ciberseguridad - H1 2023*. Disponible en: https://documentacion.adjudicacionestic.com/inversion-tic-de-las-administraciones-publicas-en-ciberseguridad-h1-2023/

[2] PwC (2023). *Informe Global Digital Trust 2023 España*. Disponible en: https://www.pwc.es/es/publicaciones/transformacion-digital/global-digital-trust-insights-2023.html

[3] Gobierno Vasco (2021). *Estrategia para la Transformación Digital de Euskadi 2025*. Disponible en: https://bideoak2.euskadi.eus/2021/03/30/news_67948/ETDE2025_Estrategia_ES.pdf

[4] Gobierno de España (2022). *Plan de España Digital 2026*. Disponible en: https://espanadigital.gob.es/sites/espanadigital/files/2022-07/Espa%C3%B1aDigital_2026.pdf

[5] SPRI (2024). *Tercera edición del Libro Blanco.* Disponible en: https://www.spri.eus/es/

[6] RENIC (2023). *Líneas de investigación en Euskadi*. Disponible en: https://renic.es/es/mapa-idi-en-ciberseguridad

[7] Contratación Pública en Euskadi (2023). *Pliegos públicos Euskadi*. Disponible en: https://www.contratacion.euskadi.eus/webkpe00-kpeperfi/es/ac70cPublicidadWar/busquedaAnuncios?locale=es

[8] Eustat (2023). *Empleados TIC en los establecimientos de la C.A. de Euskadi por territorio histórico, rama de actividad (A3) y estrato de empleo (%).* Disponible en: https://www.eustat.eus/elementos/ele0016600/empleados-tic-en-los-establecimientos-de-la-ca-de-euskadi-por-territorio-historico-rama-de-actividad-a3-y-estrato-de-empleo-/tbl0016641_c.html

[9] 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

[10] ObservaCIBER (2022). *Análisis y diagnóstico del talento de ciberseguridad en España.* Disponible en: https://www.observaciber.es/sites/observaciber/files/media/documents/EstudioDiagnosticoTalento2022.pdf

[11] Eustat (2023). *Alumnado que finalizó sus estudios de grado en las universidades de la C.A. de Euskadi por rama de estudios y titulación, según territorio histórico y sexo.* Disponible en: https://es.eustat.eus/elementos/ele0003200/ti_Alumnado_que_finalizo_sus_estudios_de_grado_en_las_universidades_de_la_CA_de_Euskadi_por_titulacion_segun_territorio_historico_y_sexo_201718/tbl0003210_c.html

[12] Eustat (2023). *Alumnado matriculado en Formación Profesional en la C.A. de Euskadi por grado y familia profesional, según territorio histórico y sexo.* Disponible en: https://www.eustat.eus/elementos/ele0000000/alumnado-matriculado-en-formacion-profesional-en-la-ca-de-euskadi-por-grado-y-familia-profesional-segun-territorio-historico-y-sexo-202122/tbl0000096_c.html

[13] Eustat (2023). *Alumnado matriculado en Formación Profesional en la C.A. de Euskadi por*

grado y familia profesional, según territorio histórico y sexo. Disponible en: https://www.eustat.eus/elementos/ele0000000/alumnado-matriculado-en-formacion-profesional-en-la-ca-de-euskadi-por-grado-y-familia-profesional-segun-territorio-historico-y-sexo-202122/tbl0000096_c.html

[14] 42 Urduliz Bizkaia Fundación Telefónica. *Apúntate a nuestro Bootcamp de Ciberseguridad*. Disponible en: https://www.42urduliz.com/actualidad/apuntate-a-nuestro-bootcamp-de-ciberseguridad/

[15] STEAM Euskadi (2022). Disponible en: https://steam.eus/es/

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

Paseo Uribitarte, 3 - 3º

48001 – Bilbao

COPYRIGHT © ASOCIACIÓN DE INDUSTRIAS DE CONOCIMIENTO Y TECNOLOGÍA APLICADA (GAIA)