OBSERVACIBER

ANÁLISIS Y DIAGNÓSTICO DEL TALENTO DE CIBERSEGURIDAD EN ESPAÑA

Marzo 2022

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

ontsi

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

OBSERVACIBER

ÍNDICE

1_ INTRODUCCIÓN

El mundo digitalmente conectado se sigue expandiendo rápidamente y el viaje hacia la transformación digital continúa hoy más que nunca. Ni siquiera el reciente evento de **la pandemia global de COVID-19 ha ralentizado la transformación digital**, de hecho, ha forzado a los gobiernos y organizaciones a buscar la adopción de tecnologías digitales para garantizar el servicio a los ciudadanos y la continuidad de los negocios.

La necesidad de desplegar nuevas tecnologías y capacidades que den respuesta a las tendencias empresariales actuales ha suscitado riesgos cada vez más latentes, y se debe reconocer que **estamos en un entorno complejo** para las instituciones públicas y privadas, **con ciberataques cada vez más sofisticados** que ponen en riesgo el bienestar de toda la sociedad.

Al considerar los riesgos políticos, sociales y económicos a los que estamos expuestos, se espera que **la seguridad tenga un rol fundamental en todas las iniciativas de transformación digital** y los planes de inversión en tecnología de los próximos años. En este sentido, la capacidad de proteger las infraestructuras críticas y la integridad de las empresas y ciudadanos se ha convertido en uno de los principales retos de los gobiernos.

España tiene actualmente **una apuesta decidida por la ciberseguridad**, que busca responder a las diferentes amenazas implícitas en la era de la disrupción tecnológica. La colaboración público-privada y el apoyo de una ciudadanía consciente y con cultura de la ciberseguridad es aparentemente el camino idóneo para atender los distintos retos y desafíos en esta época de secuelas económicas, políticas y sociales que afronta el país.

Existe entonces un compromiso de desarrollar y emprender una estrategia inclusiva que permita alcanzar la resiliencia en el espacio cibernético, y a su vez la prosperidad y confianza de las instituciones públicas y privadas en el mundo digital. A través de organismos como INCIBE (Instituto Nacional de Ciberseguridad) se ha alcanzado un significativo progreso para **ayudar a proteger la infraestructura crítica y los servicios al ciudadano de ciberataques**, a gestionar incidentes a gran escala, a promover el talento y las capacidades en un amplio espectro y a mejorar la seguridad a la que se está expuesto por naturaleza en el ciberespacio.

1.2_ La importancia del talento en ciberseguridad

En 2021, los datos de este estudio señalan que España había alcanzado **una fuerza laboral en ciberseguridad cercana a los 149.774 trabajadores** con una brecha de talento estimada en **26.024**. En consecuencia, una de las mayores prioridades que tiene la administración actualmente es hacerle frente al reto de identificar, atraer, desarrollar, y retener el talento en los diversos campos de la ciberseguridad

Prueba de este compromiso es el desarrollo de la **Estrategia Nacional de Ciberseguridad 2019** del gobierno español, que enfatiza en la nece-

sidad no solamente de tener una postura de defensa y protección para las empresas y ciudadanos, sino de apoyar el impulso de la industria cibernética. Por otra parte, el **Plan España Digital 2025** busca reforzar las palancas que faciliten volver a la senda de crecimiento de la economía, y presenta como uno de sus ejes estratégicos reforzar la capacidad española en ciberseguridad para mitigar los riesgos e incrementar la confianza en el camino hacia una economía digital y sostenible.

Estas iniciativas nacionales generan un escenario adecuado que favorece la investigación, la innovación, e involucra a los agentes más relevantes de la cadena de valor, como las instituciones educativas y las organizaciones, para que vean el beneficio de gestionar los conocimientos, capacidades y experiencias tecnológicas que respondan a los grandes retos que tiene el país en materia de ciberseguridad.

Una estrategia significa actuar, y para poder actuar con decisión se necesita de conocimiento. En este sentido, **INCIBE ha puesto en marcha un proceso de análisis y diagnóstico del talento en ciberseguridad en España**, en línea con su Plan Estratégico 2021-2025, que sitúa la promoción y detección de talento en ciberseguridad como un objetivo estratégico e identifica la generación de conocimiento sobre ciberseguridad —a través de la investigación y el estudio de realidades concretas— como una línea de actuación clave dentro de otro de sus objetivos estratégicos: la promoción de una cultura de ciberseguridad.

Con el objetivo de ofrecer una visión clara del talento en ciberseguridad en España, INCIBE publica los resultados de este análisis, cuyo proceso se ha llevado a cabo mediante premisas de rigurosidad analítica, enfoque global de trabajo y procesos participativos e integradores que han tenido en cuenta a los principales actores del ecosistema de ciberseguridad.

2_ OBJETIVOS Y ALCANCE DEL ESTUDIO.

El objeto del presente informe es la elaboración de un completo diagnóstico del estado actual del talento en el sector de la ciberseguridad en España, así como unas recomendaciones donde se definan métricas, procedimientos y metodologías para atajar los problemas detectados y que sirvan como líneas base para las actuaciones a poner en marcha a continuación.

El proyecto persigue el cumplimiento de los siguientes objetivos:

Identificación de buenas prácticas internacionales de gestión de talento en ciberseguridad

Cuantificar y segmentar (incluyendo la caracterización) la fuerza laboral actual de profesionales de la ciberseguridad en España y la demanda existente

Caracterizar la fuerza laboral requerida en ciberseguridad y estimar la brecha actual de España

Definir los escenarios de intervención para cada tipología de profesionales de la ciberseguridad identificados

Identificar y consensuar con el ecosistema de la cadena de valor de ciberseguridad, recomendaciones a corto, medio y largo plazo.

Figura 1. Objetivos del proyecto

Para el desarrollo del trabajo se ha complementado el trabajo de gabinete con el uso de las siguientes metodologías participativas:

- **Previstas 30 → 34 realizadas**
  - Se han considerado todos los agentes que de alguna u otra manera participan y tienen relevancia en la cadena de valor o el ecosistema de la ciberseguridad

Focus Groups

- **Realizados 6 focus groups con agentes releventes en cada temática**
  - Presencia femenina en ciberseguridad
  - Gestión y retención de talento de ciberseguridad
  - Análisis del problema de escasez de profesionales de ciber
  - Formación autodidacta
  - La ciberseguridad en los distintos niveles educativos
  - Colectivos con potencial de reciclaje hacia la ciberseguridad

Encuestas

- **+1000 encuestas on-line totalmente completadas**
- **Muestra y distribución:**

OFERTA: Previstas 240 → 748

- Demandantes de empleo (30%)
- Estudiantes (45%)
- Trabajadores en activo (45%)

DEMANDA: Previstas 360 →399

- Empresas de recruiting (5%)
- Organismos extendidos de soporte (10%)
- Empresa privada (65%)
- *Start-ups* (10%)

El análisis y diagnóstico del talento en ciberseguridad pretende sentar las bases para asegurar que España tenga una industria de la ciberseguridad bien estructurada y que la profesión sea ampliamente entendida y aceptada. El ecosistema de profesionales, empresas de la industria, asociaciones, autodidactas, academia y sector público deben representar, apoyar e impulsar la excelencia en las diferentes especialidades de la ciberseguridad para que esta sea una industria sostenible que aporta al país.

El plan de acción y las iniciativas que deriven del proyecto permitirán que España refuerce los sistemas de educación y capacitación para que los componentes básicos de enseñanza ayuden a formar y motivar el talento de ciberseguridad en las instituciones académicas y en las organizaciones.

Una definición clara del panorama del talento de ciberseguridad es un factor determinante para posicionar a España como un jugador relevante en la industria de la ciberseguridad a nivel europeo. Fortalecer la industria es un esfuerzo que permitirá un reconocimiento que atraiga los mejores talentos y se puedan desarrollar capacidades distintivas de las cuales toda la sociedad se podrá beneficiar.

3_ ANÁLISIS DE LA INDUSTRIA DE CIBERSEGURIDAD

La digitalización está redefiniendo el futuro de economías, industrias y sociedades tal como las conocemos. La creciente demanda de mayor agilidad, velocidad y flexibilidad marca el inicio de una nueva generación de empresa más distribuida y conectada. Ello requiere transformarse en una organización ágil que utilice modelos de negocio rentables y adaptados de una manera rápida y continua a la dinámica del mercado

En el ámbito específico de las empresas, este proceso va más allá de la simple oferta de sus productos a través de la web. Los cambios disruptivos asociados a tecnologías digitales abarcan desde la gestión de los datos, a la optimización de procesos mediante automatización, la predicción de la demanda o la mejora y particularización de la experiencia de compra del cliente.

En este escenario, la seguridad está siendo una palanca esencial debido a varios factores:

Crecimiento exponencial de los datos. Estamos asistiendo a un crecimiento exponencial en la creación de datos en el universo digital y las organizaciones deben estar preparadas para proteger esta cantidad enorme de datos que se generan a diario. Se espera que el total de estos datos alcancen los 180 Zettabytes, en 2025, lo que supone una tasa anual de crecimiento compuesta del 23% desde 2020. Para poner ese número en perspectiva, podemos decir que la cantidad de datos creados en los próximos tres años será mayor que los datos creados en los últimos 30 años.

El crecimiento de las operaciones digitales en las empresas. La importancia creciente de la seguridad como vector de desarrollo del negocio (el número de operaciones digitales ha crecido en 2020 un 40% respecto del año anterior) y la necesidad de securizar los datos está impulsando la adopción de nuevos modelos y arquitecturas de seguridad que permitan hacer frente a este cambio de paradigma y lograr la resiliencia digital que se requiere.

Incremento de ciberamenazas. Cada vez existen más amenazas de todo tipo, que son altamente sofisticadas, sigilosas y evasivas, por lo que requieren de mayor diversidad de defensas, y la razón por la cual las organizaciones buscan mejorar la seguridad de su infraestructura de red y recibir servicios avanzados de asesoramiento para proteger adecuadamente sus organizaciones.

El teletrabajo, impulsado por la pandemia de la COVID-19, ha difuminado las fronteras de la ciberseguridad en las organizaciones, lo que requiere del uso de tecnología y soluciones que permitan securizar no solo los datos.

Por tanto, en este epígrafe se analiza la composición de este mercado, principales categorías tecnológicas que impactan en el mismo, así como las tendencias más relevantes desde el punto de vista de la tecnología y su impacto en los diferentes sectores productivos, donde el impacto se hace evidente en las organizaciones y perfiles profesionales.

3.1_ La industria de la ciberseguridad en cifras

Todos estos factores impulsan el mercado de la ciberseguridad en España, que alcanzó en 2020 casi los 1.500 millones de euros y que, según datos de IDC, alcanzará los 2.000 millones de euros en 2024, creciendo a una tasa de crecimiento anual compuesto del 8,12%, tal y como muestra la figura.

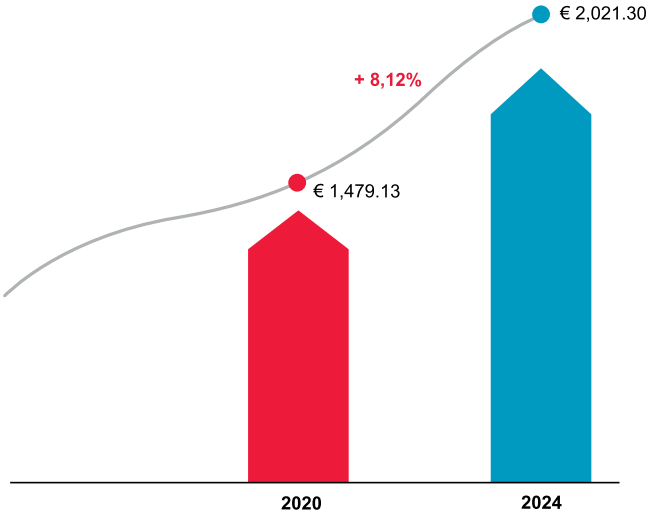


Figura 3. Tamaño de mercado de la seguridad (en M€). Fuente: Security Spending Guide IDC 2021

Si analizamos el mercado en función del grupo de tecnologías (*hardware*, *software* y servicios), el mercado de *hardware* es el de menor tamaño y el que previsiblemente menor crecimiento tendrá en el periodo 2021-2024 (CAGR de 4,6%), en comparación con el de *software* y servicios (8,3% y 8,8% respectivamente), fundamentalmente debido al proceso de sustitución de este tipo de productos *hardware* por *software*, que abarata costes y está alineado con las necesidades actuales que impone el trabajo en remoto. Por citar algún ejemplo, la autenticación multifactor va integrada ahora con el dispositivo móvil como *software*, mientras que antes era necesario llevar un dispositivo adicional para verificar la identidad del usuario.

Por otro lado, el mercado de servicios es a su vez, el de mayor volumen y el que más va a crecer, en parte debido a la necesidad de las empresas de asesoramiento para protegerse de las múltiples amenazas que van en auge, así como de soluciones a medida que entran dentro del grupo de servicios.

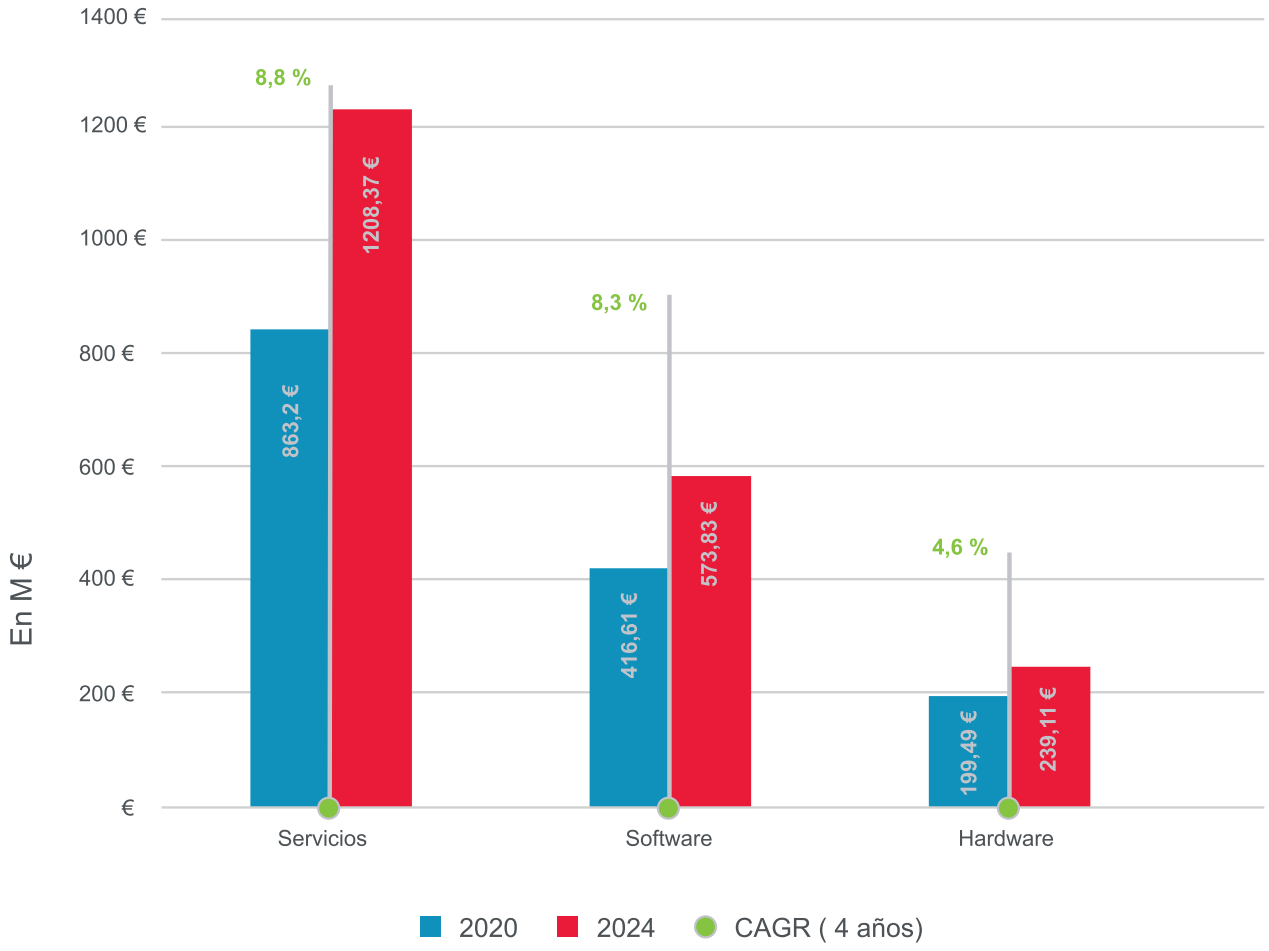


Figura 4. Tamaño de mercado por grupo de tecnología. Fuente: Security Spending Guide IDC 2021

La importancia de la ciberseguridad es transversal a todos los sectores de la economía, puesto que la incorporación de la digitalización en los mismos está favoreciendo un crecimiento del mercado de la ciberseguridad. Según datos de mercado de IDC, el mercado de la ciberseguridad en los diferentes sectores productivos experimentará un crecimiento en el periodo 2021-2024, tal y como muestra la figura.

Distribución y servicios, el sector financiero e industria y recursos serán aquellas industrias que van a experimentar un mayor impulso. Sin embargo, el sector público junto con el sector de distribución y servicios serán los sectores que más crezcan en materia de ciberseguridad con un CAGR de 8,8% respectivamente. La tasa anual de crecimiento compuesto del sector infraestructura (energía y telecomunicaciones) ascenderá un 8,7%.

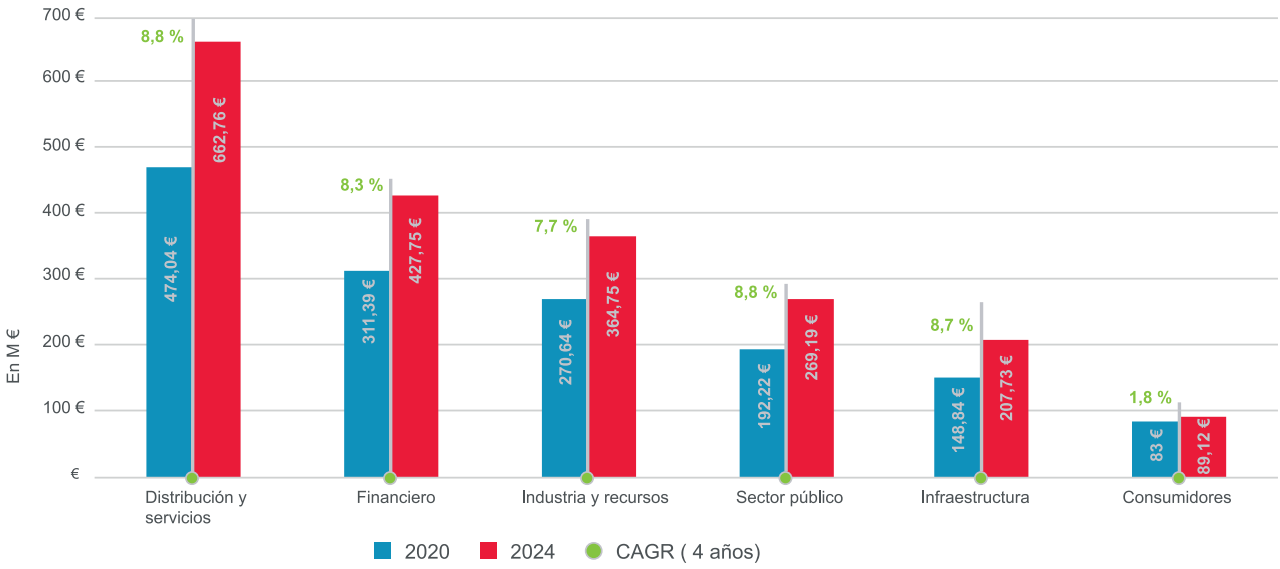


Figura 5. Tamaño de mercado de la ciberseguridad por sectores – Fuente: Security Spending Guide IDC 2021

3.2_ Tendencias del mercado de la ciberseguridad y el impacto en otras industrias.

El mercado de la ciberseguridad, tanto en volumen como en configuración de servicios y talento, se ha visto impactado por una serie de tendencias que están configurando un nuevo escenario con impacto en el resto de las industrias productivas. Por citar algunos aspectos significativos, nos referimos a como la pandemia de COVID-19 ha afectado a la demanda de servicios digitales. Asimismo, el crecimiento exponencial de los datos y auge del análisis de estos por parte de las organizaciones está impulsando la demanda de profesionales que hagan seguro este nuevo universo digital.

Por otra parte, otra tendencia destacada es la creciente importancia de la privacidad de los datos, muy especialmente en el ámbito europeo y por tanto el impacto que la normativa asociada tiene en todo el ecosistema de la ciberseguridad. El trabajo en remoto que se popularizó con la crisis pandémica es otro aspecto a analizar en este entorno.

Impacto de la pandemia de la COVID-19 en la demanda de servicios digitales

La pandemia del COVID-19 ha supuesto indudablemente un impulso a la digitalización de las organizaciones al forzar a la ciudadanía a interactuar por canales digitales con empresas y administraciones públicas.

Crecimiento exponencial de los datos y auge de las Data Driven Companies

Los datos han cambiado la forma en que somos educados y entretenidos, y en este contexto de digitalización se transforman en el alma de lo que podemos definir como nuestra existencia digital.

Privacidad de los datos y el impacto de la normativa GDPR

No sólo se debe proteger el dato, sino establecer mecanismos de protección antes, durante y después de las amenazas, lo que requiere que las organizaciones cuenten con diferentes herramientas para cumplir con la regulación (GDPR).

Trabajo en remoto

Las empresas convertirán los programas de transformación del puesto de trabajo en una prioridad de inversión en los próximos dos años.

3.3_ Contexto del estado actual del talento de ciberseguridad en España

España tiene actualmente una apuesta decidida por la ciberseguridad, que busca responder a las diferentes amenazas implícitas en la era de la disrupción tecnológica. La colaboración público-privada y el apoyo de una ciudadanía consciente y con cultura de la ciberseguridad es aparentemente el camino idóneo para atender los distintos retos y desafíos en esta época de secuelas económicas, políticas y sociales que enfrenta el país.

El gap de la fuerza laboral en ciberseguridad es una problemática de la que España no se salva. Lo cierto es que **el deseequilibrio entre oferta y demanda de profesionales es algo de lo que adolecen en la actualidad todos los países que han sido parte de este estudio.** Cabe resaltar que la estimación del gap es un ejercicio complejo y varía en función de la metodología empleada y otros factores, incluso países como UK, se han enfocado más allá del número en tratar de comprender mejor la naturaleza y los matices de la oferta y la demanda para darse una imagen más completa de dónde se percibe el *gap*.

Ahora bien, **los profesionales de la ciberseguridad en España son valorados a nivel internacional**, pero el **reto de identificar, atraer, nutrir, desarrollar, y retener el talento** en los diversos campos de la ciberseguridad requiere de un alto compromiso por parte de las Administraciones Públicas y esto una de las principales prioridades en España.

Prueba de esto es el desarrollo de la Estrategia Nacional de Ciberseguridad 2019 del gobierno español, que enfatiza la necesidad no solamente de tener una postura de defensa y protección para las empresas y ciudadanos, sino de apoyar el impulso de la industria cibernética. En este sentido, cabe destacar otras iniciativas:

INCIBE emprende: programa para emprendedores y *start-ups* de ciberseguridad dotado con 191 millones de €. El programa tiene entre sus objetivos el apoyo a la creación de nuevas empresas en el ámbito de la ciberseguridad, la internacionalización de *start-ups*, el impulso de la innovación y la atracción de la inversión.
https://www.incibe.es/sala-prensa/notas-prensa/incibe-emprende-el-nuevo-programa-emprendedores-y-start-ups-ciberseguridad

National Cyberleague, Guardia Civil: En el marco del objetivo IV de la estrategia de ciberseguridad nacional, esta iniciativa (por ediciones) de la Guardia Civil reúne talentos de diferentes niveles de España y otros países alrededor de una serie de pruebas (hacking ético, jurídico, comunicación, etc) en las que los participantes asumen unos desafíos y demuestran sus capacidades. Este es un mecanismo que permite identificar talentos con potencial en ciberseguridad. Además, es un escenario ideal para compartir con otras personas de la industria, compartir conocimientos y experiencias con el objetivo de acercas a los jóvenes a las empresas y a las instituciones públicas.
https://www.nationalcyberleague.es/

Comenzamos con Ciberseguridad, INCIBE: Este es un recurso educativo para que los menores hagan un uso seguro de Internet desde edades tempranas (5 a 8 años). De esta manera se pretende que los más pequeños tomen un primer contacto con la ciberseguridad, aprendan a utilizar las tecnologías de forma segura y positiva y eviten riesgos. Esta es una iniciativa que responde al hecho de que los menores desde muy temprana edad están en contacto con el mundo digital, y por consiguiente hay riesgos que deben mitigarse.
https://www.incibe.es/sala-prensa/notas-prensa/incibe-acerca-ciberseguridad-ninos-5-8-anos-mediante-nuevo-recurso

Internet Segura for Kids (IS4K): Es el centro de seguridad en internet para menores de edad, y su objetivo principal es la promoción del uso seguro y responsable de Internet y las nuevas tecnologías entre los niños y adolescentes. Esta iniciativa provee múltiples recursos para diferentes audiencias, entre ellos destaca las plataformas que ponen a disposición de los educadores para sensibilizar y educar a este grupo y que ellos a su vez puedan transmitir ese conocimiento en ciberseguridad a los estudiantes.
https://www.is4k.es/educadores

A través de estas medidas e iniciativas España quiere consolidar un ecosistema de ciberseguridad dinámico, que se adapta a diferentes casuísticas, responde a diferentes amenazas y desafíos, e incrementa la autonomía tecnológica. Esto se logra a través del despliegue de iniciativas de I+D+i, la gestión del talento y un modelo de gobernanza en el que participa activamente el sector privado y la población civil.

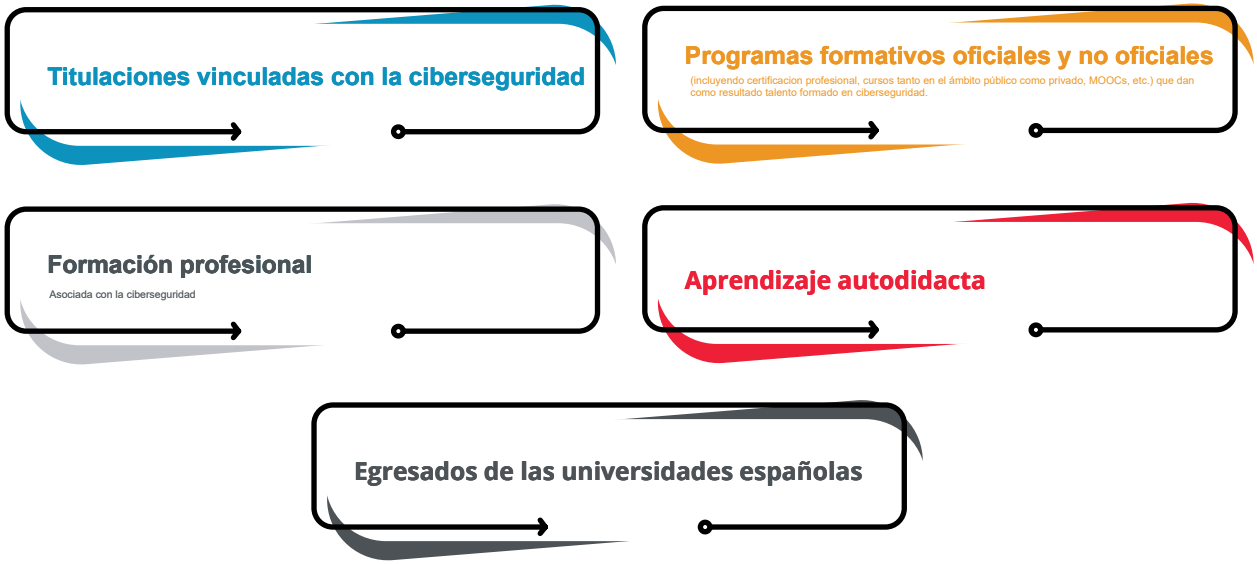
4_ DIAGNÓSTICO DEL TALENTO EN CIBERSEGURIDAD EN ESPAÑA.

4.1_ Caracterización de la oferta de talento en ciberseguridad

4.1.1_ Análisis cuantitativo de la oferta de talento en ciberseguridad

Cuando nos referimos a oferta de talento en ciberseguridad, nos referimos a todas aquellas actuaciones orientadas a generar talento capacitado para poder acometer una posición o perfil de ciberseguridad, tanto a nivel técnico como de gestión.

En este caso, nos referimos a los resultados del análisis de:



De esta forma, es posible establecer un escenario de oferta de talento de ciberseguridad que se traduzca en una primera aproximación al análisis actual de generación de talento de ciberseguridad del sistema educativo de España.

Nos encontramos en la actualidad en un momento en el que están emergiendo nuevos trabajos, profesiones en el mundo digital que requieren de un conocimiento exhaustivo de ciberseguridad. Esto tiene su traslado en la necesidad de un incremento en la cantidad y calidad de la formación en este ámbito.

A este hecho debemos unir que la formación es sin duda una de las grandes prioridades dentro del marco del Plan de Competencias digitales, el Plan de Digitalización de Pymes 2021-2025 y el Plan España Digital 2025. Al igual que la necesidad de talento en ciberseguridad ha evolucionado enormemente en estos últimos años, la estructura de la formación también debe hacerlo tanto en su parte central como en la parte de especialización, es decir, más allá de dar una formación sólida que sirva de base para que los profesionales se especialicen, debemos ser capaces como sociedad de adecuar los contenidos a las necesidades de las organizaciones.

Para estimar la oferta de perfiles de ciberseguridad, la literatura recoge como método de medida fundamentalmente la revisión de la generación del nuevo talento de ciberseguridad proveniente de aquellas personas que realizan formación reglada o no reglada en dicho campo. Sin embargo, utilizar únicamente esta cifra incorporaría sesgo en el resultado, ya que cuando estamos considerando la generación de talento en ciberseguridad es necesario tener en cuenta no solo la generación de nuevo talento, sino también el reciclado del talento existente (y que ocupa posteriormente posiciones de ciberseguridad en las organizaciones).

Por tanto, la oferta total de talento de ciberseguridad se calcula como la suma de los siguientes indicadores:

Volumen total de oferta de talento de ciberseguridad que el propio sistema es capaz de generar funcionando a pleno rendimiento. Asumiendo que cada plaza que se ocupa para formar a una persona se traduce directamente en la ocupación de un puesto en el ámbito de la ciberseguridad.

Volumen de personal existente en las organizaciones que se recicla hacia posiciones de ciberseguridad. Este dato se obtiene directamente de la encuesta realizada al lado de la demanda de talento de ciberseguridad y muestra la estimación del número de vacantes de ciberseguridad que se cubren mediante talento propio de la organización, tras realizar los ajustes correspondientes.

A efectos de minimizar el sesgo introducido, será necesario realizar los siguientes ajustes al modelo:

Para los cálculos se tomará como base la tasa neta de escolarización en Educación Universitaria que considera el Ministerio de Educación, y que se sitúa en el 31,5%.

Las titulaciones que, de manera general, están relacionadas con el talento de ciberseguridad y que son: Matemáticas, Ingeniería de Informática y Telecomunicaciones. Por ello, se introduce un porcentaje de ajuste al número de plazas totales ofertadas por el Ministerio de Educación en todas las Universidades Españolas, y que se obtiene directamente del SIIU (Sistema Integrado de Información Universitaria).

Tendencia de crecimiento o decrecimiento en el número de matriculados en el ámbito universitario. A pesar de que existe un decrecimiento en el número de matriculados en grados universitarios, la realidad es que estos estudios universitarios han recibido en los últimos años más preinscripciones que plazas disponibles. De hecho, en el año 2020 los estudios de Ingeniería Informática recibieron un total de 16.022 peticiones de inscripción como primera opción en España, según los datos del Ministerio de Universidades. Sin embargo, según esta misma fuente, splo el 60% de ellos pudo finalmente matricularse, por lo que no asumiremos en el cálculo ningún factor de ajuste debido a posibles pérdidas de matriculaciones.

Número de plazas disponibles. El número de plazas disponibles para estudiar Ingeniería Informática o de Telecomunicaciones tampoco ha sido modificado de manera sustancial durante los últimos 10 años (el último de ellos con formación mixta presencial y virtual debido al impacto de COVID-19), por lo que, a efectos del cálculo de la situación actual de oferta, no requiere de incorporación de ningún ajuste adicional.

El talento de oferta en ciberseguridad en España por tanto se calcula siguiendo la siguiente ecuación:

Oferta de talento ciberseguridad=Oferta del sistema+Oferta personal reciclado

Dónde:

$$Oferta\ del\ Sistema = \sum Oferta\ en\ diferentes\ grados\ formativos$$

Esto es, número de nuevos Graduados Universitarios, de Formación Profesional y de másteres (oficiales y no oficiales), teniendo en cuenta las diferentes convocatorias que se realizan a lo largo del año.

Teniendo en cuenta por tanto los diferentes cálculos realizados en cada uno de los diferentes factores que inciden en la generación de talento, la oferta total del sistema sería la siguiente:

$$Oferta\ del\ Sistema = Nº\ Graduados + Nº\ alumnos\ de\ Master + Nº\ alumnos\ FP$$

El número de graduados se calcula partiendo del total de matriculaciones en las principales carreras técnicas que, a juicio de la muestra consultada y los expertos entrevistados, dan lugar a talento formado en ciberseguridad (Matemáticas, Ingeniería Informática y de Telecomunicaciones). Según los datos del Ministerio de Educación el número de matriculados en el curso 2020-2021 ascendió a 132.007 en el total de ingenierías, y de 17.379 en Matemáticas y Estadística[1]. Asimismo, otras fuentes de información publicadas indican que las matriculaciones en informática y telecomunicaciones ascienden a las 20.000 en España en el año 2020, por lo que **se utilizará como ratio que el 15% de las matriculaciones en ingeniería, se producen en estas dos carreras**. En el caso de las carreras de matemática y estadística, existe una mayor adopción de la primera sobre la segunda, por lo que **se asume una ratio del 60% de las matriculaciones de dichas carreras como generación de talento anual**.

Esto totaliza un volumen de talento total de **30.427** personas.

Una vez calculada la generación de nuevo talento a través del circuito formativo (reglado y no reglado), para calcular la oferta total es necesario ajustar esta cifra con el número de profesionales que, estando actualmente en activo en las organizaciones, se están reciclando para ocupar posiciones de ciberseguridad.

Para hacer el cálculo de dicha cifra, es necesario acudir a la encuesta realizada al lado de la demanda de talento de ciberseguridad en el proyecto, y que arroja los siguientes resultados.

1 https://public.tableau.com/views/Academica20_EEU/InfografiaEEU?%3AshowVizHome=no&%3Aembed=true#7

la estimación de la oferta de talento formado en ciberseguridad ascendería a 39.072 personas

El **40,1% de las organizaciones consultadas** reconoce que ha **reciclado talento proveniente de otros departamentos** para el área de ciberseguridad.

De estas organizaciones, **el 52% reconoce que cubre entre el 10% y el 25% de las posiciones abiertas en ciberseguridad**. Tomando como base la media de las vacantes que se cubren, arroja una cifra del **15,7%**.

De esta manera, **la estimación de la oferta de talento formado en ciberseguridad ascendería a 39.072 personas.**

Proyección de la oferta

Teniendo en cuenta el proceso de implantación de los Cursos de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información de FP, la ratio en las CC.AA de 25 alumnos por clase, un mantenimiento tanto de los programas formativos como de las plazas en las carreras universitarias únicamente sería necesario considerar el crecimiento del talento reciclado en las organizaciones.

Asumiendo los mismos datos que los que se han obtenido en la encuesta realizada, la proyección de la oferta de talento en los próximos años es como sigue:

	2021	2022	2023	2024
Total	39,072	41,123	41,677	42,283

Tabla 1. Proyecciones de oferta de talento en ciberseguridad en España.

ANALISIS CUALITATIVO DE LA OFERTA

Una vez hecho el análisis cuantitativo de la oferta de talento en ciberseguridad, cabe preguntarnos qué características o cualidades específicas tiene esta oferta en España.

Para este propósito se plantea abordar el estudio del escenario actual desde el punto de vista cualitativo destacando potenciadores y limitadores de esta oferta de talento de ciberseguridad.

4.1.1.1_ Potenciadores

Aprendizaje autodidacta en el sector de la ciberseguridad.

La autoformación puede ser abordada como una alternativa a la formación reglada, sin embargo, en la mayor parte de los casos se enfoca como un complemento o potenciador de la misma. Este complemento puede ser simultáneo a la formación reglada, un paso previo a la misma, es decir, una manera de aumentar el interés o la vocación en el ámbito de la ciberseguridad, accediendo posteriormente a una formación reglada. Finalmente, también se puede enfocar como un paso posterior o una manera de continuar formándose en un mundo tan volátil y cambiante como el de la ciberseguridad.

Lo que es innegable es que supone una herramienta potente para generar conocimiento o experiencia, algo que cada vez tiene más extensión entre la oferta de talento en ciberseguridad como se puede apreciar en la figura.

Figura 11. ¿Cómo ha adquirido los conocimientos y competencias en seguridad?

Podríamos resumir las distintas posibilidades para autoformarse e iniciarse en el mundo del *hacking* y de la ciberseguridad agrupándolas en foros, MOOC, cursos presenciales, *bootcamps*, tutoriales online, autoformación con libros y asistencia a ferias.

Respecto a las preferencias de unos métodos autodidactas sobre otros, cabe destacar que todos ellos presentan un elevado índice de aceptación, pero destacan principalmente los eventos y conferencias, así como

los sitios para practicar y aprender *hacking* como podemos apreciar en la figura. La oferta de todos ellos en la actualidad en España es elevada y los datos confirman que no tenemos nada que envidiar a nuestros comparables europeos tanto en la calidad como en la cantidad de oferta autodidacta.

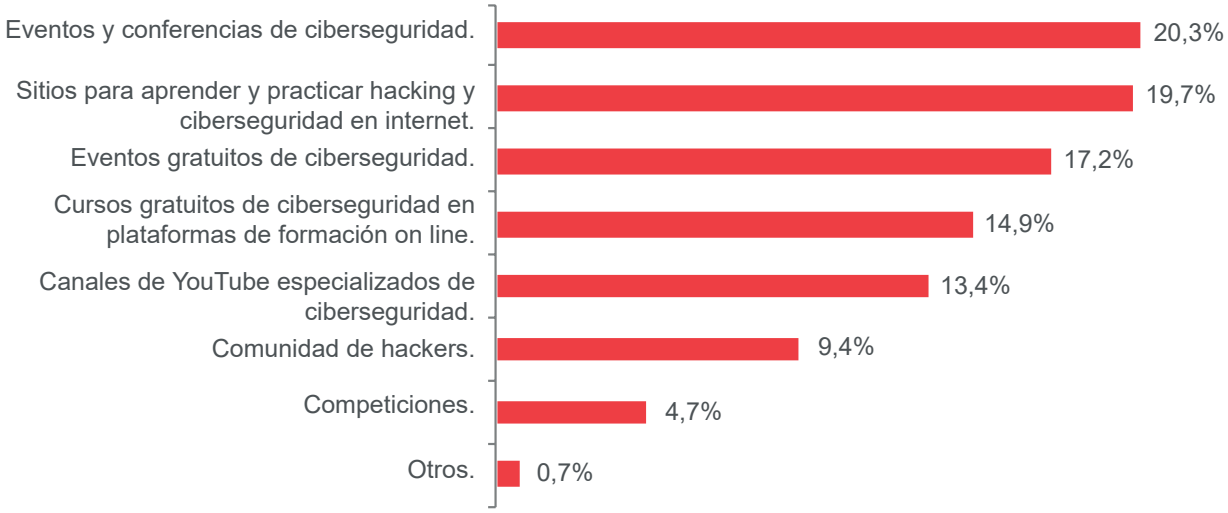


Figura 12. Opciones preferidas para desarrollar competencias y conocimientos de manera autodidacta

4.1.1.2_ Limitadores

Escasez de profesorado

Es cierto que existe una tendencia creciente en relación con la oferta formativa en materia de ciberseguridad en España, tanto de pago como gratuita, reglada y no reglada que cubre todo el espectro de trabajo asociado a la ciberseguridad. No obstante, no es menos cierto que la oferta total no cubre las necesidades globales del sector en cuanto a necesidad de talento.

Uno de los problemas principales detectados en este sentido tiene que ver con la escasez de profesorado cualificado para impartir formación en ciberseguridad, añadiendo la falta de competencias docentes del profesorado, ya que no todos los profesionales que imparten cursos de ciberseguridad las tienen, ni tampoco certificaciones o experiencia docente. Este problema deriva en una posterior escasez de oferta de formación, por lo que se hace necesario estructuras estables de formación de docentes que erradiquen este problema de raíz.

Diferencia por género

Del total de estudiantes especializándose en materia de ciberseguridad, únicamente el 18% corresponde a alumnas lo que hace presagiar que la gran diferencia por género entre el número de profesionales en el mundo de la ciberseguridad va a continuar manteniéndose.

Respecto a las iniciativas que posibilitarían incrementar la presencia de mujeres en posiciones de ciberseguridad, destacan los programas de impulso de mujeres en investigación como se aprecia en la figura, aunque se pone de manifiesto la necesidad de implementar programas a medidas con orientación de género de manera que se potencie la presencia femenina en estas disciplinas.

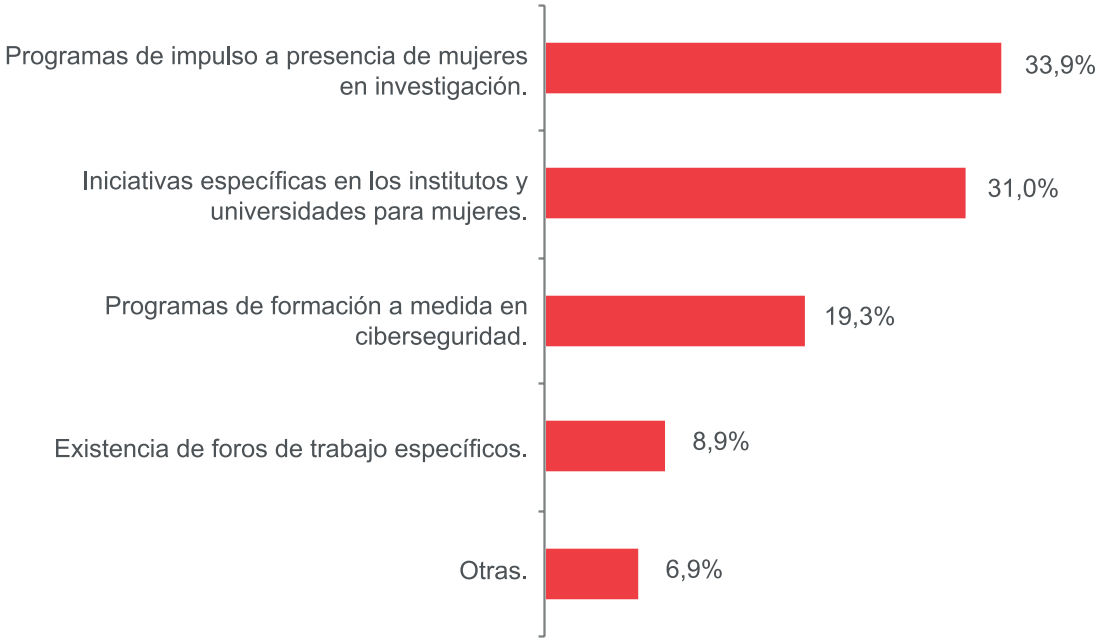


Figura 13. Iniciativas que ayudarían a incrementar la presencia de mujeres en posiciones de ciberseguridad

Importancia de la gestión de vocación hacia la ciberseguridad y la divulgación de los pasos formativos necesarios para acceder al mercado

Uno de los principales problemas detectados durante todo el trabajo de investigación y tras interactuar con los diferentes actores que forman parte del ecosistema de la ciberseguridad en España es la escasez de vocaciones tempranas. Un segundo hándicap y muy relacionado con el anterior es la escasa divulgación de los pasos formativos necesarios para acceder al mercado.

Para cuantificar este último punto, basta resaltar que un 37% de los encuestados declaran tener poco claro o nada claro las habilidades, itinerario formativo y cualificación que deben tener para dedicarse a la ciberseguridad.

Respecto a las causas de la falta de claridad en este itinerario formativo, podemos afirmar que existe desconocimiento, tanto de los perfiles necesarios como de los conocimientos demandados por parte de las empresas (incluso a veces las propias empresas tampoco tienen claridad sobre los perfiles que realmente necesitan). Este último punto está asociado, además, con otro aspecto relevante que es la demanda de conocimientos y capacidades por parte de la industria que no se incluyen dentro de la formación reglada, como vemos en la figura siguiente.

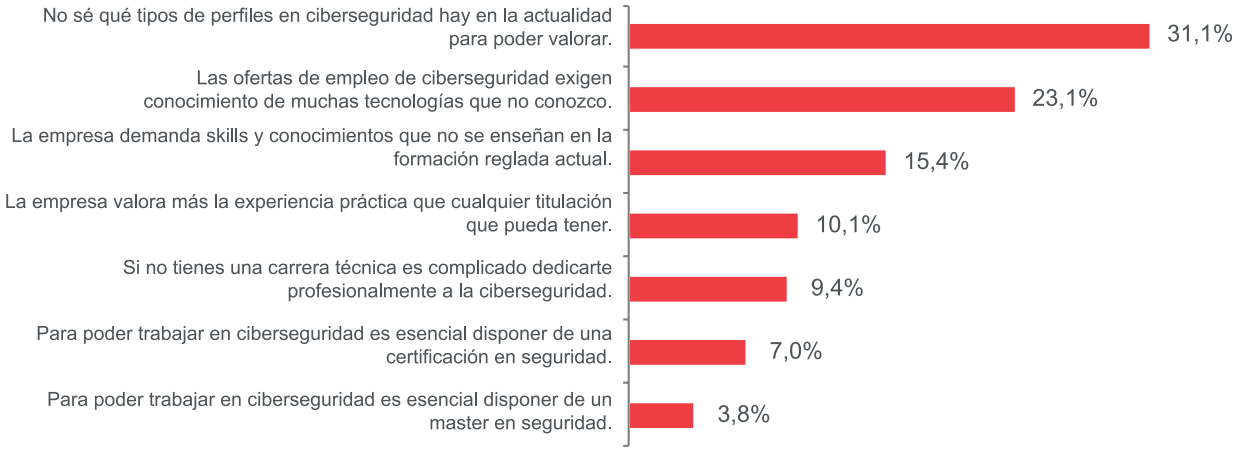


Figura 14. ¿A qué cree que se debe que no conozca el itinerario formativo y de capacitación requerido?

En cuanto a la falta de vocación entre la población hacia la ciberseguridad, cabe destacar que se relaciona con una falta de planificación formativa adecuada desde edades tempranas que aporte la base que genere el posterior interés. De este modo, algo resaltado por numerosos expertos del sector consultados es la capacidad de mejora en la comunicación de la importancia de la ciberseguridad en educación primaria y secundaria.

Podemos concluir por tanto que no está identificado un itinerario claro en educación asociado a la ciberseguridad. Por otra parte, la existencia de muchos organismos con capacidades para poder estructurar programas de formación es una fortaleza, pero se convierte en amenaza cuando no hay suficiente comunicación entre ellos.

4.2_ Caracterización de la demanda de talento en ciberseguridad

Calcular la demanda de talento en ciberseguridad no es una tarea fácil, ya que existen factores críticos que van a impactar en la actividad empresarial de las organizaciones y en sus demandas anticipadas de talento. Por ello, tratar de establecer este parámetro requiere conocer no solo cómo las empresas están estructurando sus procesos de contratación, sino tener en cuenta el número de talento interno que está reciclándose hacia posiciones de ciberseguridad, o la previsión anticipada de la demanda que puedan requerir debido al proceso de transformación digital que están sufriendo en la actualidad.

Por ello, para realizar una estimación de la demanda de talento de ciberseguridad en España se ha realizado un análisis de las diferentes aproximaciones llevadas a cabo por organizaciones como la ISC2[2], y que están basadas en su mayoría, en datos provenientes de una encuesta que requiere posteriormente adaptarse a la realidad de España mediante un proceso de extrapolación (alimentado con fuentes de información nacionales) que tenga en cuenta la realidad de cada país, dando como resultado el total de trabajadores demandados.

Este tipo de aproximaciones utiliza, de manera general, una combinación de las siguientes medidas:

Estimación de la mano de obra representada por profesionales de la ciberseguridad. Se trata de una medida basada en población que estima, en base al censo (si es posible) el tamaño actual de mano de obra multiplicada por el porcentaje de mano de obra de ciberseguridad prevista (dato que se obtiene de la encuesta).

Cálculo **del número medio de profesionales de ciberseguridad por entidad empresarial.** Es un dato basado en población que se obtiene a partir del censo empresas y multiplicado por el número previsto de profesionales de ciberseguridad por organización. En este caso, y para el presente estudio, este número proviene de la encuesta realizada, donde se ha preguntado el número medio de trabajadores que componen el departamento de ciberseguridad, ajustado por un parámetro de corrección que tiene en cuenta el porcentaje de empresa que no disponen de dicho departamento.

Número de profesionales de ciberseguridad en otros países. Esta estimación parte del análisis realizado por organizaciones de la realidad de Estados Unidos y que, a partir de las ratios calculadas para ese país, proyecta los datos estimados para el resto de los países en base a determinados criterios comunes.

Sin embargo, es necesario incorporar factores de corrección que eliminen el sesgo del análisis:

En el caso de las pymes, la mayoría de las ocasiones **el personal dedicado a labores de ciberseguridad realiza también otro tipo de tareas.** Por ello, se aplica un factor de corrección en función del tipo de tamaño de empresa para mantener una estimación más conservadora.

2 Metemos el título del informe aquí

Impacto de COVID-19 que ha provocado un incremento en el gasto de TI asociado a tecnología y, por tanto, ha cambiado sensiblemente tanto las demandas de personal de TI como de ciberseguridad.

Incremento del gasto de TI, y análisis del impacto que el gasto de TI tiene sobre el crecimiento del empleo cualificado del sector (dentro del cual se incorpora el empleo en ciberseguridad). Incluye un ajuste para incorporar el crecimiento del consumo de la seguridad como servicio.

Impacto del incremento de PIB sobre la economía. Un incremento del PIB tendrá efectos positivos en la contratación de empleo en general, y de ciberseguridad en particular. Esto es así porque existe una correlación bilateral entre crecimiento del PIB y crecimiento del empleo; es decir, una determinada variación porcentual de la tasa de empleo por cada variación porcentual de la tasa de crecimiento y viceversa. El crecimiento del empleo es una función del crecimiento de la producción, del coste laboral real y de la productividad total de los factores (PTF). A su vez, el crecimiento de esta última variable, junto con el de los inputs empleo y capital (físico y humano), determinan el crecimiento del PIB[8].

Sin embargo, relacionado con lo anterior, existe un **umbral de crecimiento** necesario tanto para evitar que el desempleo siga creciendo, como para crear empleo neto a medio y largo plazo. Según los resultados de un estudio[9] que analiza la relación del PIB con la creación de empleo, utilizando una función de producción CES (elasticidad de sustitución constante) con capital y trabajo como inputs, se estima una ecuación de demanda de empleo.

Personal reciclado de la empresa hacia posiciones de ciberseguridad. Este factor considera la ocupación de vacantes de talento de ciberseguridad en las organizaciones a través de la promoción de talento interno de la organización. Por ello, esta variable influye (como se ha visto antes), en la generación de oferta de talento de ciberseguridad. El dato para poder calcular este factor se obtiene directamente de la encuesta utilizada.

Número de vacantes de ciberseguridad actuales, publicadas en los principales buscadores de empleo. Teniendo en cuenta que un porcentaje de las vacantes se cubre con personal propio al que se forma de manera interna en la organización, este factor debe tenerse en cuenta a la hora de computar el talento en ciberseguridad total. Del trabajo realizado, eliminando las duplicidades de ofertas en diferentes buscadores y caracterizando la búsqueda de perfiles a todo el territorio español, la cifra que se obtiene es 3.692[10].

Análisis de la demanda actual de talento de ciberseguridad

Para estimar la demanda de ciberseguridad es necesario partir de un dato que permita aplicar los diferentes métodos de estimación que se han descrito en la literatura (y en este informe) ajustándolos con los factores de corrección mencionados.

3 En 2010 la Organización Internacional del Trabajo (OIT) realizó un estudio econométrico global de dicha correlación bilateral (ILO-KILM, 2010) para el periodo 1992-2008, calculando que la elasticidad del empleo global al crecimiento real global del PIB oscilaba entre 0,32 y 0,37, es decir, que por cada punto adicional de PIB el empleo aumentaba en dicha proporción.

4 https://www.eco.uc3m.es/temp/dolado2/GDP%20Growth%20Thresholds%20_PdC-JD_.pdf

5 El documento completo del que el lector está visualizando el resumen ejecutivo, recoge el trabajo de búsqueda realizado para la caracterización de la demanda actual de talento en ciberseguridad en España a través de las ofertas de trabajo que las empresas tienen publicadas en los principales buscadores de empleo

Ello obliga a tomar como base la estimación de la fuerza laboral para 2020 que proporciona (ISC)[2] en su informe *Cybersecurity Professionals Stand Up to a Pandemic*, donde según la extrapolación de su metodología y aproximaciones con base en fuentes nacionales de cada país, se ha determinado que el total de trabajadores en ciberseguridad en España está en una cifra cercana a los **122.284**, es decir, que atendiendo a los datos de población, esto representa un 0.26% del total.

Teniendo en cuenta las premisas anteriores, la demanda de talento de ciberseguridad en España se calcula mediante la siguiente ecuación:

$$Demanda_{talento\ ciberseguridad} = Empleo_{PIB} + Empleo_{TI\ en\ Seg} + Demanda\ actual$$

Dónde:

$Empleo_{PIB}$

Que es el empleo generado en la economía como consecuencia del incremento de PIB y ajustado por el coeficiente de empleo en ciberseguridad calculado por ISC2 y particularizado para España.

$Empleo_{TI\ en\ Seg}$

Cálculo del total de empleos de ciberseguridad dentro de la cifra global de empleos del sector TIC debido a un incremento del gasto de este. Para su cálculo, se toman los empleos generados en el Sector TIC en el año 2019 y se ajusta por el parámetro correspondiente para cada año en función del gasto de TI de dicho año (actual y proyecciones). Una vez calculada dicha cifra, se ajusta con el impacto del crecimiento del mercado de la ciberseguridad, de forma que se obtiene el multiplicador final que se aplica sobre el total del empleo de TI para obtener el crecimiento global del empleo en ciberseguridad para dicho año.

Demanda actual

Es el total de ofertas de empleo actuales publicadas en los principales buscadores de empleo del país. Consideramos incluida en esta cifra los procesos que están desarrollándose también a través de empresas especializadas en *headhunting* o selección de talento ya que, según las entrevistas realizadas, los procesos de selección en estas empresas se desarrollan publicando igualmente el perfil en portales de empleo especializados.

Por ello, la demanda actual de talento en ciberseguridad para el año base es la siguiente:

$$Demanda_{talento\ ciberseguridad} = Empleo_{PIB} + Empleo_{TI\ en\ Seg} + Demanda\ actual$$

Donde por tanto la $Demanda_{talento\ ciberseguridad}$ asciende a **63.191** empleos.

4.2.1.1.2_ Análisis de la proyección futura de demanda de talento de ciberseguridad

Partiendo del análisis realizado y proyectando al periodo 2022-2024, la siguiente tabla recoge la estimación de demanda de talento de ciberseguridad en España.

	2021	2022	2023	2024
Total	63.191	67.147	74.904	83.007

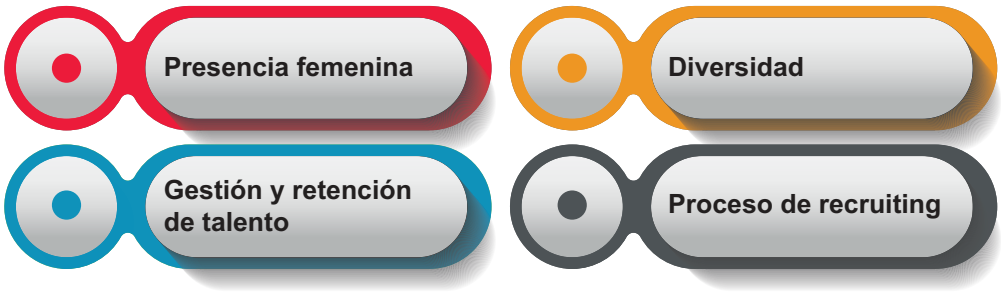
Tabla 2.Proyecciones de estimación de la demanda de talento en ciberseguridad en España

4.2.2_ Análisis cualitativo de la demanda de talento en ciberseguridad

La aceleración de la digitalización provocada sobre todo por la pandemia de COVID-19 ha acelerado significativamente la incorporación de nueva tecnología dentro de las organizaciones, que se encuentran además con una necesidad de talento que les permita abordar el proceso de transición al ámbito digital de una manera exitosa.

Sin embargo, los datos publicados por la Comisión Europea indican que el 58% de las empresas encuentran dificultades a la hora contratar empleados para suplir la demanda de perfiles TIC. En esa misma línea, la escasez de talento es palpable en las organizaciones en España, aun reconociendo que en las grandes organizaciones el ámbito profesional de la ciberseguridad es de calidad, es evidente que las empresas de manera generalizada (especialmente las pymes) están teniendo dificultad a la hora de acceder a talento en ciberseguridad.

Para el análisis de la demanda, nos fijamos en los verticales de análisis:



PRESENCIA FEMENINA EN LA CIBERSEGURIDAD

Tradicionalmente, existe una presencia baja de mujeres en carrearas relacionadas con ciencia, tecnología, ingeniería y matemáticas (STEM). Esto se hace aún más visible cuando se considera una especialización, como lo es el campo de la ciberseguridad. De hecho, tomando como base los resultados del trabajo realizado, la ciberseguridad en la actualidad es una profesión de hombres, acorde a los resultados del trabajo de campo desarrollado. **El 46,2% de las organizaciones consultadas consideran**

que la presencia femenina no está aún a la par de sus compañeros. En función de la industria y el tamaño de empresa, la proporción de mujeres en las diferentes plantillas de trabajadores de la ciberseguridad disminuye, **a pesar de que el gap de estudiantes de carreras universitarias tecnológicas se está cerrando de manera significativa en los últimos años**. De hecho, **el porcentaje de mujeres que han elegido estudiar carreras tecnológicas ha aumentado en 5 puntos porcentuales en 5 años, al pasar del 24% de mujeres matriculadas en el curso 2016-17 al 29% de matriculadas en el curso 2019-20**.

En este sentido, según los resultados un estudio en *UK National Cyber Security Centre (NCSC)*, la presencia femenina es una de las temáticas centrales en la gestión del talento en ciberseguridad en la actualidad para las organizaciones. Los datos indican que **la representación femenina en la industria es del 31%**.

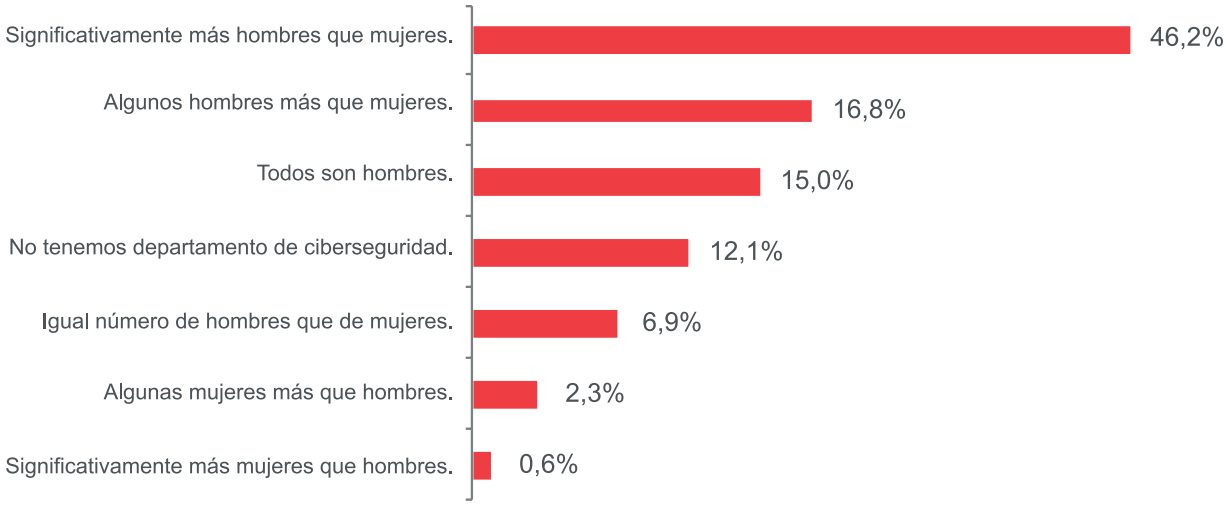


Figura 18. Presencia femenina en la industria de ciberseguridad

La presencia, además, es menor según el tipo de posición dentro del ámbito de la ciberseguridad. Según los resultados obtenidos, **aquellos perfiles más técnicos a menudo tienen una menor presencia de mujeres, si los comparamos con otros perfiles más vinculados con la gestión y el cumplimiento normativo** (DPO, y otros perfiles donde la componente de ciberseguridad es importante – derecho, etc.-). De hecho, **se observa una presencia muy minoritaria en niveles de dirección de seguridad** (CISO o responsables de seguridad), donde la presencia de la mujer es muy pequeña.

Los expertos consultados apuntan igualmente a que, entre las posibles razones puedan estar el sesgo en la educación o la falta de referentes femeninos visibles que sirvan de tracción al resto de mujeres, como pueda ocurrir en el caso de los hombres, por lo que es necesario incorporar la perspectiva de igualdad en toda acción de comunicación a realizar y no estigmatizar la profesión. En cualquier caso, el bajo porcentaje de mujeres en la profesión debería abordarse más como una oportunidad de mejora, que como un problema de desigualdad entre géneros.

De hecho, **a pesar de la exigencia que demanda la ciberseguridad, esta es una profesión que permite la conciliación familiar y facilita la incorporación de la mujer en la industria, como se muestra en el 76,6% de la muestra consultada que dispone de políticas de trabajo flexible** para la organización (en general) y el departamento de seguridad (en particular)

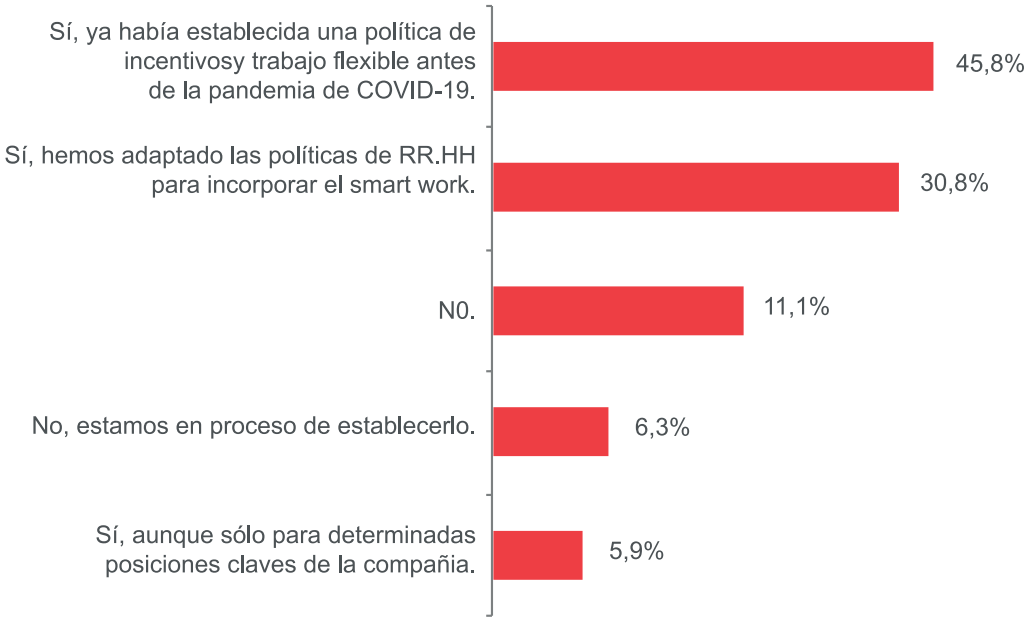


Figura 19. Existencia de políticas flexibles en la industria de la ciberseguridad

Aunque es cierto que las organizaciones reconocen que la presencia femenina en la fuerza laboral es baja, también disponen mayoritariamente de planes de igualdad, fomentando la inclusión de mujeres en todas las posiciones de la organización, incluyendo la ciberseguridad. De hecho, reconocen que, para ciertos temas enfocados a la gestión, tienen más aptitud que algunos de sus compañeros hombres.

Preguntadas a las empresas por la iniciativa de contratación de mujeres en roles de ciberseguridad, el 37,8% de las empresas reconoce que no realiza distinciones a la hora de contratar talento de ciberseguridad para el departamento, sea masculino o femenino, aunque es cada vez más común que las organizaciones, conscientes de las ventajas de disponer de talento mixto en las plantillas estén poniendo en marcha acciones para tratar de incrementar la presencia femenina en los equipos de ciberseguridad.

DIVERSIDAD

La diversidad en la industria de la ciberseguridad está presente de igual manera que ocurre en el resto de las industrias, aunque solo el 39% de la muestra consultada reconoce disponer de un plan de diversidad para apoyar a los profesionales de ciberseguridad.

La ley impone la obligación de contar con un número mínimo de trabajadores discapacitados para plantillas superiores a 50 empleados. Sin embargo, solo el 20,9% de las empresas consultadas reconoce que está incorporando plantilla de personas con discapacidad o colectivos en riesgo de exclusión social. Las principales razones que aducen las empresas que trabajan con estos colectivos se refieren al desconocimiento que estos trabajadores tienen sobre los requisitos que deben tener para poder aplicar a estas posiciones, así como la formación necesaria para poder acometerlo.

Sin embargo, otras iniciativas actuales que están trabajando en la incorporación de este tipo de profesionales al ámbito de la ciberseguridad como la Fundación GoodJobs, realiza, a través de un análisis inicial de las capacidades de la persona, un análisis de las capacidades de la persona que traduce a un itinerario formativo en materia de ciberseguridad. Este proceso de formación y capacitación culmina con la realización de prácticas en empresas dentro del ámbito de la ciberseguridad. De estas prácticas, existe una transición natural al empleo.

GESTIÓN Y RETENCIÓN DE TALENTO DE CIBERSEGURIDAD

La seguridad es una de las principales prioridades de inversión en las empresas españolas, que han entendido la necesidad de gestionar la seguridad en la empresa, bien a través de la creación de un departamento específico de ciberseguridad (51% de los casos), o bien delegando las responsabilidades de ciberseguridad a otros perfiles técnicos como el CIO, CTO, etc. (25%) o subcontratándolas (20,5%) tal y como muestra la figura.

Sin embargo, las **plantillas** de estos departamentos son **pequeñas**. En prácticamente la mitad de las organizaciones consultadas (46,9%) el departamento de seguridad dispone de menos de 5 personas, mientras que en el 33% de los casos este departamento es amplio, ya que cuenta con perfiles tanto internos como incorporados mediante subcontratación.

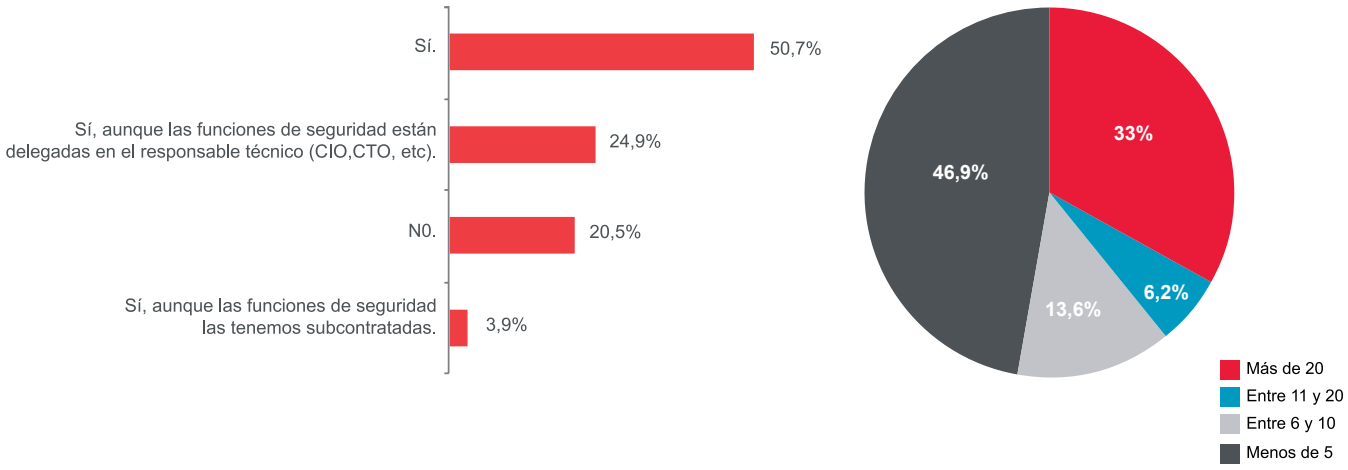


Figura 20. Existencia de departamentos de seguridad en las organizaciones

La **rotación** en este tipo de perfiles es **alta**, como muestra que el 52% de las empresas consultadas confirme que anualmente entre el 10% y el 40% del personal de ciberseguridad deja la organización, lo que supone un duro revés para garantizar la continuidad de los equipos y hacerlos crecer y madurar en la organización.

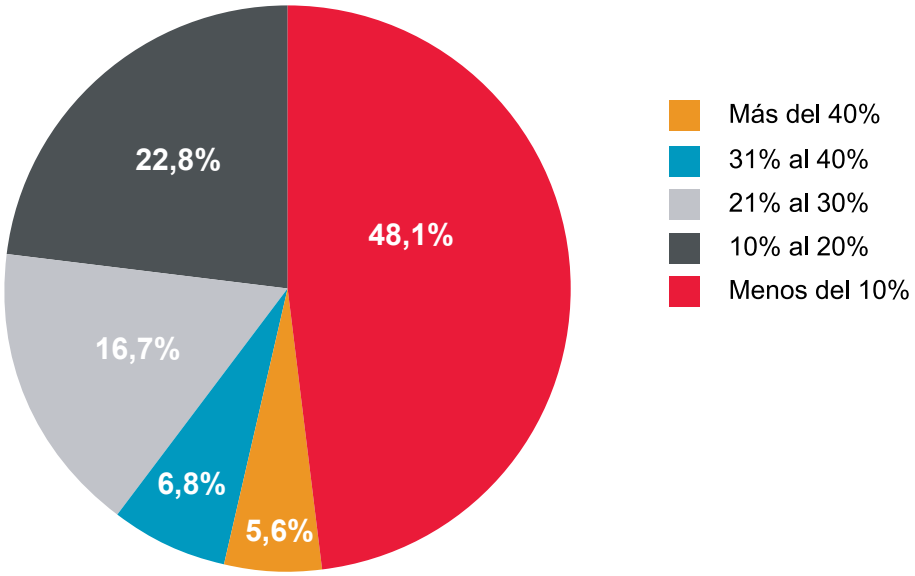


Figura 21. Rotación de personal de los equipos de ciberseguridad en la empresa española

Los principales motivos por los que existe una alta rotación en la industria de la ciberseguridad son muy variados, aunque en general podríamos decir que existen dos tipos de factores: los **coyunturales** que impactan en el número de profesionales actuales que conforman la oferta de perfiles actual de trabajo, y otros más asociados a **aspectos del proyecto y condiciones** donde estos trabajadores desempeñan su actividad profesional.

El actual desalineamiento entre la oferta y demanda de talento de ciberseguridad está motivando que el **salario** sea una variable clave que afecta a la rotación de personal. No solamente en términos de sueldo, sino otros complementos como incentivos asociados a participaciones sobre la compañía, *bonus* o beneficios sociales, que conforman la principal razón de cambio (22,7% de la muestra). Sin embargo, la alta demanda de estos profesionales está haciendo que otros aspectos asociados al proyecto empresarial de la compañía, planes de desarrollo y promoción personal, así como disponer de políticas de trabajo flexible o el ambiente del trabajo sean factores cada vez más importantes para este tipo de talento.

De hecho, los bajos sueldos que en la actualidad se están pagando dentro de la industria (a opinión de la muestra consultada), son una barrera muy importante a la hora de poder retener y atraer nuevo talento de ciberseguridad, ya que el 59,6% de la muestra consultada reconoce que el sueldo bruto que reciben los empleados en el área de la ciberseguridad en su empresa está entre los 30.000 y 60.000€, atendiendo a los diferentes perfiles que componen la escala.

Este hecho se agrava si tenemos en cuenta que el auge de la implantación de las políticas flexibles de trabajo como consecuencia de la pandemia de COVID-19 está provocando que empresas extranjeras vean en los profesionales españoles candidatos ideales a incorporar en sus plantillas, dado que tienen sueldos mucho más competitivos (en otros países, estos sueldos se pueden llegar a duplicar o triplicar, incorporando, además, *bonus* o pagos en acciones), lo que unido con la posibilidad de realizar teletrabajo, hacen que la retención de talento en la compañía sea un reto difícil de alcanzar.

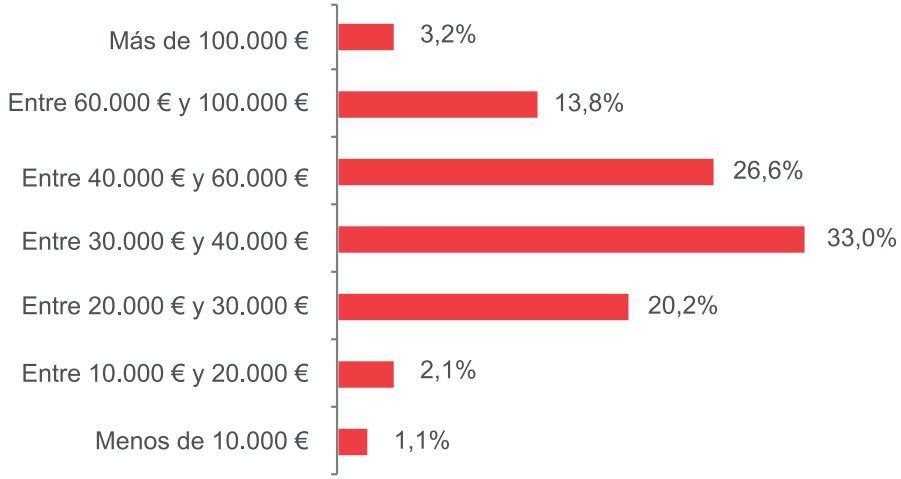


Figura 22. Escala salarial en la que se distribuye la muestra consultada

En este escenario, no es raro pensar en la posibilidad de poder reclutar talento interno para cubrir vacantes relacionadas con ciberseguridad. De hecho, los datos del trabajo realizado apuntan a que el **40,1% de la muestra reconoce que está reciclando talento interno** de la compañía para el departamento de ciberseguridad, preferentemente de las áreas de negocio y ventas (un 33,3% y 18,3% respectivamente), motivado en gran medida por el conocimiento del negocio, aspecto clave como se ha visto anteriormente.

En este sentido, el 48% de las empresas está utilizando la formación y cualificación de personal interno para cubrir las vacantes de ciberseguridad existentes, lo que apunta en una tendencia creciente a reciclar personal de la organización para este tipo de posiciones, en gran parte derivada de la escasez de talento específico para determinadas posiciones.

Sin embargo, aunque la tendencia a la provisión de vacantes de ciberseguridad a través de talento interno es un hecho, únicamente 2 de cada 10 posiciones internas se cubren con talento interno de la organización al que se forma con conocimientos para poder desempeñar las funciones que se requieren.

El 47,1% de la muestra reconoce que la falta de este talento tiene un efecto negativo crítico de la empresa (cifra que asciende al 85,1% si incluimos aquellas respuestas parciales), fundamentalmente derivado de la imposibilidad de adaptar el *framework* de seguridad de la empresa a un nivel de madurez suficiente para no disponer de vulnerabilidades que puedan aprovechar los ciberdelicuentes así como la reducción de la capacidad de crear productos y servicios nuevos (34,2% cada una de ellas).

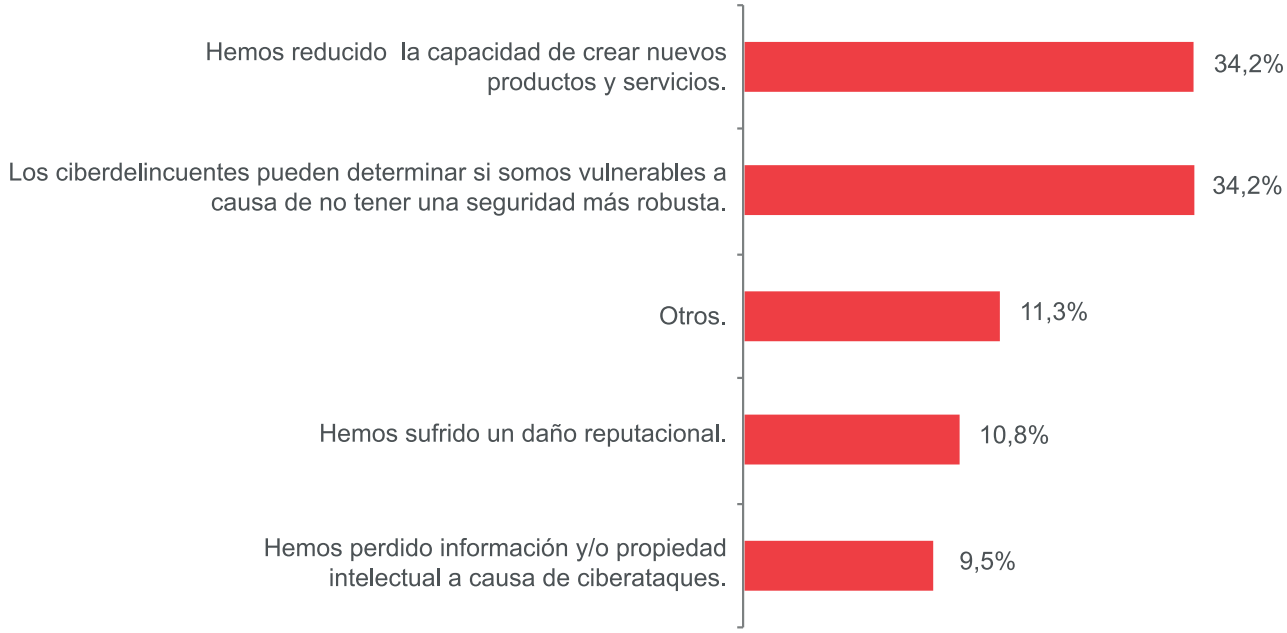
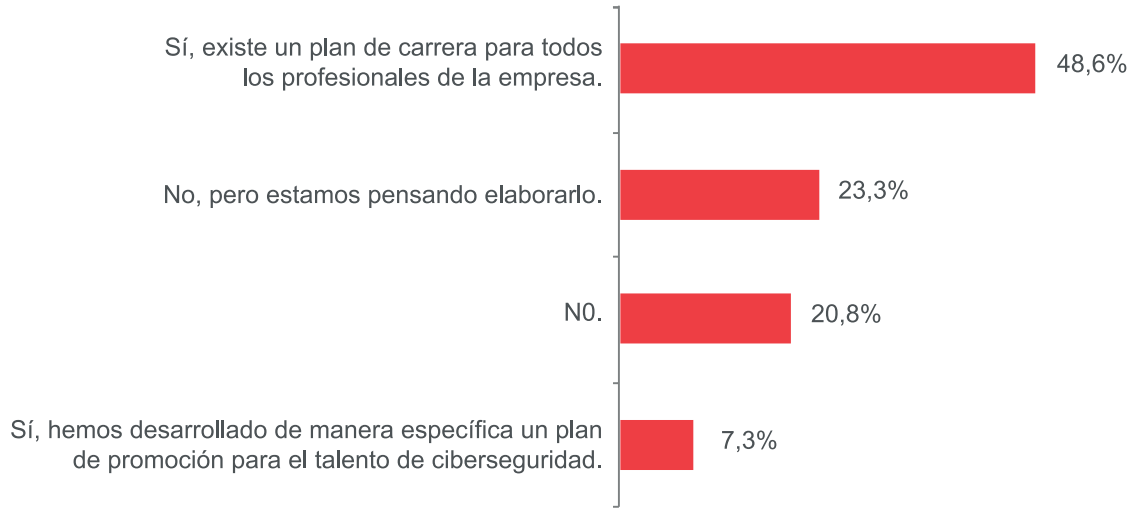


Figura 23. Principales efectos negativos de la escasez de talento de ciberseguridad en las empresas

Para hacer frente a la escasez de talento y prevenir la fuga de este, las empresas consideran clave disponer de **políticas claras de incentivos y desarrollo de carrera**, como reconocen el 74,6% de las organizaciones consultadas.



En este escenario de escasez de profesionales y de alta rotación, el 42,2% de las empresas consultadas está en la actualidad contratando perfiles provenientes de cursos de especialización de FP en ciberseguridad, frente al 29,5% que no. Sin embargo, el peso de estos perfiles dentro del total de contrataciones aún es pequeño, ya que el 67,8% de la muestra consultada reconoce que está entre el 10% y el 30% de las contrataciones que realiza, fundamentalmente para labores de SIEM y personal de SOC.

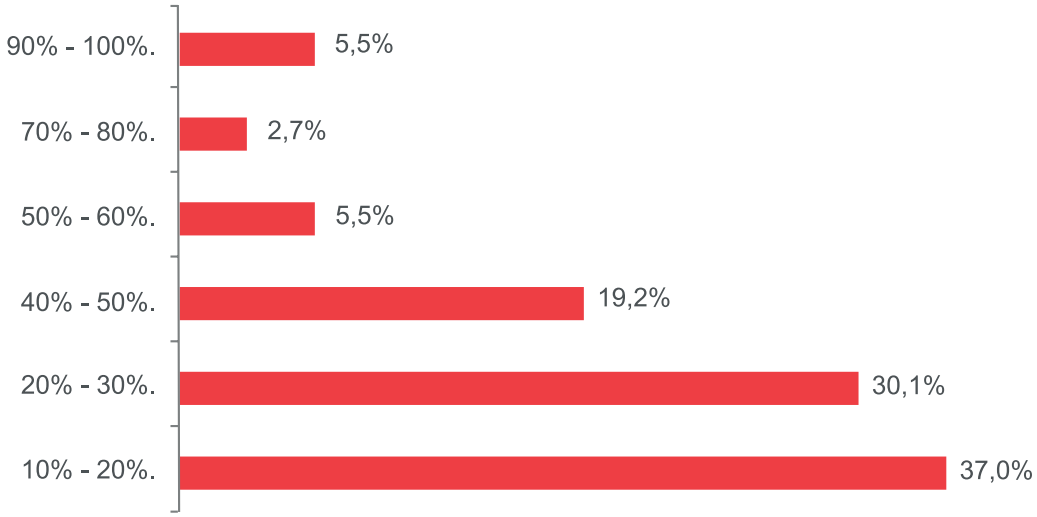


Figura 24. Porcentaje de contrataciones de talento procedente de FP

Asimismo, analizando la contratación de perfiles de '*entry level*' o de primer empleo en ciberseguridad, la opinión de la empresa española no es clara al respecto. Si bien a nivel porcentual el 57,4% reconoce que el título en este tipo de perfiles es importante, la realidad muestra que únicamente 2 de cada 10 empresas consultadas reconocen como importante que el candidato disponga de título universitario para el desempeño de las tareas que posteriormente acometerá.

Las razones detrás de este tipo de decisiones, más allá de la falta de conocimientos técnicos y experiencia que la formación reglada actual aporta a este tipo de perfiles (y que se han tratado de manera extensa en este documento) están asociadas al coste de la formación para lograr superar la curva de aprendizaje y que empiecen a ser productivos, con el riesgo inherente de rotación o fuga de talento hacia una empresa tras haber realizado la formación inicial.

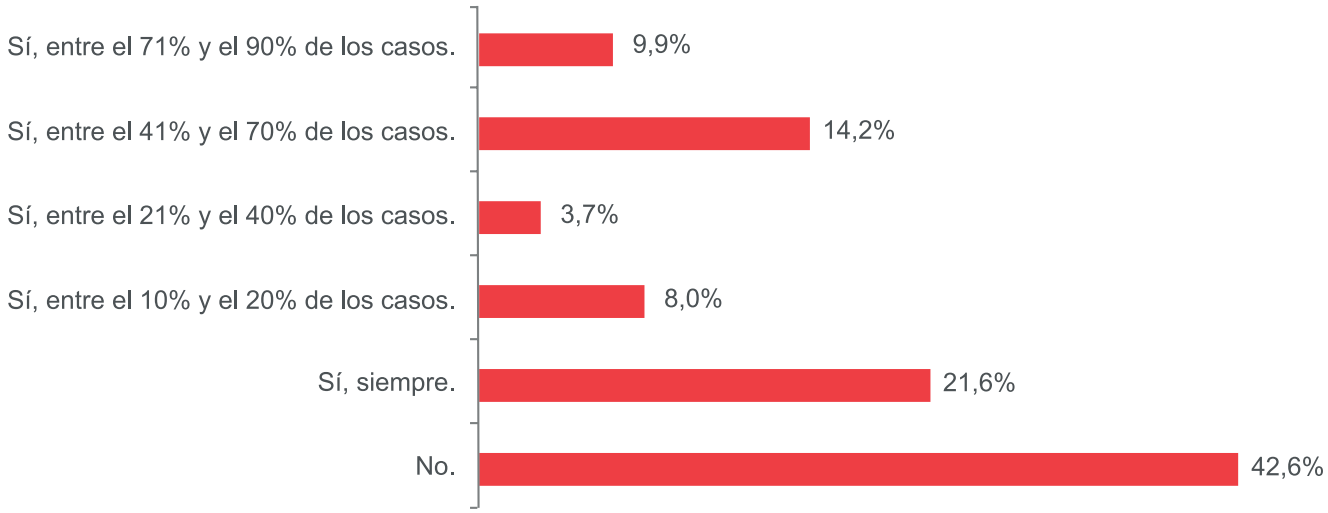


Figura 25. Importancia del título universitario en posiciones de entry level en ciberseguridad

Por ello, la sensibilización en materia de ciberseguridad es esencial en las empresas en la actualidad. Disponer de un plan de sensibilización y formación en materia de ciberseguridad para los empleados se convierte en esencial para el 53,4% de las empresas consultada, que han entendido que la primera barrera de defensa de las organizaciones son los empleados. Aunque la formación no está extendida a lo largo de toda la muestra, únicamente un 7,3% de la muestra no ha realizado ninguna acción de sensibilización.

LA GESTIÓN Y RETENCIÓN DEL TALENTO EN START-UPS

La velocidad a la que este tipo de empresas debe pivotar para alcanzar un modelo de negocio replicable y escalable, a menudo ofrece aprendizajes laborales más intensos y fomenta el trabajo en grupo. Por ello, suelen ser opciones muy interesantes para los perfiles de talento de ciberseguridad que encuentran en ellas mayor autonomía, un proyecto interesante en el que tienen la capacidad de tomar decisiones y amplia flexibilidad.

De hecho, la autonomía y flexibilidad son las principales razones que las empresas reconocen como elementos más atractivos de este tipo de organizaciones (33,3% y 20% respectivamente). Sin embargo, la incertidumbre asociada al desarrollo empresarial y a la dificultad de acceder a financiación es una razón que pesa bastante a la hora de retener talento de ciberseguridad, ya que no existe a priori un plan de carrera que permita establecer una hoja de ruta clara, así como tampoco una estabilidad laboral y económica.

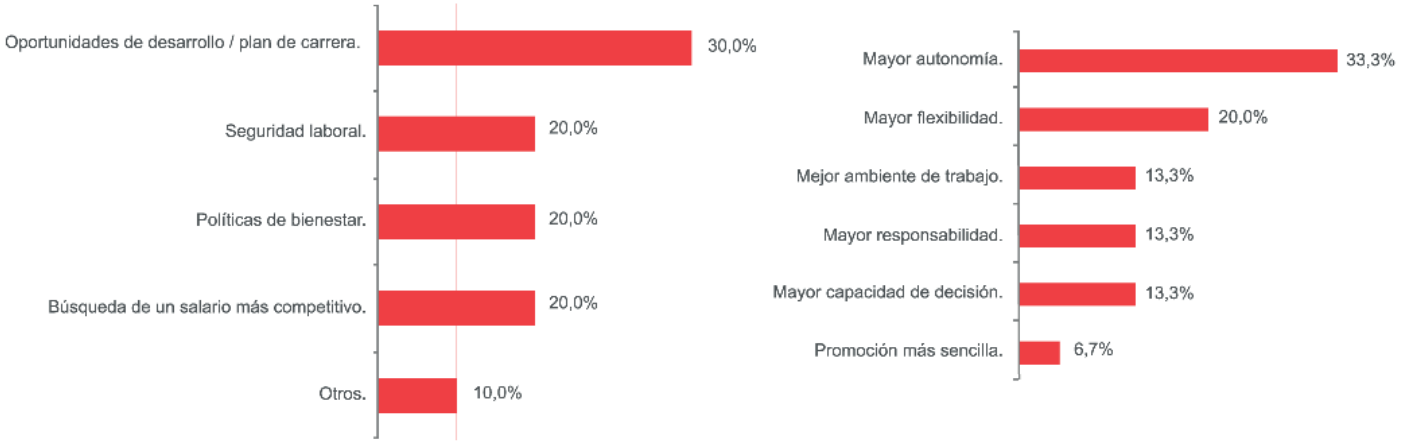


Figura 26. Análisis de los factores de atracción y retención de talento en start-ups

Por ello, no sorprende que **los principales motivos asociados a la fuga de talento, según la muestra consultada, se estén dando debido a la búsqueda de oportunidades en organizaciones de mayor tamaño o prestigio, así como por falta de interés en el proyecto o sentimiento de no avance en el mismo** (37,5% respectivamente para cada categoría). Parece claro por tanto que las claves para evitar la fuga de talento en una startup pasan por disponer de un proyecto empresarial interesante, dinámico y con capacidades de desarrollo y formación, disponer de un buen ambiente de trabajo, así como la existencia de un plan de carrera.

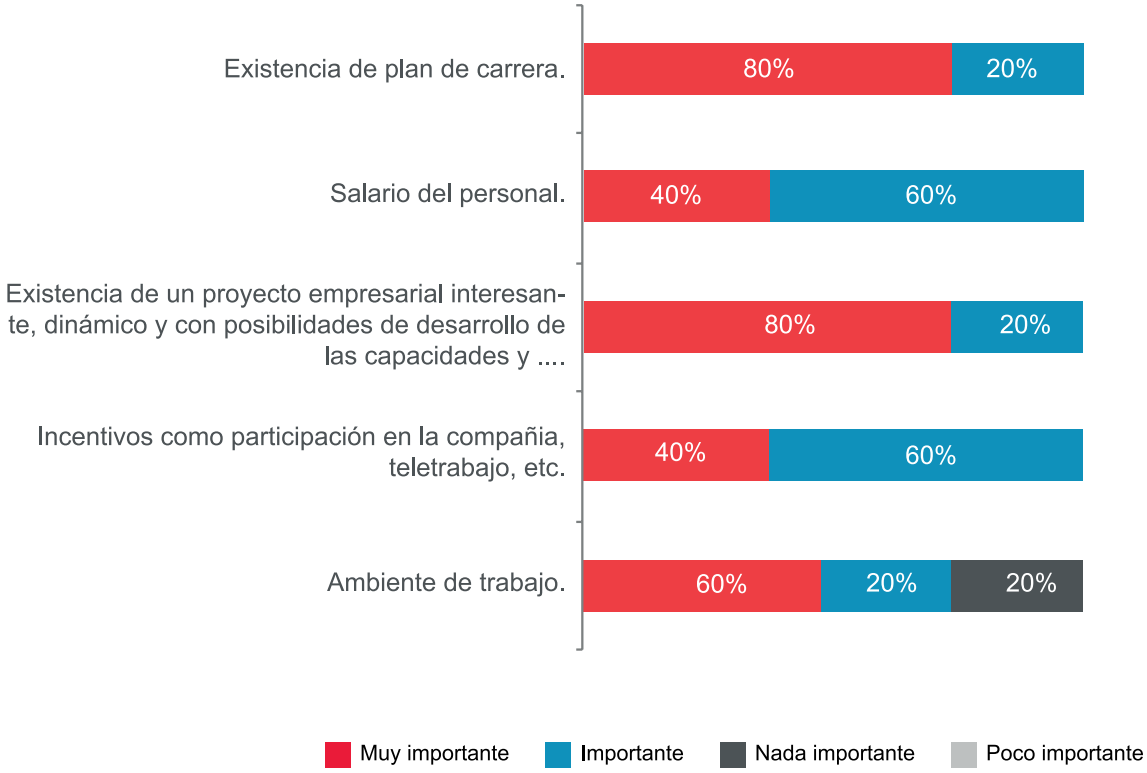


Figura 27. Importancia de los factores con relación a la retención de talento en una start-up

CARACTERIZANDO EL PROCESO DE RECRUITING DE PERFILES DE CIBERSEGURIDAD

Reclutar talento de ciberseguridad es una tarea complicada según la opinión del 45,1% de la muestra consultada, que considera además que, de media, se **requieren entre 1 y 6 meses para poder seleccionar e incorporar a una persona**, para lo que es necesario entrevistar entre 1 y 5 candidatos (69,35% de las empresas consultadas). Si bien es cierto que, en función del tipo de perfil que se requiere, el tiempo será mayor, así como el número de personas involucradas en el proceso.

Las principales razones estriban en la complejidad de aunar la experiencia en ciberseguridad con la experiencia en la industria en la que opera

la empresa (señalada por el 25% de la muestra), así como la dificultad de acceder a talento senior (más de 5 años de experiencia en ciberseguridad), y que para el 24,1% de las compañías es la principal razón.

En general, la opinión de la industria es que el candidato puede disponer de una buena base técnica, pero carecer de la experiencia práctica real, valorada como un requisito por las empresas entrevistadas en el proceso de diagnóstico.

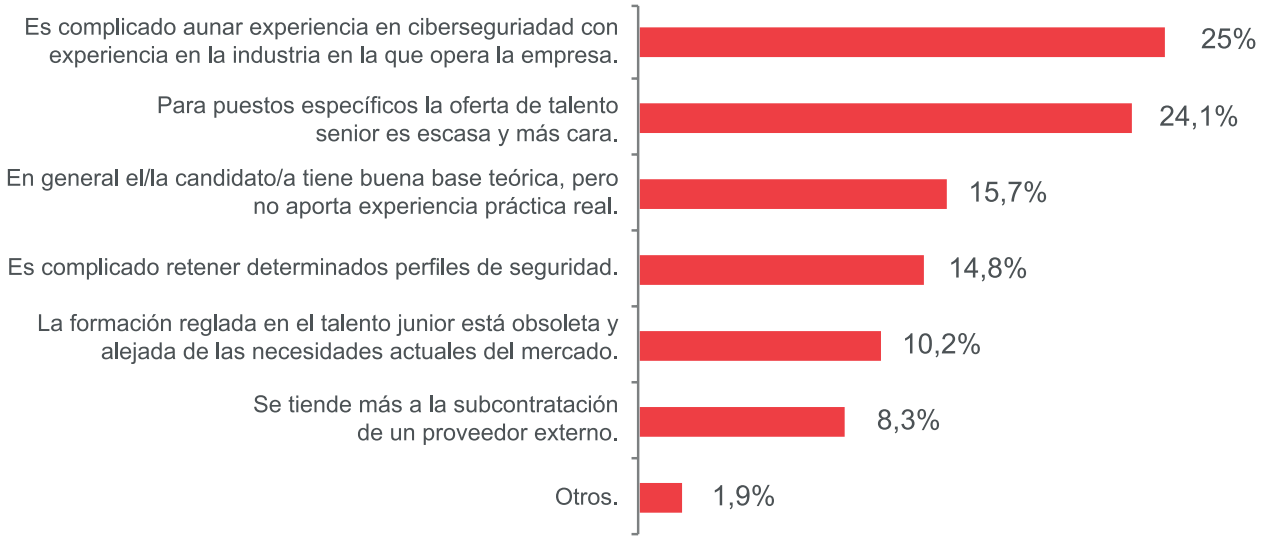


Figura 28. Principales barreras encontradas en el proceso de recruiting de talento de ciberseguridad en las empresas

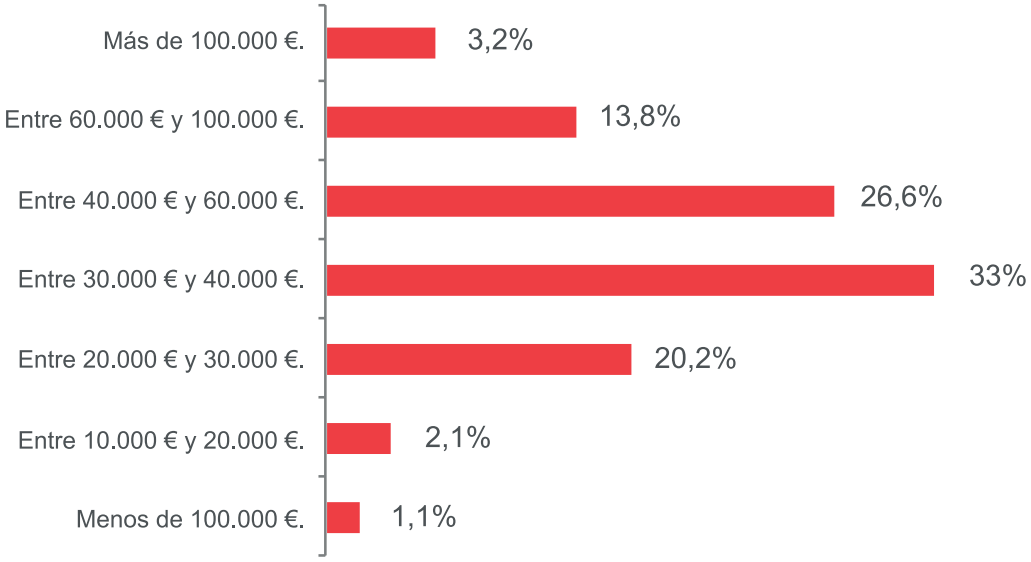
Entender adecuadamente las necesidades de la organización en términos de talento de ciberseguridad se hace imprescindible para poder mejorar la gestión y atracción del mismo. Sin embargo, existe un desalineamiento en cuanto al entendimiento de las necesidades de reclutamiento por parte de los departamentos de ciberseguridad y recursos humanos. Esto hace que, en muchas ocasiones, no se esté reclutando al mejor talento y que los procesos no den respuesta a las necesidades que tienen las empresas.

Esto hace que, según la opinión de las organizaciones consultadas, **tres de cada cuatro evaluaciones** de un candidato a incorporar en una posición de ciberseguridad estén mal cualificadas. A medida que se van requiriendo perfiles menos específicos o posiciones de '*entry level*', el porcentaje disminuye a la mitad (34,3% de las empresas consultadas) o a una de cada tres evaluaciones (15,7% de la muestra).

Sin embargo, este desalineamiento se convierte en un problema para las empresas que se ven compitiendo por un talento escaso al que, además, hay que añadir una variable que complica la ecuación y es el salario.

De hecho, **uno de los principales obstáculos para la atracción y retención de talento de ciberseguridad está asociado al salario**. La dificultad de acceder a talento capacitado y los sueldos contenidos que se están pagando a los diferentes perfiles dentro de la industria, hacen que la rotación de personal sea muy elevada y que el acceso a talento capacitado sea complicado.

Casi el 60% de las empresas en España reconoce que paga entre 30.000 y 60.000€ a los profesionales de ciberseguridad (entendiendo los diferentes perfiles que componen la escala), mientras que, en otros países, estos sueldos se pueden llegar a duplicar o triplicar, incorporando, además, *bonus* o pagos en acciones, que unido con la posibilidad de realizar teletrabajo, hacen que la incorporación de talento en la compañía sea un reto difícil de alcanzar.



5_ ANÁLISIS DE LAS INICIATIVAS INTERNACIONALES DE GESTIÓN DEL TALENTO

El desafío que tienen los diferentes países de cerrar la brecha de la fuerza laboral en ciberseguridad es complejo. Estamos en un periodo muy atípico, donde el mercado aún no se ha acomodado nuevamente a una nueva realidad, y en este sentido hay ciertos fenómenos con respecto a los puestos de trabajo en ciberseguridad a nivel mundial. Si bien aunque es cierto que algunos estudios afirman que los puestos de trabajo demandados en el mercado de la tecnología han disminuido durante el periodo de pandemia, lo cierto es que las habilidades y el talento escasean de manera generalizada, y en niveles que bordean niveles críticos. Es igualmente importante destacar que algunas de las iniciativas identificadas van a estar impactadas por la masiva transición al trabajo en remoto y a la necesidad de desarrollar nuevas capacidades, tanto tecnológicas como de los equipos de trabajo, que permitirán mantener los entornos tecnológicos en funcionamiento y de una manera segura.

A través del informe *Cybersecurity Professionals Stand Up to a Pandemic*[6], realizado por el International *Information System Security Certification Consortium* o (ISC)², de donde derivan resultados de encuestas realizadas a 3.790 profesionales de la seguridad de todos los niveles y en instituciones gubernamentales, académicas y organizaciones de todos los tamaños en EE.UU, Europa, LATAM y Asia-Pacífico (APAC), se ha podido verificar que este periodo atípico representa un gran desafío tanto para la industria como para los profesionales.

De este modo, el informe destaca por su esfuerzo en cuantificar dos variables que son esenciales para entender las iniciativas y mejores prácticas identificadas en el análisis de las iniciativas internacionales de gestión del talento. La primera es la brecha de la fuerza laboral en ciberseguridad, y la segunda es la estimación de la fuerza laboral en ciberseguridad. En consecuencia, uno de los datos de mayor relevancia que arroja el estudio, es que la fuerza laboral tanto global como local en ciberseguridad, necesita crecer un 89% para defender de manera efectiva los activos críticos de las organizaciones.

Según (ISC)², a pesar de los desafíos económicos presentados por la pandemia, por primera vez se ha visto disminuir la brecha de la fuerza laboral en ciberseguridad, de 4 millones a 3,1 millones. Cabe señalar que, a pesar de una posible brecha de la fuerza laboral reducida, más de la mitad de los encuestados (56%) dice que la escasez de personal de ciberseguridad está poniendo en riesgo a sus organizaciones.

Esta ha sido la principal fuente para conocer el gap de la fuerza laboral en ciberseguridad, y vale la pena destacar que este varía según la región. Si bien la mayor población individual de profesionales de la ciberseguridad se encuentra en los EE. UU, junto con la mayor brecha de ciberseguri-

6 Cybersecurity Professionals Stand Up to a Pandemic, (ISC)² Cybersecurity Workforce Study, 2020.

dad, existen importantes grupos de talentos en ciberseguridad en todo el mundo, así como una escasez constante de personal de ciberseguridad.

El tamaño de la fuerza laboral y las brechas en ciberseguridad de algunos de los países incluidos en el análisis son:

Canadá

Fuera laboral 101.963 puestos de trabajo y brecha de (16.552).

EE.UU

Fuera laboral 879.157 puestos de trabajo y brecha de (359.236).

Reino Unido

Fuera laboral 365.853 puestos de trabajo y brecha de (27.408).

Francia

Fuera laboral 879.157 puestos de trabajo y brecha de (359.236).

Adicionalmente, como una referencia se identifica que para el caso de España el tamaño de la fuerza laboral estimado es de 122.284 y la brecha de 29.293, sin embargo, estos valores varían en función de la fuente y metodología implantada para su estimación[7].

Esta escasez además distorsiona las escalas salariales del mercado, donde se ha encontrado, según un informe publicado por McAfee en 2020[8], que Francia refleja una prima salarial cercana al factor 2.5x (respecto a la media salarial anual en las profesiones de TI) para profesionales que se dedican a la ciberseguridad. Incluso, en Israel este factor multiplicador alcanza aproximadamente un 3.3x.

La aceleración en la transformación digital que están sufriendo todas las industrias está provocando que el gap de la fuerza laboral en ciberseguridad en los países analizados[9] sea muy notable, y que se extienda no solo a la propia industria de la ciberseguridad. Así, por ejemplo, se requieren de profesionales en otros sectores de la economía que dispongan de capacidades en ciberseguridad.

Algunas iniciativas analizadas han sido la *National Initiative for Cybersecurity Careers and Studies (NICCS), Framework NICE* (EE.UU), *la Government Security Profession (GSP) (UK)*, Cybersecurity Talent Alliance

7 De hecho en este estudio se proporciona una estimación igualmente para esta cifra

8 Hacking the Skills Shortage, A study of the international shortage in cybersecurity skills. McAfee, 2020.

9 EEUU, UK, Israel, Malasia, China, Canadá, Francia y Rusia.

(Canadá) ó la *Education and Training Catalog*, NICCS, (EE.UU), con el objetivo de consolidar un ecosistema de ciberseguridad con la capacidad de adaptación e innovación, que permitan reforzar el ecosistema de ciberseguridad y, de esta manera, abordar conjuntamente el gap de talento en ciberseguridad.

6_ DEFINICIÓN DE UN MODELO DE CARACTERIZACIÓN DE LOS PERFILES DE CIBERSEGURIDAD EN ESPAÑA.

El análisis de las diferentes taxonomías de perfiles de ciberseguridad, tanto en Europa como en otros países (anexo a este informe) ha permitido establecer que existen diversos factores (políticos, económicos, sociales, tecnológicos, legales, etc.) que pueden impactar en la industria de la ciberseguridad, y en consecuencia, en la escasez de talento, brechas y en general un desajuste entre oferta y demanda.

Uno de esos factores relevantes en la unión europea, es la falta de estandarización de la definición de roles de ciberseguridad y skills asociados a esos roles. SPARTA, uno de los proyectos financiados por la Comisión Europea, ha sido uno de los trabajos que han confirmado que los roles de ciberseguridad se encuentran en un área gris y carecen de una definición clara y concisa. Es allí donde se espera que el trabajo en marcha que está realizando ENISA cobre mucha relevancia, a través de una clasificación de roles que se convierta en el estándar de facto en Europa.

De esta manera, la Agencia de la Unión Europea para la ciberseguridad,ENISA , es la agencia dedicada a lograr un nivel común de ciberseguridad en toda Europa, y en el marco de desarrollo de sus iniciativas ha formado un grupo de trabajo (15 miembros representandos por diferentes stakeholders e intereses) designado al *European Cybersecurity Skills Framework* (ECSF), el cual se basa en crear un entendimiento común de los roles, competencias, capacidades y conocimientos utilizados por y para ciudadanos, organizaciones, y proveedores de capacitación, formación o educación a través del territorio europeo, con la finalidad de alcanzar un nivel común que permita contribuir positivamente a la brecha de profesionales y analizar el estado del conocimiento sobre la manera en que se está gestionando el talento y los *skills* en ciberseguridad.

En consonancia con esto, los perfiles de ciberseguridad que se detallan en este estudio son el resultado de profundizar en el *European Cybersecurity Skills Framework* (ECSF). Es importante notar que los esfuerzos apuntan a poner en marcha un proceso de desarrollo de un *Framework* europeo integral de *skills* en ciberseguridad, que proporcionaría una base para la comunicación continua entre diferentes stakeholders (gobierno, industria, academia, responsables de políticas y la misma ciudadanía).

La estructura que permite visualizar la consolidación y el trabajo realizado por ENISA mantiene la misma forma que la mayoría de taxonomías y consiste fundamentalmente de los siguientes elementos:

El Framework de ENISA es un proyecto actualmente en proceso de diseño, revisión y validación por parte de un grupo de trabajo específico que lo componen expertos de la cadena de valor de la ciberseguridad tanto del ámbito público, como privado y académico de diferentes regiones en Europa. En este sentido, es imperativo destacar que los perfiles de ciberseguridad reflejados a continuación van a ir evolucionando durante los próximos meses en función de los talleres y sesiones de trabajo que están teniendo lugar actualmente y también con base en las necesidades de la UE y cada uno de sus estados miembros.

12 Perfiles de Ciberseguridad

1 Chief Information Security Officer (CISO)	7 Incident Responder
2 Legal, Policy and Compliance Officer	8 Digital Forensics Investigator
3 Cibersecurity Architect	9 Penetration Tester
4 Cibersecurity Implementer	10 Cybersecurity Auditor
5 Researcher	11 Cybersecurity Risk Manager
6 Educator	12 Cyber Threat intellligence specialist

Tabla 3. Perfiles de ciberseguridad del ECSF Framework

Estos perfiles son los que ENISA actualmente considera tienen una mayor aplicación en el ámbito empresarial a nivel europeo, pero no se debe ignorar la complejidad que tiene la ciberseguridad por naturaleza, lo cual indica que los roles irán evolucionando, y con ellos nuevos conocimientos y capacidades serán necesarias. Adicionalmente, se presume que la aplicación de un *Framework* como el ECSF y los perfiles allí incluidos, tienen un uso específico tanto para la industria de la ciberseguridad o las empresas (públicas y privadas), como para las instituciones educativas o el sector de la educación (academia). Por esta razón es importante procurar hacer esta distinción, ya que de esta manera es posible notar que los beneficios que se pueden obtener para ambos grupos también difieren considerablemente.

De cualquier forma, las organizaciones deben hacer un ejercicio de autoevaluación que les permita conocer realmente qué componentes les está aportando más valor a la organización y por qué. Esta es una práctica que permite actualizar o revisar la aplicabilidad de la herramienta y permite una mayor sinergia con la información contenida en los perfiles de ciberseguridad. Idealmente, este tipo de herramientas sirven de base para lograr una fuerza laboral más competente, completa y que se entiende en un mismo lenguaje con otros profesionales a nivel europeo.

7_ CONCLUSIONES Y RECOMENDACIONES

Durante la elaboración del diagnóstico del talento de ciberseguridad en España ha quedado en evidencia que el ecosistema de ciberseguridad refleja una gran experiencia y profesionalización, además de un alto compromiso en lograr que España se posicione como un país líder en la región en materia de ciberseguridad.

Las recomendaciones que derivan de este proyecto de análisis son el punto de partida para garantizar una industria de ciberseguridad robusta y rentable que se caracterice por poner en el núcleo de las iniciativas el talento de las personas. En este sentido, toda la cadena de valor de ciberseguridad puede ver este estudio como una oportunidad de conectarse más y comprender mejor el talento de ciberseguridad en España, ayudando a dar forma y refinar aún más las iniciativas futuras que serán la esencia para superar los desafíos que se tienen como industria.

Sin embargo, abordar la problemática de dicho talento es una tarea en la que intervienen múltiples agentes. No basta con poder formar de manera adecuada el talento en ciberseguridad. Es necesario actuar sobre la parte de la generación del talento de ciberseguridad, de la atracción y contratación de dicho talento, así como la gestión y retención. Por ello, se recogen de manera específica, recomendaciones encaminadas a mejorar la función de los agentes que tienen responsabilidad en cada una de estas etapas del ciclo de gestión el talento de ciberseguridad. Desde la Administración Pública en la definición de políticas y actuaciones que incidan en la mejora de dicho talento, las organizaciones encargadas de la formación, empresas de selección de personal, así como el propio tejido empresarial.

Todo ello, para establecer un conjunto de palancas clave que ayudan a definir el plan de acción que establezca los objetivos y acciones concretas que deberán ponerse en práctica con el objetivo de incrementar el talento de ciberseguridad en España.

7.1_ Recomendaciones generales de gestión de talento digital

Tras el análisis realizado, se presentan a continuación un conjunto de recomendaciones que inciden en los diferentes bloques del ciclo de vida del talento segmentados en función del área dentro del ciclo de vida del talento donde pertenece, tal y como muestra la siguiente tabla:

	Identificación	Atracción	Gestión	Estructurales
Evolución de la función de recursos humanos.	✓	✓	✓	✓
Crear cultura de atracción e incorporación de talento.		✓		
Formación y capacitación de los empleados.	✓	✓	✓	
Establecer una trayectoria profesional clara y plan de desarrollo individual.		✓	✓	
Nuevos modelos de trabajo flexible en las organizaciones.		✓	✓	✓
Identificación de necesidades de talento.	✓	✓		✓
Modelos de retribución adaptados a la transformación digital.			✓	✓
Autoformación y certificados como complemento.	✓	✓	✓	✓

Tabla 4. Encuadre de las recomendaciones en las diferentes etapas del ciclo de gestión del talento. Fuente: propia

A continuación, se detallan y desarrollan las recomendaciones propuestas, describiendo tanto el contexto en el que se proponen, así como las acciones requeridas para su desarrollo.

Evolucionar la función de Recursos Humanos hacia la gestión de personas y talento en el nuevo contexto digital

· La gestión del talento en el contexto digital requiere transformar la operativa de los departamentos de recursos humanos. El mundo del trabajo del futuro le demanda al área una transformación para contribuir, con una perspectiva humana, a resolver desafíos de negocio e impactar en la rentabilidad con sus acciones. Las principales problemáticas que enfrenta el área hoy tienen que ver con la alta rotación, el engagement de los empleados y la necesidad de generar el hábitat adecuado para la convivencia intergeneracional.
· De manera específica, estableciendo mecanismos para identificar e incorporar el talento que requiere la organización, acordes con los requerimientos y visiones específicas de las distintas unidades de negocio, favoreciendo de esta forma, un proceso de identificación, atracción y gestión del talento adaptado a las casuísticas de los diferentes departamentos de las organizaciones.

Establecer una trayectoria profesional clara con planes de desarrollo y mentores para apoyarles.

· Incorporar revisiones enfocadas al establecimiento de objetivos y la gestión del rendimiento que permitan a los empleados desarrollar las áreas que necesitan dominar para llegar al siguiente nivel es una necesidad en el contexto actual.
· Es necesario demostrar a los empleados que sus roles son valiosos y cuál es su encaje dentro de la estrategia de la organización. Por tanto, es fundamental comunicar cómo los objetivos individuales de cada trabajador se alinean con las estrategias corporativas de manera frecuente y continua.

Crear cultura de atracción e incorporación de talento en las organizaciones.

· Crear una estrategia de atracción de talento multicanal (*off line y on line*) que combine el reclutamiento tradicional más reactivo y orientado a cubrir vacantes abiertas, con el *inbound recruiting*, plataformas de *e-recruiting*, redes sociales profesionales como LinkedIn, bases de datos optimizadas con diferentes tecnologías relacionadas con la inteligencia artificial (*data mining*, por ejemplo) y mucho más, estructurando un canal de atracción del talento adecuado con independencia de si existe o no una vacante abierta.
· Así mismo, el diseño de un programa de on boarding que facilite la rápida integración y que el nuevo empleado se familiarice con la empresa y la cultura es una parte fundamental de la experiencia de incorporación del empleado.
· Requiere proporcionar a los nuevos empleados información sobre cómo gestionar sus objetivos profesionales desde el primer momento.

Incorporar nuevos modelos de trabajo flexibles en las organizaciones.

· La transformación del puesto de trabajo sufrida como consecuencia de la pandemia de COVID-19 ha supuesto el desarrollo e implantación de modelos de trabajo flexible dentro de las organizaciones. Según datos de IDC, el 30% de los trabajadores en 2021 estaría en movilidad, y esta tendencia es creciente en el periodo 2022-2025.
· Por ello, disponer de modelos de teletrabajo que permitan al empleado desarrollar su actividad en movilidad será un factor diferencial en las organizaciones.
· De hecho, el Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia, regula el contexto en el que los trabajadores pueden acceder a este tipo de teletrabajo, por lo que será fundamental contar con planes de transición al trabajo flexible, compatibles con el desarrollo del negocio.

Formación y capacitación de los empleados como elemento a fortalecer en este contexto digital.

· Mantener a los empleados comprometidos mediante la creación de una experiencia digital superior para ellos a través del autoaprendizaje, las herramientas de recursos humanos y las tecnologías modernas, es esencial en el contexto actual.
· Esto les permite desempeñar su función de manera más eficiente y gestionar el equilibrio entre la carrera profesional y la vida personal.

Autoformación y certificados como complemento.

· Una de las palancas en las que se está apoyando la industria a la hora de conseguir la oferta necesaria de talento es sin duda el autoaprendizaje.
· La autoformación, puede ser abordada como una alternativa a la formación reglada, sin embargo, en la mayor parte de los casos se enfoca como un complemento o potenciador de la misma, ya sea de manera simultánea, previa o posterior a una formación reglada.

Modelos de retribución adaptados a la transformación digital.

· La pandemia de COVID 19 ha acelerado la digitalización en las organizaciones, transformando no sólo las estrategias de tecnología, sino los modelos de negocio y la organización y gestión del talento . La monitorización del empleado y la búsqueda de incrementar la productividad de los empleados en este nuevo contexto digital requiere repensar cómo se está realizando la gestión y retención del talento en un entorno híbrido , ya que el incremento de ofertas de trabajo en modo remoto de organizaciones puede influir de manera directa la fuga de talento.
· Por ello, las empresas deben abordar el análisis de los salarios, complementos y prácticas organizacionales como vía para ayudar a la atracción y retención del talento digital.

7.2_ Recomendaciones específicas de gestión de talento en ciberseguridad

Es necesario estructurar e implementar prácticas eficaces que incidan en la gestión de este tipo de talento específico en las organizaciones. La importancia de la ciberseguridad para la supervivencia de las organizaciones exige la necesidad de afrontar el problema de la identificación de este tipo de talento específico en ciberseguridad, la evolución en el proceso de reclutamiento y *onboarding*, así como la adopción de acciones que contribuyan a mejorar la gestión y paliar la fuga del talento.

Por ello, el impulso de políticas nacionales, coordinadas desde la administración que pongan el foco en potenciar e impulsar iniciativas para que la ciberseguridad sea una prioridad estratégica en las organizaciones, así como estructurar y vertebrar un itinerario formativo para el desempeño de la ciberseguridad como actividad profesional se erigen como prioridades sobre las que tanto organizaciones como empresas de reclutamiento de personal establecerán en sus acciones para la identificación, atracción, reclutamiento y gestión del talento de ciberseguridad.

De esta forma, en este epígrafe, se establecen un conjunto de recomendaciones que esta tipología de agentes (Administración Pública, empresas de reclutamiento de personal y otras organizaciones) podría implementar para incrementar el talento en ciberseguridad en España.

7.2.1_ Para el sector público.

Los resultados del diagnóstico y del trabajo de campo realizado, muestran la necesidad de establecer políticas y actuaciones coordinadas desde la administración que incidan en la sensibilización de la importancia de la ciberseguridad a todos los niveles, así como establecer mecanismos que faciliten la estructuración de los programas educativos en sintonía con las demandas de las empresas. En este sentido, las principales recomendaciones son las siguientes:

Sensibilizar a las empresas y la sociedad sobre la importancia de la ciberseguridad y el valor del profesional de la ciberseguridad.

La importancia creciente de la seguridad en los datos y sistemas gestionados por las empresas para el funcionamiento y sostenibilidad de su negocio, hacen que el papel y valor del profesional de la ciberseguridad sea cada vez más relevante.
Es importante establecer campañas de sensibilización que pongan de relevancia el coste de un ciberataque, así como la labor de este tipo de profesionales.

Impulso de la formación profesional para generar talento de ciberseguridad.

La nueva Ley de Formación Profesional sin duda ayudará a generar talento en ciberseguridad.
Sin embargo, debe ir acompañada de una mejora en el acceso a la misma (modificación de los requisitos de acceso[10]), así como un profesorado amplio y mixto (que incorpore profesionales del ámbito privado) capacitado que facilite su extensión a toda la geografía nacional.

Estimulación de la vocación en edades tempranas.

Generar el talento de ciberseguridad desde edades tempranas es la base para poder desarrollar y articular posteriores programas que incidan en el desarrollo y capacitación del talento.
Por ello, la generación de futuros talentos en ciberseguridad pasa necesariamente por la incorporación de programas que incidan (mediante técnicas de gamificación y otros recursos) en la estimulación de estos estudiantes hacia estudios relacionados con tecnología y, de manera específica, en ciberseguridad.

Marco de responsabilidades de las organizaciones en materia de ciberseguridad y confianza digital.

Establecimiento de la normativa necesaria que contemple el marco de responsabilidades de las organizaciones en materia de ciberseguridad y confianza digital, así como hacia los requisitos, responsabilidades y capacitaciones que deben cumplir los profesionales que ocupen puestos críticos en esta materia, en particular, los responsables de privacidad, ciberseguridad o auditoría informática.

Establecer un itinerario formativo para el desempeño de la ciberseguridad como actividad profesional.

Determinar una hoja de ruta que detalle de manera clara la tipología de perfiles que existen en el ámbito de la ciberseguridad, así como los conocimientos, habilidades y experiencia necesaria para poder acceder a ellos.
De igual forma, disponer de una hoja de ruta específica que establezca la formación, capacidades y habilidades que debe disponer un profesional que quiera evolucionar de un perfil de ciberseguridad definido a otro, se erige como una necesidad que aporta eficiencia a los procesos de búsqueda de talento interno en la organización y fomenta el reciclaje del talento.
Para ello, disponer de un programa de estudios, becas o ayudas asociadas a los diferentes programas formativos, certificaciones, eventos disponibles, puede ayudar a facilitar el proceso de formación y transición.

Revisión del marco de certificación de capacidades autodidactas.

De forma que las capacidades que los estudiantes y trabajadores adquieren de manera autodidacta a través de MOOC, retos, hackatones, jornadas, eventos, etc., puedan consolidar y demostrar las habilidades adquiridas ante una empresa o un nuevo reto profesional.

10 Para acceder a este curso de especialización se debe acreditar alguna de las Formaciones Profesionales Superiores de Administración de Sistemas Informáticos en Red, Desarrollo de Aplicaciones Multiplataforma, Desarrollo de Aplicaciones Web, Sistemas de Telecomunicaciones e Informáticos, o Mantenimiento Electrónico.

7.2.2_ Para los reclutadores de talento y/o empresa.

Fruto de las conclusiones y recomendaciones identificadas en los apartados anteriores, se propone la puesta en marcha de una serie de acciones que incidan específicamente en el papel que reclutadores de talento y departamentos de selección de personas en las empresas tienen en la actualidad para la incorporación del talento de ciberseguridad. En concreto:

Mejorar los procesos de reclutamiento del talento de ciberseguridad.

Los resultados del diagnóstico realizado arrojan que el talento de ciberseguridad requiere de un proceso de reclutamiento diferente al que se realiza en la actualidad. La necesidad de afinar en el establecimiento del perfil del candidato, así como el tiempo medio en incorporación del profesional, requieren repensar la forma en la que se está realizando el proceso de reclutamiento con la posibilidad de incorporar tecnología para mejorar los procesos de reclutamiento mediante la incorporación de gaming y otras acciones.
Por ello, es esencial establecer un proceso de definición del perfil requerido, responsable del proceso de reclutamiento y las diferentes etapas del proceso.

Disponer de una taxonomía de puestos de ciberseguridad dentro de la organización que permita establecer las necesidades del talento de ciberseguridad.

Disponer de una taxonomía de referencia alineada con lo que se está trabajando en Europa, facilitará no solo la tarea de empresas de reclutamiento de personal, así como de empresas y profesionales, facilitará establecer la tipología de perfiles que existen en las empresas y aquellos que se requieren, así como facilitará el establecimiento de una hoja de ruta común para escoger aquellos perfiles que les interesan y poder especializarse en ellos.
De esta forma, será más sencillo establecer el perfil del talento a reclutar, identificando claramente las competencias y capacidades que se requieren para los diferentes perfiles.

Mejorar los programas de formación de las empresas.

Los resultados del estudio arrojan que 2 de cada 10 posiciones de ciberseguridad se están provisionando con personal interno.
Por ello, como primer paso será necesario disponer de un perfil de cada trabajador, que identifique claramente cómo prefiere relacionarse el empleado con los trabajadores, cómo reúne y utiliza la información, cómo toma decisiones o cómo se organiza a sí mismo y a los demás. De esta forma, será posible disponer de un conjunto de perfiles potenciales para reciclar en la organización y se podrá proponer un programa de formación que facilite el reciclaje y capacitación de empleados internos para futuras vacante en este ámbito.

Mejorar los modelos retributivos para el personal de ciberseguridad.

Más allá de la necesidad de adaptar los modelos retributivos de los empleados al contexto digital, el dinamismo del mercado de la ciberseguridad requiere entender las necesidades económicas y de carrera de estos empleados, así como la oferta existente en el mercado. Por ello, establecer, claramente, el plan de carrera, las promociones e incentivos de cada posición, o el modelo de trabajo, responsabilidades y oportunidades de desarrollo es clave para luchar contra la fuga del talento.

Reclutar donde está el talento.

La especificidad en cuanto a conocimientos y competencias del talento de ciberseguridad requiere abordar el problema de la identificación del talento de una manera diferente a cómo se está realizando en la actualidad. Iniciativas como la Liga Nacional Interuniversitaria de retos en el ciberespacio (desarrollada por la Guardia Civil), C1b3rWall Academy (ofrecida por la Policía Nacional), hackatones, eventos y ferias específicas son algunos ejemplos que muestran la necesidad de orientar las acciones de reclutamiento específico de este tipo de talento.

7.2.3_ Para las instituciones formativas

La formación, sin duda, es uno de los principales pilares de actuación para incrementar el número y calidad del talento de ciberseguridad en España. De las conclusiones obtenidas en el diagnóstico, se requieren actuaciones que incidan en el alineamiento de la oferta de formación con las necesidades de las empresas. En gran parte, es debido a la ausencia, como ya se ha comentado, de un itinerario formativo claro para trabajar en ciberseguridad, así como los requisitos para el acceso, etc.

Por ello, a continuación, se propone un conjunto de recomendaciones específicas para este tipo de instituciones que facilitarían el incremento del número y calidad del talento de ciberseguridad en España.

Alineación de los programas formativos a las necesidades de las empresas.

A pesar de la oferta disponible en España, la realidad muestra que hay un desalineamiento entre oferta y demanda. Por ello, es esencial estructurar programas que incorporen la visión y necesidades de la industria en los diferentes currículos formativos, así como introducir contenidos prácticos que permitan adquirir las competencias y capacidades que se requieren en la profesión. De esta forma, posteriormente será posible establecer convenios de colaboración entre los centros participantes y las empresas del sector que vertebren un sistema de becas, facilitando la identificación y posterior incorporación de talento de ciberseguridad.

Refuerzo de las soft skills dentro del itinerario formativo.

El análisis realizado enfatiza la necesidad de las soft skills como base para el desarrollo de competencias en el talento. Se hace indispensable la adecuación de los programas formativos, o la creación de otros nuevos específicos que incidan en el desarrollo de estas soft skills como elemento fundamental en el proceso de desarrollo de talento de ciberseguridad.

Modificar los requisitos de acceso a los programas de formación actuales.

Actualmente se requiere un estudio de grado para el acceso a programas de máster, así como a otro tipo de formación certificada. Flexibilizar y modificar los requisitos de acceso, facilitaría el acceso a los mismos a talento autodidacta, favoreciendo el proceso de reconocimiento de competencias y capacidades, incrementando la oferta de talento de ciberseguridad.

Formación del profesorado en materia de ciberseguridad.

La adecuación de los programas formativos o la creación de otros nuevos específicos no será posible si no se dispone de profesorado correctamente capacitado para poder impartirlo. Se deben impulsar fórmulas de apoyo a profesores e investigadores para que puedan acceder a una especialización e investigación avanzada, con el objetivo último del desarrollo de sus capacidades en aras de la excelencia en ciberseguridad. Entre estos podrían considerarse la trasferencia de profesionales al ámbito empresarial (de manera temporal o permanente), colaboraciones con empresas, emprendimiento, etc., así como programas estables de formación para el profesorado.