ANÁLISIS Y DIAGNÓSTICO DEL TALENTO DE CIBERSEGURIDAD EN ESPAÑA

marzo 2022

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

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Carme Artigas Brugal
Secretaria de Estado de Digitalización e Inteligencia Artificial

PRESENTACIÓN

España está inmersa en una transformación digital de su economía y sociedad. Esta realidad ha experimentado un salto disruptivo como consecuencia de la pandemia, extendiendo de este modo la superficie de riesgo cibernético para ciudadanos, empresas y gobiernos.

La protección frente a ciberamenazas y la generación de confianza en el entorno digital, aprovechando a su vez las potencialidades de un sector industrial emergente, es fundamental para el desarrollo socioeconómico y confirman que la ciberseguridad debe ser abordada desde una perspectiva multidimensional, como elemento clave de la seguridad nacional, pero también para asegurar una transformación digital confiable y segura así como para impulsar el crecimiento económico y la generación de empleo de calidad.

En este contexto, España debe seguir avanzando de manera decidida hacia la consolidación de una industria de la ciberseguridad resiliente y robusta, que permita hacer frente a todos estos desafíos y explotar nuestras potencialidades como país. En ese sentido, uno de los elementos comunes, y clave, para el desarrollo de esta industria es el talento multidisciplinar en ciberseguridad, que se ha convertido en un recurso escaso a nivel global para esta industria.

Para conocer la realidad especifica de nuestro país, el Instituto Nacional de Ciberseguridad (INCIBE), ha realizado el presente *Análisis y Diagnóstico del Talento de Ciberseguridad en España*, que identifica de manera detallada la situación actual, al tiempo que ofrece escenarios futuros para ayudar a la industria y las administraciones públicas en la búsqueda de soluciones para la identificación, generación y transformación de talento.

Lo que este informe nos señala es que la detección y promoción del talento en ciberseguridad debe ser una prioridad para alcanzar un proceso de transformación digital confiable y seguro. España debe seguir trabajando para consolidar una industria de ciberseguridad comprometida con la diversidad e inclusión, y el desarrollo de talento será el motor que permitirá que la ciberseguridad continúe siendo un activo económico y estratégico nacional.

Del mismo modo, el entorno cambiante de la ciberseguridad evoluciona rápidamente y las ciberamenazas están en constante transformación. Por ello, es necesario el desarrollo de una estrategia de gestión del talento en ciberseguridad a nivel nacional que permita adelantarse a las necesidades del sector y que contribuya a cerrar la brecha de profesionales existente actualmente.

Este estudio también nos invita a abordar que la escasez de talento es una de las prioridades más apremiantes en toda la cadena de valor de la ciberseguridad, y se necesita invertir recursos para mejorar las capacidades y apoyar a los profesionales actuales y futuros, así como involucrar distintos colectivos y alinear las agendas intelectuales e intereses particulares de la academia y las instituciones públicas y privadas. Sólo de esta manera se logrará generar confianza e impulsar el potencial digital que tiene España.

El estudio constituye un análisis del panorama actual de ciberseguridad y pone de manifiesto la necesidad de continuar el progreso a nivel mundial para poder prevenir los ataques disruptivos a los que se enfrenta la industria, así como el obligado impulso al talento humano, clave en este proceso de defensa. Las organizaciones participantes reconocen el valor y la necesidad del talento en ciberseguridad, y es, por tanto, un compromiso ineludible entender las necesidades específicas de la oferta y la demanda, contar con políticas públicas bien definidas y estandarizar el trabajo realizado en ciberseguridad, todo ello alineado con las directrices europeas.

Abordar los retos de identificar, atraer, desarrollar y retener talento es un ejercicio dinámico que debe llevarse a cabo de manera rigurosa y comprometida. Este estudio es un recurso con una visión holística de la situación en materia de gestión de talento de ciberseguridad en España, y es también una invitación a la colaboración de los diversos agentes y actores del ecosistema de ciberseguridad para actuar y poder aprovechar así, en mejores condiciones, los beneficios de la transformación digital.

ÍNDICE

PRESENTACIÓN	2
ÍNDICE	5
1. Introducción.	11
2. Objetivos y alcance del estudio.	13
2.1. Antecedentes e introducción al proyecto	13
2.2. Objetivo y visión global del proyecto	14
3. Análisis de la industria de ciberseguridad	17
3.1. La industria de la ciberseguridad en cifras	17
3.2. Tendencias del mercado de la ciberseguridad y el impacto en otras industrias.	23
3.2.1. Impacto de la pandemia de la COVID-19 en la demanda de servicios digitales	23
3.2.2. Crecimiento exponencial de los datos y auge de las Data Driven Companies	24
3.2.3. Privacidad de los datos y el impacto de la normativa GDPR	25
3.2.4. Trabajo en remoto	26
3.2.5. Tendencias específicas para las industrias más relevantes	27
3.3. Análisis de los agentes de la cadena de valor de la ciberseguridad en España. Mapa de agentes y relaciones.	33
3.4. Contexto del estado actual del Talento de Ciberseguridad en España	34
4. Diagnóstico del talento en ciberseguridad en españa.	38
4.1. Caracterización de la oferta de talento en ciberseguridad	38
4.1.1. Análisis cuantitativo de la oferta de talento en ciberseguridad	38
4.1.2. Análisis cualitativo de la oferta de talento en ciberseguridad	49
4.1.3. Conclusiones	62
4.2. . Caracterización de la demanda de talento en ciberseguridad	64
4.2.1. Análisis cuantitativo de la demanda de talento en ciberseguridad	64
4.2.2. Análisis cualitativo de la demanda de talento en ciberseguridad	68

4.2.3. Conclusiones	94
5. Análisis de las iniciativas internacionales de gestión de talento	**97**
6. Definición de un modelo de caracterización de los perfiles de ciberseguridad en españa.	**110**
6.1. Perfiles	112
6.2. KSA	113
6.3. Aplicación en la Industria de la Ciberseguridad o Empresas (públicas y privadas)	116
6.4. Aplicación en Instituciones Educativas (academia)	116
7. Recomendaciones	**118**
7.1. Generales de gestión de talento digital	119
7.2. Específicas de gestión de talento en ciberseguridad	122
7.2.1. Para el sector público.	123
7.2.2. Para los reclutadores de talento y/o empresa.	124
7.2.3. Para las instituciones formativas	125
ANEXOS	**126**
Anexo I. Detalle de formaciones profesionales superiores que dan acceso al curso de especialización en ciberseguridad	126
Anexo 2. Características de las certificaciones de ciberseguridad más relevantes	131
Anexo 3. Análisis de taxonomías de ciberseguridad	133
Anexo 4. Benchmark internacional de gestión de talento en ciberseguridad.	161
Ministerios y Secretarías de Estado afectadas	162
Panel de Expertos	163
ÍNDICE DE FIGURAS	**162**
ÍNDICE DE TABLAS	**165**
Colaboradores	166

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 el INCIBE 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.

1.1_ La importancia del talento en ciberseguridad

La eficacia en proteger un país depende en gran medida de las capacidades de su gente, y las estimaciones que se tienen en este respecto es que para 2022, **España podría alcanzar una fuerza laboral en ciberseguridad cercana a los 122.284** trabajadores con una brecha de talento que se estima en 24.119. 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 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. 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 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

2.1_ Antecedentes e introducción al proyecto

El Instituto Nacional de Ciberseguridad de España (INCIBE) es una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial; y la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, y las empresas, y de la red académica y de investigación española (RedIRIS).

La misión de INCIBE es mejorar la ciberseguridad y la confianza digital de ciudadanos, menores y empresas privadas de España. Además, su cometido incluye la protección y defensa de estos colectivos, el impulso de la industria española y la I+D+i en ciberseguridad, así como la identificación, generación y atracción de talento al sector de la ciberseguridad.

Para ello, INCIBE mantiene una visión que guía su actuación e implica que:

El nivel de ciberseguridad de ciudadanos y empresas en España se sitúe entre los cinco mejores del mundo.

La innovación y oferta de productos, servicios y profesionales relacionados con la ciberseguridad en España esté considerado entre los cinco mejores del mundo.

INCIBE se posicione como referente europeo en al ámbito de la ciberseguridad.

La Estrategia Nacional de Ciberseguridad de 2019[1] reconoce el papel clave que juega la ciberseguridad en el entorno actual de transformación e incertidumbre y la oportunidad que ofrece para incrementar la competitividad de España.

Alineado con el objetivo 4 de la Estrategia, la línea de acción 5 pone de manifiesto la importancia de potenciar la industria española de ciberseguridad, además de la generación y retención de talento para el fortalecimiento de la autonomía digital

Por su parte, el Plan España Digital 2025[2] , cuaderno de bitácora para la transformación digital del país, destaca la urgencia de articular una Agenda actualizada que impulse la transformación digital de España

1 https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

2 https://portal.mineco.gob.es/ca-es/ministerio/estrategias/Pagines/00_Espana_Digital_2025.aspx

como una de las palancas fundamentales para relanzar el crecimiento económico, la reducción de la desigualdad, el aumento de la productividad y el aprovechamiento de todas las oportunidades que brindan las nuevas tecnologías.

En su eje estratégico 4, dedicado monográficamente a la ciberseguridad, incorpora las medidas que configuran los 3 ejes de actuación de INCIBE para los próximos años: incrementar las capacidades de ciberseguridad de ciudadanía y empresas, impulsar el ecosistema de ciberseguridad español en torno a su industria, el I+D+i y el talento en ciberseguridad; y consolidar a España como nodo internacional en el sector. España Digital 2025 ya reconoce el papel clave del talento en ciberseguridad como motor para el impulso del sector. INCIBE, a través de su Plan Estratégico 2021-2025[3], apoya el proceso de transformación digital segura y confiable en el marco de seguridad nacional y alineada con la Agenda España Digital 2025. En estos esfuerzos, INCIBE cuenta con los fondos del Plan de Recuperación, Transformación y Resiliencia 'España Puede', que destinan a la institución una financiación extra de más de 560 millones de euros para acometer iniciativas estratégicas, entre las que se encuentran algunas de ellas vinculadas al talento en ciberseguridad.

El talento en ciberseguridad es una piedra angular de las acciones realizadas desde INCIBE. Sin talento es imposible desarrollar una industria fuerte ni las soluciones de alto valor añadido necesarias para participar en un mercado altamente competitivo como es el de la ciberseguridad. Sin embargo, la información existente sobre el estado del talento en el sector de la ciberseguridad en España es variada y fragmentada, procedente de diversas fuentes, que dificulta la comprensión profunda del entorno necesaria para encauzar acciones.

En este contexto, con el objetivo de estar más preparados para el cumplimiento y seguimiento de los mandatos encomendados, se hace necesario un diagnóstico del talento en el sector de la ciberseguridad en España como punto de partida para calibrar y orientar acciones futuras, así como sentar las bases para un análisis evolutivo.

2.2_ Objetivo y visión global del proyecto

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.

3 https://www.incibe.es/que-es-incibe/que-hacemos#estrategico

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

Figura 2. Estructura de fases del trabajo de diagnóstico de talento de ciberseguridad en España

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 en las organizaciones y los perfiles profesionales es evidente.

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.

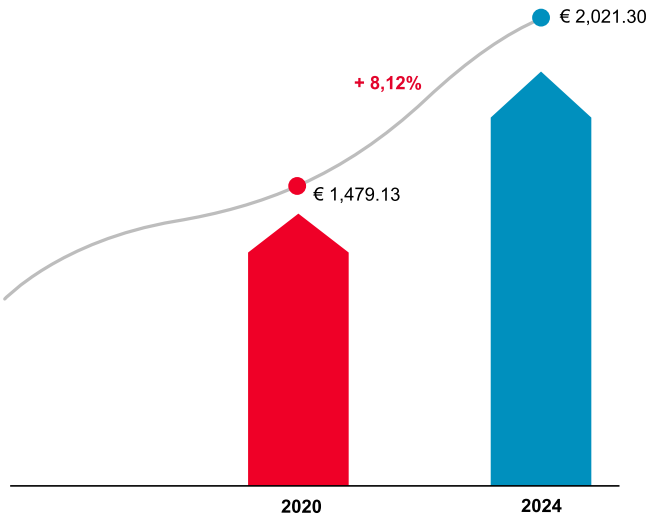


Figura 3. Tamaño de mercado de la seguridad (en M€). Fuente: Security Spending Guide IDC 2021

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.

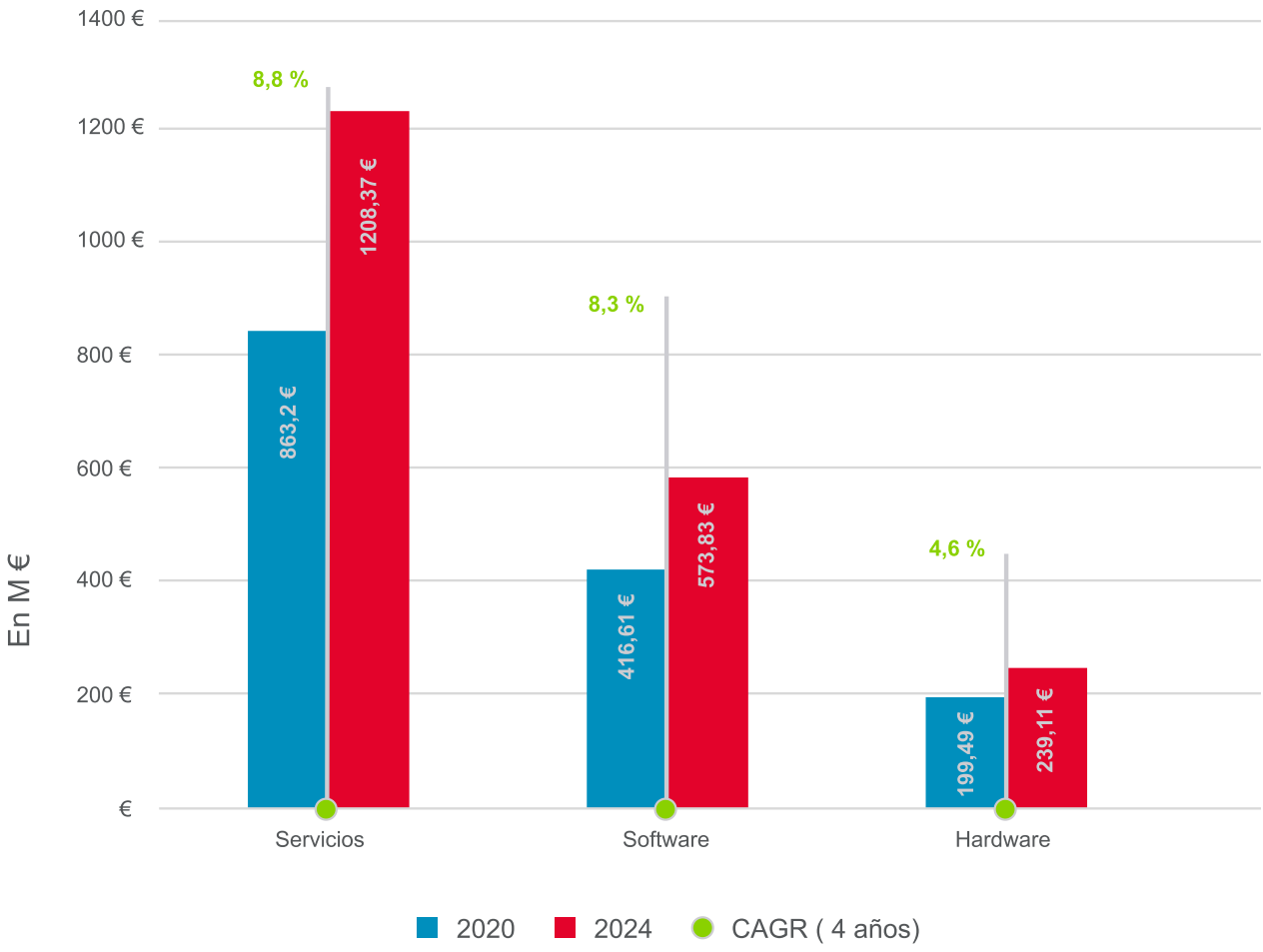


Figura 4. Tamaño de mercado por grupo de tecnología. Fuente: Security Spending Guide IDC 2021

En relación con el talento en ciberseguridad, es importante analizar cómo es la estructura del mercado de la ciberseguridad, ya que la incorporación de tecnología y la rápida velocidad de cambio en las empresas está provocando una migración hacia el consumo de la seguridad como servicio (*Security as a Service*), fundamentalmente para hacer frente a:

Gestión de amenazas: incremento exponencial del volumen y variedad de amenazas, lo que requiere incrementar la diversidad de defensas necesarias. Así mismo, el alto grado de sofisticación de estas, sigilosas y evasivas, así como la gama de actores de amenazas (ciberdelincuentes, estado nación, ideológico, etc.), están configurando un escenario de complejidad que demanda nuevos perfiles de profesionales y soluciones de seguridad

Escasez de habilidades de seguridad: incremento de la dificultad y gastos de reclutamiento y retención de profesionales de seguridad cualificados de un grupo de mano de obra finito, que se suma la importancia de evitar el agotamiento de los analistas de seguridad.

El mercado de la ciberseguridad muestra como en los últimos años ha habido una tendencia en cuanto al crecimiento de los **servicios gestionados de seguridad**, con un 25,2%, seguido de los **servicios de integración de sistemas** con una cuota de mercado del 18,8%, lo cual supone casi la mitad del mercado de la ciberseguridad en España.

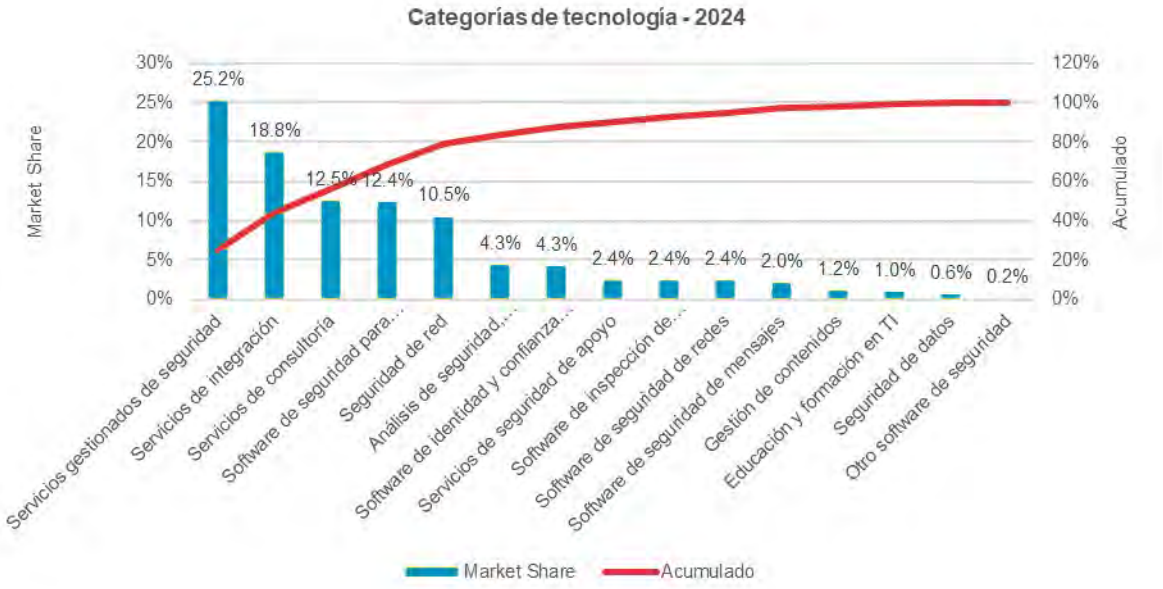


Figura 5. Tamaño de mercado por categorías de tecnología. Fuente: Security Spending Guide IDC 2021

Resulta necesario analizar las principales categorías dentro del mercado de ciberseguridad, ya que la prestación de los diferentes servicios que se encuadran en las mismas determina la necesidad de incorporar perfiles más específicos en las organizaciones.

La integración de sistemas, los servicios de externalización de redes y *endpoint*, así como la gestión unificada de amenazas se erigen como las principales áreas que están impulsando la demanda de talento de ciberseguridad. Las razones se centran en asegurar el proceso de digitalización que están acometiendo las empresas y el impacto que la transformación del puesto de trabajo supone sobre la gestión de los datos y los procesos de negocio.

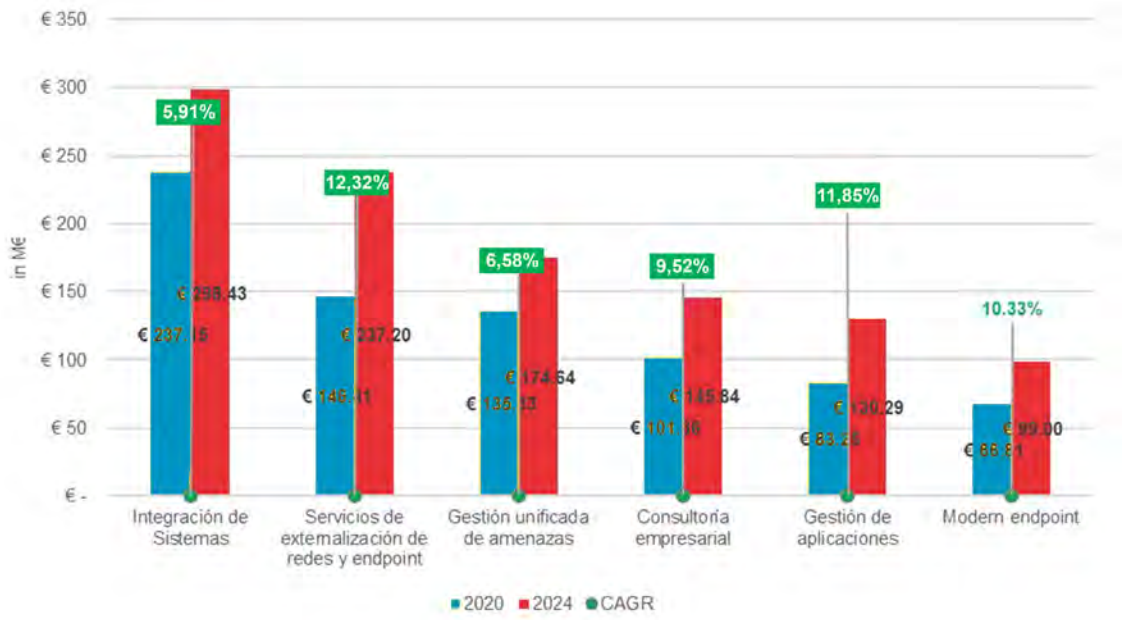


Figura 6. CAGR top 6 detalle de tecnologías. Fuente: Security Spending Guide IDC 2021

El tamaño de las organizaciones es relevante cuando hablamos de ciberseguridad, especialmente en relación con las prioridades de inversión en este mercado. Como se observa en la figura, el segmento de mediana y gran empresa está centrando sus demandas en la integración de sistemas, los servicios de externalización de redes y *endpoint* y gestión unificada de amenazas.

Figura 7. Gasto en ciberseguridad en mediana y gran empresa (M€). Fuente: Security Spending Guide IDC 2021

Sin embargo, en la pequeña empresa y micropyme, la prioridad es la protección del punto final (dispositivos móviles, ordenadores, etc.), por lo que la prioridad es el *modern endpoint* fundamentalmente para empresas que trabajen en los servicios profesionales y venta minorista, ya que en estos subsectores se presta especial atención a la protección al punto final.

Figura 8. Gasto en ciberseguridad en gran empresa. Fuente: Security Spending Guide IDC 2021

Por último, 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 experimentarán 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%.

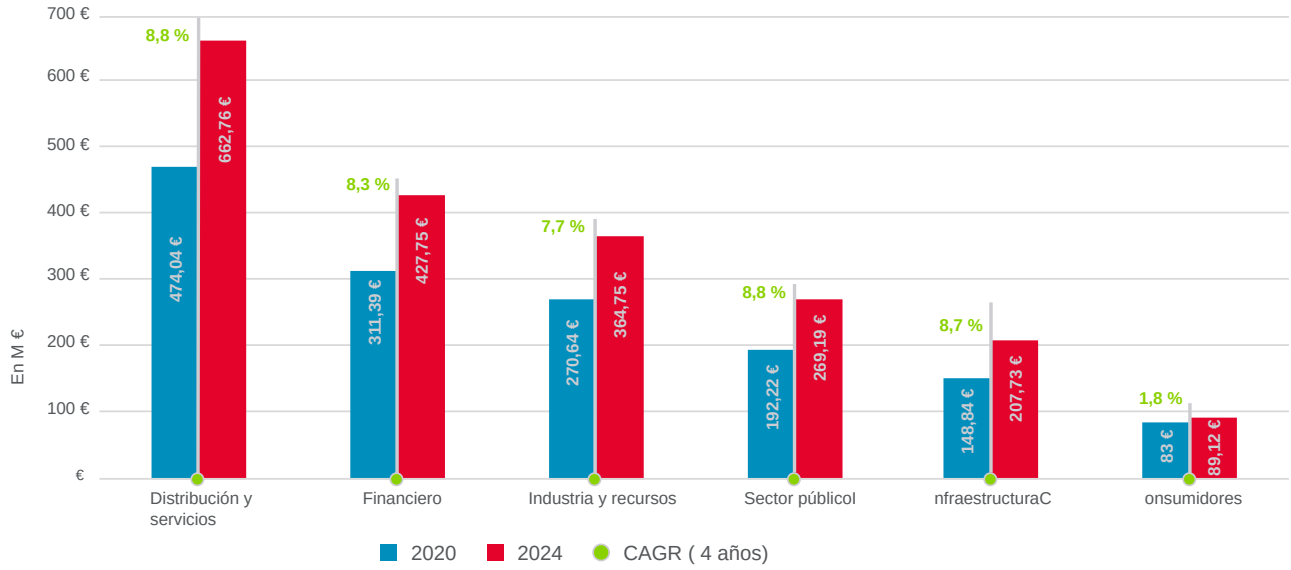


Figura 9. Tamaño de mercado de la ciberseguridad por sectores – Fuente: Security Spending Guide IDC 2021

Específicamente, banca, servicios profesionales y manufactura discreta, serán los principales subsectores que abarcarán mayor cuota de mercado de ciberseguridad en 2024. El subsector banca siempre ha tenido que prestar especial atención a la seguridad en todos sus procesos, ya que siempre ha sido un sector propenso a recibir todo tipo de ataques, pero ahora con la mayor adopción de la banca digital y la gestión del fraude creciente mucho más.

No obstante, las industrias que tendrán mayor tasa anual de crecimiento compuesto en el periodo 2020-2024, son la industria de venta al por mayor, cuyo CAGR ascenderá a un 9,0%, seguido de la venta al por menor con un 8,9% y la industria de los servicios profesionales con un CAGR del 8,4%. Esto puede explicarse debido al aumento en el comercio electrónico que se ha visto incrementado debido a la pandemia y afecta, tanto al comercio al por menor como al por mayor. Debido a esto, las empresas del sector tienen que invertir mucho más actualmente en materia de ciberseguridad para proteger a sus negocios de las múltiples ciberamenazas que están sufriendo ahora más que nunca.

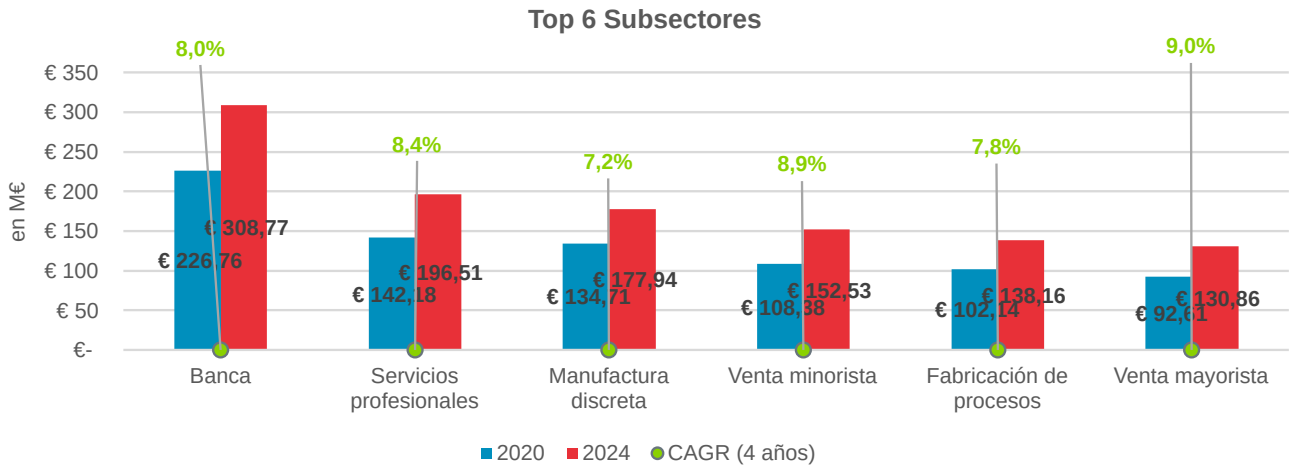


Figura 10. Tamaño de mercado de la ciberseguridad por subsectores – Fuente: Security Spending Guide IDC 2021

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 los mismos 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.

Finalmente abordaremos estas tendencias con un enfoque específico por los principales sectores del entorno económico español.

3.2.1_ Impacto de la pandemia de la COVID-19 en la demanda de servicios digitales

La pandemia del COVID-19 ha supuesto un impulso a la digitalización de las organizaciones al forzar a la ciudadanía a interactuar por canales digitales con empresas y administraciones públicas. Esto indudablemente ha tenido ciertos aspectos negativos, como el aumento de las amenazas en el universo cibernético, sin embargo, también ha hecho incrementar el mercado global de ciberseguridad y la demanda de talento y el planteamiento de nuevos perfiles o el consumo de la seguridad como servicio.

Todos los sectores están experimentando una transformación en la que la digitalización general del negocio y las disposiciones de servicios di-

gitales resultantes han sembrado el camino para nuevas formas de interactuar con el cliente.

En lugar de simplemente recibir bienes o servicios, los clientes están en una nueva posición de poder exigir servicios y personalizar la forma en que se presentan de manera que satisfaga sus necesidades actuales y futuras.

Las organizaciones deben encontrar formas de satisfacer esas necesidades para construir y asegurar experiencias y relaciones rentables y seguras con los clientes. La capacidad de ofrecer nuevos servicios innovadores basados en capacidades digitales distintivas es actualmente la única forma de retener y atraer nuevos clientes, especialmente los nativos digitales.

Las instituciones han implementado sistemas de validación digital, tratan la documentación digitalmente, emplean tecnología biométrica, unifican su gestión de seguridad con diferentes áreas de negocio, cuantifican y mitigan riesgos y en muchos casos, ya incursionan con inteligencia artificial para apoyar las soluciones de ciberseguridad.

La evolución del cliente digital es una realidad y la omnicanalidad segura es aparentemente el terreno donde las instituciones deben moverse, no hacerlo es sinónimo de ignorar el comportamiento del consumidor de hoy y podría deteriorar drásticamente la experiencia del cliente.

Por todo lo anterior, la demanda de servicios y talento relacionado con la ciberseguridad es un denominador común creciente en el conjunto de los sectores económicos en España.

3.2.2_ Crecimiento exponencial de los datos y auge de las *Data Driven Companies*

Los datos se han vuelto críticos para todos los aspectos de la vida humana en el transcurso de los últimos 30 años. 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. Esta existencia digital, definida por la suma de todos los datos creados, capturados y replicados en nuestro planeta en un año dado, está creciendo rápidamente, y lo llamamos la '*esfera de la información global*'.

En los últimos 10 años, la sociedad ha sido testigo de la transición de lo analógico a lo digital. Lo que la próxima década traerá usando el poder de los datos es virtualmente ilimitado. Mientras que nosotros como consumidores disfrutaremos de los beneficios de una existencia digital, las empresas de todo el mundo estarán abrazando oportunidades de negocios nuevas y únicas, impulsadas por esta riqueza de datos y el conocimiento que proporciona. Según datos de IDC, para el año 2025 la esfera de datos mundial crecerá hasta los 180 zettabytes (un billón de gigabytes). Todos estos datos permitirán desarrollar experiencias de usuario únicas y hacer posible un nuevo mundo de oportunidades de negocio. Por ello, es necesario pensar en los datos como un activo, de igual forma que es habitual considerar otros como el capital, recursos

humanos, o algunos intangibles, como patentes, marcas, etc. Esto está derivando en que, según datos de IDC, en 2021, el 50% del gasto de TI de las organizaciones está asociado al dato. Es en este contexto donde el desarrollo de nuevos productos o servicios apalancados en datos cobra una importancia capital en las organizaciones.

Por ello, se requiere un cambio en las estrategias de TI de las organizaciones para hacer frente al procesado y almacenamiento de estos datos, así como la gestión segura de los mismos.

3.2.3_ Privacidad de los datos y el impacto de la normativa GDPR

La entrada en vigor de GDPR ha establecido claramente las directrices a incorporar para la gestión y protección de los datos. La gestión del riesgo y el cumplimiento normativo tienen una clara implicación dentro del ámbito de la seguridad. La propia ley recoge consideraciones clave en materia de ciberseguridad, que van a condicionar en gran medida la necesidad de contar con estructuras, perfiles humanos y soluciones de seguridad que den respuesta a las exigencias de la ley en cuanto a adoptar 'medidas de seguridad apropiadas' que estén alineadas con el nivel de riesgo.

Sin embargo, en el contexto actual, existe una nueva dimensión interconectada del riesgo digital. En este escenario de interconectividad global, las fronteras de seguridad se difuminan y la inversión en seguridad necesaria para garantizar tanto la seguridad de dispositivos como de evitar fuga de datos, aumenta. El ciberterrorismo y el cibercrimen son las principales amenazas a las que nos enfrentamos en cualquiera de las industrias. Por ello, es necesario articular mecanismos de seguridad que permitan detectar, analizar y eliminar las amenazas, así como planes de actuación que permitan establecer con claridad qué hacer ante una brecha de seguridad. Si bien la ley deja a criterio de cada departamento de seguridad definir cómo proteger su información y demostrar a los auditores de GDPR que la infraestructura y procesos planteados son adecuados, de forma que sea posible notificar una brecha de seguridad dentro de las 72 horas posteriores al descubrimiento.

Para ello, la tendencia en la industria requiere una redefinición de la seguridad y enfoque hacia un modelo más seguro y proactivo frente a las amenazas. No solo 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), entre las que destacan las soluciones y políticas de acceso, de seguridad de red, soluciones de protección frente a amenazas avanzadas, así como soluciones de protección contra fugas de información por parte de los usuarios.

La protección contra las fugas de información es un punto crítico para el cumplimiento normativo, así como las soluciones de seguridad web y de correo electrónico. Según datos de Checkpoint y de IDC, el 60% de los ciberataques se produce a través del compromiso del correo electrónico

corporativo (BEC por sus siglas en inglés).

Por último, la regulación exige que la información que viaja por la red esté cifrada. Por ello, es necesario disponer de herramientas que permitan el cifrado de la información, incluyendo posibles indicadores de compromiso, así como posibles vulneraciones de la normativa al enviar información sin cifrar.

De hecho, la gestión de la información (37%), la privacidad y cumplimiento normativo (36%) y crear una cultura de seguridad (35%) son las tres principales prioridades de seguridad para las empresas europeas.

3.2.4_ Trabajo en remoto

La transformación del puesto de trabajo es una realidad que se ha visto impulsada por la pandemia del COVID-19. La adopción masiva del trabajo en remoto a nivel global ha manifestado las ventajas tanto para las empresas como para sus empleados, ya que mejora la experiencia del trabajador, permite la conciliación, aporta mayor flexibilidad e hiperconectividad.

Esta realidad se convierte en una tendencia compartida por la mayoría de las organizaciones, como se muestra en los datos de encuestas de organizaciones públicas y privadas.[4] Por ejemplo, para finales de 2021, el 30% de los trabajadores no volverán a la oficina de igual forma que antes de la pandemia. Por ello, los cambios de este nuevo espacio de trabajo tienen implicaciones no solo en el uso de herramientas de colaboración empresarial y de conexión y comunicación, sino también en la parte del espacio físico, y la propia cultura de la organización, que se vuelve más horizontal y colaborativa.

Por este motivo, disponer de un puesto de trabajo seguro y adaptado a las necesidades del empleado se ha convertido en una de las principales palancas para atraer y retener talento en las organizaciones. Las empresas han entendido que implantar un modelo de trabajo híbrido se traduce en una mayor movilidad del empleado, lo que requiere una cultura más abierta, colaborativa y horizontal que permite introducir nuevos recursos, como la monitorización de la productividad del empleado, o la automatización de procesos, o como, por ejemplo, la automatización de detección automática de amenazas de seguridad.

Cada vez más, las empresas convertirán los programas de transformación del puesto de trabajo en una prioridad de inversión en los próximos dos años, lo cual incluye inversiones en espacios de trabajo colaborativos, desarrollo del talento y herramientas de gestión para aumentar la experiencia y la productividad de los empleados. Además, la pandemia ha puesto de manifiesto la necesidad de que las organizaciones introduzcan cambios tecnológicos, de procesos y de políticas para lograr agilidad y adaptabilidad garantizando así la resiliencia y el éxito de la empresa a largo plazo.

En este escenario, las claves de este puesto de trabajo serán la seguri-

4 Encuesta europea IDC FoW (Futuro del trabajo), 2021

dad, la automatización y la mejora de las instalaciones. Pero para que sea así, se requiere garantizar un acceso equivalente a los recursos corporativos (incluyendo aplicaciones, datos, contenidos y colaboradores), no solo para impulsar la productividad y ofrecer una gran experiencia, sino también para permitir el crecimiento y la innovación de la organización.

La fuerza laboral híbrida incluye a los empleados comunes, así como a los contratistas y a los *GIG Workers* (trabajadores especializados que trabajan por proyecto en diferentes empresas – un tipo de subcontratación). Muchos de estos trabajadores no están necesariamente por sistema en el puesto de trabajo físico de la empresa para la cual esté haciendo el proyecto, por lo que es vital contar con los recursos para poder llevar a cabo el trabajo remotamente protegiendo los datos y facilitando un intercambio de información seguro y eficaz. Es por ello por lo que un 23% de las organizaciones europeas esperan que la arquitectura de la red se rediseñe y otro 26% espera que los sistemas de seguridad se rediseñen para apoyar a los trabajadores remotos.

Este hecho impacta de una manera muy clara en el talento y la escasez de habilidades de ciberseguridad, debido a la dificultad a la hora de reclutar talento con las habilidades necesarias. Los gastos en reclutamiento y la retención de profesionales de seguridad cualificados de un grupo de mano de obra limitado tampoco ayuda. Al no haber talento, las empresas destinan los recursos que de otro modo estarían destinados a personal cualificado, a la automatización y a la integración de entornos de seguridad. Precisamente por esto, según IDC, para 2023, como consecuencia de disponer de equipos pequeños en el área de seguridad, el 55% de las inversiones en seguridad empresarial se realizarán en marcos unificados de ecosistemas y plataformas de seguridad.

3.2.5_ Tendencias específicas para las industrias más relevantes

Tendencias distribución y servicios (retail)

Antes de que comenzase la pandemia, el papel de la tienda física seguía siendo fundamental, ya que representaba una oportunidad para aumentar las tasas de alcance, el compromiso y el volumen y la velocidad del canal de ventas. Entre los consumidores que utilizaban una aplicación de comercio móvil y de fidelización para comprar, el 75% completaba su recorrido de compra en la tienda. El 44% de los minoristas europeos consideraba que el nuevo concepto de tienda es un área de actividad importante en términos de generación de ingresos.

Sin embargo, con la pandemia, el acceso a la tienda física es limitado y los minoristas han tenido que reinventarse. Ahora se enfrentan al cliente digital, un cliente que requiere una experiencia online mejor y más segura que en una tienda física. Además, es un hecho que con la pandemia se producirá una desaceleración económica y la consiguiente recesión. Por ello, los minoristas lucharán por la continuidad del negocio y la optimización de los costes, seguidos de la resiliencia del negocio durante

la recesión en su camino hacia la 'nueva normalidad'. Debido al COVID-19, los minoristas han tenido que actuar inmediatamente para garantizar la seguridad y la salud de sus clientes y aumentar su confianza. En consecuencia, los comercios introducirán la tecnología contactless y habilitarán el autoservicio a través de los sitios de comercio electrónico y mediante aplicaciones móviles. Para hacer frente a los retos de la pandemia ahora los comercios ahora están invirtiendo en este tipo de tecnologías ahora y seguirán siendo su prioridad en los próximos años.

El sector minorista también se enfrenta a una serie de retos, como por ejemplo ofrecer máxima seguridad, a la vez que mantener una experiencia satisfactoria del cliente. La complicación es que cuanta más seguridad añada un minorista a su negocio, más difícil le resultará también cumplir la promesa de un comercio sencillo y seguro.

En general, puede haber incidentes de seguridad, pero el problema es cuando hay pérdidas y vulneraciones de los datos. Estos abarcan: ataques físicos, robos en tiendas, piratería informática, *ransomware*, DDoS, ingeniería social, violaciones de privilegios/autenticación, cuentas de correos electrónicos comerciales que se han visto comprometidas, fraude con tarjetas de crédito y débito, fraude con tarjetas de regalo, robo de identidad, *malware*, fraude de devoluciones, vulnerabilidades de *software*, manipulación, fraude amistoso, errores de configuración, suplantación de identidad, suplantación de red, ataques con violencia, falsificación de productos y *criptojacking*.

El aumento de la seguridad instalada en los dispositivos de los puntos de venta (TPV), en particular Europay/Mástercard/Visa (EMV), ha motivado a los ciberdelincuentes a desplazar su atención a otros puntos más vulnerables que antes podían pasar desapercibidos.

A medida que el comercio se ha ido desplazando hacia el comercio electrónico, las amenazas de ciberseguridad se han ido sucediendo, de tal manera que los ataques a las aplicaciones de comercio electrónico predominan en el sector minorista.

En la actualidad, los datos personales son tan atractivos como los datos de pago para los ciberdelincuentes.

Tendencias del sector financiero

Se ha dicho que la revolución digital ha desafiado modelos de negocio tradicionales en la mayoría de los sectores, y los servicios financieros no son la excepción. Todo el sector parece estar experimentando una transformación en la que la digitalización general del negocio y las disposiciones de servicios digitales resultantes han sembrado el camino para nuevas formas de interactuar con el cliente.

En lugar de simplemente recibir servicios financieros, los clientes están en una nueva posición de poder exigir servicios y personalizar la forma en que se presentan de manera que satisfaga sus necesidades actuales y futuras.

Las instituciones financieras deben encontrar formas de satisfacer esas

necesidades para construir y asegurar experiencias y relaciones rentables con los clientes, empezando por la validación de su identidad digital; deben ofrecer nuevos servicios innovadores basados en capacidades digitales distintivas como la única forma de retener y atraer nuevos clientes, especialmente los nativos digitales.

A medida que las instituciones financieras ofrezcan transacciones seguras online y preserven una sofisticada experiencia del cliente, la verificación de identidad digital es una táctica fundamental clave en cualquier estrategia de transformación digital. La actual crisis sanitaria provocada por el COVID-19 está provocando además que las empresas aceleren su proceso de digitalización, lo que incluye la gestión eficiente de las identidades digitales de sus clientes.

Las instituciones financieras han implementado sistemas de validación digital semiautomática en su gran mayoría, tratan la documentación digitalmente, emplean tecnología biométrica, unifican su gestión de *back office* con diferentes áreas de negocio, cuantifican y mitigan riesgos de fraude y en algunos casos ya incursionan con inteligencia artificial para apoyar las soluciones. Pero más importante aún, es la necesidad de comprender que tecnología no es innovación, ya que cualquiera puede adquirir este *commodity*, y el verdadero diferenciador en la industria lo determinará la capacidad de ejecutar y accionar cambios que impacten realmente en la experiencia del cliente en este nuevo panorama del *onboarding* financiero en la era digital.

Esto queda plasmado en que los clientes que prefieren interactuar digitalmente con su entidad financiera es un 14% superior a los que prefieren medios tradicionales. Es más, en el grupo de 18-34 años, la preferencia por la interacción digital asciende casi al 60%. Según IDC, para el año 2024, solo un 1% de los clientes financieros europeos optarán por canales no digitales (figura 23). Esto expone la situación a la que se enfrenta el sector financiero, tanto en España como a nivel global.

Figura 11. Tendencia de canales a 2024. Fuente: IDC Consumer Survey

En relación con esto, si bien es cierto que las Fintech están sirviendo como dinamizadores del sector, en numerosos casos lo están siendo de la mano de la banca tradicional, en muchos casos como partners o proveedores de servicios. Se podría afirmar que estos nuevos *players*, las Fintech, juegan ahora un papel más bien complementario e incluso de apoyo a las grandes entidades financieras.

Tendencias de la industria y recursos *(manufacturing)*

El proceso de digitalización unido a la incorporación de tecnologías de tercera plataforma (IA, IoT, Cloud, etc.), permiten a las empresas mejorar y optimizar las operaciones, y está impulsando que muchos sistemas de tecnología operacional (OT) se estén conectando al mundo exterior por primera vez. Esta tendencia promete grandes beneficios para las organizaciones, pero también expone a los sistemas a amenazas persistentes y avanzadas, ya que estos entornos aislados se enfrentan ahora a una variedad de vectores de ataque.

La 'brecha de aire' que protegía a los sistemas - de los ciberdelincuentes y del *malware* - ya no existe en muchas organizaciones y, como resultado, los atacantes tienen cada vez más a los sistemas OT en su punto de mira, ya que la falta de estandarización de protocolos de este tipo de sistemas hace que las partes más débiles de las redes de OT sean muy vulnerables. Esto hace que según datos de IDC el 90% de los clientes de entornos OT hayan sufrido algún tipo de ataque en los últimos dos años.

A medida que los sistemas de OT se vuelven más conectados, es probable que continúe la tendencia al aumento de los ataques. Esta nueva exposición requiere que las organizaciones se adhieran a operaciones de seguridad más rigurosas y a las prácticas recomendadas de gestión del ciclo de vida para proteger a sus organizaciones de las principales amenazas para el núcleo de su negocio. Como resultado, los equipos de tecnología necesitarán trabajar juntos para responder de manera integral a una amenaza cada vez mayor.

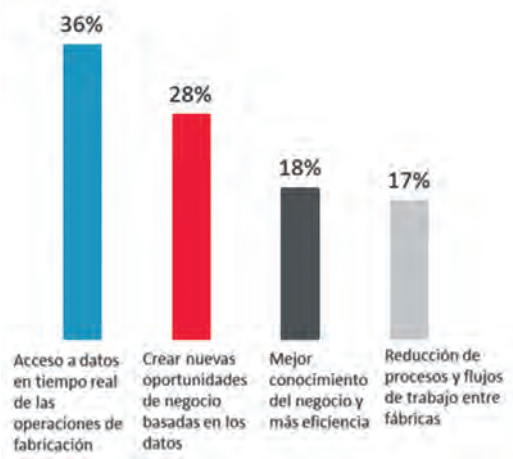
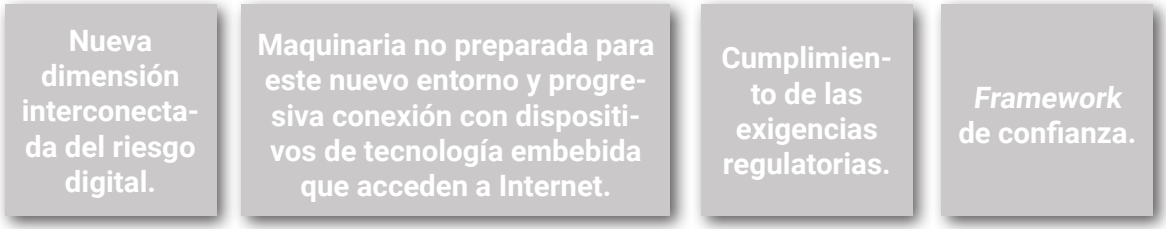


Figura 12. Beneficios de la convergencia IT/OT para las empresas. Fuente: IDC

Por ello, en este escenario actual donde hay una explosión de datos, se requiere no solo automatizar los procesos internos para poder sacar partido a los altos volúmenes de información sino de implementar procesos inteligentes que doten de valor al dato en este contexto de convergencia IT/OT.

La convergencia IT/OT pone de manifiesto varios riesgos que las organizaciones deben abordar en este nuevo escenario:



Tendencias del sector público

Los últimos ataques de *ransomware* por parte de organizaciones de ciberdelincuentes han demostrado que las bandas están formando alianzas al estilo de los cárteles para manipular a sus respectivas víctimas para que paguen las demandas de rescate. Según *Coalition*, un servicio de ciberseguros en Norteamérica, los incidentes de *ransomware* han representado el 41% de las reclamaciones de ciberseguros presentadas en el primer semestre de 2020.

Según IDC, en 2021, el aumento mundial de los intentos de *ransomware* organizados y al estilo de los cárteles hará que el 70% de los centros educativos fortalezcan sus defensas de ciberseguridad y cifrado de datos.

Otro caso interesante es lo que pasó en octubre de 2019, cuando la Universidad Nacional de Australia (ANU), tras meses de análisis forense con las agencias de seguridad del gobierno, descubrió que los ciberdelincuentes consiguieron utilizar sofisticadas técnicas de '*spear phishing*' para colarse en los registros personales de 200.000 estudiantes y empleados y lograron huir prácticamente sin dejar rastro. Se descubrió que los ciberdelincuentes buscaban registros financieros y de RRHH que abarcaban un periodo de 19 años, incluyendo nóminas, detalles de cuentas bancarias, archivos fiscales, números de pasaporte, contactos de emergencia y algunos registros académicos. Sin embargo, estos datos no eran suficientes. En posteriores incidentes de piratería, se observó que estos individuos trataban activamente de robar la propiedad intelectual de instituciones terciarias y centros de investigación de todo el mundo, lo que subyace a un intento dirigido de robar información de cierto valor financiero, social o personal para poder exigir un rescate.

Por otro lado, en el sector de la sanidad, el Internet de las Cosas (IoT) ya está cobrando cada vez más protagonismo, incluso ya podríamos hablar del Internet de los Objetos Médicos, en inglés, *Internet of Medical Things* (IoMT). A medida que los proveedores de servicios sanitarios europeos confían cada vez más en los dispositivos médicos conectados, la mayor exposición a los ataques y el aumento de la vulnerabilidad del IoMT plantean graves amenazas. En este escenario, la mayoría de las organizaciones sanitarias están empezando a realizar evaluaciones de riesgos y a identificar las amenazas de seguridad. La seguridad es, tanto un reto como una motivación para los proveedores sanitarios europeos que planean transformar sus organizaciones mediante la implantación de proyectos de IoT.

El problema es que las organizaciones sanitarias europeas carecen de una estrategia de seguridad del IoT a largo plazo y de un enfoque de gestión de riesgos a nivel de toda la empresa, ya que se centran en el cumplimiento de los marcos normativos. Por eso, están perdiendo la oportunidad de aprovechar plenamente y de forma segura el potencial del IoT y utilizar el valor de los datos para impulsar nuevos modelos de negocio.

Dado que los proveedores de atención sanitaria dependen cada vez más de los dispositivos médicos conectados (marcapasos, electrocardiogramas, desfibriladores, monitores fetales, etc.) para diversas actividades, la vulnerabilidad de los dispositivos IoMT plantea graves amenazas. Un número cada vez mayor de dispositivos médicos en el mercado puede enviar y recibir datos sensibles de los pacientes sin las medidas de seguridad adecuadas, lo que los hace vulnerables a los ataques de piratas informáticos que pueden perjudicar a los pacientes o utilizar sus dispositivos como portales para acceder a datos médicos y otra información.

Tendencias *utilities*

El sector *utilities* se enfrenta a una nueva era de eficiencia y rentabilidad, principalmente explicado por la subida del precio del petróleo y a la volatilidad del entorno, que exigen al sector cambios constantes. La ventaja que el IoT proporciona al sector es la mejora de la productividad del negocio y la reducción de costes, lo que supone un giro fundamental, ya que crea una nueva ventaja competitiva. Así, con el IoT, se prevé que el valor del petróleo y el gas aumenten gracias a la optimización de la exploración y la producción.

Se espera que las inversiones en IoT se incremetan a través de la asociación con empresas tecnológicas que tienen soluciones probadas para mejorar la eficiencia y la rentabilidad, al tiempo que combaten el riesgo y las amenazas a la seguridad. Los factores críticos de éxito son ofrecer valor al negocio y aumentar el retorno de las inversiones (ROI). Es necesario establecer un liderazgo y una cooperación entre los proveedores de IoT y el sector *utilities* para gestionar una adopción que cumpla los objetivos de la organización.

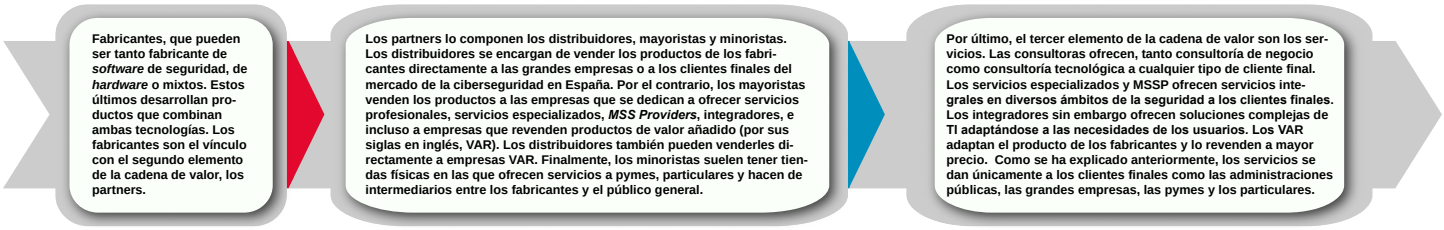
La seguridad de las tecnologías de la información es una de las principales preocupaciones de los ejecutivos del sector en los últimos años. Con las crecientes iniciativas de digitalización y la experimentación de tecnologías emergentes que se han trasladado a un número significativo de despliegues de campo en los últimos tres a cinco años, la seguridad de TI y OT ha ganado una enorme atención en la industria de la infraestructura. A medida que las empresas del sector han ido respondiendo al COVID-19, la ciberseguridad ha acaparado aún más atención cuando las empresas de *utilities* han introducido más sistemas de trabajo en remoto en sus dominios de tecnología. Es innegable que un inhibidor de la convergencia IT/OT es la falta de experiencia en ciberseguridad en las operaciones. Este hecho supone además, en muchos casos, falta de alineamiento interna en las organizaciones al hacer más escépticos a los

responsables de operaciones sobre la conveniencia de la unificación de aplicaciones y sistemas con el resto de la TI de la organización.

3.3_ Análisis de los agentes de la cadena de valor de la ciberseguridad en España. Mapa de agentes y relaciones.

Cuando nos referimos a la cadena de valor del sector de la ciberseguridad, hablamos de establecer un modelo que permita describir cuáles son y cómo se relacionan entre sí las principales actividades y fases o eslabones de la cadena, necesarias para la prestación de los productos y servicios de ciberseguridad a los destinatarios o clientes finales.

La cadena de valor en España puede diferenciarse entre fabricantes, partners y servicios.



No obstante, existen otros agentes que, sin ser claramente parte de los descritos, influyen y aportan valor a la cadena. Hablamos de incubadoras, aceleradoras y entidades o sociedades de capital riesgo que apoyan a los elementos participes de la cadena de valor de la ciberseguridad en España. Los centros tecnológicos y las universidades son otros componentes claves del ecosistema de la ciberseguridad. Pueden apoyarlo dotando de recursos a los diferentes agentes que se incorporan a la cadena de valor.

Además, existen asociaciones, foros y clústeres que reúnen a los diferentes agentes del mercado de la ciberseguridad en España y fomentan el intercambio de datos y recursos. Finalmente, están las certificaciones, el reglamento y cumplimiento normativo y la formación que afecta a todos los agentes de la cadena de valor de la ciberseguridad en España.

A continuación, se muestra una aproximación actualizada a la cadena de valor de la ciberseguridad en España.

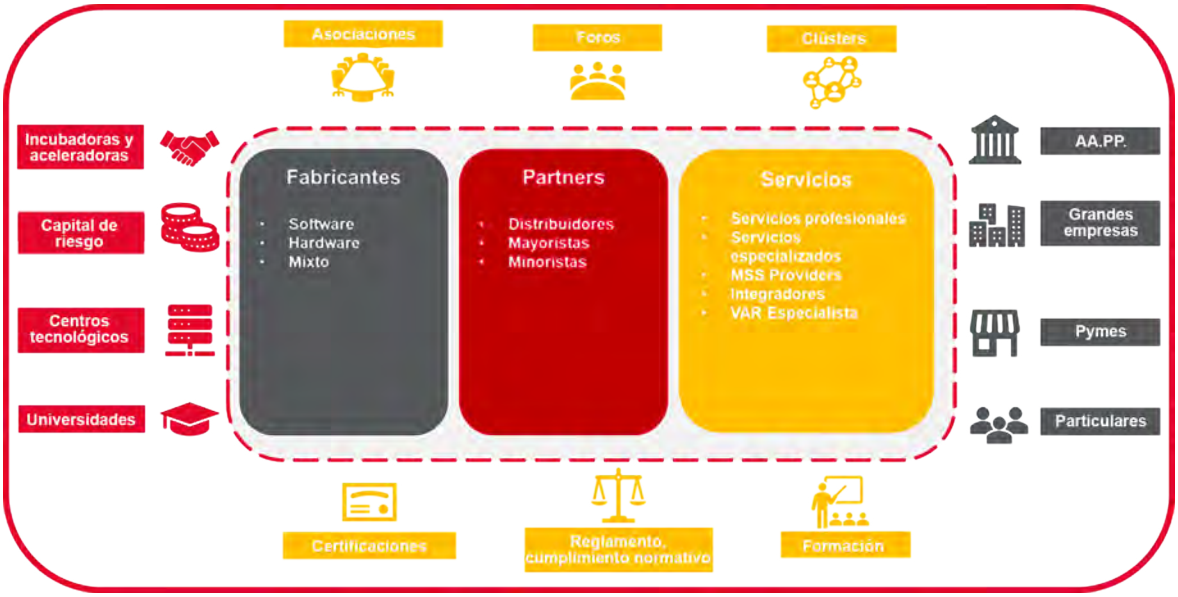


Figura 13. Ecosistema de la ciberseguridad en España – elaboración propia basada en mapa del sistema de valor de INCIBE publicada en abril 2015[5]

3.4_ 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 desequilibrio 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**, y con base en el informe 'Cybersecurity Professionals Stand Up to a Pandemic[6]', realizado por el International Information System Security Certification Consortium o (ISC)², se identifica que en España para 2020 el tamaño de la fuerza laboral estimado fue de 149.774 y la brecha de (26.024) profesionales. 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,**

5 https://www.incibe.es/protege-tu-empresa/blog/caracterizacion-mercado-ciberseguridad-spain

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

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. Esta promoción conlleva 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 conocimientos, habilidades y experiencias tecnológicas que respondan a los grandes retos que tiene el país en materia de ciberseguridad.

El objetivo general de esta estrategia es garantizar el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico. Pero más específicamente, el objetivo IV de la estrategia hace referencia a la cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas. En este sentido, España es consciente de la importancia de contar con los recursos humanos y las capacidades técnicas y tecnológicas como un habilitador clave para el uso seguro del ciberespacio y el progreso de las organizaciones, lo cual pasa necesariamente por gestionar el talento.

En este contexto, con relación al talento de ciberseguridad la estrategia pretende a través de una de sus líneas de acción, potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital. Adicionalmente, para el desarrollo de esas líneas de actuación que responden a los objetivos específicos de la estrategia, se establecen unas medidas que se presentan a continuación:

Detectar, fomentar y retener el talento, con especial atención al campo de la investigación.

Promover la difusión de la cultura de la ciberseguridad como una buena práctica empresarial, e incrementar las campañas de concienciación a ciudadanos y empresas.

Actualizar, o en su caso desarrollar marcos de competencias en ciberseguridad, que respondan a las necesidades del mercado laboral.

Impulsar programas de apoyo a la I+D+i en seguridad digital y ciberseguridad en pymes, empresas, universidades y centros de investigación, facilitando el acceso a programas de incentivos nacionales e internacionales y mediante programas de compra pública innovadora.

Identificar las necesidades de capacidades profesionales de ciberseguridad, fomentando la colaboración con las instituciones educativas y formativas impulsando la formación continua, la especialización, la formación para el empleo y universitaria, promoviendo sistemas de acreditación y certificación profesional.

Promover las capacidades de generación de conocimiento, el desarrollo actividades de I+D+i en ciberseguridad y el fomento del uso de productos y servicios certificados.

Incrementar las campañas de concienciación a ciudadanos y empresas, y poner a su disposición información útil adaptada a cada perfil, especialmente en el ámbito de los autónomos y las pequeñas y medianas empresas.

Conjuntamente, estas medidas deberían ir acompañadas de iniciativas puntuales que reflejan el compromiso, tanto de las Administraciones Públicas como del sector privado, para alcanzar los objetivos de la Estrategia Nacional de Ciberseguridad.

Dentro de las más destacas se encuentran:

INCIBE emprende: programa para emprendedores y *start-ups* de ciberseguridad dotado con €191 millones. 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.

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 acercar a los jóvenes a las empresas y a las instituciones públicas.

Comenzamos con Ciberseguridad (recurso de 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.

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.

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:

- **Titulaciones** vinculadas con la ciberseguridad.
- **Formación profesional** asociada con la ciberseguridad.
- **Programas formativos oficiales y no oficiales** (incluyendo certificaciones profesionales, cursos tanto en el ámbito público como privado, MOOC, etc.) que dan como resultado talento formado en ciberseguridad.
- **Aprendizaje autodidacta.**
- **Egresados de las universidades españolas.**

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.

4.1.1.1_ Oferta formativa universitaria en grados y másteres

La especialización en ciberseguridad se sostiene principalmente a través

de la impartición de másteres más que de grados. Si bien las carreras en las que la ciberseguridad tiene más presencia y se abordan aspectos de la ciberseguridad como Ingeniería de Telecomunicación o Informática, la realidad es que en España solo existen cuatro grados específicos sobre ciberseguridad, impartidos bajo modalidad presencial y diseñados para complementar el conocimiento sobre ciberseguridad con otros aspectos como el derecho, la consultoría o aspectos de negocio.

Nombre del grado	Institución	Modalidad	Número de plazas por edición	Posibilidad de becas
Doble Grado en Gestión de la Ciberseguridad y Análisis de Negocios	Universidad Francisco de Vitoria (UFV)	Presencial	No especifica	Becas del Ministerio de Educación, Becas de la Comunidad de Madrid
Doble Grado en Gestión de la Ciberseguridad y Derecho	Universidad Francisco de Vitoria (UFV)	Presencial	No especifica	Becas del Ministerio de Educación, Becas de la Comunidad de Madrid
Grado en Ingeniería de la Ciberseguridad	Universidad Rey Juan Carlos (URJC)	Presencial	60	Becas del Ministerio de Educación, Becas de la Comunidad de Madrid
Grado en Gestión de la Ciberseguridad + Mención en Consultoría de la Seguridad Digital	Universidad Francisco de Vitoria (UFV)	Presencial	60	Becas del Ministerio de Educación, Becas de la Comunidad de Madrid

Tabla 1. Grados oficiales en ciberseguridad.

Respecto a la oferta de másteres, en el curso 2020-2021 se han ofertado un total de **76 másteres universitarios** en los que se ofrecen, de media, 32 plazas. Este número podría indicar que, en el caso hipotético de cubrirse todas las plazas, cada año podría aumentar la oferta de talento de ciberseguridad en 2.432 personas con un máster especializado en ciberseguridad y formados en España. No obstante, considerando la modalidad de programas en línea ofrecidos por organizaciones como UNIR o el IMF habría lugar a un mayor número de egresados.

Cabe destacar que la mayoría de los másteres otorgan la posibilidad de contar con una beca oficial del Ministerio de Educación o de la Comunidad Autónoma en la que se encuentre la universidad. En algunos casos se ofertan becas específicas por desempleo por importes entre el 15% y el 70% del total.

Respecto al número de egresados en la oferta de másteres, de acuerdo con los datos del Ministerio de Universidades, el número aproximado de egresados anuales con un máster universitario especializado en ciberseguridad es de 1.725 y el número de plazas disponibles son 2.432, por lo que aproximadamente llegan a graduarse un 72% del total de plazas ofertadas en los másteres.

El perfil de los estudiantes de este tipo de formación (los requisitos de acceso varían en función del perfil), se agrupan en las siguientes tipologías:

- **Recién titulados y estudiantes de últimos cursos** que quieren una formación actual práctica que les permita orientarse profesionalmente y entrar a trabajar a un mercado laboral complejo y competitivo
- **Profesionales del mundo de la informática y derecho** que quieren actualizar sus conocimientos para resolver problemas que surgen en su quehacer profesional y tomar decisiones tácticas y estratégicas en sus puestos.
- **Responsables de medios de Departamento de Seguridad, Consultoría y Asesoría Informática** de entidades públicas y privadas que deseen apoyarse y compartir la visión de otros profesionales de prestigio e intensa actividad profesional.
- Miembros de las Fuerzas y Cuerpos de Seguridad del Estado.

Respecto a la **distribución geográfica** de la oferta de formación universitaria en Ciberseguridad, destaca la amplia oferta concentrada en Madrid que supone más del 40% del total como podemos apreciar en la figura.

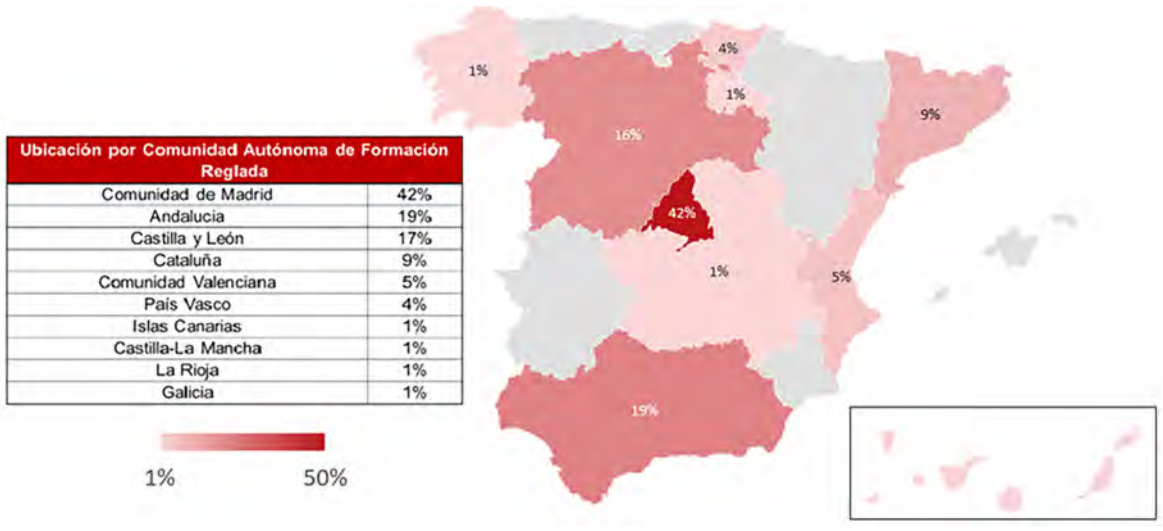


Figura 14. Distribución geográfica de la oferta de másteres en ciberseguridad en España. Fuente: elaboración propia

4.1.1.2_ Cursos y formación no oficial en ciberseguridad

En España existen en la actualidad 81 organizaciones en las que es posible realizar algún estudio vinculado con la ciberseguridad. Asimismo, existen un conjunto de plataformas de formación en las que, organizaciones públicas (universidades) como privadas de todo el mundo ofre-

cen formación en ciberseguridad. Esta formación puede adquirirse en formato gratuito (en la mayoría de las ocasiones) o bien acceder a un **certificado profesional,** previo pago de unas tasas y matrícula para la formalización del título.

INCIBE cuenta multitud de programas de formación en ciberseguridad[7] en los que se puede acceder no sólo a formación (virtual) sino acceder a laboratorios virtuales y sitios de Internet que ofrecen la posibilidad de desarrollar las habilidades prácticas necesarias para la aplicabilidad del contenido al trabajo real, incluyendo:

Herramientas.

Laboratorios.

Proyectos, en los que se ponen a prueba las destrezas mediante el desarrollo de un proyecto de aplicación al contenido del curso, de forma que tenga una analogía clara con la posición que se ocuparía en el mercado laboral.

En la mayoría de las ocasiones, los cursos se desarrollan en formato de programa, por lo que es necesario cursar varios módulos para poder recibir el certificado profesional.

Asímismo, YouTube se ha convertido en los últimos años en una herramienta fundamental de acceso a contenido de formación. La proliferación de canales de formación temáticos para aprender seguridad informática y hacking ha sido creciente en los últimos años, y en la actualidad engloban a una comunidad de usuarios cada vez mayor y con contenido más transversal, cubriendo, tanto aspectos técnicos como de gestión. A continuación, se relacionan algunos ejemplos de los principales canales:

- Dedsec. Hacking con fines educativos.
- The New Boston. Canal de información de ciberseguridad.
- Vivek Romanchandran. Tutoriales para Android y Windows.
- Justprogramming. Esta plataforma ofrece tutoriales de 'hacking ético'.
- Penetration Testin in Linux. Tutoriales para sistemas Linux.
- Hack5. Ofrece recursos de formación en temas complejos de ciberseguridad.
- Network Security Fundamentals. Cursos sobre hacking.
- Bhargav Tandel. Trucos y consejos sobre Linux.
- Open Security Training. Ofrece análisis de posibles virus y tutoriales sobre informática.
- Hacking Ético – Seguridad Informática. Hacking con fines educativos.

7 https://www.incibe.es/catalogos-formacion-ciberseguridad

- Curso de Hacking. Curso de hacking.
- TutorialBotss. Presenta vídeos sobre 'hacking ético' y enseña a programar con C++.

4.1.1.3_ Formación Profesional

Hasta la fecha no existe ninguna Formación Profesional Básica, de Grado Medio o de Grado Superior específica para ciberseguridad o con un componente alto de contenidos relacionados con la ciberseguridad.

No obstante, se ha creado un **'Curso de Especialización en Ciberseguridad en Entornos de Tecnologías de la Información'[8] establecido por Real Decreto 479/2020**, de 7 de abril dentro de la familia profesional de informática y comunicaciones con una duración de 720 horas que se implanta en un curso académico abordando los siguientes módulos profesionales:

- Incidentes de ciberseguridad.
- Bastionado de redes y sistemas.
- Puesta en producción segura.
- Análisis forense informático.
- Hacking ético.
- Normativa de ciberseguridad.

La competencia general de este curso de especialización consiste en definir e implementar estrategias de seguridad en los sistemas de información realizando diagnósticos de ciberseguridad, identificando vulnerabilidades e implementando las medidas necesarias para mitigarlas aplicando la normativa vigente y estándares del sector, siguiendo los protocolos de calidad, de prevención de riesgos laborales, privacidad y respeto ambiental.

Este profesional tiene la posibilidad de ejercer su actividad en entidades de los sectores donde sea necesario establecer mecanismos y medidas para la protección de los sistemas de información y redes de comunicaciones. Las principales salidas profesionales asociadas a este título se podrían sintetizar en:

- Experto/a en ciberseguridad.
- Consultor/a de ciberseguridad.
- Auditor/a de ciberseguridad.
- Hacker ético.

Para acceder a este curso de especialización se debe acreditar alguna de las siguientes Formaciones Profesionales Superiores (en el **Benchmark** se muestran los requisitos específicos para cada tipo de perfiles):

- Título de Técnico Superior en Administración de Sistemas Informáticos

8 https://www.todofp.es/que-estudiar/loe/informatica-comunicaciones/ciberseguridad-entornos-tecnologias-informacion.html

en Red establecido por el Real Decreto 1629/2009, de 30 de octubre.

- Título de Técnico Superior en Desarrollo de Aplicaciones Multiplataforma, establecido por el Real Decreto 450/2010, de 16 de abril.
- Título de Técnico Superior en Desarrollo de Aplicaciones Web, establecido por el Real Decreto 686/2010, de 20 de mayo.
- Título de Técnico Superior en Sistemas de Telecomunicaciones e Informáticos, establecido por el Real Decreto 883/2011, de 24 de junio.
- Título de Técnico Superior en Mantenimiento Electrónico establecido por el Real Decreto 1578/2011, de 4 de noviembre

4.1.1.4_ Certificaciones de seguridad

En función del tipo de perfil de seguridad, en la actualidad tenemos las siguientes (en el **Benchmark** se detallan las características técnicas de las diferentes certificaciones):

Desarrollo: tienen como objetivo frenar la proliferación de las vulnerabilidades de seguridad que resultan de los procesos de desarrollo del *software* durante todo su ciclo de vida. Entre ellas, podemos encontrar las siguientes:

- CISSLP, Certified Secure Software Lifecycle Professional ((ISC)2).
- ECSP, EC-Council Certified Secure Programmer (EC-Council).
- OPSA, Professional Security Analyst Accredited Certification (ISECOM).

Hacking ético. Es una forma de referirse al acto de una persona de usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño. Las principales certificaciones en este ámbito, son las siguientes:

- CEH, Certified Ethical Hacking (EC-Council).
- ECSA, EC-Council Certified Security Analyst (EC-Council).
- EDRP, EC-Council Disaster Recovery Professional (EC-Council).
- SMSP, Social Media Security Professional (CompTIA).
- OPST, Professional Security Tester (ISECOM).
- CPTE, Certified Penetration Testing Engineer (MILE 2).
- CPTC, Certified Penetration Testing Consultant (MILE 2).

Informática Forense. Es la aplicación de técnicas científicas y analíticas que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Las principales certificaciones en, este sentido, son las siguientes:

- CCFP, Certified Cyber Forensics Professional ((ISC)2).
- CHFI, Certified Hacking Forensic Investigator (EC-Council).
- CNFE, Certified Network Forensics Examiner (MILE 2).

Redes. Los problemas de las redes pueden venir, tanto del exterior como del interior. En este sentido, el mercado presenta las siguientes certificaciones en este ámbito:

- CISSP-ISSAP, Information Systems Security Architecture Professional ((ISC)2).
- CISSP-ISSEP, Information Systems Security Engineering Professional ((ISC)2).
- ENSA, EC-Council Network Security Administrator (EC-Council).
- OWSE, Wireless Security Expert (ISECOM).
- CompTIA Mobile App Security+ (CompTIA).

Sistema de Gestión de la Seguridad de la Información (SGSI). El objetivo de un SGSI es proteger la información, por lo tanto, es necesario identificar los 'activos de información' a proteger y en qué grado. Entre las certificaciones en este ámbito, podemos encontrar las siguientes:

- CAP, Certified Authorization Professional ((ISC)2).
- CISSP, Certified Information Systems Security Professional ((ISC)2).
- CISSP-ISSMP, Information Systems Security Management Professional ((ISC)2).
- SSCP, Systems Security Certified Practitioner ((ISC)2).
- CISM, Certified Information Security Manager (ISACA).
- CISA, Certified Information Systems Auditor (ISACA).
- CRISC, Certified in Risk and Information Systems Control (ISACA).
- CGEIT, Certified in the Governance of Enterprise IT (ISACA).
- GIAC, Global Information Assurance Certification (GIAC).
- GSE GIAC Security Expert (GIAC).
- CompTIA Security+ Professional (CompTIA).
- CPP, Certified Protection Professional.
- OPSE, Professional Security Expert Accredited Certification (ISECOM).
- CTA, Certified Trust Analyst (ISECOM).
- CDFE, Certified Digital Forensic Examiner (MILE 2).

Protección de datos. La protección de datos es una disciplina jurídica que tiene por objeto proteger la intimidad y demás derechos fundamentales de las personas físicas. Entre las certificaciones orientadas a este ámbito, se encuentran las siguientes:

- CCISO, Chief Information Security Officer (MILE 2).
- CDPP, Certified Data Privacy Professional (ISMS).
- CCSK, Certificated of Cloud Security Knowledge (ISMS).

Legal. La seguridad de la empresa no es solo responsabilidad de los profesionales de la ciberseguridad de una organización. Mantener la seguridad de la empresa requiere la aportación de todos los niveles de liderazgo.

Gestión (Management). En la organización es necesario disponer de perfiles que valide y monitorice los controles técnicos centrados en la protección, la detección y la respuesta a los problemas de seguridad, así como establecer la política de seguridad de la empresa o disponer de las capacidades necesarias para llevar a cabo la puesta en marcha de proyectos dentro del ámbito de la ciberseguridad.

- GIAC Law of Data Security & Investigations (GLEG).
  - GIAC Security Leadership Certification (GSLC).
  - GIAC Strategic Planning, Policy, and Leadership (GSTRT).
  - GIAC Certified Project Manager (GCPM).

4.1.1.5_ Estimación de la oferta de perfiles de ciberseguridad

El análisis anterior muestra las capacidades que dispone el ecosistema de ciberseguridad en España para generar nuevo talento con conocimientos y capacidades en ciberseguridad.

Para ello, 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, 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*[4,5] que considera el Ministerio de Educación, y que se sitúa en el 31,5%.

Las titulaciones que, de manera general, aportan al talento de ciberseguridad se sitúan en Matemáticas, Ingeniería de Informática y Telecomunicaciones, entre otros. 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[6] (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, solo 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 del COVID-19), por lo que, a efectos del cálculo de la situación actual de oferta, no requiere de incorporación de ningún ajuste adicional.

4.1.1.5.1_ Análisis de la oferta actual

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

Oferta de Talento en Ciberseguridad=Oferta del sistema+Oferta del personal reciclado

Donde:

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

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.

9 https://www.universidades.gob.es/stfls/universidades/Estadisticas/ficheros/Datos_y_Cifras_2020-21.pdf. Último acceso 12/9/2021

10 Número de estudiantes de 18-24 años en enseñanzas de Grado, 1er y 2º ciclo y Máster / población de 18-24 años total

11 https://www.universidades.gob.es/portal/site/universidades/menuitem.78fe777017742d34e0acc310026041a0/?vgnextoid=3b80122d36680710VgnVCM1000001d04140aRCRD

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 de graduados+Nº alumnos de máster+Nº de 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[12]. 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 del 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.

- 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%.

Tomando como base para el análisis los datos publicados por el Ministerio de Trabajo y Economía Social[13], en la actualidad existen en España 15.976.297 contratos registrados. Para poder estimar la oferta, es necesario realizar la estimación de cómo va a crecer la demanda de trabajadores de ciberseguridad en las organizaciones, ya que, como hemos

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

13 https://www.sepe.es/HomeSepe/que-es-el-sepe/estadisticas/publicaciones-estadisticas/sintesis-anual-MT

visto, el 15,7% de los nuevos empleos que se generen, corresponderán a nuevo talento de ciberseguridad (ya que se producen como consecuencia de un proceso de formación y capacitación interna para poder desempeñar las actividades en dicha área de actividad).

Tal y como se explica en el apartado 4.2.1 relativo a la determinación de la estimación de la demanda, dicho cálculo se obtiene estimando el crecimiento total de trabajadores en la economía y ajustando dicha cifra con un factor de corrección que relaciona el total de empleos creados, con aquellos que se crean específicamente en el ámbito de la ciberseguridad.

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

4.1.1.5.2_ Proyecciones futuras

Teniendo en cuenta que la implantación de los Cursos de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información de FP (que para este año 2022 se habilitan en 56 centros de FP[14], así como el relativo al de Especialización en Ciberseguridad en Entornos de las Tecnologías de Operación[15] (que se imparte en 22 centros en el territorio nacional), está teniendo implantación en las diferentes CC.AA, la oferta de talento de ciberseguridad sufrirá un importante incremento.

Para estimar la aportación de este programa a la oferta de talento de ciberseguridad se toma la ratio que se estableció en 2020 debido a la pandemia y que, de manera general, se ha tomado en las CC.AA de 20 a 25 alumnos por clase.

Esto haría un total de 1.716 nuevos alumnos por año, que se traducirían en talento formado de ciberseguridad que podría incorporarse al mercado laboral. Hay que tener en cuenta que nos referimos a programas educativos nuevos, por lo que la tasa de implantación será muy suave. Factores como la formación del profesorado para poder impartir estos estudios, así como encaje en los diferentes itinerarios educativos de los centros, serán aspectos a tener en cuenta a la hora de proyectar el crecimiento futuro. Teniendo esto en cuenta, asumimos un crecimiento en el número de alumnos del 15% anual a partir de 2023 y un 20% en 2024, lo que implicaría que, en ambos cursos de especialización, el crecimiento en centros fuera del 20%-30%, lo que tiene sentido dada la importancia de la ciberseguridad en el mercado actual.

Por otra parte, en relación con la oferta de grado, debemos asumir que se mantendrá constante a lo largo de los próximos tres años. Analizando el histórico de información proporcionada por el Ministerio de Educación,

14 https://www.todofp.es/que-como-y-donde-estudiar/que-estudiar/familia/loe/informatica-comunicaciones/ciberseguridad-entornos-tecnologias-informacion/donde-estudiar.html

15 https://www.todofp.es/que-como-y-donde-estudiar/que-estudiar/familia/loe/electricidad-electronica/ciberseguridad-tecnologias-operacion/donde-estudiar.html

las plazas en dichas carreras no han sido modificadas de manera significativa durante los últimos años, por lo que no es erróneo pensar que la tendencia seguirá siendo la misma.

En relación con la oferta de másteres, un estudio realizado por INCIBE en 2018 arrojaba la existencia de 74 másteres en España vinculados con la ciberseguridad. A fecha de realización del presente trabajo, esta oferta se ha incrementado en 2 hasta totalizar 76 los programas de máster que especializan a la persona en ciberseguridad. Por ello, vamos a asumir una tendencia constante de generación de talento para los próximos tres años.

Por último, la variable de talento reciclado la calculamos como el porcentaje equivalente de posiciones de talento de ciberseguridad que se cubren con talento existente de la empresa que ha sufrido un proceso de formación para adecuarlo a la posición. Estos datos se obtienen directamente del cálculo de estimación de la demanda y se aplica el peso relativo asociado de 0,2 (ya que, de cada 10 posiciones, 2 se están cubriendo en la actualidad con talento de la propia organización).

El total, por tanto, de las proyecciones de la oferta a lo largo de los próximos tres años se calcula aplicando la ecuación anterior y da el resultado que aparece en la siguiente tabla.

	2021	2022	2023	2024
Graduados	34,427	34,427	34,427	34,427
Másteres	2,432	2,432	2,432	2,432
Formación Profesional		1,760	2,024	2,328
Talento reciclado	2,213	2,504	2,794	3,096
Total	**39,072**	**41,123**	**41,677**	**42,283**

Tabla 2. Proyecciones de oferta de talento en ciberseguridad en España.

4.1.2_ Análisis cualitativo de la oferta de talento en ciberseguridad

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.

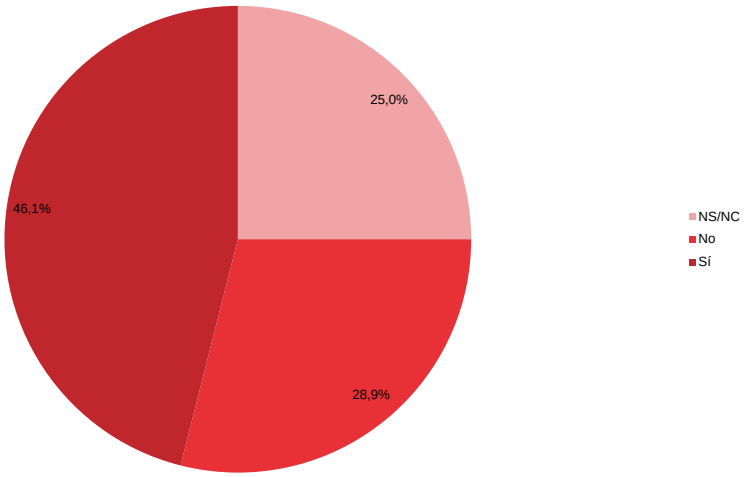
Para este propósito se plantea abordar el estudio del escenario actual desde el punto de vista cualitativo, destacar los potenciadores que hacen que esta oferta sea mayor, tanto en cantidad como en calidad e identificar los limitadores que necesitaríamos abordar para optimizar este proceso.

4.1.2.1_ Escenario actual

El aumento de la oferta formativa en ciberseguridad en España en los últimos años ha sido evidente como demuestra que, en el año 2021, existen 120 instituciones que ofrecen formación en esta materia y 76 máste-

res en ciberseguridad. Esta cifra muestra la importancia que la ciberseguridad está adquiriendo en el contexto de la sociedad actual.

Sin embargo, el análisis desarrollado muestra que, a pesar de la oferta disponible para formar talento en ciberseguridad, existe una desalineación entre oferta y demanda, ya que solo el 46% de las personas dedicadas a la ciberseguridad considera que reúne el perfil de competencias, conocimientos y habilidades necesarios para trabajar en el sector como podemos apreciar en la figura.



Por ello, en base al trabajo de campo desarrollado (cuestionario y entrevistas), para realizar un correcto diagnóstico es necesario establecer un escenario de análisis que tenga en cuenta las diferentes dimensiones del mismo.

Comenzando por el perfil de los encuestados, cabe destacar que la mayor parte de los mismos (65%) son trabajadores por cuenta ajena frente a un 3% de trabajador por cuenta propia lo que denota la relativa poca extensión de freelance o autónomos en el ámbito de la ciberseguridad.

Aproximadamente, un 27% de la muestra lo componen estudiantes, principalmente universitarios que suponen la gran mayoría de los perfiles que se dedican a la ciberseguridad y un 4% desempleados. Este bajo porcentaje de desempleados con interés o experiencia en la ciberseguridad corrobora el gap constatado entre oferta y demanda de talento en el sector.

Un aspecto fundamental de análisis en el escenario actual es la **percepción que tiene el mercado de las diferentes tipologías de oferta**

4.1.2.1.1_ Educación superior

A pesar de la falta de alineamiento que hemos destacado entre la oferta educativa universitaria y las necesidades del mercado, el presente estudio observa que las organizaciones perciben como útil y necesaria la formación universitaria. El mercado percibe que una persona formada de manera autodidacta no tiene las mismas competencias, habilidades y conocimiento que otra que disponga formación reglada de como

muestra la figura. Una de las causas de esta ventaja de la formación reglada es la capacidad de conseguir prácticas asociadas a esta formación reglada.

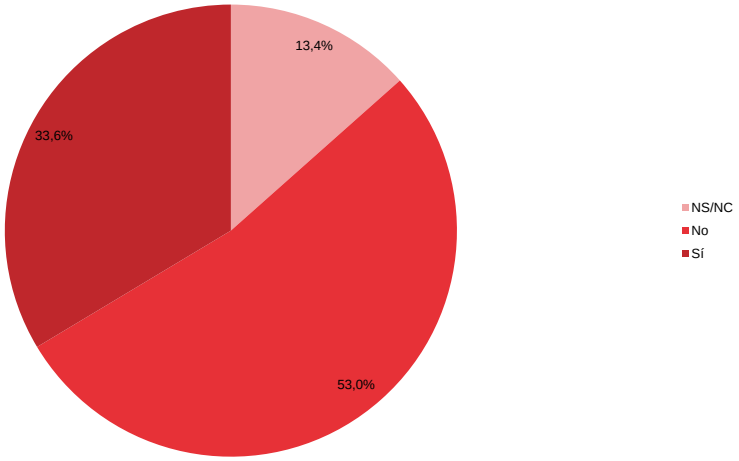


Figura 15. ¿Una persona formada de manera autodidacta tiene las mismas competencias, habilidades y conocimientos que otra que disponga de formación reglada?

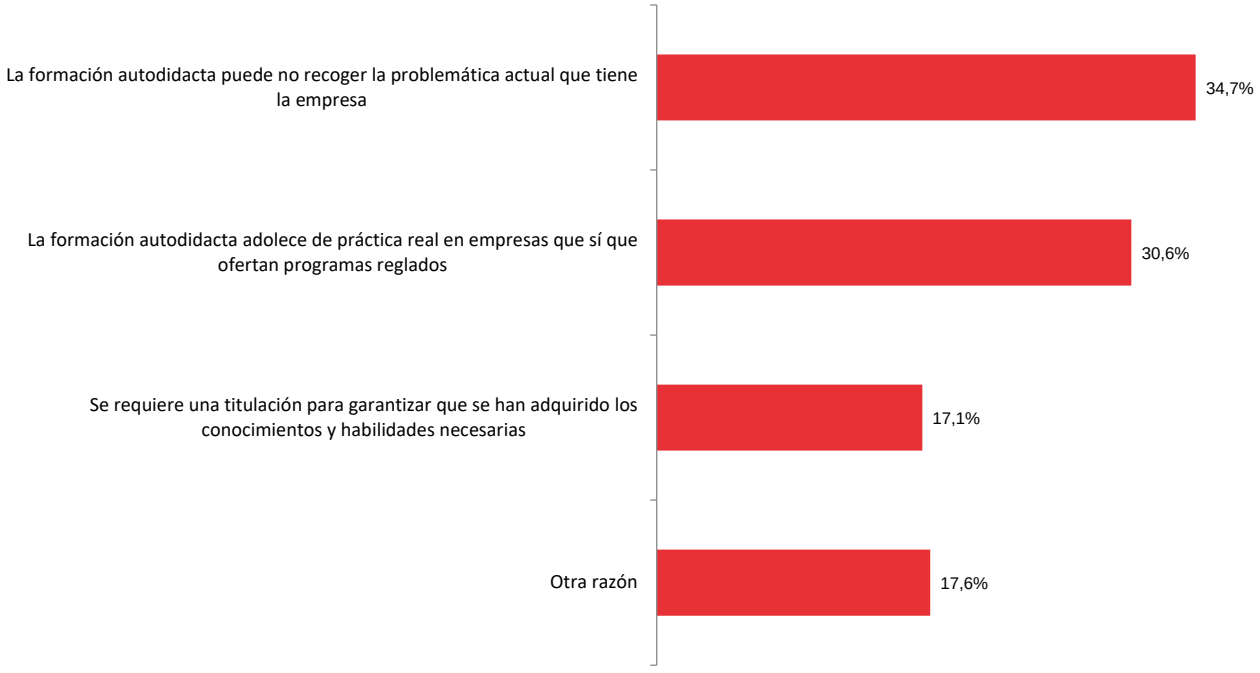


Figura 16. ¿Por qué considera que no es así?

El perfil más demandado por parte del mercado es el que aúna el conocimiento técnico con la experiencia. Como era previsible, un 93% de los encuestados está de acuerdo o muy de acuerdo con esta afirmación. Los datos también muestran que los másteres tienen una mejor acogida que los grados entre la propia industria como podemos apreciar en la figura.

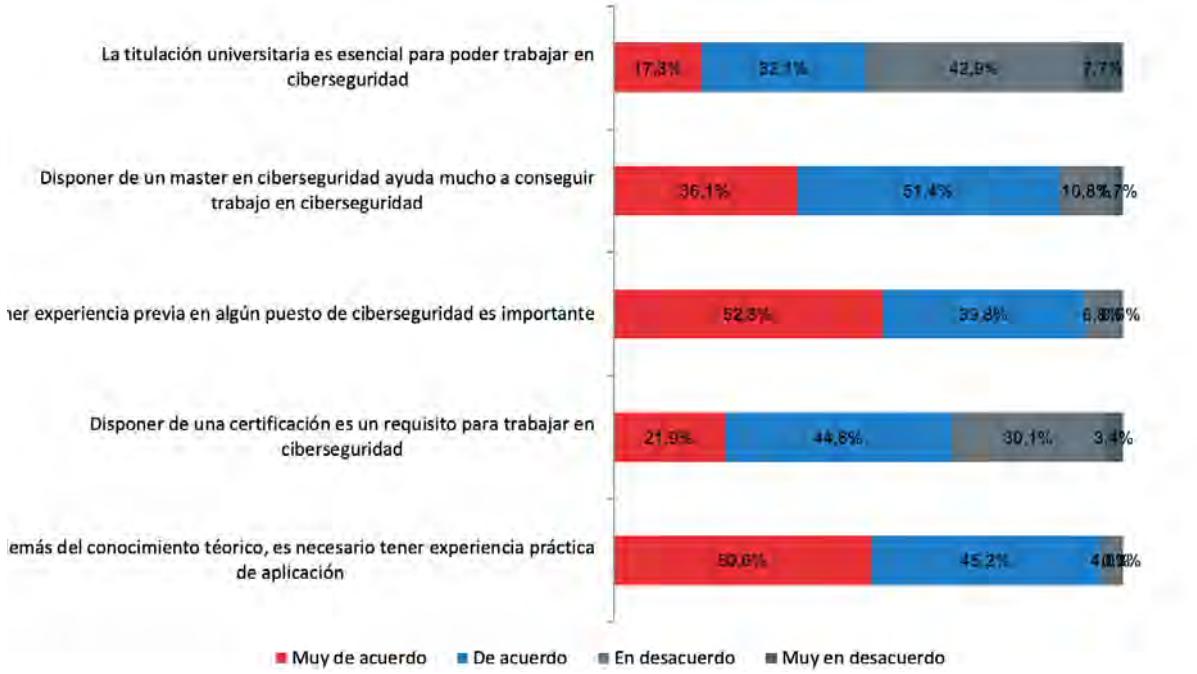


Figura 17. Aspectos valorados por el mercado de ciberseguridad en la oferta de talento

4.1.2.1.2_Formación Profesional

Es indudable que la Formación Profesional es una palanca fundamental a nivel global para disminuir los niveles de paro juvenil que desafortunadamente diferencian a España de nuestros comparables europeos.

En el ámbito de la ciberseguridad, la FP es altamente valorada por el mercado de nuestro país y se trata de una de las áreas donde el paro juvenil se produce en menor proporción.

Un dato destacable, es que, como vemos en la figura, si sumamos el porcentaje de agentes del ecosistema que considera la titulación técnica como importante o muy importante, supone más del 72% del total, porcentaje superior al que considera la titulación universitaria como importante o muy importante. Aún más, el Curso de Especialización en Ciberseguridad en Entornos de Tecnologías de la Información podemos decir que estaría incluido dentro de la categoría de cursos especializados, que supone el requisito mejor valorado por el mercado

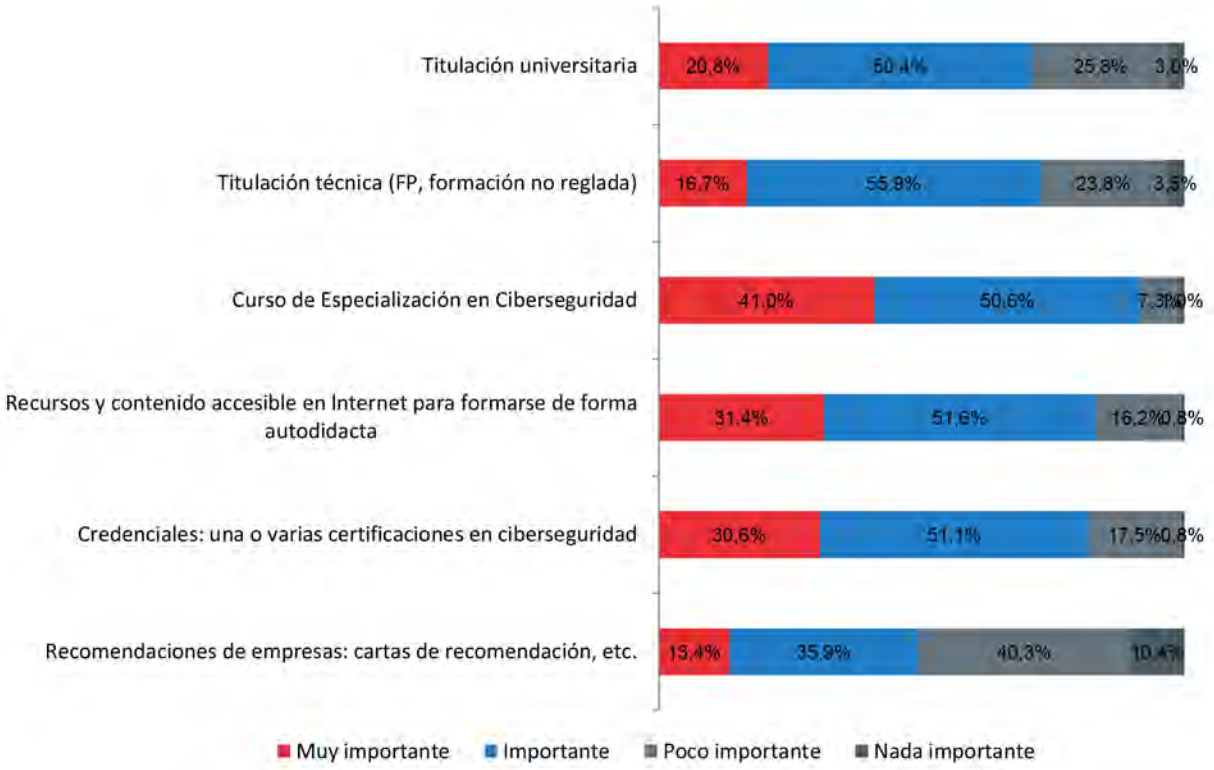


Figura 18. Grado de importancia de los requisitos que debería cumplir una persona que se quiera dedicar a la ciberseguridad

4.1.2.1.3_Certificaciones

Las certificaciones son altamente valoradas en el sector de la ciberseguridad, tal y como se refleja en la gráfica: el 80% de los trabajadores, estudiantes o demandantes del empleo en el sector considera la falta de credenciales o certificaciones en seguridad como un hándicap importante o muy importante para acceder al mercado.

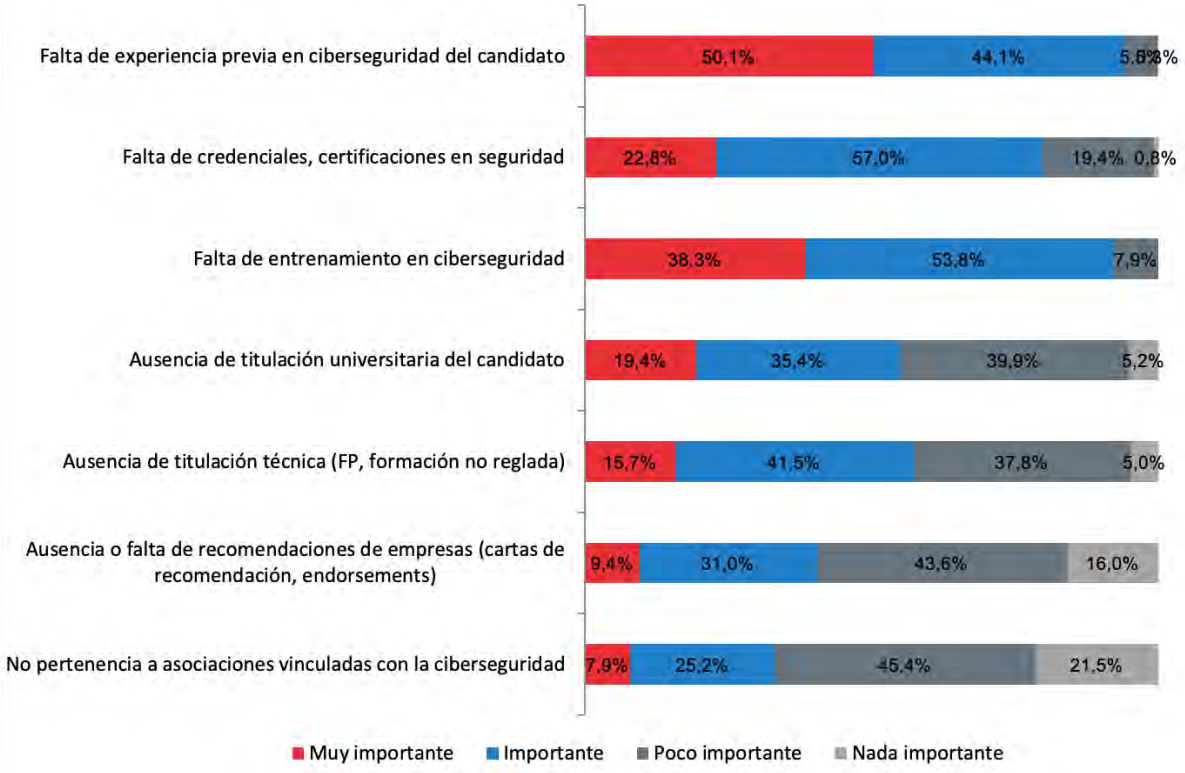


Figura 19. Hándicaps que las empresas se encuentran a la hora de contratar talento en ciberseguridad

Por otro lado, estos encuestados destacan que las certificaciones que consideran más prioritarias las empresas son las certificaciones de fabricantes, seguidas de la certificación CEH, OSCP, CCNA, CISSP, CISA, y OWSP, como se puede apreciar en la figura.

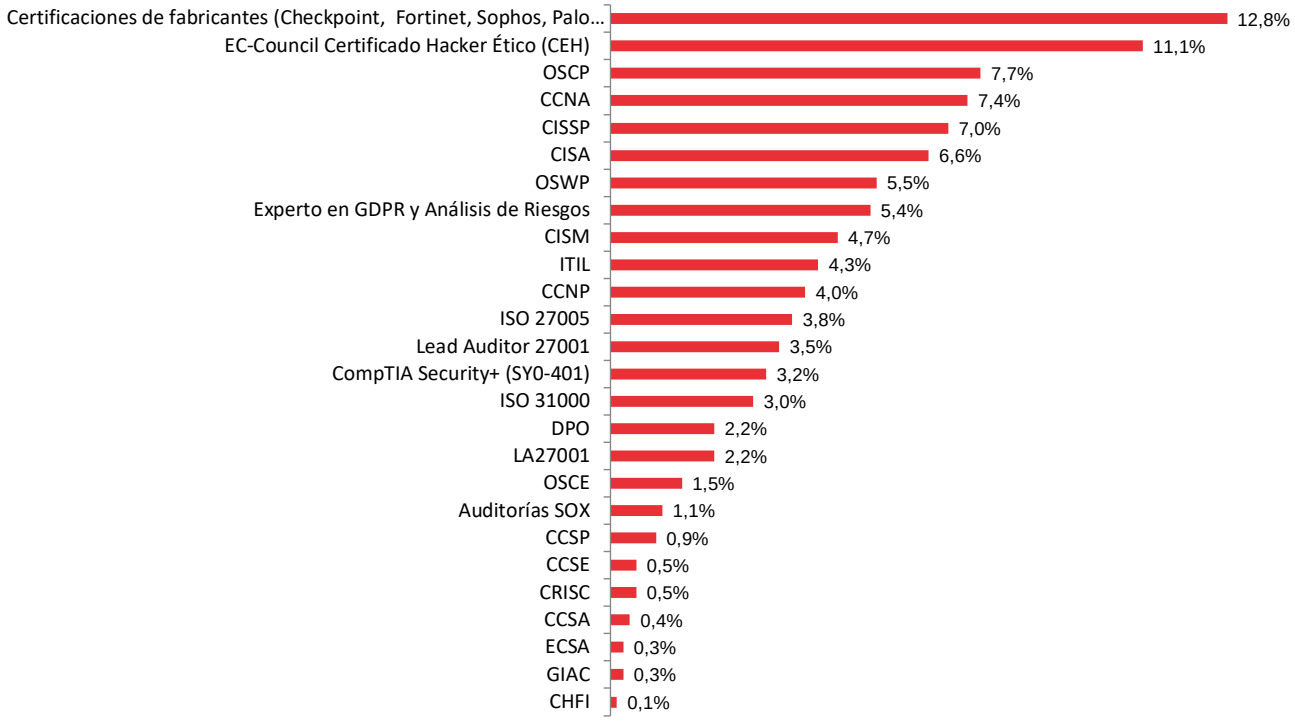


Figura 20. Certificaciones demandadas de manera prioritaria

4.1.2.2_Potenciadores

4.1.2.2.1_ Aprendizaje autodidacta en el sector de la ciberseguridad.

Uno de los potenciadores de la oferta de talento de ciberseguridad es, sin duda, la creciente tendencia de autoaprendizaje. La autoformaciónpuede 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 21. ¿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. A continuación, se ofrece una tabla comparativa de las mencionadas.

	Foros	MOOC	Cursos presenciales	Bootcamps	Tutoriales on-line	Libros	Ferias
Descripción	Reunión de personas competentes en determinada materia, que debaten ciertos asuntos ante un auditorio que a veces interviene en la discusión. En Internet, sitio en el que se opina, se debate o se intercambia información sobre un tema determinado.	MOOC es el acrónimo en inglés de Massive Online Open Courses (o cursos online masivos y abiertos). Los cursos masivos no han sido otra cosa que la evolución de la educación abierta en Internet.	Los cursos presenciales cuentan con un profesor especializado en la materia que explica y forma a los alumnos. La diferencia con los cursos MOOC es que son presenciales y con un horario fijado previamente.	Formación intensiva práctica en ciberseguridad para gente que tiene interés en iniciarse hasta gente con muchos conocimientos en la materia.	Los tutoriales suelen ser videos de corta duración accesibles para todo el mundo de forma gratuita que instruye al visualizador a través de diferentes maneras y transfiere el conocimiento acerca de la ciberseguridad de manera genérica al usuario.	Los libros son otra manera de formarse en ciberseguridad y adquirir el conocimiento teórico para sentar las bases de una formación más práctica.	Las ferias de ciberseguridad son eventos puntuales dedicados únicamente a la temática de la ciberseguridad, que cuentan normalmente con el área de congreso y de exposición de empresas.
Ventajas y desventajas	Es un espacio flexible que permite intercambiar pensamientos acerca de la ciberseguridad y comunicarse con otros expertos e interesados en la materia. Permite el aprendizaje en grupo y puede motivar a las personas más introvertidas a participar (cuando es online).	Mayor flexibilidad que un curso presencial y suelen ser gratuitos. No obstante, no se cuenta con atención en tiempo real y resulta más complicado establecer nuevos contactos.	Suelen ser de pago , pero permiten la interacción en tiempo real con otros alumnos y profesores para solventar dudas e intercambiar ideas al instante. Permiten establecer una red de contactos basada en el contacto real y directo.	Formación intensiva en muy poco tiempo y muy bien valorada en el mercado laboral.	Es gratuito, no requiere horario ni compromiso fijo, disponibles en toda la web y en múltiples idiomas. Sin embargo, no cuenta con atención y formación personalizada para el usuario/alumno.	Una vez adquirido es fácil volver a consultar ciertos temas y puede servir para despertar el interés inicial en un futuro profesional. Están escritos por profesionales con una trayectoria y conocimientos en ciberseguridad muy amplios. No obstante, pueden quedarse obsoletos ya que la ciberseguridad avanza muy rápido. Son útiles para la teoría y las bases de la ciberseguridad.	Las ventajas de ir a ferias de ciberseguridad es que permite conseguir contactos del sector, conocer el mercado actual, posicionarse a sí mismo. Conocer las caras más relevantes del mundo de la ciberseguridad en España.
Ejemplos	INCIBE, Departamento de Seguridad Nacional, Foro Nacional de Ciberseguridad, ISMS Forum, Foros online	INCIBE, edX, Coursera, Udemy, Miriadax	INCIBE, Upgrade Hub, The Security Sentinel, Cámara de Comercio	INCIBE (Summer BootCamp), INCIBE (Academia Hacker), KeepCoding, Ironhack, The Bridge, Upgrade Hub	INCIBE (videotutoriales, YouTube), Universidades Públicas, Administración Pública	Ciberdiccionario: Conceptos de ciberseguridad en lenguaje #entendible (Javier Zubieta) El arte de la invisibilidad: El hacker más famoso del mundo enseña seguridad en la era del Big Brother y Big Data (Kevin Mitnick)	Madrid Tech Show, SICUR, Security Forum, Cloud & Cyber Security Expo Madrid

Tabla 3. Principales vías para adquirir conocimiento y competencias en ciberseguridad

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 22. Opciones preferidas para desarrollar competencias y conocimientos de manera autodidacta

4.1.2.2.2_Impacto positivo de la extensión de la formación online en la oferta de ciberseguridad

Es indudable que los estudios sobre ciberseguridad son altamente susceptibles a impartirse de manera online respecto a otras materias, lo que potencialmente facilita el acceso a los mismos desde diferentes zonas geográficas, como pueden ser las zonas rurales o incluso desde el exterior. Igualmente, se debe tener en cuenta que la mayoría de los profesionales a la hora de seleccionar un trabajo en un puesto de ciberseguridad, le dan mucha importancia al trabajo remoto y al grado de flexibilidad que les otorguen los potenciales empleadores. Igualmente, es importante el reciclaje de profesionales desde otras áreas de la tecnología hacia la ciberseguridad, cuando la empresa no ofrece cursos para permitir una movilidad interna.

La figura que hay a continuación, muestra que más de la mitad de la formación universitaria en ciberseguridad únicamente se imparte de manera online, mientras que tan solo un 22% de los másteres y grados se imparten de forma exclusivamente presencial.

Figura 23. Modalidades de impartir formación universitaria en ciberseguridad

4.1.2.3_Limitadores

4.1.2.3.1_ Escasez de profesorado

Si bien 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.

4.1.2.3.2_ 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.

Cabe destacar en este sentido que las formaciones que combinan los conocimientos de ciberseguridad con otras materias sí que tienen un mayor grado de aceptación entre las estudiantes. Sirva como ejemplo el máster en Derecho de la Ciberseguridad y Entorno Digital de la Universidad de León con un 50% de mujeres egresadas.

Este gap en cuanto al porcentaje de alumnos y alumnas no es algo exclusivo del área de la ciberseguridad, es extensible al conjunto de la formación reglada en tecnología, si bien parece que esta brecha se está cerrando de manera progresiva. Así, el porcentaje de mujeres que han elegido estudiar carreras tecnológicas ha aumentado en 5 puntos porcentuales en 5 años, al pasar del 24% de chicas matriculadas en el curso 2016-17 al 29% de matriculadas en el curso 2019-20[16].

Cabe destacar que, en la encuesta realizada, a pesar de una distribución homogénea de la muestra entre todas las franjas de edad y regiones, tampoco existe proporción entre género (70% hombres) lo que refleja la desproporción real en el mercado de oferta.

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. De cualquier modo, este es un problema que seguramente se debe abordar de manera previa, con la gestión de las vocaciones, ya sea a edad temprana (educación primaria o secundaria obligatoria) o en ciclos educativos superiores. Además, los obstáculos culturales se deben remover para que las mujeres puedan tomar una elección libre con respecto a su futuro profesional.

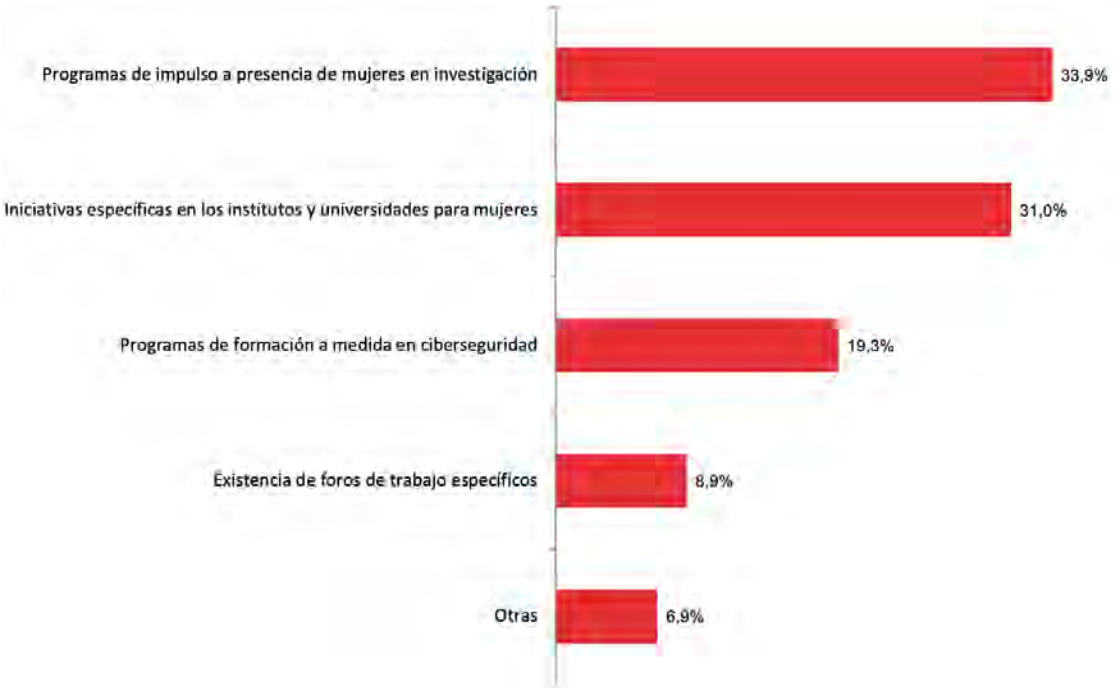


Figura 24. Iniciativas que ayudarían a incrementar la presencia de mujeres en posiciones de ciberseguridad

16 Datos correspondientes a la Universidad Politécnica de Cataluña, Noviembre 2020

4.1.2.3.3_ 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 como muestra la figura 25.

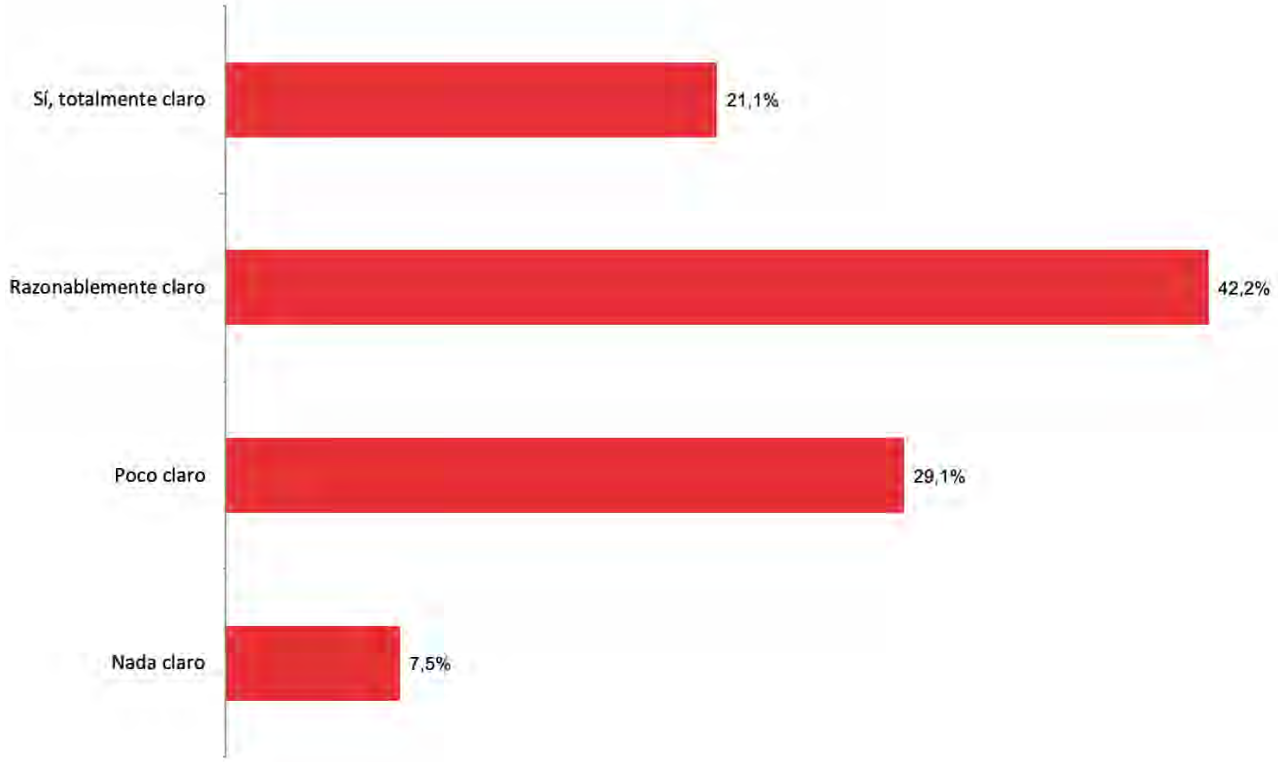


Figura 25. Grado de conocimiento respecto de las habilidades, itinerario formativo y cualificación necesaria para dedicarse profesionalmente a la ciberseguridad en España

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** 26. ¿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.

Se hace necesario por tanto impulsar programas de generación de talento a largo plazo que abarquen programas educativos en primaria e incluyan la formación en habilidades electrónicas (*e-skills*) dentro de estudios de primer ciclo.

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 comunicación entre ellos.

4.1.3_ Conclusiones

A continuación, se presentan, de manera agregada, las principales conclusiones obtenidas tras analizar la oferta de talento de ciberseguridad en España y estructuradas en áreas de impacto:

Necesidad de mejorar la cantidad y calidad de la oferta existente. La primera conclusión destacable es la necesidad de un incremento destacable en la cantidad y calidad de los recursos formados en ciberseguridad en España para cerrar el gap entre oferta y demanda de talento.

Resulta comprobado, que, a pesar del incremento en la oferta disponible en los últimos años, existe una desalineación entre oferta y demanda, como demuestra de que solo el 46% de las personas dedicadas a la ciberseguridad considera que reúne el perfil de competencias, conocimientos y habilidades necesarios para trabajar en el sector.

No existe un itinerario formativo claro para trabajar en ciberseguridad. A pesar de que existe mucha formación, la realidad muestra que un estudiante no dispone de información clara para poder determinar qué debe estudiar si quiere dedicarse a la ciberseguridad. Por ello, es esencial determinar una hoja de ruta que detalle de manera clara la tipología de perfiles que existen en el ámbito de la ciberseguridad tanto en organizaciones públicas como privadas, así como los conocimientos, habilidades y experiencia necesaria para poder acceder a ellos, y lo que se requiere para el reciclaje de un perfil a otro.

La formación reglada es la base de la oferta, pero requiere de una profunda revisión y actualización para alinearla con las necesidades actuales de las empresas. La especialización en ciberseguridad se sostiene principalmente a través de oferta reglada, expresada en grados, másteres y formación profesional.

Dentro de la oferta universitaria cabe destacar que existen grados técnicos en los que se abordan aspectos de la ciberseguridad, como Ingeniería de Telecomunicaciones o Informática. Sin embargo, la realidad es que en España solo existen cuatro grados específicos sobre ciberseguridad, y diseñados en algunos casos para complementar el conocimiento sobre ciberseguridad con otros aspectos como el derecho, la consultoría o aspectos de negocio.

La solución a este problema de acuerdo al análisis efectuado estaría relacionada con varias acciones simultáneas: aumento del número de asignaturas que aborden la ciberseguridad desde distintos grados técnicos, creación o aumento en la oferta de grados específicos sobre ciberseguridad y complemento de perfiles generalistas con másteres en ciberseguridad que doten al mercado de una mayor cantidad y calidad de talento.

La formación profesional, clave para aportar talento de ciberseguridad. La FP es altamente valorada por el mercado de nuestro país y se trata de una de las áreas donde el paro juvenil se produce en menor proporción. En este contexto, cabe destacar la introducción de la nueva Ley de Formación Profesional en la que se tiende a dar una mayor relevancia a la formación dual. Una medida en línea con alguno de nuestros comparables europeos que busca disminuir los niveles de paro juvenil.

Si bien se están dando los pasos necesarios para dotar al mercado de profesionales con los perfiles necesarios para cubrir el gap actual como lo demuestra la reciente creación de un 'Curso de Especialización en Ciberseguridad en Entornos de Tecnologías de la Información', la realidad es que 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, lo que puede suponer un freno a la hora de generar talento de ciberseguridad.

Formación del profesorado en materia de ciberseguridad. No será posible incorporar formación más específica alineada con las demandas de las empresas, si el profesorado no adquiere los conocimientos y competencias necesarias para poder incorporar contenido más específico en las diferentes asignaturas, programas y titulaciones.

Una acción fundamental tiene que venir, por tanto, en la promoción de vocación entre los formadores hacia este tipo de materias. Así, se hace necesario contar con estructuras estables de formación de formadores como paso previo para la extensión de la oferta.

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.

Las certificaciones son altamente valoradas en el sector de la ciberseguridad, principalmente las expedidas por los propios fabricantes, lo que enfatiza la necesidad de alinear la oferta actual de programas con la demanda de las empresas, así como la experiencia práctica en las tecnologías y entornos de seguridad que maneja la empresa para poder reducir la curva de aprendizaje y maximizar el ROI en la inversión de contratación de nuevo talento.

Aumento de la vocación (de estudiantes y alumnos) como primer paso. 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.
Cabe destacar que se relaciona con una falta de planificación formativa adecuada desde edades tempranas que aporte la base que genere el posterior interés. Algo resaltable es la capacidad de mejora en la comunicación sobre la importancia de la ciberseguridad en todos los niveles educativos, pero principalmente en educación primaria y secundaria.
Es por tanto fundamental impulsar programas de generación de talento a largo plazo que incluyan la formación en habilidades electrónicas (*e-skills*) dentro de estudios de primer ciclo.

Disminuir el gap en cuanto a género. Uno de los datos más preocupantes del estudio tiene que ver con que del total de estudiantes que se especializan 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.

Este gap en cuanto al porcentaje de alumnos no es algo exclusivo del área de la ciberseguridad, es extensible al conjunto de la formación reglada en tecnología, si bien parece que esta brecha se está cerrando de manera progresiva.

Respecto a las iniciativas que posibilitarían incrementar la presencia de mujeres en posiciones de ciberseguridad, seguramente se debe abordar con la gestión de las vocaciones, ya sea a edad temprana (educación primaria o secundaria obligatoria) o en ciclos educativos superiores.

4.2_ Caracterización de la demanda de talento en ciberseguridad

4.2.1_Análisis cuantitativo 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 realizado un análisis de las diferentes aproximaciones llevadas a cabo por organizaciones como la ISC2[17] , 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 de 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 la empresa en la 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.

17 https://www.isc2.org/Research/Workforce-Study

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

En el caso de las pymes, en 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 la empresa para mantener una estimación más conservadora.

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 el crecimiento del PIB y el 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 de empleo y capital (físico y humano), determinan el crecimiento del PIB[18] .

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[19] 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. Para el presente documento, asumimos como principales conclusiones que, a corto plazo, un umbral de crecimiento del 0,3% del PIB estabilizaría el crecimiento neto de la tasa de desempleo y que, a largo plazo, un umbral del 1,35% del crecimiento del PIB, generaría empleo neto.

18 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.

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

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[20] .

4.2.1.1_ Análisis de la demanda actual de talento de ciberseguridad

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

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 **149.774**, 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:

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

20 El Benchmark 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

Donde:

EmpleoPIB: 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. Para su cálculo, tomamos como dato las cifras de varias fuentes de información como el Consejo General de Economías y Bankinter, que muestran crecimientos proyectados cercanos al 6% para los años 2021 y 2022 (y una desaceleración posterior que ubicaría este dato en torno al 2%) para 2023 y 2024. Por tanto, únicamente se estaría generando empleo de haber un crecimiento que supere el umbral del 1.35% neto en un periodo de un año.

EmpleoTI 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.
Este estado cero lo establece Red.es en 533.000 trabajadores en el sector TIC para 2019 y creciendo un 7,3% en conjunto. Sin embargo, otras fuentes asumen que el crecimiento del empleo dentro del sector TIC se establece en un 5% anual, por lo que partiendo de este estado inicial, la proyección inicial del crecimiento de la demanda se incrementaría en el total del sector TIC en un 5%. No obstante, si tenemos en cuenta que el mercado de la ciberseguridad está creciendo comparativamente más que el resto de los mercados de tecnología es necesario adicionar un factor de corrección a dicho cálculo que tenga en cuenta los efectos de aceleración o desaceleración de dicho mercado en el total del empleo.

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.

4.2.1.2_ 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.

Estimación fuerza laboral						
Año	**2019**	**2020**	**2021 P**	**2022 P**	**2023 P**	**2024 P**
ESPANA - metodología de (ISC)²						
Representación de profesionales en ciberseguridad de la fuerza		0,26%				
# de profesionales de ciberseguridad por cada millón de trabajadores		2.580				
Población España 2021		47.394.223				
Total fuerza laboral en ciberseguridad en España		**122.284**				
Gasto de TI y de ciberseguridad en España - Como factor de corrección (cifra en millones)						
Gasto de TI	48.185	46.749	49.274	49.965	50.836	52.358
Gasto de ciberseguridad	1.413	1.521	1.624	1.749	1.890	2.044
Representación de ciberseguridad dentro de Total TI	2,9%	3,3%	3,3%	3,5%	3,7%	3,9%
Relación de Crecimiento YoY		0,3%	0,0%	0,2%	0,2%	0,2%
Datos para Proyección						
Crecimiento PIB España			6,0%	5,8%	1,9%	2,3%
Inflación			2,4%	1,4%	1,2%	0,9%
Crecimiento neto			3,6%	4,4%	0,7%	1,4%
Crecimiento anual fuerza laboral sector TIC		5,0%	5,0%	5,0%	5,0%	5,0%
Representación fuerza laboral de ciber dentro de TI		22,9%				
Factor de incremento por cada punto porcentual del PIB			0,3%			
Estimación fuerza laboral						
Empleos en el sector TIC	533.333	579.066	627.342	681.965	742.898	810.422
Contratos activos en España		15.976.297				
Crecimiento empleo en función del PIB				172.544	213.165	0
Crecimiento empleo en ciberseguridad en función del PIB				**445**	**550**	**0**
Crecimiento empleo TIC en función del gasto de TI		45.733	48.276	54.623	60.933	67.524
Crecimiento empleo en ciberseguridad en función del gasto de			3.846			
Crecimiento empleo en ciberseguridad en función del gasto de		10.486	11.069	12.524	13.971	15.482
Total fuerza laboral en ciberseguridad en España			122.284	135.253	149.774	165.256

Figura 27. 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.

En la actualidad las organizaciones públicas y privadas reciben más de 150.000 ataques de malware diarios

En concreto, la demanda de profesionales en el ámbito de la ciberseguridad no ha parado de crecer, sobre todo, debido al incremento de los ataques cibernéticos y la necesidad de las organizaciones para responder a ellos y contrarrestarlos. Según datos de CheckPoint, en la actualidad las organizaciones públicas y privadas reciben más de 150.000 ataques de *malware* diarios. Más aún, otro importante catalizador de la demanda es el cumplimiento regulatorio y normativo en ciberseguridad. Las empresas deben cumplir cada vez más con requisitos legales y obtener certificaciones que poder mostrar a sus clientes. Estas tareas requieren esfuerzo de profesionales en todas las categorías profesionales de ciberseguridad dentro de una empresa.

La demanda de profesionales en el sector de la seguridad cibernética lleva en aumento estos últimos años y sigue in crescendo. Esto es debido al incremento de ataques cibernéticos y la necesidad de las organizaciones para responder a ellos y contrarrestarlos. Se refleja en las ofertas de empleo que se publican a diario, solo superadas por los puestos relacionados con el análisis masivo de datos y el aprendizaje de las máquinas. Este tipo de trabajos, generados por las TIC, tienden a ser estables y suelen facilitar la movilidad entre compañías y sectores.

Asimismo, *STEAM IMMUNE Technology Institute, hub* de educación en tecnología y centro de generación de talento, publicó las tendencias en programación de cara a 2020, de las que destacó la inteligencia artificial, data science y la ciberseguridad para las empresas. En dicha publicación subrayó que, *"la ciberseguridad es la gran tendencia para los próximos años. Las empresas apostarán por contar con sistemas a prueba de ataques y con equipos capaces de reaccionar ante cualquier ataque"*.

En esta situación, formarse en esta disciplina es, sin lugar a duda, una salida profesional con plenas garantías de empleabilidad. Y es que la demanda crece y la oferta escasea. Otro dato interesante es la remuneración en este sector, donde en el 2020 el sueldo de estos especialistas creció un 7%. Las opciones para los profesionales se encuentran en sectores tecnológicos y servicios de la información, consultoría, seguridad informática, defensa, telecomunicaciones, contabilidad, industria espacial y en el sector bancario.

Sin embargo, uno de los principales frenos que encuentran las organizaciones a la hora de contratar este talento específico es la necesidad de que dicho talento esté bien formado. En opinión de las organizaciones consultadas, la oferta actual de formación en materia de ciberseguridad ronda el 70,5% de la muestra, y la existente está desalineada con las necesidades de la empresa y es muy generalista (40,6% y 39,3% respectivamente). A nivel de grado, destacan el bajo número de asignaturas de ciberseguridad más que el hecho en sí mismo de disponer de más grados en ciberseguridad. Entender la importancia y trascendencia de ésta dentro del contexto actual lleva a la necesidad de repensar el currículo académico que en la mayoría de los casos, está desactualizado y no tiene en cuenta la evolución tecnológica, del mercado de la ciberseguridad y de las amenazas actuales.

Figura 28. Características de los programas actuales de formación en ciberseguridad

De hecho, tanto los expertos consultados como el trabajo de campo realizado, apuntan a la necesidad de actualizar el currículo formativo que se está impartiendo en la actualidad en carreras técnicas de manera sistemática, de forma que se adapte a las necesidades actuales que demanda el mercado.

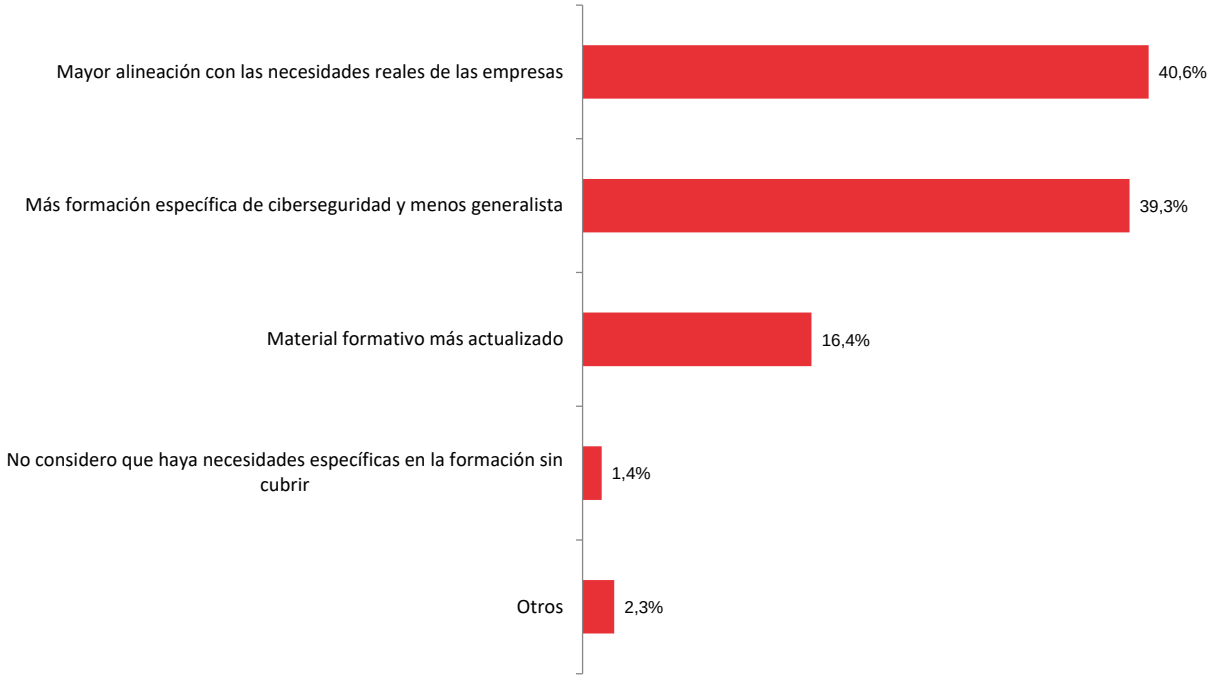


Figura 29. Principales requerimientos asociados la formación. Percepción de la demanda.

Sobre todo, la empresa está demandando en la actualidad formación aplicada que incorpore experiencia práctica, por lo que la formación dual realizada de manera conjunta con una empresa aparece como la principal vía para adaptar la formación existente a las necesidades de las empresas (34,1%), así como mayor presencia práctica en los programas curriculares reglados (24,5%).

Se requiere a juicio de la muestra consultada, en definitiva, alinear la oferta actual con las necesidades actuales y futuras de las organizaciones, y esto solo es posible si existe un material formativo más actualizado, más contacto estrecho entre ambos mundos y donde la incorporación de prácticas dentro de los programas curriculares sea obligatoria y con un detalle de las tareas realizadas.

Sin embargo, para poner en marcha estas iniciativas de formación se requiere de un elemento fundamental y es que el profesorado esté formado para poder impartirlas. A juicio de los expertos y la muestra consultada en el trabajo de campo, en la actualidad en España el nivel de los formadores en materia de ciberseguridad requiere de un riguroso estudio previo de competencias docentes del profesorado del sector.

De esta forma, será posible establecer las competencias, conocimientos y capacidades del candidato a incorporar ante un proceso de selección y poder acelerar la curva de aprendizaje en un contexto donde la aparición de nuevos perfiles profesionales derivados del proceso de digitalización exige, en muchos casos, la adquisición de competencias muy específicas.

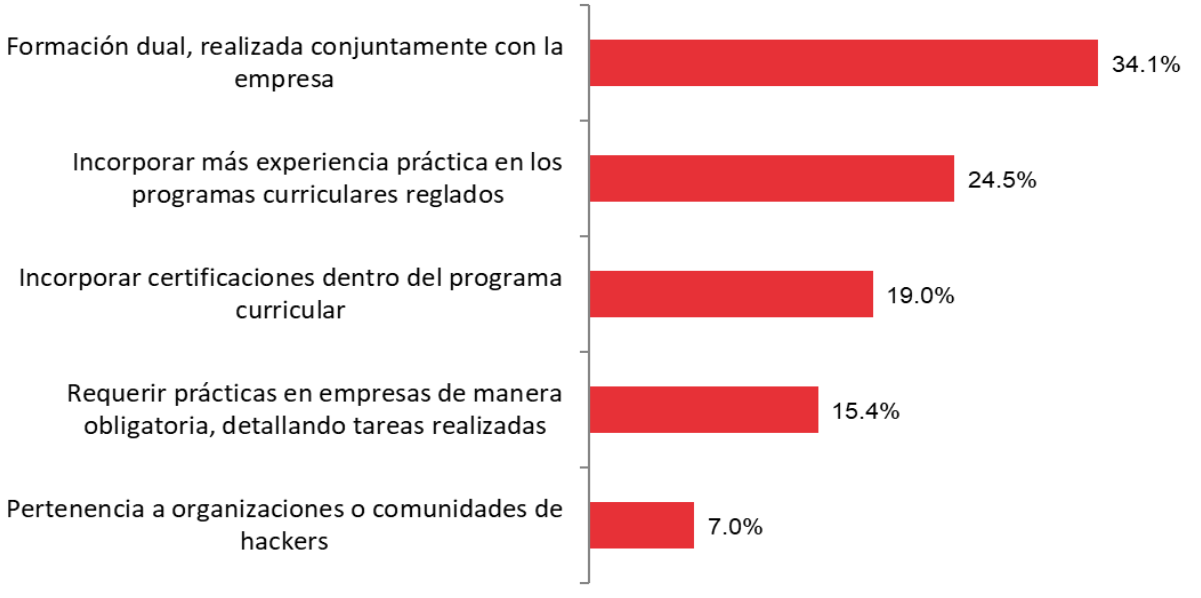


Figura 30. Necesidades específicas de formación consideradas por las organizaciones para alinear la oferta y demanda de talento en ciberseguridad

El papel del sector TIC y de la industria de la ciberseguridad tiene parte de la responsabilidad de incrementar el talento en ciberseguridad. Por ello, más allá del desarrollo de programas de formación *in-house* en las empresas del sector (formación dual) que reconocen el 33,3% de las

organizaciones consultadas, las acciones se estructuran alrededor de la necesidad de dar a conocer las demandas que el propio sector de la ciberseguridad tiene en materia de talento. Solo de esta forma, será posible establecer programas conjuntos entre el sector público y privado orientados a la capacitación de estudiantes (tanto de grado, como de posgrado), así como fortalecer el ecosistema de seguridad aumentando el número de centros especializados de formación para estudiantes tal y como señala la figura. Sin embargo, disponer de más centros no es garantía de una mejor formación. Se requiere igualmente repensar la forma en la que los centros están abordando la formación al colectivo de estudiantes, así como los criterios de admisión a los diferentes programas formativos, de manera que pueda certificar que el talento que se forma da respuesta a las necesidades de la empresa.

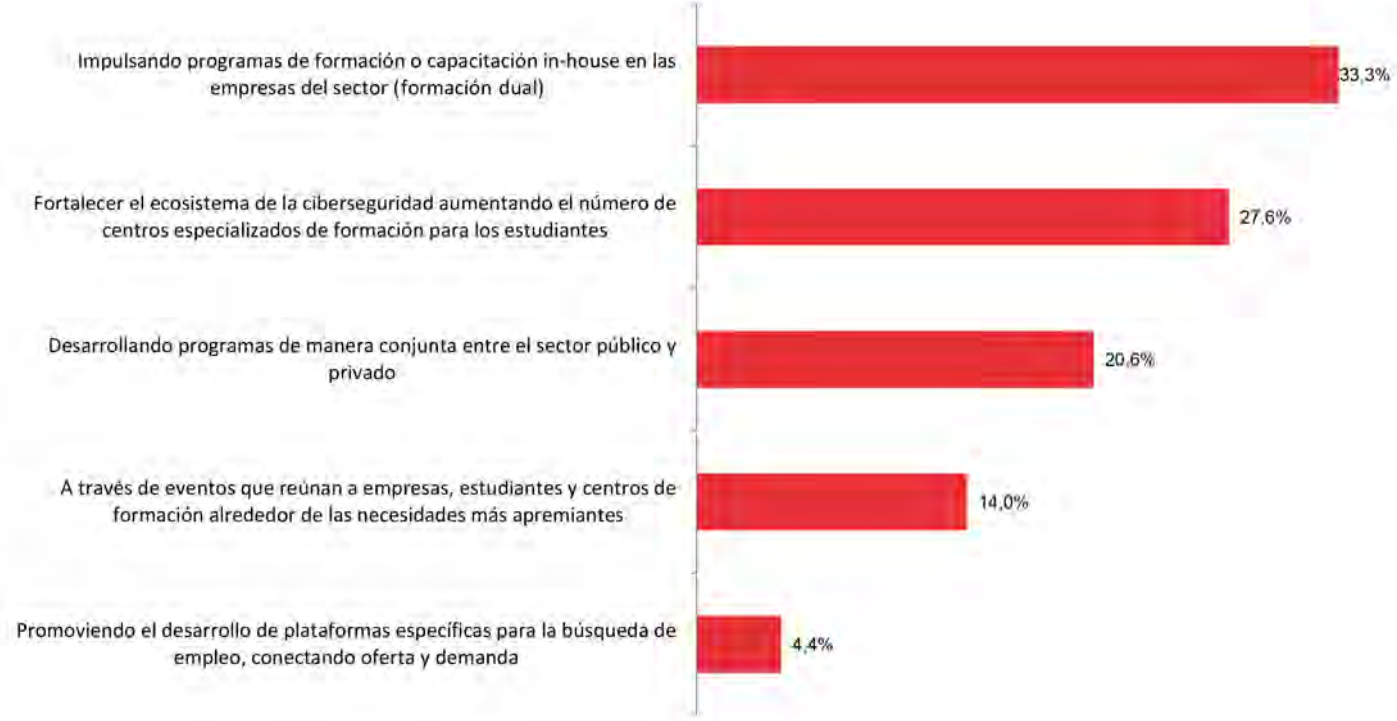


Figura 31. Acciones para el impulso del talento de la ciberseguridad por parte del sector TIC / ciberseguridad

4.2.2.1_ PRESENCIA FEMENINA EN LA CIBERSEGURIDAD

Tradicionalmente, existe una presencia baja de mujeres en carreras 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 propor-

ción 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, **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[21] 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%**.

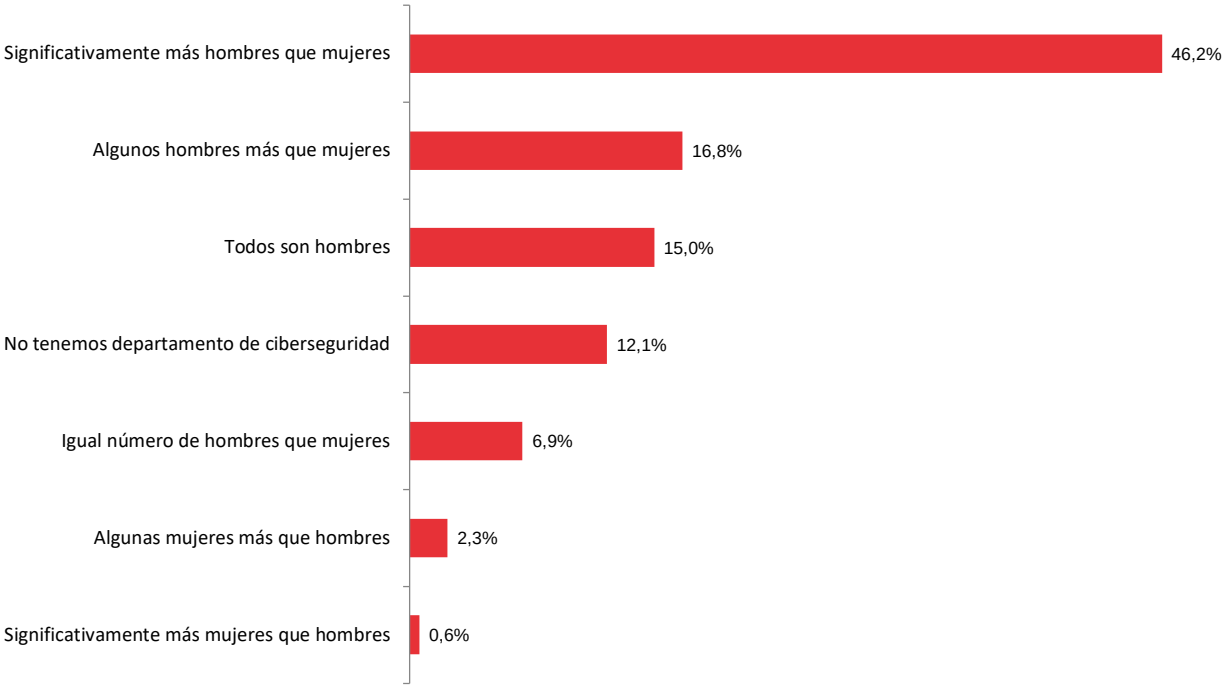


Figura 32. Presencia femenina en la industria de ciberseguridad

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 pue-

21 Fuente: Decrypting Divesity, Diversity and Inclusion in Cyber Security, KPMG, 2020

da 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).

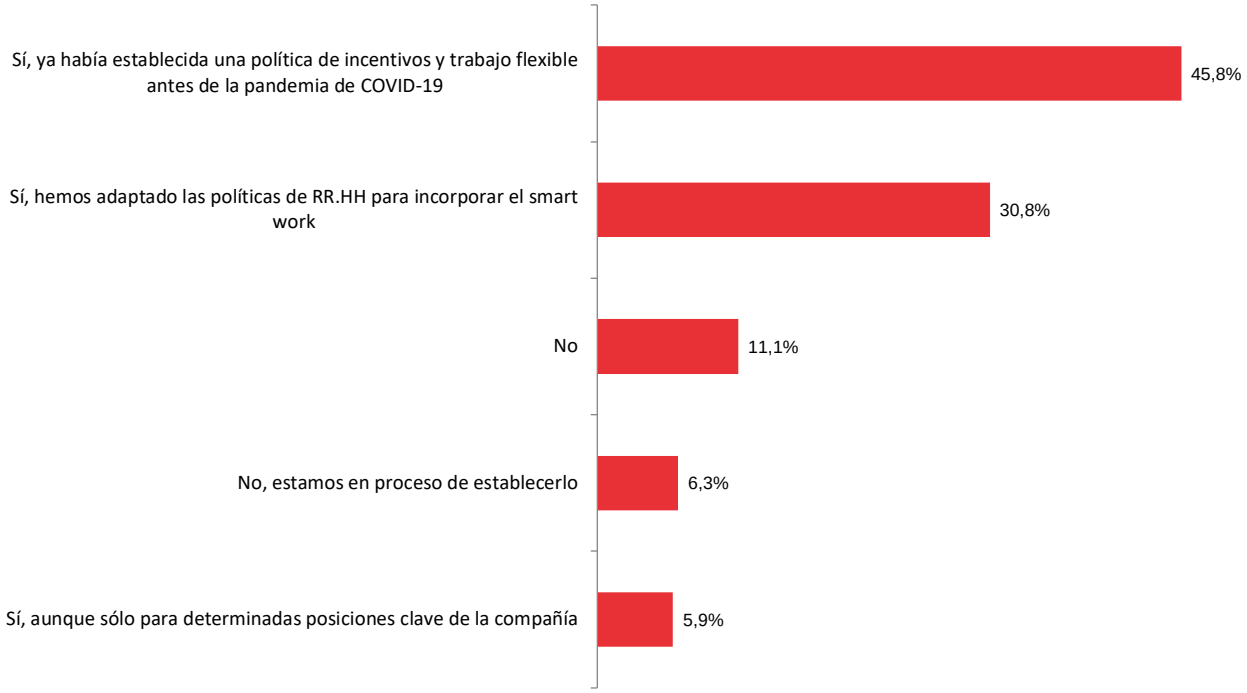


Figura 33. Existencia de políticas flexibles en la industria de la ciberseguridad

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.

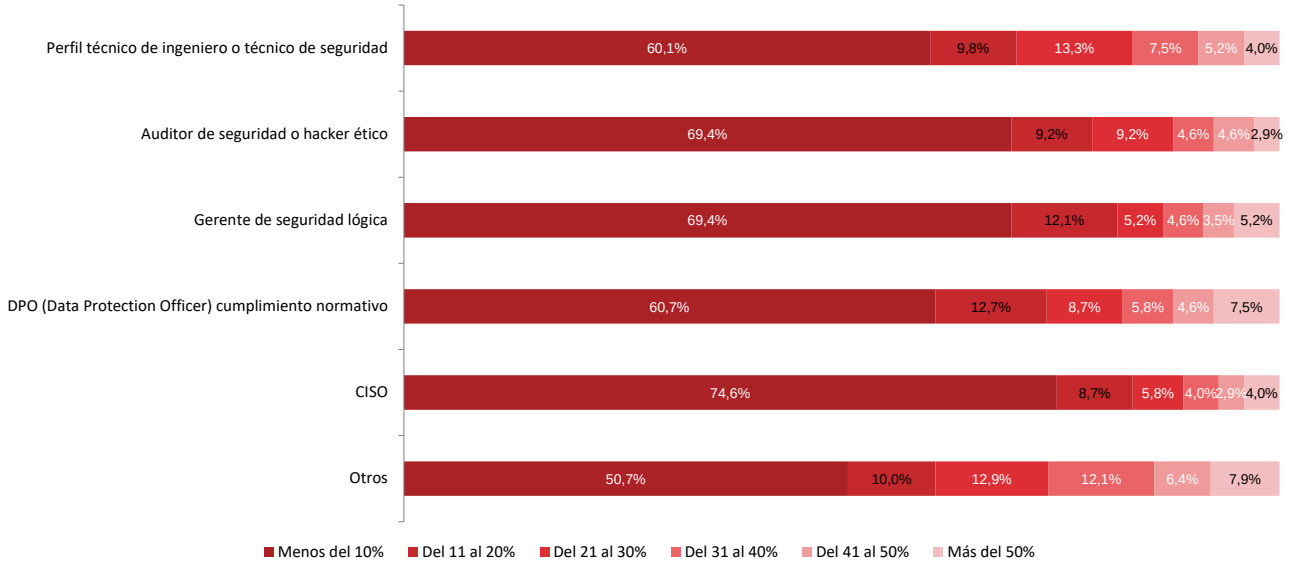


Figura 34. Presencia femenina en función del perfil considerado

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.

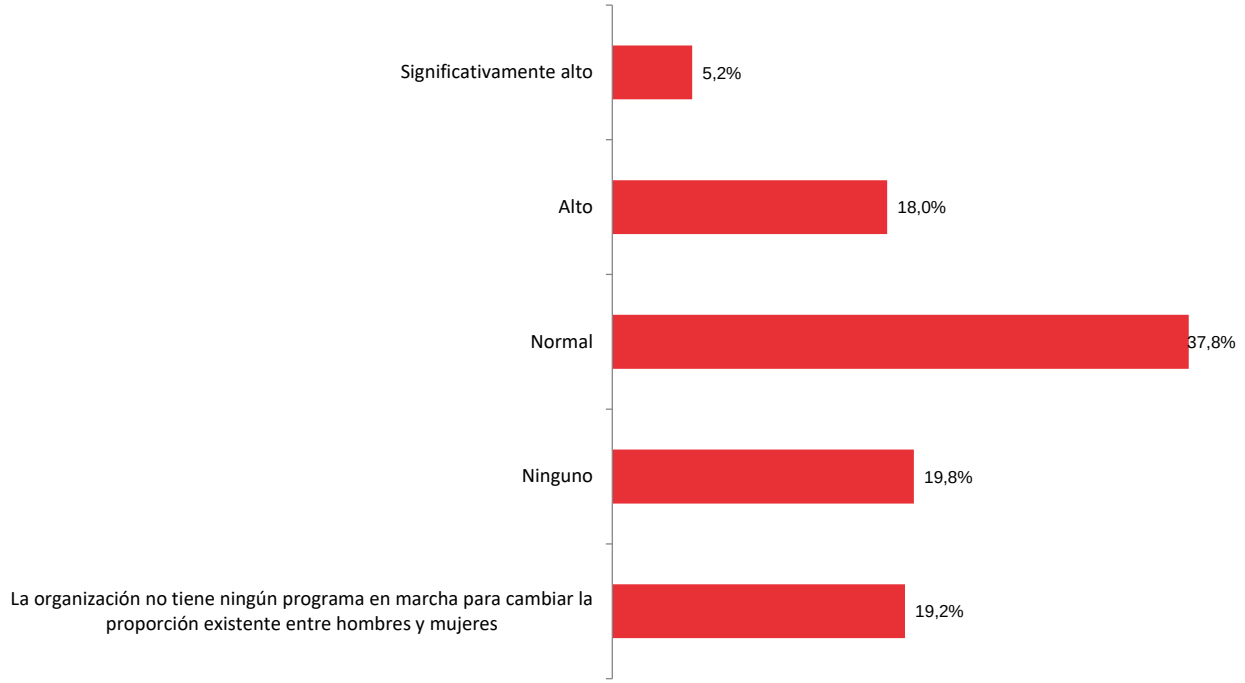


Figura 35. Existencia de planes de refuerzo para la contratación de mujeres en la industria de ciberseguridad

Una de las posibles razones que aducen los expertos a este hecho es la necesidad de definir correctamente la profesión para alinear las acciones pertinentes a la hora de seleccionar el talento de ciberseguridad y, de esta forma, desmitificar conceptos como el 24x7, etc., que pueden servir como frenos para la incorporación de nuevo talento, así como la necesidad de alinear los mecanismos de contratación para realizar un equilibrio entre oferta y demanda, eliminando el riesgo de exclusión.

4.2.2.2_ 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, 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.

4.2.2.3_ 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.

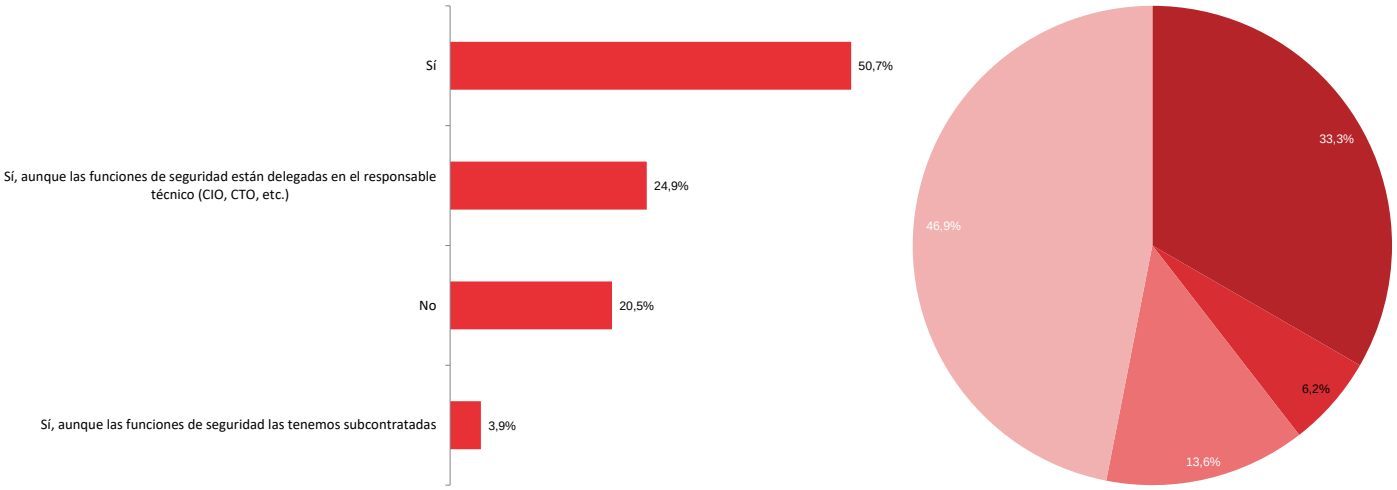


Figura 36. Existencia de departamentos de seguridad en las organizaciones

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.

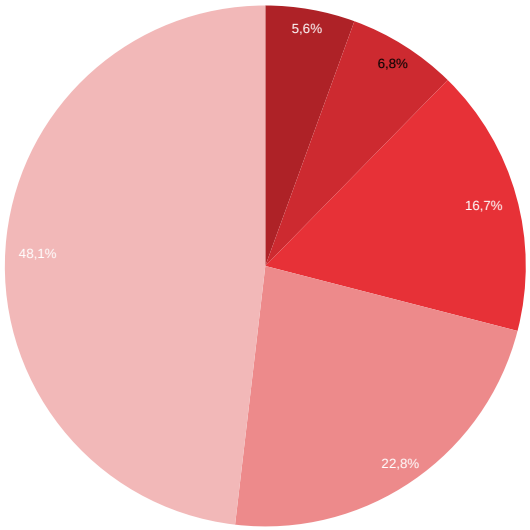


Figura 37. Rotación de personal de los equipos de ciberseguridad en la empresa española

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.

Figura 38. Principales factores para la rotación del talento de ciberseguridad en España.

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 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.

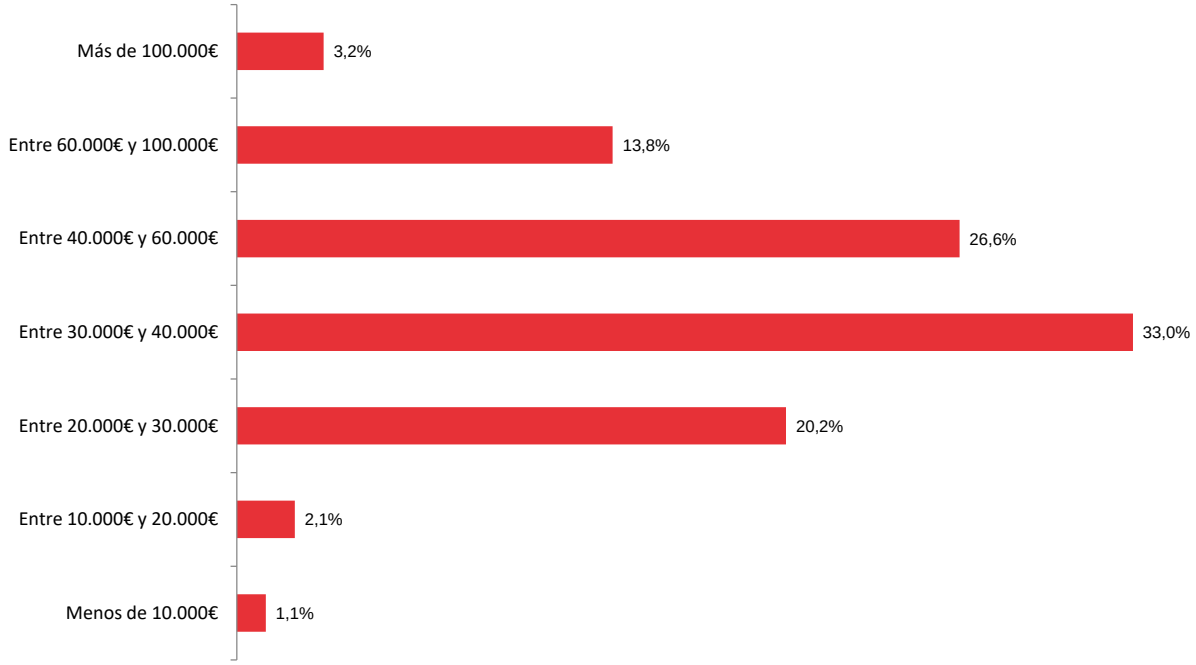


Figura 39. Escala salarial en la que se distribuye la muestra consultada

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.

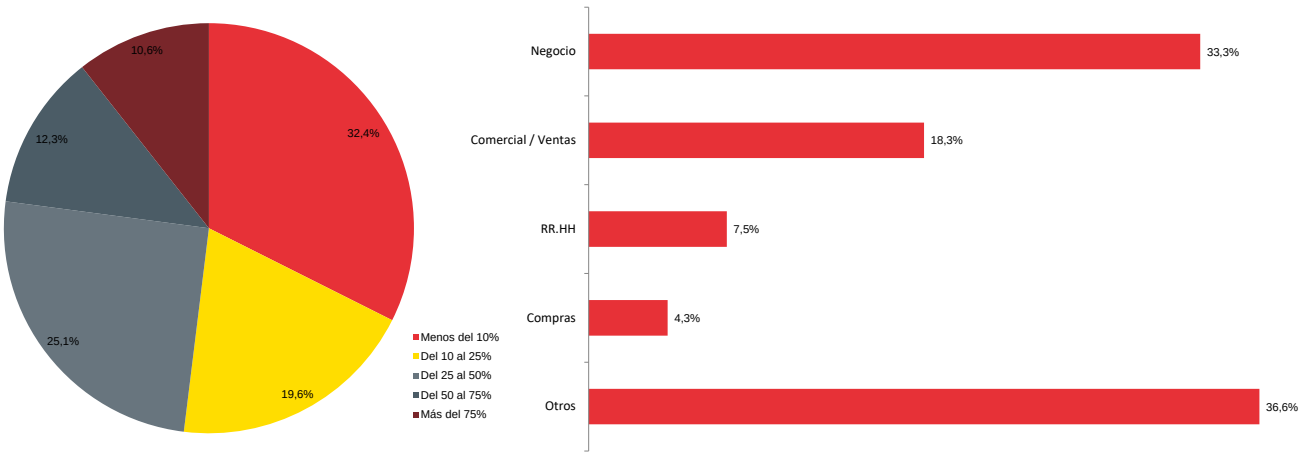


Figura 40. Talento reciclado de otras áreas de la organizacióninterno

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.

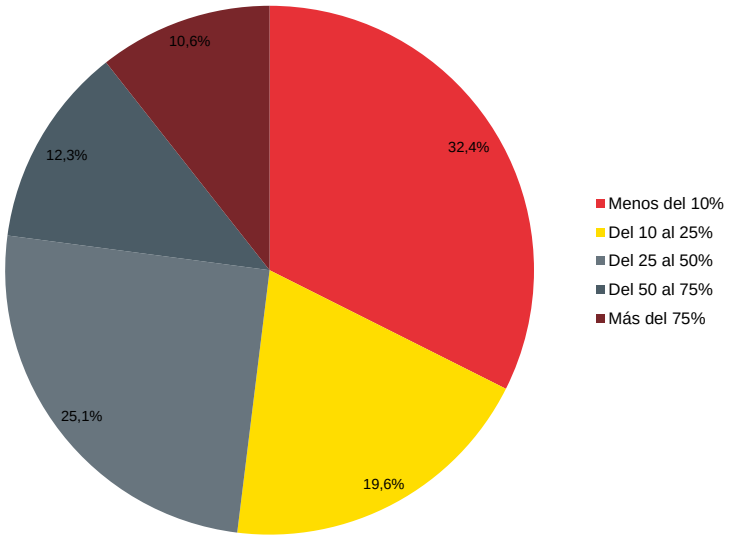


Figura 41. Porcentaje de posiciones abiertas de ciberseguridad que se cubren con reciclaje interno

Otros perfiles requieren de conocimientos y tecnologías específicas y por tanto deben provenir del mercado. En este sentido, los conocimientos en sistemas y redes, arquitectura SIEM, *pentest* y *hacking*, así como seguridad de aplicaciones web y móviles son las tecnologías más demandadas por las empresas a los perfiles de seguridad que se van a incorporar en la organización.

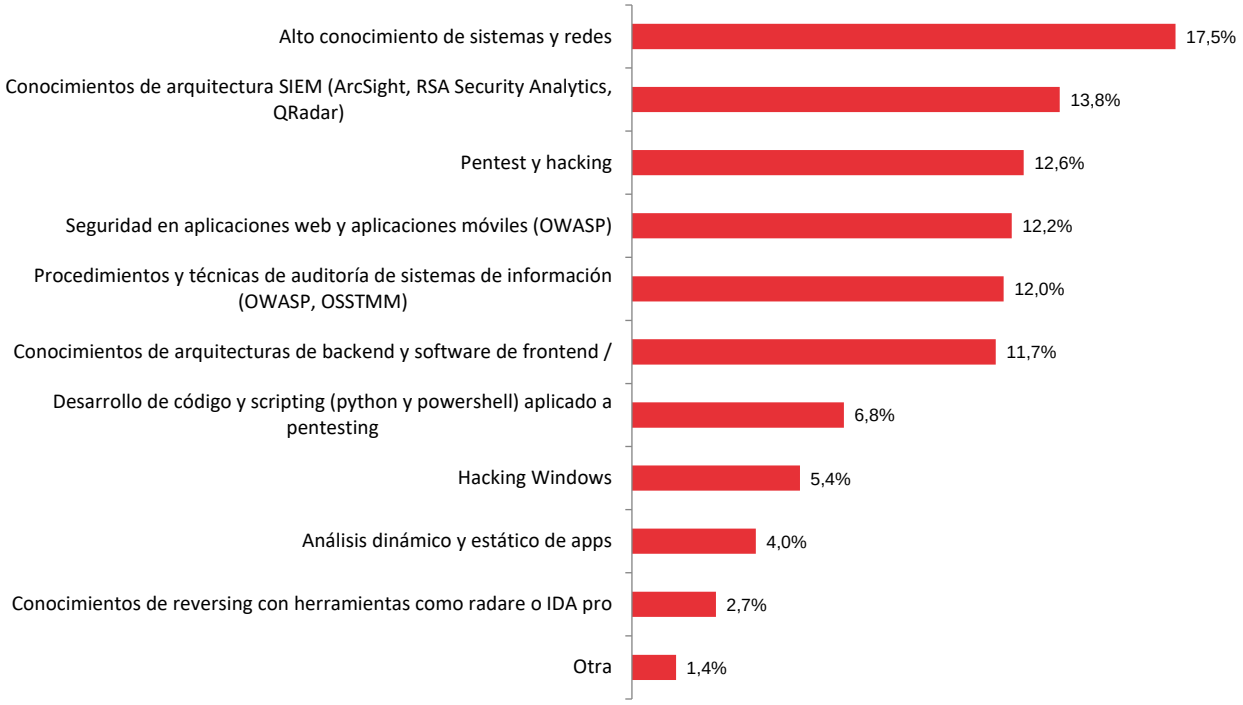


Figura 42. Principales conocimientos demandados para los perfiles de ciberseguridad

Como se ha mencionado anteriormente, la importancia de la seguridad en las organizaciones está motivando la aparición de nuevos perfiles, no tan técnicos, pero que están adquiriendo importancia y que deben tener conocimientos en seguridad. La entrada en vigor de RGDP obliga a disponer de perfiles técnicos asociados a aspectos, como el cumplimiento normativo, etc., y la empresa española está optando por la incorporación directa de este tipo de perfiles (57,6%) frente a otras opciones, como la subcontratación (18,1%), o la autoformación de personal interno para acometer estas tareas cuando sea requerido, tal y como muestra la figura.

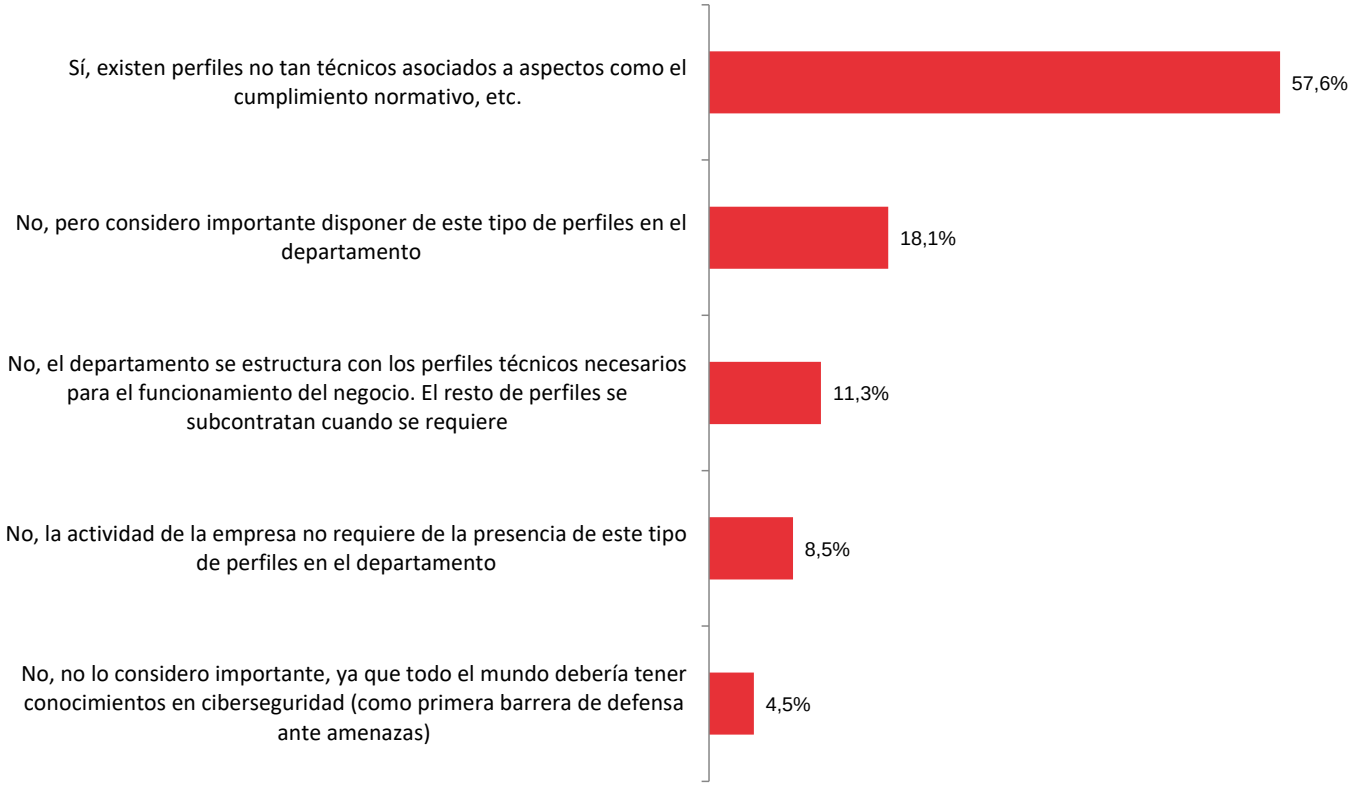


Figura 43. Presencia de perfiles transversales con conocimientos en ciberseguridad en la empresa española

De hecho existe, a tenor de los resultados del estudio realizado, una relación directa entre la falta de talento de ciberseguridad de las empresas y su competitividad, dado que 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).

De hecho, mantener un entorno de seguridad robusto es una prioridad esencial para las organizaciones, sobre todo por el daño reputacional que un ciberataque puede suponer para la organización, así como la pérdida de información y/o propiedad intelectual asociadas a dichos ataques, por no mencionar la necesidad de garantizar una correcta protección del dato y privacidad de este.

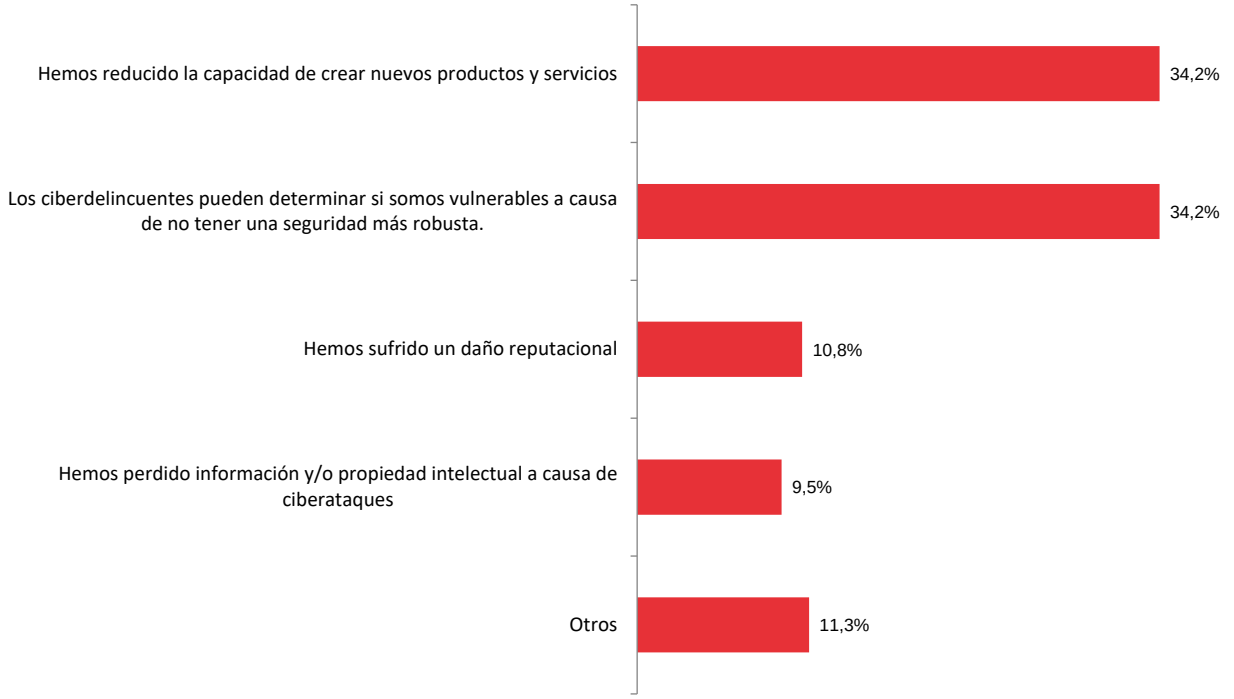


Figura 44. Principales efectos negativos de la escasez de talento de ciberseguridad en las empresas

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.

Sin embargo, para la retención del talento la empresa está desarrollando en la actualidad tres tipos de acciones diferentes:

Mejora de las condiciones salariales, incorporando beneficios sociales, etc, y planes de carrera atractivos que faciliten retener el talento de ciberseguridad. El 79% de la muestra reconoce disponer de un plan de carrera (o está elaborándolo) para incidir en la mejora de la retención del talento en la empresa, detallando acciones específicas para el personal del área de ciberseguridad.Dado que puede ser insuficiente habida cuenta de la competencia existente por este tipo de perfiles, así como la opción de incrementar el número de trabajadores mediante formación a personal de la organización que no es de seguridad. Este tipo de acciones se complementan con otras como la certificación de la formación basada en el rendimiento para certificar el dominio real de las habilidades.

Subcontratar talento externo mediante empresas que proveen de los perfiles que se requieren, aunque al coste asociado aparecen aspectos asociados a la disponibilidad de este tipo de perfiles de certificaciones para garantizar que efectivamente disponen de la experiencia real requerida por la organización.

Automatización como mecanismo por un lado de evitar la sobrecarga y fatiga de los equipos de seguridad en la gestión y administración de herramientas de seguridad en el lugar del trabajo. En la actualidad, según datos de IDC el 70% del tiempo de los equipos de seguridad de las empresas se destina al mantenimiento de soluciones y herramientas de seguridad. Por ello, avanzar en automatización y orquestación de seguridad, así como la integración / racionalización de entornos de herramientas de seguridad se convierte en una prioridad para poder combatir la escasez de talento en ciberseguridad y luchar contra la fuga de talento.

Figura 45. Factores limitantes de la capacidad de las empresas para mejorar sus capacidades de seguridad de TI. Fuente: IDC European Security Survey, June 2020, n=702, n= 50 (Spain)

La muestra consultada reconoce que está desarrollando en la actualidad en mayor o menor proporción las iniciativas descritas, si bien es cierto que mayoritariamente, está tratando de incrementar la base de trabajadores de ciberseguridad mediante la formación, habida cuenta de la dificultad que existe en competir en salario y en el proyecto de desarrollo empresarial con las empresas del sector.

Asímismo, las certificaciones son el principal mecanismo que está utilizando la empresa española para certificar la experiencia práctica y de dominio de los contenidos reales de las habilidades que requiere, tal y como muestra la figura.

Figura 46. Principales acciones llevadas a cabo por las empresas para mitigar la fuga de talento

La subcontratación de perfiles o consultores externos se está viendo sustituida por la creciente adopción de la seguridad como servicio mediante la subcontratación del servicio de seguridad a una empresa tercera que provee no solo del perfil, sino que se hace cargo de la gestión y ejecución del servicio.

La necesidad de racionalidad e integrar las herramientas y soluciones de seguridad y evolucionar hacia una plataforma de gestión integral de la seguridad, está provocando la adopción de la seguridad *cloud* en las organizaciones y, en general del auge como veíamos en el capítulo 3, de los servicios gestionados de seguridad y servicios de integración.

Sin embargo, la facilidad de incorporación de este tipo de perfiles es desigual siendo precisamente estos perfiles asociados a los servicios gestionados de seguridad, los perfiles más complicados de incorporar.

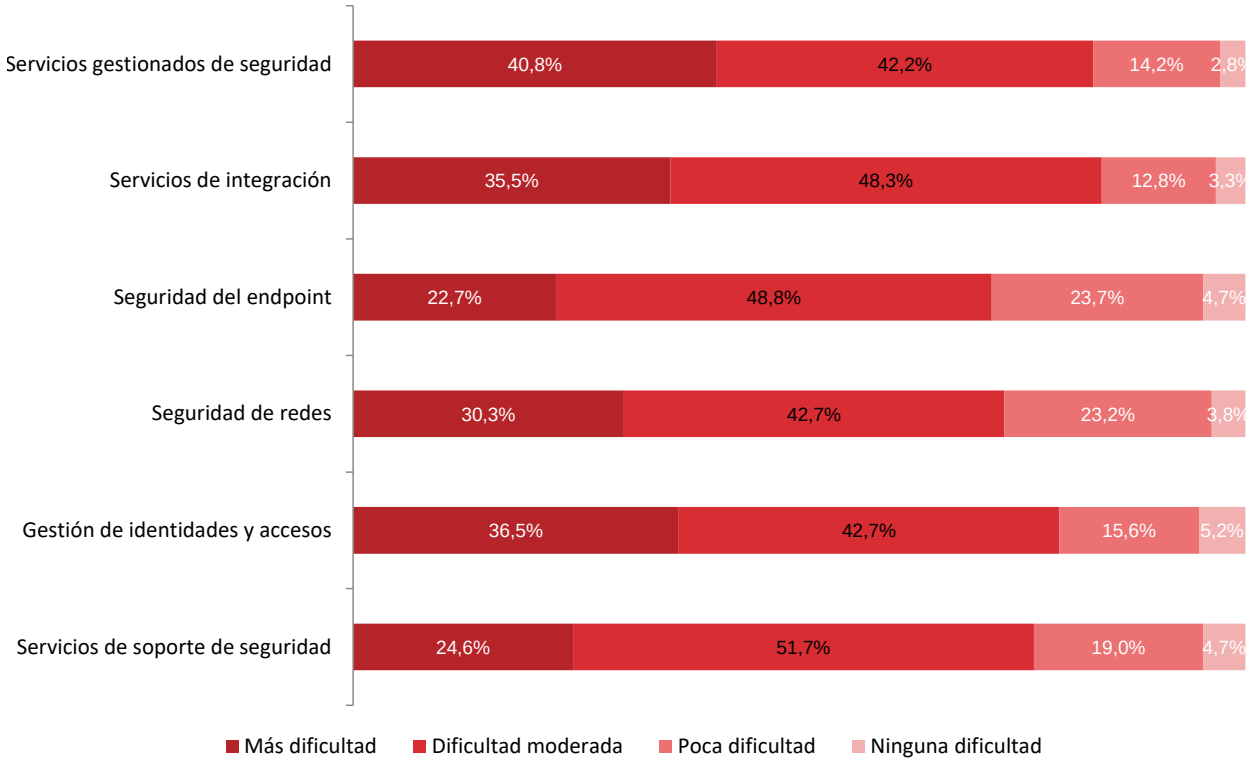


Figura 47. Dificultad de incorporar perfiles de seguridad en modo subcontratación

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.

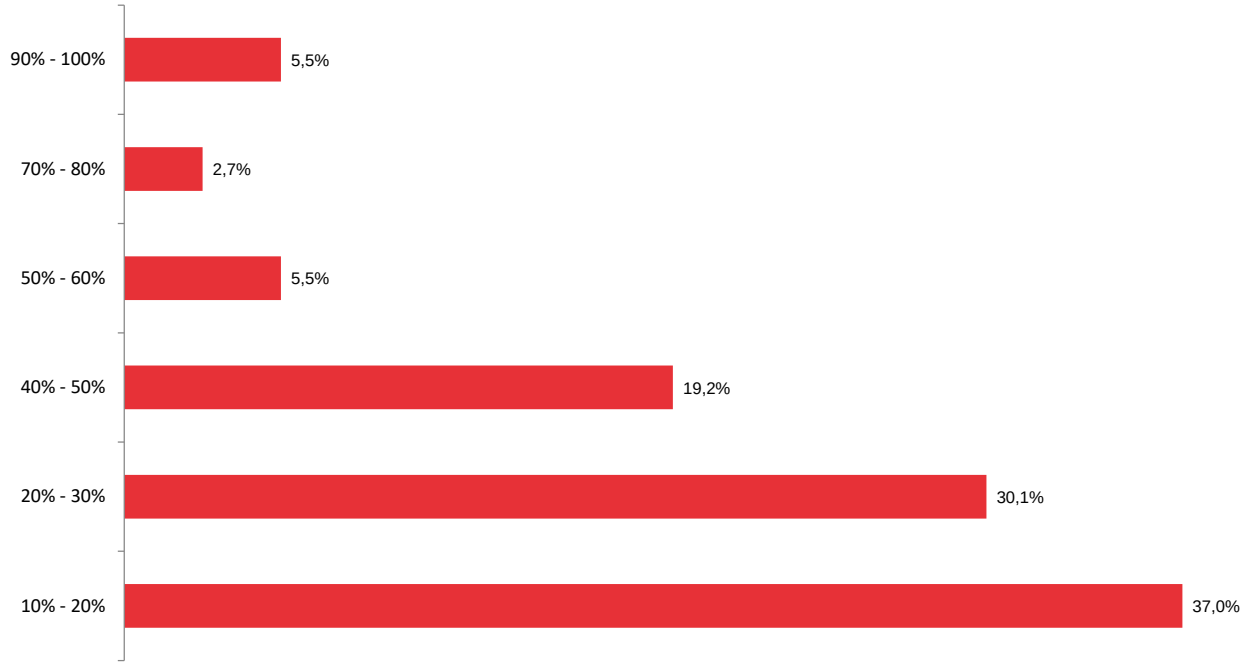


Figura 48. Porcentaje de contrataciones de talento procedente de FP

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 de este tipo de perfiles 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.

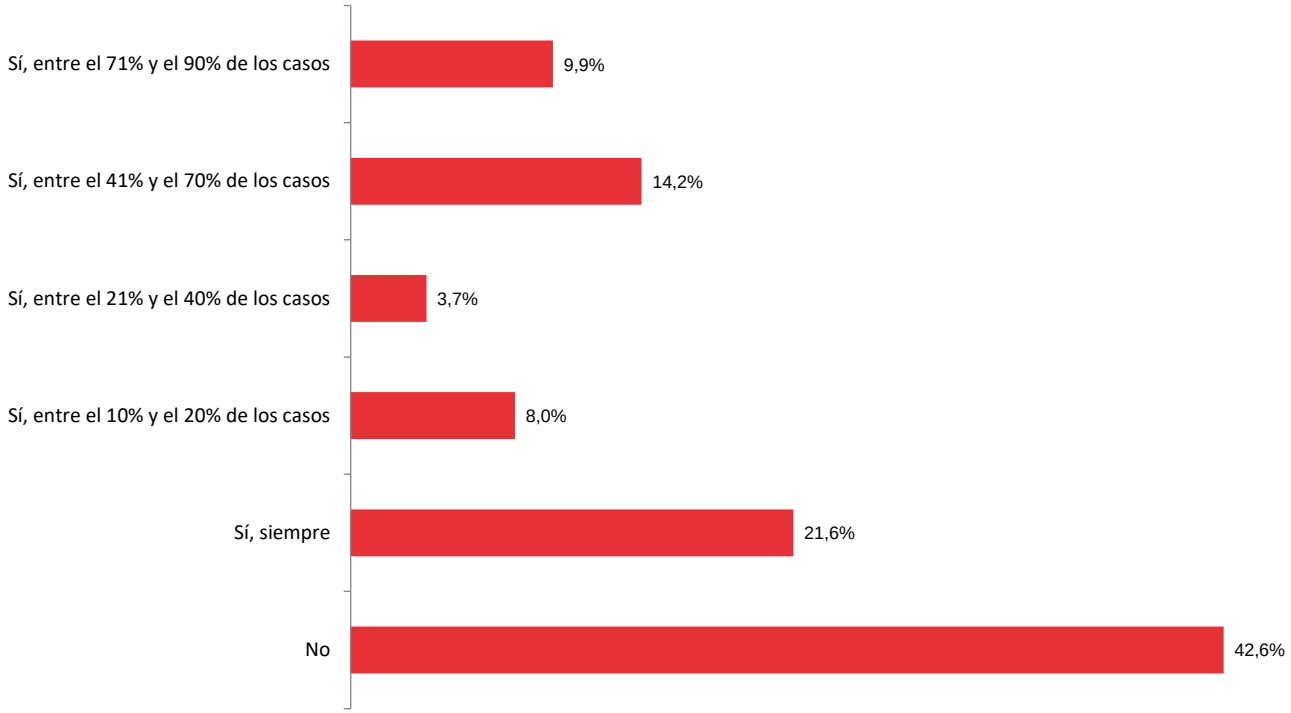


Figura 49. Importancia del título universitario en posiciones de entry level en ciberseguridad

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 consultadas, 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.

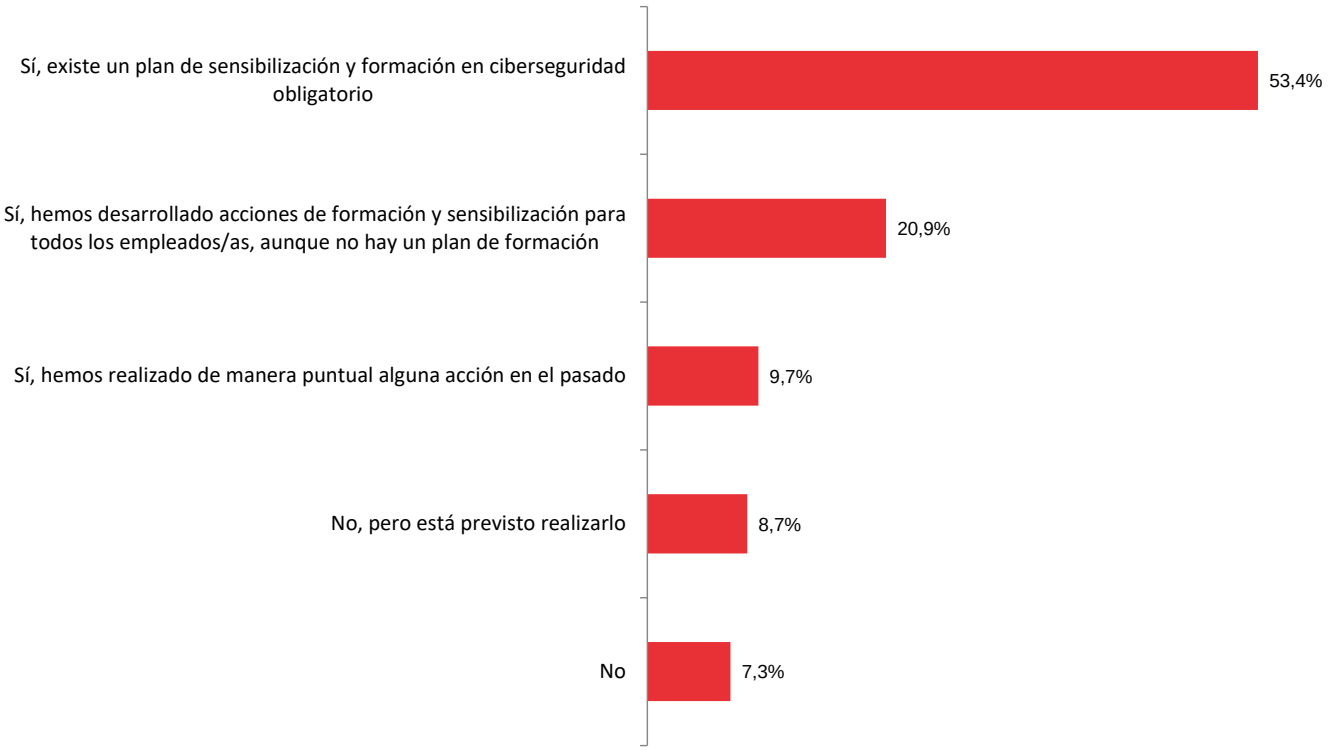


Figura 50. Ejecución de programas de sensibilización y formación en ciberseguridad en la empresa

De hecho, el 54% de las empresas consultadas reconocen que tienen en la actualidad abierta alguna posición, y de ese porcentaje, el 31% de las empresas lo tiene en el área de la ciberseguridad, donde existe una amplia heterogeneidad de perfiles requeridos, ya que influyen, tanto la industria como el nivel de madurez tecnológica de la organización.

A la hora de contratar, la mayoría de la muestra consultada (68%) reconoce que da prioridad a los candidatos provenientes de su sector, en gran medida por la necesidad de encontrar perfiles que combinen, tanto conocimiento de ciberseguridad como de la industria donde opera la organización.

No obstante, ante un proceso de contratación de trabajadores de otro sector, se da preferencia a las industrias de telecomunicaciones, medios de comunicación y tecnología (33,3%), banca y seguros (20,4%) e industria, construcción y energía (14,8%), ya que el nivel de madurez de la ciberseguridad en dichos sectores está por encima del resto y las capacidades y experiencia en la industria son activos valiosos que pueden ser complementados con programas de autoformación interna en la empresa para dotarlos de conocimientos y competencias en ciberseguridad.

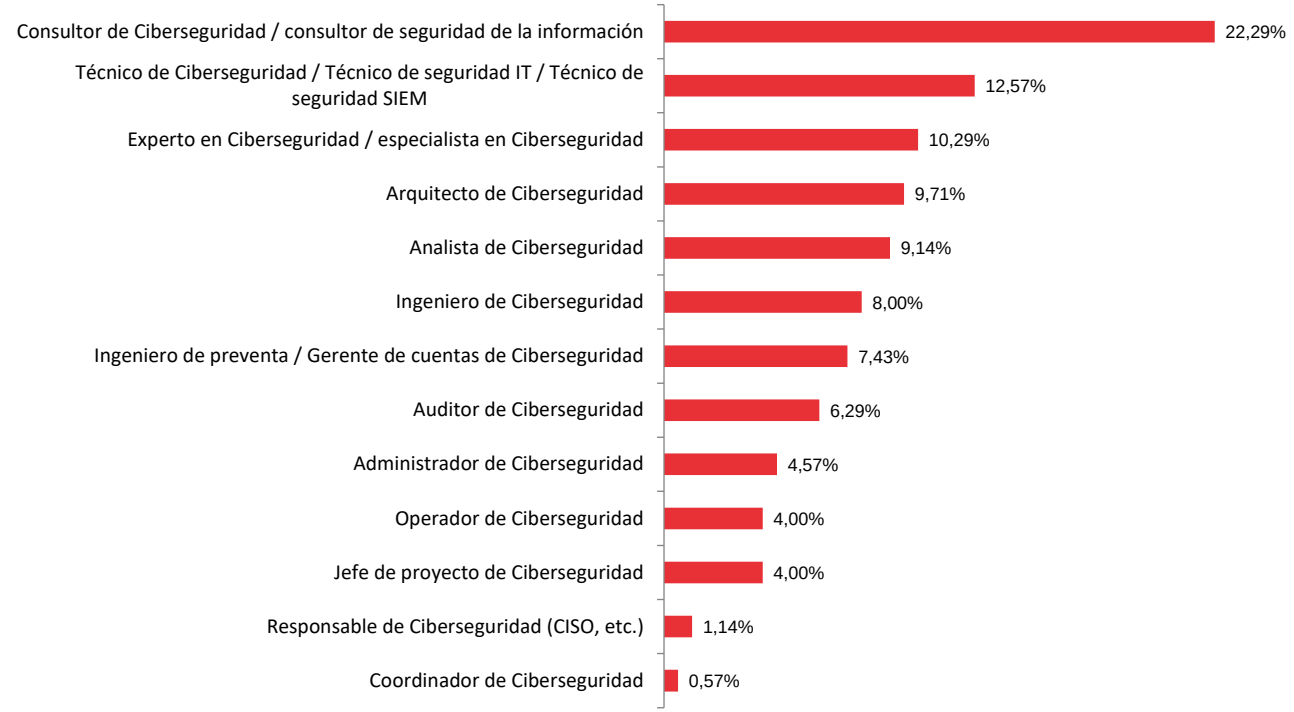


Figura 51. Tipología de perfiles de ciberseguridad que demanda la empresa española.

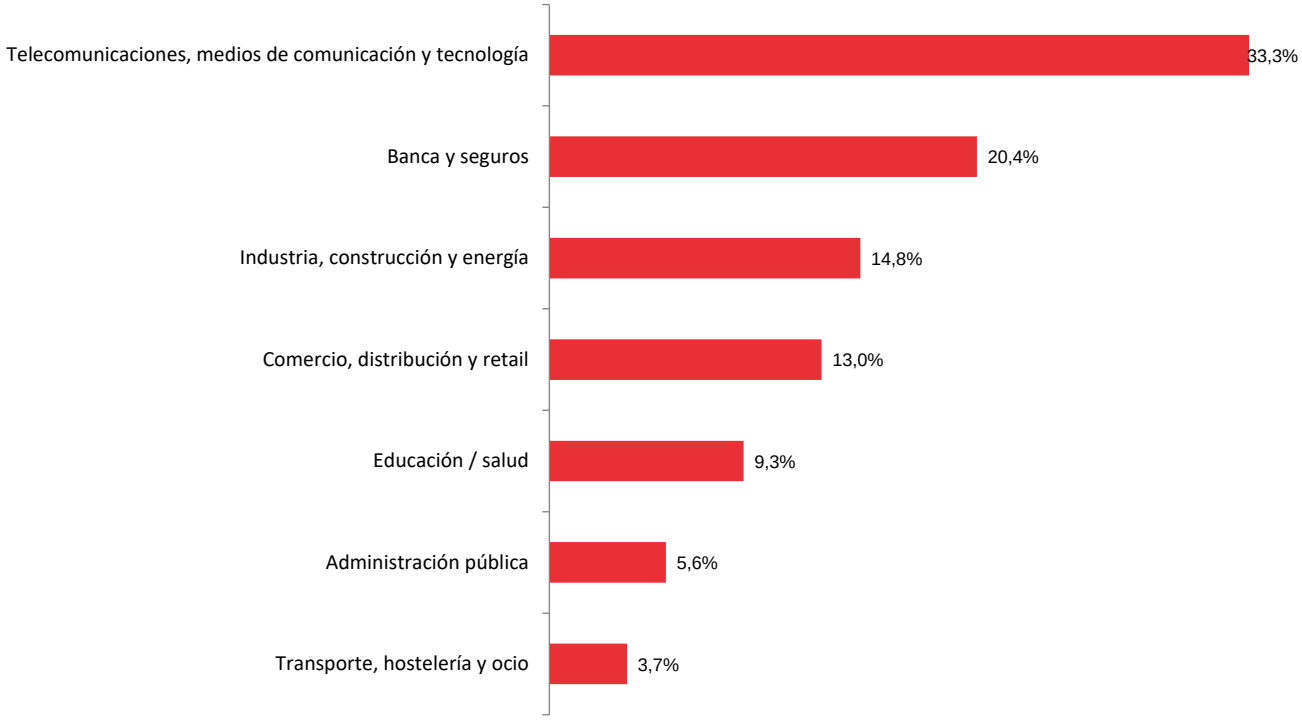


Figura 52. Principales industrias de las que se contrata talento de ciberseguridad

4.2.2.4_ 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 organizaciones reconocen como elementos más atractivos de este tipo de empresas (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.

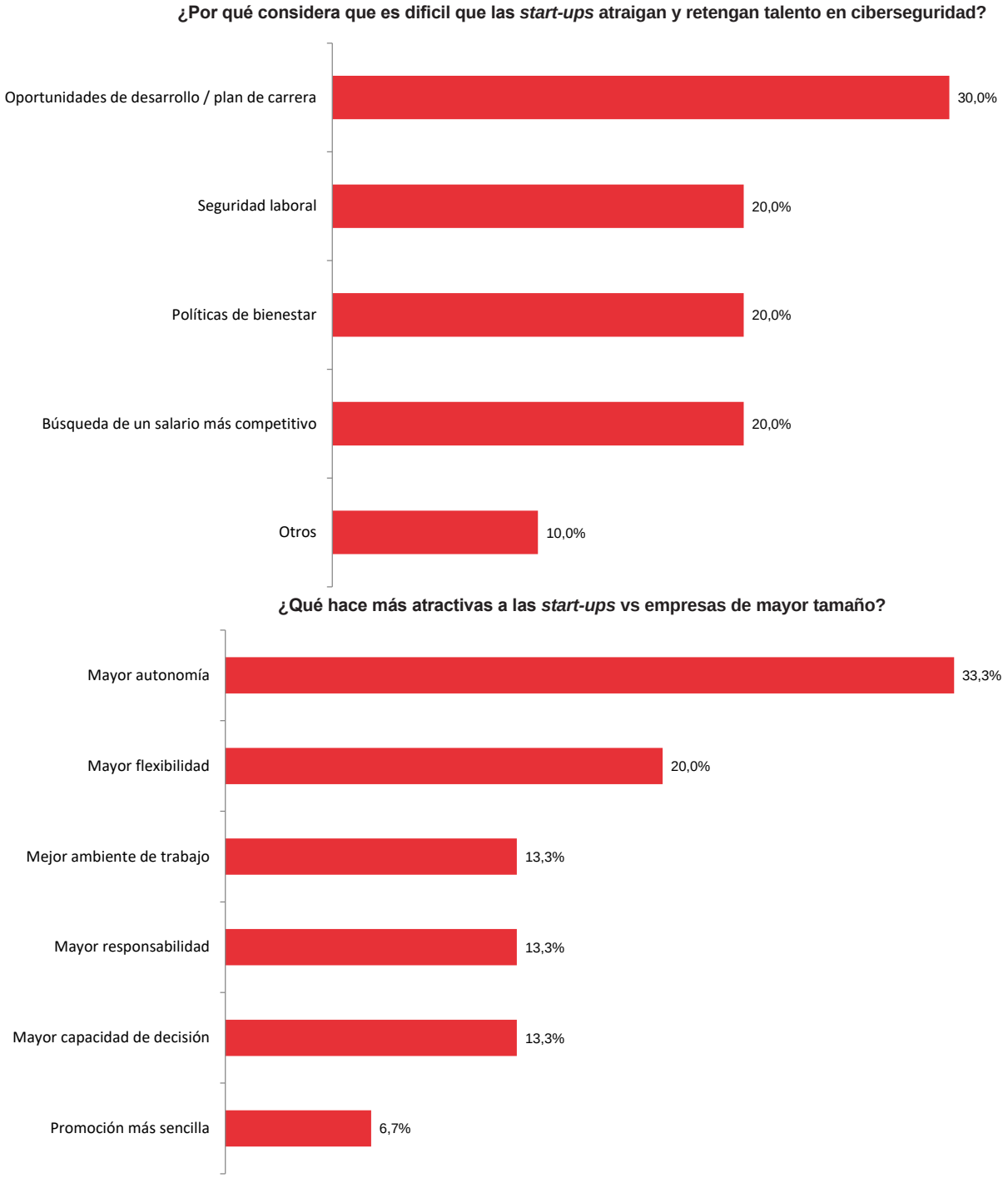


Figura 53. Análisis de los factores de atracción y retención de talento en start-ups

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 *start-up* 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.

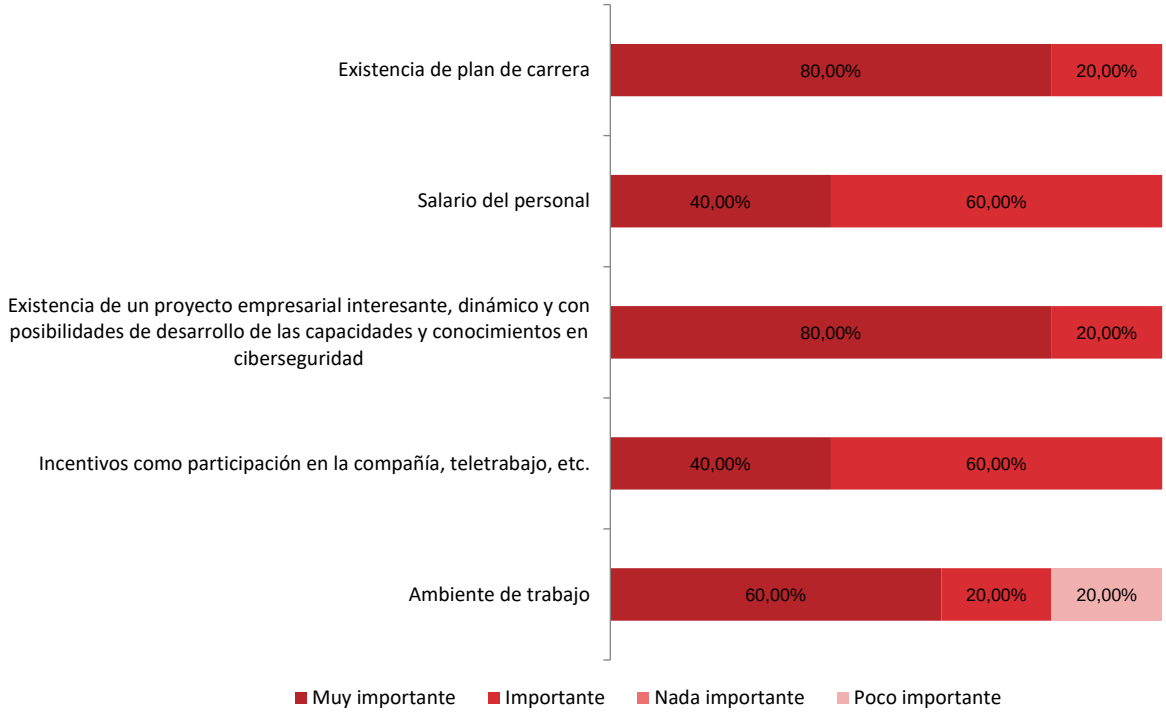


Figura 54. Importancia de los factores con relación a la retención de talento en un start-up

4.2.2.5_ 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 55. 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.

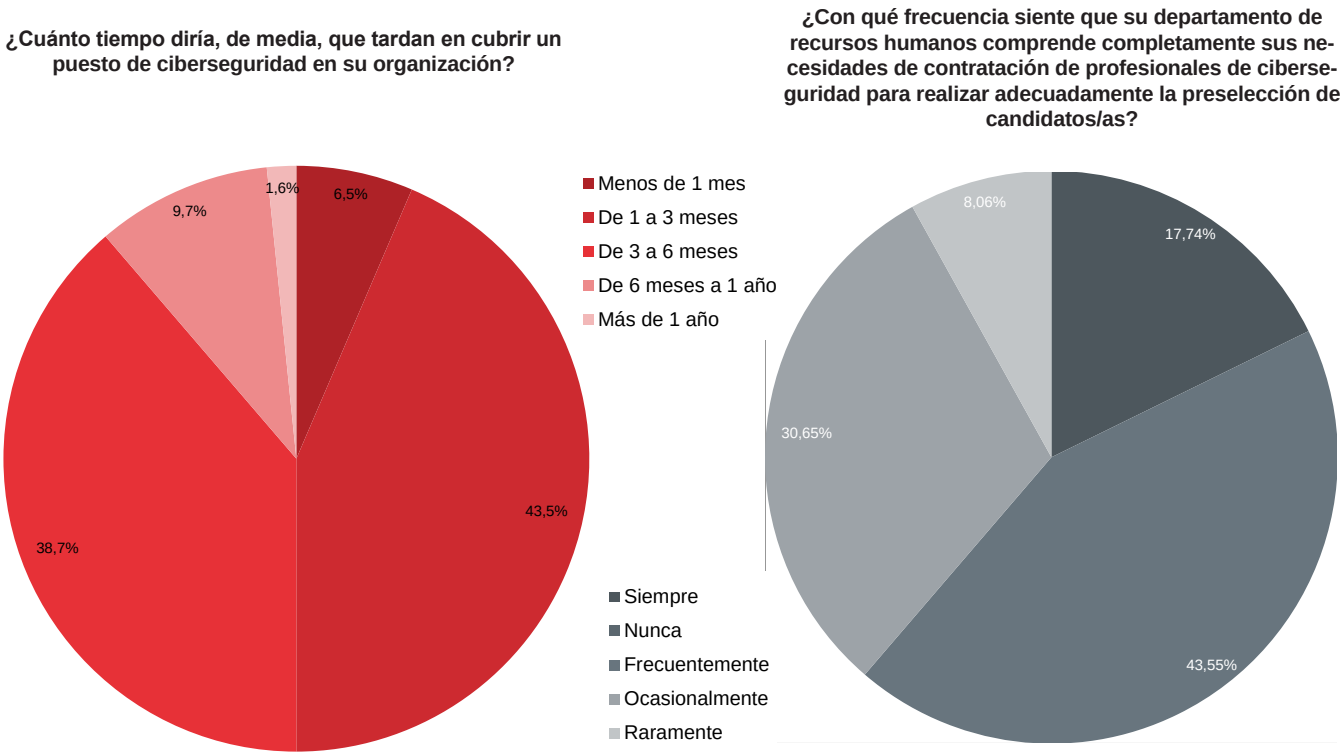


Figura 56. Tiempo medio para cubrir una posición de ciberseguridad en la empresa española

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, 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.

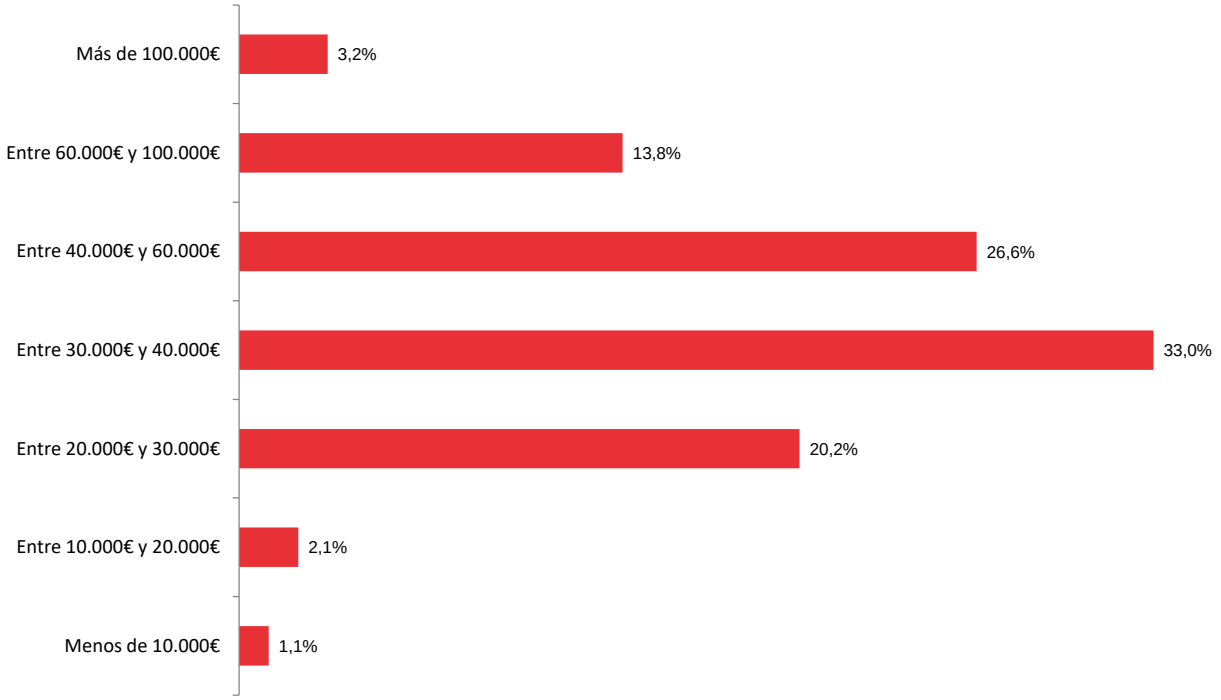


Figura 57. Salario actual para las posiciones de ciberseguridad en España

Por otra parte, unido a la propia dificultad en sí de atraer talento en ciberseguridad, el proceso de transformación digital de las organizaciones y el impacto que la pandemia de COVID-19 ha redefinido la estrategia de tecnología de las empresas, haciendo que la industria esté demandando perfiles para los que existe una alta demanda y muy poca oferta, como es el caso de los *expertos en ciberseguridad cloud y threat Intelligence,* las empresas reconocen que tienen una complejidad superior a la hora de atraer este tipo de perfiles.

4.2.3_ Conclusiones

A continuación, se presentan, de manera agregada, las principales conclusiones obtenidas tras analizar la demanda de talento de ciberseguridad en España y estructuradas en áreas de impacto:

Existe una desalineación entre la oferta disponible y las necesidades de las empresas. Más allá de si existe suficiente formación o no, en opinión de las empresas, la formación existente es insuficiente (especialmente en formación de grado) y no está alineada con las necesidades y tempo de la empresa privada, y requiriendo mayor presencia de la empresa en el currículo e itinerario formativo.

No hay suficiente práctica de la ciberseguridad en los diferentes programas formativos. Una de las cualidades que más valoran las empresas de un candidato es la experiencia práctica en ciberseguridad (bien adquirida en la misma industria o en programas formativos, pero se requiere de demostración real de que se tienen las capacidades y conocimientos que se demandan para el desarrollo de la profesión). Sin embargo, el currículo existente en la mayoría de los programas de grado y posgrado adolece de parte práctica (incluidas las prácticas en empresas que detallen las tareas realizadas).

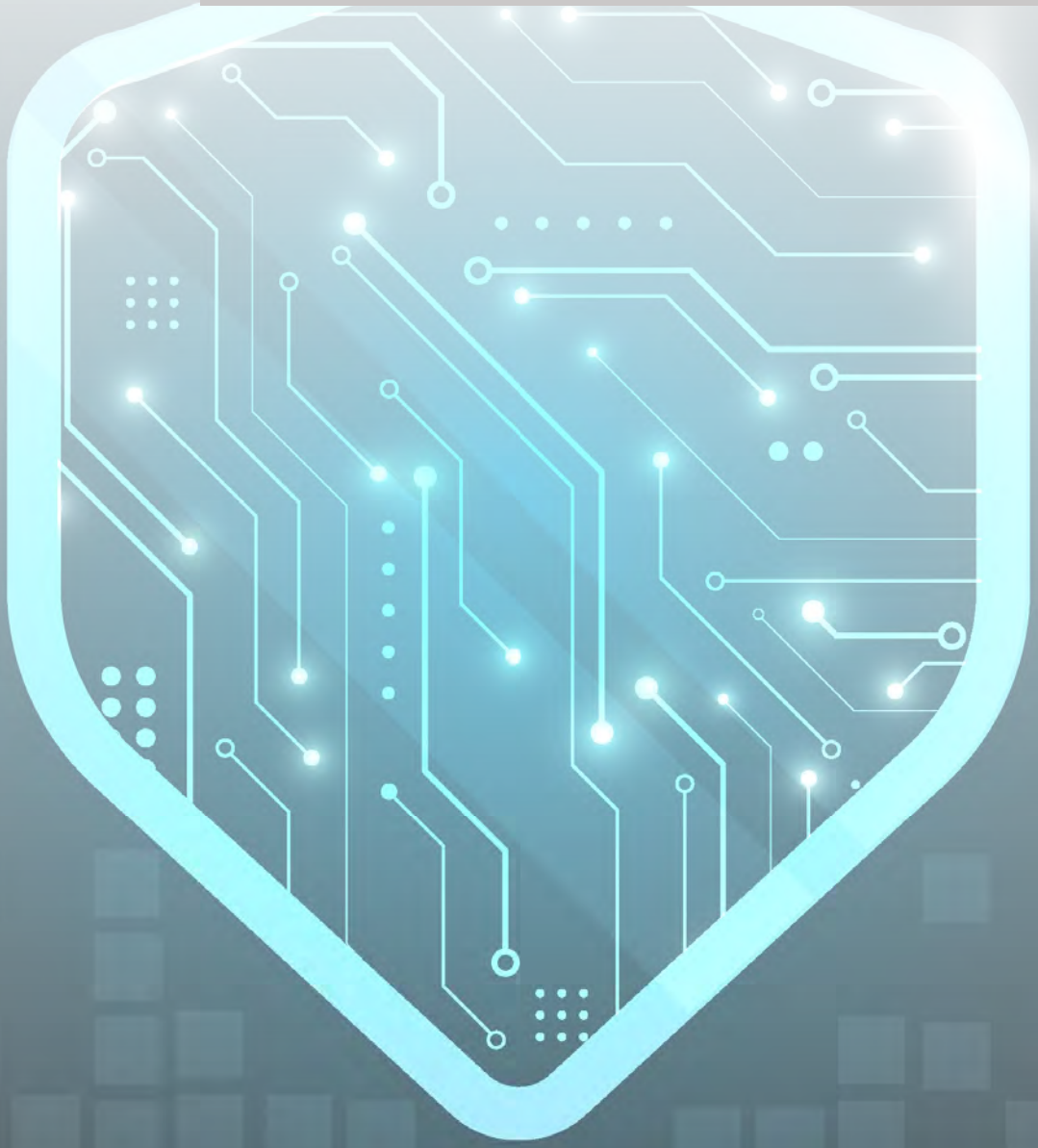
Este hecho, en cierta manera, hace que las empresas consideren las certificaciones como muy valiosas cuando están cualificando un candidato, especialmente si dichas certificaciones corresponden a fabricantes, ya que son una vía de demostrar los conocimientos y la experiencia que se requiere para acometer posteriormente el trabajo y maximizar el ROI en la inversión de contratación de nuevo talento.

No se utiliza, en general, ninguna taxonomía para la provisión de puestos de trabajo dentro de la industria de la ciberseguridad. Si bien la empresa considera que es esencial disponer de una descripción de las competencias y capacidades que se requieren para los diferentes perfiles. La realidad muestra que, en raras ocasiones, se realiza una correcta identificación de las necesidades a la hora de acometer un proceso de contratación, lo que suele conducir a procesos de selección confusos donde el resultado no obedece a las expectativas y necesidades buscadas. Por lo tanto, se requiere posteriormente un proceso de *on boarding* o formación inicial que permita al trabajador acometer las tareas para las que 'en principio' debería estar capacitado para desempeñar.

La alta rotación en ciberseguridad tiene muchos orígenes y no solo es el salario la variable que condiciona la fuga de talento. La escasez de profesionales en el ámbito de la ciberseguridad unido al impacto de COVID-19 que ha permitido a los trabajadores poder desarrollar su actividad profesional de manera transparente desde sus domicilios (más allá de que el propio sector ya tuviera implantadas políticas de trabajo flexibles). Una política de salarios más competitivos, existencia de programas de carrera o más responsabilidad y autonomía son variables que impactan de manera especial en la retención del talento de ciberseguridad. Asi mismo, determinadas posiciones pueden ser desarrolladas con formación profesional, lo que ayudaría a ajustar mejor el mercado de trabajo y evitar la rotación debido a la sobrecualificación en determinadas posiciones.

Establecer un itinerario claro y definido que ayude a los futuros profesionales a conocer las diferentes profesiones y salidas dentro de la industria de la ciberseguridad es clave para poder estructurar el empleo y facilitar la inclusión de otros colectivos (incluidos aquellos con necesidades especiales). El desconocimiento sobre las diferentes profesiones y salidas profesionales que se pueden desarrollar en ciberseguridad es uno de los principales motivos de la demanda de profesionales. Un itinerario claro, que comunique de forma sencilla las necesidades de la profesión, así como las diferentes opciones de desarrollo profesional en función del tipo de perfil que disponga el candidato sería una opción que facilitaría a las organizaciones a identificar el talento requerido.

La autoformación es valorada por las empresas, pero enmarcada en el contexto de un profesional formado y con un título. Las entrevistas desarrolladas encuadran la formación autodidacta como un elemento de valor en un profesional que ya conoce los fundamentos y que se está formando para ampliar conocimientos (pero ya ha adquirido una base). De hecho, rara vez se contratan profesionales autodidactas a no ser que se requieran tareas muy específicas, pero no es la tendencia. No obstante, la empresa está buscando mecanismos para poder certificar los conocimientos autodidactas que el profesional va adquiriendo, de forma que sea posible consolidar y demostrar las habilidades adquiridas ante la empresa o un nuevo reto profesional. El mecanismo actual de certificación de capacidades no satisface las necesidades actuales de empresas y trabajadores.



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 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 ', 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 ciberseguridad, 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

Fuerza laboral de 101.963 puestos de trabajo y brecha de 16.552.

EE.UU

Fuerza laboral de 879.157 puestos de trabajo y brecha de 359.236.

Reino Unido

Fuerza laboral de 365.853 puestos de trabajo y brecha de 27.408.

Francia

Fuerza laboral de 118.301 puestos de trabajo y brecha de 27.562.

Adicionalmente, como una referencia se identifica que para el caso de España el tamaño de la fuerza laboral estimado es de 149.774 y la brecha de 26.024, sin embargo, estos valores varían en función de la fuente y metodología implantada para su estimación.

Esta escasez además distorsiona las escalas salariales del mercado, donde se ha encontrado, según un informe publicado por McAfee en 2020, 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 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.

A continuación, se enumeran algunas iniciativas destacables por su énfasis en las estrategias encaminadas a abordar la problemática de la escasez de talento en ciberseguridad.

National Initiative for Cybersecurity Careers and Studies (NICCS), Framework NICE, EE.UU[22]: la herramienta más robusta de la que se pueden beneficiar los profesionales y la industria en general es probablemente el Framework NICE. Teniendo presente las herramientas dinámicas que permiten navegar por el contenido, de manera que los profesionales puedan enfocarse en los conocimientos más idóneos para los diferentes planes de carrera. El *framework* denota una taxonomía común para describir roles de trabajo y establecer expectativas en los niveles de competencia, y además, está conduciendo a datos realmente interesantes que se derivan del análisis de la propia fuerza laboral de las organizaciones.

Government Security Profession (GSP), UK[23]: GSP es un programa gubernamental que reúne a los profesionales de seguridad que trabajan en el gobierno para ayudarlos a adquirir habilidades y conocimientos. En UK se tiene la visión de crear una profesión de seguridad gubernamental dinámica líder en el mundo que involucre, apoye e inspire a los profesionales existentes y continúe construyendo una comunidad alrededor de la ciberseguridad diversa, motivada y próspera.

Cybersecurity Talent Alliance, Canadá[24]: uno de los objetivos del plan de acción en ciberseguridad 2019-2024 es lograr consolidar un ecosistema de ciberseguridad con la capacidad de adaptación e innovación, a través de la inversión en actuaciones específicas como el *Cybersecurity Talent Alliance* que están destinadas a reforzar el ecosistema de ciberseguridad en Canadá y conjuntamente abordar el gap de talento en ciberseguridad.

Education and Training Catalog, NICCS, EE.UU[25]: plataforma de formación con un catálogo con más de 5,000 cursos y cuenta con un mapa interactivo y filtros para una mejor experiencia de búsqueda. El objetivo es que el profesional pueda desarrollar habilidades, aumentar el nivel de experiencia, obtener certificaciones o incluso hacer la transición a una nueva carrera.

22 https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework

23 https://www.gov.uk/government/organisations/government-security-profession/about

24 https://technationcanada.ca/en/future-workforce-development/cybersecurity/cybersecurity-talent-alliance/

25 https://niccs.cisa.gov/training/search

Finalmente, en UK hay un panorama divergente con respecto al resto de países en esta temática. A pesar de que el gap de la fuerza laboral en Reino Unido asciende a 27.408 puestos de trabajo, según (ISC)², el gobierno británico plantea que dada la escasez de definiciones en la industria y la velocidad de la evolución en ciberseguridad, es importante definir con precisión el tamaño del gap es un gran desafío, más aún si se consideran las variables multidisciplinarias en las especialidades (roles) de la ciberseguridad por sector. En consecuencia, han tratado 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.

En esencia, uno de los objetivos de las diferentes estrategias de ciberseguridad analizadas se centra en 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 del talento en ciberseguridad.

5.1_ Impacto de las iniciativas y actuaciones.

Se han identificado diferentes grupos en donde las actuaciones tienen impacto:

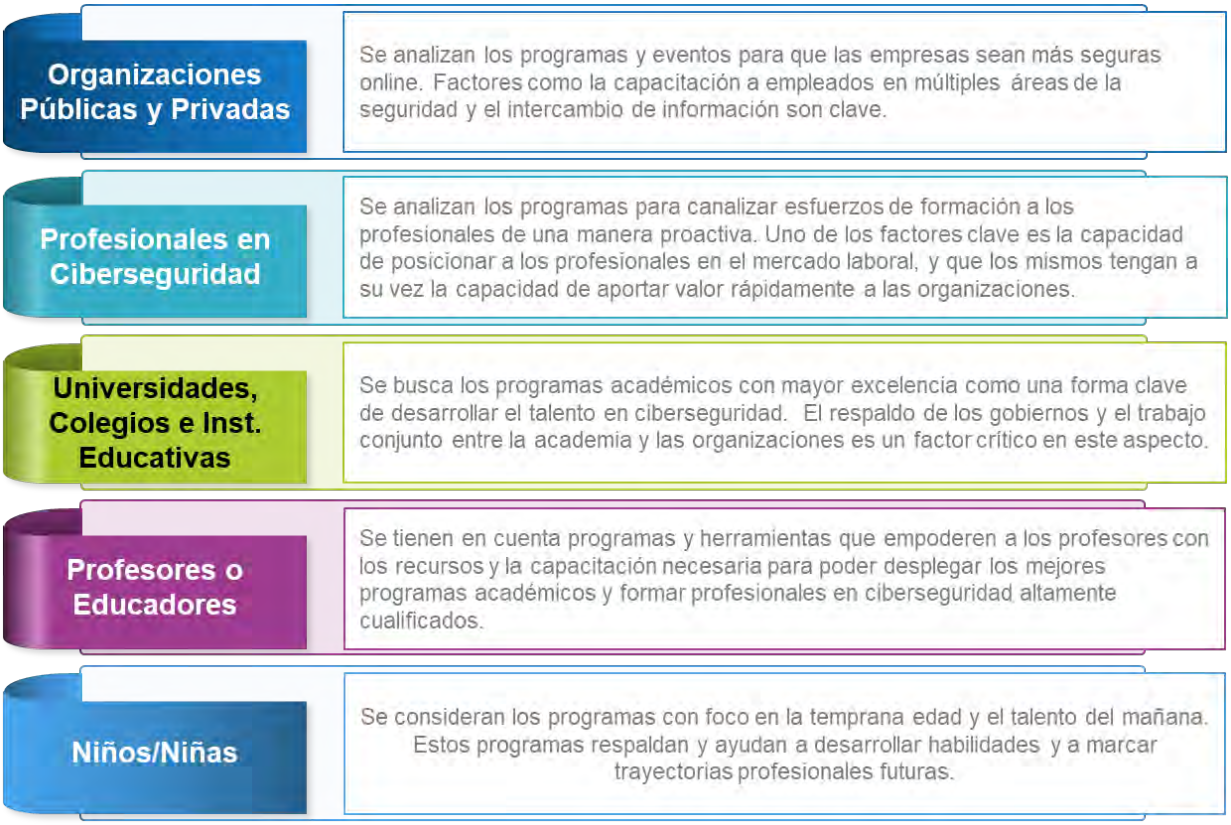


Figura 59. Grupos de impacto de las actuaciones analizadas. Fuente: propia

Organizaciones públicas y privadas.

A continuación, se enumeran algunas iniciativas destacables por su énfasis en las estrategias encaminadas a fortalecer las capacidades de las empresas tanto públicas como privadas.

Cyber Storm: Securing Cyber Space, Cybersecurity Infrastructure Security Agency (CISA) y Department of Homeland Security (DHS) EE.UU[26]: ejercicios cibernéticos que reúnen al sector público y privado para simular la respuesta a una crisis cibernética que afecta la infraestructura crítica de la nación. Esta iniciativa se realiza por ediciones que han iniciado en el año 2006, y la próxima se realizará en la primavera de 2022. Fundamentalmente lo que busca es examinar la capacidad de las organizaciones para poder responder y protegerse de los ciberataques. Adicionalmente, esto servirá para una mejor toma de decisiones estratégicas y mayor coordinación interinstitucional.

Open Playbook, Tech Talent Charter (TTC), U.K[27]: catálogo de código abierto de recursos y casos de estudio para ayudar a las empresas a aumentar la inclusión y la diversidad en sus equipos tecnológicos. Se fomenta la cultura diversa e inclusiva, con la ayuda de iniciativas basadas en la práctica y en la evidencia, las empresas han podido impulsar notablemente la inclusión y diversidad en roles de tecnología.

Recursos del UK Cyber Security Council, U.K[28]: pensado directamente como parte de la Estrategia Nacional de Ciberseguridad (NCSS), y en conjunto con la Asociación de Auditoría y Control de Sistemas de Información (ISACA), esta iniciativa busca defender la profesión de la ciberseguridad en todo UK, proporcionar una amplia representación para la industria, acelerar la conciencia y promover la excelencia en la profesión. Lo hará mediante la entrega de liderazgo intelectual, herramientas profesionales y recursos educativos al sector y a aquellos que buscan ingresar al sector.

Cyber Security Assessment and Certification for SMEs, Canadá[29]: este programa está diseñado para ser un punto de partida para que las pymes mejoren su postura de ciberseguridad. El propósito último del Programa de Certificación Cibernética es elevar la postura de seguridad cibernética entre las pymes canadienses, aumentar la confianza del consumidor en la economía digital, promover la estandarización internacional y posicionar mejor a las pymes para competir globalmente. Esta iniciativa público-privada está dirigida por Innovación, Ciencia y Desarrollo Económico de Canadá (ISED), en colaboración con el Establecimiento de Seguridad de las Comunicaciones (CSE), el Consejo de Normas de Canadá (SCC) y organismos de certificación independientes acreditados por el sector privado.

Profesionales de ciberseguridad.

A continuación, se enumeran algunas iniciativas destacables por su énfasis en las estrategias encaminadas a fortalecer las capacidades de los profesionales en ciberseguridad.

Critical National Information Infraestructure (CNII), Malasia[30]: Malasia tiene una mentalidad enfocada a la concienciación y educación de los actores de su ecosistema digital como parte de un proceso esencial de mitigar los riegos a los que se exponen los ciudadanos y alcanzar cierto nivel de conocimiento para prevenir incidentes. Malasia es consciente de que enfrenta una escasez de profesionales y esto deja a las organizaciones vulnerables y expuestas a peligros incalculables. Vinculado a este hecho, una de las actuaciones en Malasia que constantemente se refleja en la estrategia de ciberseguridad nacional apunta a lograr un mayor número de graduados universitarios en campos

26 https://www.cisa.gov/cyber-storm-securing-cyber-space
27 https://www.techtalentcharter.co.uk/open-playbook
28 https://www.isaca.org/why-isaca/the-uk-cyber-security-council
29 https://cyber.gc.ca/en/guidance/cyber-security-small-business
30 https://mdec.my/

relacionados con la ciberseguridad y posicionarlos en el mercado laboral.

Malasia ha estado desarrollando e implementando capacidades con foco en los profesionales a través de la colaboración de varios ministerios, agencias y organizaciones de la Critical National Information Infraestructura (CNII). Uno de los vértices de este esfuerzo está en aumentar el número de profesionales calificados locales a través de programas de capacitación y certificación para satisfacer la demanda, tanto en el sector público como en el privado. Ahora bien, el país reconoce que faltan certificaciones profesionales reconocidas y de buena calidad para el desarrollo de habilidades especializadas en ciberseguridad.

El despliegue de esta iniciativa lo hacen con Malaysia Digital Economy Corporation (MDEC), que es la piedra angular de las iniciativas para desarrollar capacidades digitales y el foco lo ponen en empoderar a los malasios con habilidades digitales, habilitar empresas impulsadas digitalmente y potenciar la inversión del sector digital.

MyDigitalWorkforce, Malasia[31]: plataforma que busca combinar las oportunidades profesionales en el mundo digital con los talentos potenciales. Ya sea un recién graduado, un talento experto o alguien que se encuentre transitando el camino hacia la vida laboral, esta plataforma ofrece una amplia gama de oportunidades de trabajo que se han consolidado con otras plataformas de reclutamiento asociadas. El despliegue de esta iniciativa igualmente está gestionado a través de Malaysia Digital Economy Corporation (MDEC).

SecNumedu, Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI), Francia[32]: además de ser la apuesta de los franceses para fomentar una respuesta coordinada, ambiciosa y proactiva a los problemas de ciberseguridad, es la iniciativa para canalizar esfuerzos de formación a sus profesionales. La agencia a través de iniciativas, como SecNumedu ofrece: cursos de ingeniería cuyo diploma está reconocido por la comisión francesa des titres d'ingénieurs, cursos universitarios que otorgan una licencia o maestría, y el mastère spécialisé, reconocido por la Conference des grandes écoles (un máster + un año de formación). Además, SecNumedu ofrece una garantía a estudiantes y empleadores de que la formación en el campo de la ciberseguridad cumple con unos criterios definidos por ANSSI, en colaboración con actores y profesionales en la industria (instituciones de educación superior, empleadores, etc.). Estos son algunos ejemplos que denotan el compromiso con el acceso y la calidad de la formación en ciberseguridad.

Parque de Alta Tecnología Be'er-Sheva, Israel[33]: inaugurado en septiembre de 2013, es el resultado de una iniciativa conjunta del municipio de Be'er-Sheva y la Universidad Ben Gurion del Negev, con más de 8.000 es-

31 https://mdec.my/digital-economy-initiatives/for-the-people/mydigitalworkforce-jobs

32 https://www.ssi.gouv.fr/en/cybersecurity-in-france/formations/secnumedu-labeling-of-higher-education-courses-in-cybersecurity/

33 https://www.beer-sheva.muni.il/Eng/Business/Pages/AdvancedTechnologiesPark.aspx

tudiantes de ingeniería. Este parque es considerado una fuente primordial de experiencia y talento en ciberseguridad porque la planificación estratégica del área ha permitido un modelo de ecosistema único que conecta físicamente a las empresas que residen en el Parque con la Universidad, la central de TI de las Israel Defense Forces (IDF), lo que lleva a una visible colaboración entre varios sectores y organismos.

Actualmente hay tres edificios que cubren alrededor de 50,000 metros cuadrados, y están ocupados por algunas de las principales empresas internacionales del sector tecnológico (unas 70 empresas y *star-tups* total), incluidas DELL, IBM, Oracle, WIX, Mellanox, Deutsche Telecom, Incubit, Allscripts, AudioCodes entre otras, que han instalado allí sus centros de I + D globales. Estas empresas emplean actualmente a más de 2.500 ingenieros y profesionales de TI, y se espera que para la siguiente fase, el parque tenga una superficie de 200.000 metros, empleando a más de 10.000 personas.

El ecosistema único y la sinergia entre la academia, la industria, el ejército, el gobierno y una autoridad municipal que apoya los esfuerzos han ayudado a impulsar iniciativas que están ayudando a fortalecer la industria de ciberseguridad.

Universidades, colegios e instituciones educativas.

La educación formal proporciona los componentes básicos que equiparán a los jóvenes para seguir carreras en ciberseguridad. En este sentido, el acceso a una enseñanza en informática de alta calidad sentará las bases que se pueden desarrollar y aplicar de manera práctica en la educación superior, lo que permitirá finalmente asumir roles más técnicos que tienen una alta demanda. Sin embargo, es imprescindible reconocer que la educación formal no es el único vehículo para capturar y aprovechar el talento de los jóvenes, las actividades extracurriculares son una forma clave de identificar talentos y alimentar y desarrollar intereses a una edad temprana, lo que ayuda a desarrollar habilidades y a marcar trayectorias profesionales futuras.

A continuación, se enumeran algunas iniciativas destacables por su énfasis en las estrategias encaminadas a fortalecer las capacidades de las universidades, colegios e instituciones educativas.

Academic Centres of Excellence in Cyber Security Research, National Cyber Security Centre (NCSC), U.K[34]**:** la excelencia académica en UK es una prioridad alta, y en conjunto con diversos centros académicos de alta calidad despliegan más de 20 másteres, 3 másteres integrados y 3 grados profesionales en ciberseguridad, de manera que abordan de manera holística requisitos de conocimiento, habilidades y capacidades para la investigación y educación con un énfasis único en calidad.
UK reconoce que para capturar con éxito el talento futuro, deben asegurarse de que los futuros profesionales estén informados sobre los diferentes tipos de roles y las trayectorias que deben seguir para llegar allí, desde abordar determinadas materias en la escuela y en la educación superior, hasta ir adquiriendo experiencia relevante fuera del aula. Además, el Reino Unido ha puesto en marcha esquemas para crear hubs de escuelas en ciberseguridad con las administraciones descentralizadas como Gales o el Norte de Irlanda. Esto provee de un enfoque estructurado para la excelencia desde las diferentes escuelas, además de promover la colaboración entre las administraciones en busca de oportunidades.

CyberCorps: Scholarship for Service, National Science Foundation (NSF), EE.UU[35]**:** es una de las iniciativas educativas más distintivas en la cual se ofrecen becas para la educación de pregrado y posgrado en ciberseguridad, financiadas a través de subvenciones otorgadas por la (NSF), y lo interesante de esta actuación es que la magnitud del ecosistema americano permite que los estudiantes al finalizar los estudios se puedan posicionar en instituciones, como el DHS, CISA, NSA, DoD, FBI o CIA, lo que aumenta considerablemente sus capacidades en ciberseguridad.
A pesar de los elevados costes de la educación superior en EE.UU., en comparación con el mercado europeo, la calidad y amplitud es indiscutible. Los Estados Unidos reflejan por ejemplo, una red de instituciones educativas en 48 de sus 50 estados, reconocida por el Departamento de Seguridad Nacional (DHS) y la Agencia Nacional de Seguridad (NSA) en temas puntuales de ciberseguridad. Esta robustez refuerza las actuaciones para generar mejores planes de estudios y becas para los estudiantes.

Cyberspace Administration of China (CAC), China[36]**:** China demuestra a través del principal regulador de Internet, la Administración del Ciberespacio de China, y el Ministerio de Educación de China que el país planea construir de cuatro a seis escuelas de ciberseguridad de clase mundial en diez años. Esto sería entre 2017 y 2027. Además, las universidades que se ofrezcan a hacer parte de esta iniciativa recibirían todo el apoyo del gobierno chino, en cuanto a recursos financieros y otros recursos.

34 https://www.ncsc.gov.uk/information/academic-centres-excellence-cyber-security-research
35 https://www.sfs.opm.gov/
36 http://www.cac.gov.cn/

National Cybersecurity Center in Wuhan (NCC), China[37]**:** este ambicioso proyecto consiste en un campus de 15 millas cuadradas en la ciudad de Wuhan, que servirá como escuela, laboratorio de investigación, incubadora de proyectos y cultivador de innovación y talentos.
Contará con 7 centros de investigación, desarrollo del talento y emprendimiento, 2 laboratorios centrados en el gobierno y 1 Escuela Nacional de Ciberseguridad. Así, espera llegar a 1.300 estudiantes graduados a 2022, 2.500 graduados por año a partir de 2023, 6.000 profesionales recibiendo cursos y certificaciones por mes y en el largo plazo medio millón de formados en ciberseguridad.
Dentro de los beneficios que el centro aporta es que 3 componentes son un apoyo exclusivo a la innovación y otros dos a la parte del gobierno Chino. Además, los estudiantes y las *start-ups* pueden solicitar orientación empresarial y fondos de inversión en la incubadora del NCC, y finalmente, el centro realiza eventos que atraen talentos de todo el país.

Profesores o educadores.

En el contexto actual, la tecnología y la conectividad se encuentran presentes en casi todas las facetas de la vida, especialmente en los niños y jóvenes. Ante esto, la ciberseguridad no puede tratarse como un tema aislado de las iniciativas de enseñanza, más aún cuando la virtualidad se consolida cada vez más. Los profesores que comprenden esta realidad y abordan la ciberseguridad de manera integral, marcarán el camino para formar estudiantes más seguros y mejor preparados para el futuro.

Desde una perspectiva educativa, hay una escasez de acceso a profesores y currículos de ciberseguridad. En ese sentido, distintas agencias se esfuerzan por proporcionar a los educadores los recursos necesarios para capacitar a los estudiantes, y que estos se conviertan en miembros competentes de la fuerza laboral de ciberseguridad. A continuación, se enumeran algunas iniciativas destacables por su énfasis en las estrategias encaminadas a fortalecer las capacidades de los profesores o educadores.

Russia's Strategy in Cyberspace[38]: Rusia refleja que uno de las activos más valiosos del sistema educativo son los profesores, quienes se encargan de realizar las diversas actividades encaminadas a mejorar el nivel de competencias de las diferentes industrias. Por eso, tienen una notable trayectoria desde 1.985 emprendiendo planes de formación para este grupo. En este sentido, se han implementado varias medidas para apoyar a los docentes en servicio. Los institutos pedagógicos, las universidades y los institutos especiales de formación profesional para profesores realizan periódicamente cursos de actualización en los que se revisan los métodos innovadores de enseñanza de la informática. Las sociedades metodológicas de profesores de informática funcionan en varias ciudades y regiones. Además, en Rusia se han destacado por ampliar el contenido educativo y porque las escuelas tengan cierta autonomía para diseñar e implantar sus programas de estudio. Esto podría ser una señal de dinamismo en la generación de conocimiento, caso contrario es la rigidez burocrática.

37 https://cset.georgetown.edu/publication/chinas-national-cybersecurity-center
38 https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf

Cyberspace Administration of China (CAC)[39]: China tiene una apuesta decidida de consolidar escuelas de ciberseguridad de talla mundial. Pero su enfoque es lo más llamativo porque reconocen la importancia de vincular, tanto a profesores a trabajar en conjunto con empresas de la industria, así como también incentivan la contratación de personal especializado de las empresas para que sean profesores de tiempo parcial. Esta relación entre academia y empresa es la piedra angular para un cambio de estructura en la formación.

Los principales objetivos de estas iniciativas relacionadas con los docentes en China son:

- Coordinar que profesores especializados trabajen en empresas relacionadas con la industria de la ciberseguridad, unidades de investigación científica y departamentos gubernamentales, a fin de fortalecer la cooperación entre la escuela y la empresa.
- Contratar personal experimentado, incluidos expertos en gestión de ciberseguridad y talentos especializados, como profesores a tiempo parcial.

Evaluar los talentos de ciberseguridad con habilidades prácticas en lugar de calificaciones académicas o títulos.

Niños / niñas.

Es importante ser coherente con la realidad digital actual, donde los niños al tener acceso a las herramientas y dispositivos tecnológicos, están igualmente en riesgo. Ante esto, poner las semillas que se cosecharán en el futuro en materia de educación y formación es una de las medidas más contundentes para lograr cambios culturales de largo plazo que protejan a los menores.

Cyber Education Center (CEC), Israel[40]: a través de esta iniciativa se espera alcanzar un cambio social a través de la educación tecnológica, y en este sentido el país piensa cultivar la excelencia junto con el avance de la educación y capacitación cibernética y tecnológica para lograr un cambio social real, y demostrar a los niños que se pueden brindar igualdad de oportunidades en Israel.

La CEC se ha propuesto liderar el cambio hacia la igualdad de género y, con ese fin, creó la comunidad CyberGirlz. Esta comunidad ofrece a las niñas una amplia variedad de actividades en el campo de la tecnología, así como programas educativos diseñados especialmente para ellas. A través de este esfuerzo, el Cyber Education Center espera garantizar que las mujeres desempeñen un papel fundamental en el mundo tecnológico del mañana.

39 http://www.cac.gov.cn/

40 https://cyber.org.il/about-us-eng/

Otro de los programas distintivos en Israel en relación con el aprendizaje a temprana edad es el programa extracurricular Magshimim (lanzado en 2011), para estudiantes de secundaria sobresalientes de zonas desfavorecidas del país, enseñando programación, código, cifrado y cómo defender una red contra el *hacking*. Tal vez lo más llamativo de este programa es que integra temáticas que despiertan el interés de los jóvenes, como pueden ser personajes animados, y lo combina con ejercicios de simulación para el desarrollo de habilidades.

Magshimim, Israel[41]: este es un programa distintivo en Israel en relación con el aprendizaje a temprana edad, (lanzado en 2011), para estudiantes de secundaria sobresalientes de zonas desfavorecidas del país, enseñando programación, código, cifrado y cómo defender una red contra el *hacking*. Tal vez lo más llamativo de este programa es que integra temáticas que despiertan el interés de los jóvenes, como pueden ser personajes animados, y lo combina con ejercicios de simulación para el desarrollo de habilidades.

En el documento anexo a este análisis: *Benchmark internacional de gestión de talento en ciberseguridad*, se amplía la información sobre el impacto de las iniciativas en los diferentes países, reflejando numerosas actuaciones que han formado parte de la investigación.

5.2_ Inversión

Las pérdidas que sufren las organizaciones como consecuencia de ataques cibernéticos superan con creces de manera global los billones de euros. Esto ha hecho que las recientes estrategias de ciberseguridad tengan incrementos en los presupuestos, incluso duplicándose en el lapso de dos años, como es el caso de Israel.

Israel gasta entre el 6% y 8% de su PIB en defensa, y también encabeza el mundo en términos de gasto interno bruto en I+D en relación con el PIB, gastando más del 4.5% de su PIB (OCDE). Este énfasis en la investigación y el desarrollo, así como el papel estimulante de las unidades técnicas de las Israeli Defense Forces (IDF), proporcionan un entorno fértil para que las *start-ups* prosperen y haya un sector de alta tecnología.

Además de esto, el primer ministro ha afirmado que la ciberseguridad es un excelente negocio para la nación. Han desarrollado estrechas relaciones con países como Singapur, ayudándolos a establecer cerca de 300 *start-ups* de ciberseguridad, exportando soluciones de TI por valor de 6.500 millones de dólares.

Conjuntamente, de los 394 billones de dólares que registra el PIB de Israel para 2019, bajo la premisa inicial de gasto en defensa del 6% al

41 https://rashi.org.il/en/programs/magshimim/

8%, el presupuesto alcanzaría los 27.500 millones de dólares. Aunque la proporción para ciberseguridad no se conoce con precisión, pero solo para el Israel National Cyber Directorate (INCD) el presupuesto en 2019 se ha duplicado con respecto a 2017, alcanzando los 64 millones de dólares.

Mientras que el presupuesto francés para iniciativas de ciberseguridad ronda el billón de euros, en Reino Unido asciende a 1.900 millones de libras esterlinas. Más aún, la estrategia de ciberseguridad de UK señala que utilizaran la autoridad y la influencia del gobierno británico para invertir en programas que respondan a la escasez de habilidades en ciberseguridad, desde las escuelas y universidades, hasta toda la fuerza laboral. Incluso uno de los imperativos estratégicos de esta estrategia, en los cuales se basa su política de inversión es: 'UK necesita una industria de ciberseguridad dinámica y una base de habilidades de apoyo que pueda seguir el ritmo y adelantarse a la amenaza cambiante'. Así para lograr reducir su exposición a daños cibernéticos, UK considera imprescindible equilibrar los riesgos con suficiente inversión en las personas, tecnología y gobernanza.

El presupuesto de seguridad más discriminado o detallado, además de ser el de mayor cuantía, es sin duda, el de EE.UU., el cual está contenido dentro del presupuesto del Departamento de Seguridad Nacional (DHS). Allí lo que se ha identificado es que el presupuesto total del DHS para 2021 es de $49.8 billones de dólares, y los rubros que más se relacionan con la ciberseguridad son:

1.1 billones de dólares para defender y asegurar el ciberespacio, que incluye fondos para el programa Continuous Diagnostics and Mitigations (CDM) con una asignación de $281 millones, lo que proporcionará la base tecnológica para asegurar y defender la infraestructura de TI contra amenazas.

157.6 millones de dólares para comunicaciones de emergencia para entidades federales, estatales, locales, tribales y territoriales. Este programa permite mejorar los servicios de comunicaciones de seguridad pública a nivel nacional mediante la provisión de las herramientas, la capacitación y la información necesarias para comunicarse durante las operaciones de emergencia.

91,5 millones de dólares para fortalecer la infraestructura crítica y abordar el riesgo a largo plazo de las funciones críticas nacionales, incluidas las actividades relacionadas con la seguridad electoral, los pilotos 5G y el análisis de riesgos de la cadena de suministro.

El presupuesto total asignado para el organismo Cybersecurity and Infrastructure Security Agency es de 1.7 billones de dólares.

5.3_ Conclusiones

Este análisis benchmark ha permitido destacar las fortalezas de los diferentes países en varios aspectos de la gestión del talento en ciberseguridad y la manera en la que canalizan sus esfuerzos y recursos para obtener un impacto favorable en los grupos o actores más importantes para la sociedad de la información.

El desarrollo del benchmark ha sido una manera práctica de conocer los retos y prioridades a los que se enfrentan los diferentes gobiernos en materia de ciberseguridad, y tal vez uno de los insights de mayor valor que se han identificado es que los resultados del trabajo en ciberseguridad son, por lo general, el producto del esfuerzo conjunto de grupos diversos y el trabajo conjunto de múltiples organismos o instituciones.

Las estrategias inclusivas que logran la convergencia de intereses del sector público, privado, academia y la misma ciudadanía, están mucho más cerca de alcanzar sus objetivos que aquellas estrategias elitistas y fragmentadas.

Los cambios que los países esperan lograr deben estar impulsados por un nivel de conciencia hacia la ciberseguridad adecuado, y que además esté presente en todas las etapas de la vida. Ante esto, todos los países del estudio han demostrado su entendimiento y deseo de alcanzar niveles de conciencia adecuados para generar un cambio en la cultura de ciberseguridad, como la antesala del aprendizaje y del cambio del comportamiento humano.

Además, es bastante evidente que, sin una inversión considerable en recursos económicos de manera decidida, los resultados van a ser efímeros y opacos. Uno de los aprendizajes ha sido que la consolidación y desarrollo de capacidades o habilidades en materia de ciberseguridad, es directamente proporcional a la dimensión de la asignación de recursos.

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 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[42], 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[43], es la agencia dedicada a lograr un nivel común de ciberseguridad en toda Europa, y en el marco del desarrollo de sus iniciativas ha formado un grupo de trabajo (15 miembros representados 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 a continuación son el resultado de profundizar en el *European Cybersecurity Skills Framework* (ECSF)[44]. 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).

Por otra parte, reflejar un número determinado de perfiles de ciberseguridad no tiene como propósito mostrar el estado actual de los

42 https://www.sparta.eu/

43 https://www.enisa.europa.eu/

44 https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

conocimientos, capacidades y habilidades (KSA) como un panorama estático que perdería validez con cierta facilidad debido al rápido ritmo de cambio en la industria de la ciberseguridad. Los perfiles irán evolucionando y esto es algo que se debe tener en cuenta a la hora de abordar y utilizar este recurso.

Para la definición de perfiles de ciberseguridad se han aplicado los siguientes principios durante el proceso:

Los perfiles definidos dentro del *Framework* deben encajar con el entorno europeo de estandarización y legislación. Más específicamente, la normativa europea que define el *European e-Competence Framework* va a ser el punto de referencia y por ende, el ECSF seguirá el mismo enfoque de dicha normativa.

Los perfiles definidos dentro del Framework deben ser simples y pensados para que los utilicen las pymes u otras personas no profesionales en el campo. Esto se verá reflejado en el número limitado de perfiles.

Los perfiles deben incluir solo competencias y habilidades específicas de ciberseguridad. Las capacidades generales no se incluirán.

Adicionalmente, los siguientes criterios son de alta importancia a la hora de definir las mejores prácticas:

Aplicabilidad: cómo se pueden utilizar las taxonomías de perfiles y los vínculos para el desarrollo de planes educativos para la formación profesional y los sistemas de gestión de capacidades en las organizaciones.

Granularidad: qué tan descriptivas son las definiciones de roles y capacidades en niveles detallados.

Sostenibilidad: las estructuras basadas en proyectos se consideran menos sostenibles en comparación con las proporcionadas por organizaciones. Con el objetivo de crear valor más allá del proyecto, se consideran estructuras donde los *inputs* puedan ser utilizados posteriormente por organizaciones relevantes.

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 en los siguientes elementos:

- Perfiles
- KSA
- Competencias (basado en el *e-Competences Framework*)

6.1_Perfiles

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.

No obstante, la definición que se tiene actualmente de los perfiles de ciberseguridad otorga un panorama claro del alcance, es decir, lo que la persona estará realizando en la organización, área funcional, unidad de negocio, etc. Además, el ECSF indica que los perfiles no son únicos, son más una descripción simple de un rol genérico para una amplia usabilidad. Por lo tanto, en la práctica un trabajo de ciberseguridad puede constar de varios roles del ECSF y / o partes de estos roles.

Perfiles	Descripción
Chief Information Security Officer (CISO)	Gestiona la estrategia de ciberseguridad, alineándola con los objetivos del negocio. Garantiza en todo momento que la información de la organización está protegida adecuadamente.
Legal, Policy and Compliance Officer	Desarrolla y supervisa el programa de cumplimiento de privacidad y el personal del programa de privacidad, respaldando el cumplimiento de la privacidad, la gobernanza / políticas y las necesidades de respuesta a incidentes de los directivos de privacidad y seguridad y sus equipos.
Cybersecurity Architect	Diseña procesos de información y sistemas para respaldar las necesidades de la misión empresarial; desarrolla reglas y requisitos de tecnología que describen las arquitecturas de referencia y de destino.
Cybersecurity Specialist	Planifica para que los requisitos de seguridad de los stakeholders necesarios para proteger los procesos de negocio se aborden adecuadamente en todos los aspectos de la arquitectura empresarial, incluidos los modelos de referencia, las arquitecturas de soluciones y segmentos, y los sistemas resultantes que respaldan esos procesos.
Researcher	Realiza ingeniería de sistemas y software e investigación de sistemas de software para desarrollar nuevas capacidades, asegurando que la ciberseguridad esté completamente integrada. Realiza una investigación tecnológica integral para evaluar las vulnerabilidades potenciales en los sistemas del ciberespacio.
Educator	Mejora el conocimiento, capacidades, habilidades y competencias en ciberseguridad en toda la organización.
Incident Responder	Investiga, analiza y responde a incidentes cibernéticos dentro del entorno de red o enclave.
Digital Forensics Investigator	Analiza la evidencia digital e investiga los incidentes de seguridad informática para obtener información útil en apoyo a la mitigación de vulnerabilidades del sistema / red.
Penetration Tester	Planifica, prepara y ejecuta pruebas de sistemas para evaluar los resultados frente a especificaciones y requisitos, así como para analizar / informar los resultados de las pruebas.
Cybersecurity Auditor	Realiza evaluaciones de un producto de TI para determinar el cumplimiento de los estándares publicados.
Cybersecurity Risk Manager	Gestiona los riesgos relacionados con la ciberseguridad de la organización, desarrolla, mantiene y comunica los procesos e informes de gestión de riesgos.
Threat Intelligence Analyst	Desarrolla indicadores para mantener el conocimiento del estado del entorno operativo. Recopila, procesa, analiza y difunde evaluaciones de advertencias y amenazas cibernéticas.

Tabla 4. Perfiles de ciberseguridad del ECSF Framework

6.2_KSA

La tabla que se presenta a continuación es una ilustración que recoge los perfiles definidos por el ECSF con sus respectivos conocimientos, capacidades y las habilidades (KSA). Los KSA son un indicativo de lo que tiene que evidenciar una persona para desempeñarse adecuadamente en un rol de trabajo. Además, otro de los objetivos de los KSA es medir las cualidades que diferenciarán a un candidato de los demás. En algunos casos, los KSA se definen como los factores que identifican a los mejores candidatos de un grupo de personas calificadas para un rol determinado.

Perfiles	Knowledge	Skills	Abilities
Chief Information Security Officer (CISO)	• Conocimiento de los conceptos y protocolos de redes informáticas y metodologías de seguridad de redes. • Conocimiento de los procesos de gestión de riesgos (por ejemplo, métodos para evaluar y mitigar el riesgo). • Conocimiento de las posibles vulnerabilidades de ciberseguridad de las tecnologías de la industria. • Conocimiento de competencias cibernéticas como una forma de desarrollar capacidades.	• Capacidad de crear políticas que reflejen los objetivos de seguridad del sistema. • Capacidad de comunicarse con todos los niveles de administración, incluidos los miembros del consejo. • Capacidad de anticipar nuevas amenazas de seguridad. • Capacidad de utilizar el pensamiento crítico para analizar patrones y relaciones organizacionales.	• Habilidad de relacionar estrategia, negocios y tecnología en el contexto de la dinámica organizacional. • Habilidad de comprender los problemas de tecnología, gestión y liderazgo relacionados con los procesos de la organización y la resolución de problemas. • Habilidad de desarrollar políticas, planes y estrategias de conformidad con las leyes, regulaciones, políticas y estándares en apoyo de las actividades cibernéticas de la organización.
Legal, Policy and Compliance Officer	• Conocimiento de leyes, regulaciones, políticas y ética en lo que respecta a la seguridad cibernética y la privacidad. • Conocimiento de las evaluaciones de impacto en la privacidad. • Conocimiento de procedimientos legales administrativos / penales. • Conocimiento de los conceptos y protocolos de redes informáticas y metodologías de seguridad de redes.	• Capacidad de crear políticas que reflejen los objetivos de privacidad centrales de la empresa. • Capacidad de negociar acuerdos con proveedores / otros stakeholders y evaluar las prácticas de privacidad de estos grupos. • Capacidad de comunicarse con todos los niveles de administración, incluidos los miembros del consejo.	• Habilidad de desarrollar instrucciones claras y materiales de instrucción. • Habilidad de desarrollar políticas, planes y estrategias de conformidad con las leyes, regulaciones, políticas y estándares en apoyo de las actividades cibernéticas de la organización. • Habilidad de desarrollar, actualizar y / o mantener procedimientos operativos estándar. • Habilidad de trabajar en todos los departamentos para implementar los principios y programas de privacidad de la organización.
Cibersecurity Architect	• Conocimiento en tecnologías emergentes para diseñar e implementar soluciones de seguridad; monitorizar y mejorar esas soluciones mientras trabaja con un equipo de seguridad de la información. • Conocimiento de procedimientos de evaluación de riesgos, formación de políticas, metodologías de autorización basadas en roles, tecnologías de autenticación y patologías de ataques a la seguridad.	• Capacidad de funcionar como un experto en la materia de seguridad empresarial que puede explicar temas complejos a quienes no tienen experiencia técnica. • Capacidad de diseño de la integración de soluciones de hardware y software.	• Habilidad de aplicar las metas y objetivos de una organización para desarrollar y mantener la arquitectura. • Habilidad en sistemas operativos Windows y Linux. • Habilidad de diseñar y desarrollar mejores prácticas de seguridad. • Habilidad de lider proyectos y crear equipos e impulsar iniciativas en múltiples departamentos.

Tabla 5. Perfiles de ciberseguridad y sus respectivos KSA (I/IV)

Perfiles	Knowledge	Skills	Abilities
Cibersecurity Specialist	• Conocimiento de los conceptos y protocolos de redes informáticas y metodologías de seguridad de redes. • Conocimiento de la arquitectura de seguridad de la información empresarial. • Conocimientos de ingeniería eléctrica aplicados a la arquitectura de computadoras (por ejemplo, placas de circuitos, procesadores, chips y *hardware* de computadoras). • Conocimiento de vulnerabilidades y algoritmos.	• Capacidad de aplicar e incorporar las tecnologías en las soluciones propuestas. • Capacidad de diseño de contramedidas para riesgos de seguridad identificados. • Capacidad de diseño de la integración de soluciones de *hardware* y *software*. • Capacidad de determinar cómo debería funcionar un sistema de seguridad (capacidades de resistencia y confiabilidad) y cómo los cambios en las condiciones, las operaciones o el entorno afectarán estos resultados.	• Habilidad de aplicar los métodos, estándares y enfoques para describir, analizar y documentar la arquitectura de tecnología de la información empresarial (TI) de una organización (por ejemplo, Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Enterprise Architecture Framework [FEAF]). • Habilidad de aplicar las metas y objetivos de una organización para desarrollar y mantener la arquitectura.
Researcher	• Conocimiento de leyes, regulaciones, políticas y ética en lo que respecta a la seguridad cibernética y la privacidad. • Conocimiento de las evaluaciones de impacto en la privacidad. • Conocimiento de los conceptos de ingeniería aplicados a la arquitectura informática y al *hardware* / *software* informático asociado. • Conocimiento de los conceptos y protocolos de redes informáticas y metodologías de seguridad de redes.	• Capacidad de uso de reglas y métodos científicos para resolver problemas. • Capacidad de aplicación del proceso de ingeniería de sistemas. • Capacidad de diseño de la integración de procesos y soluciones tecnológicas, incluidos sistemas heredados y lenguajes de programación modernos. • Capacidad de aplicación de técnicas de codificación segura.	• Habilidad de identificar problemas de seguridad sistémicos basados en el análisis de la vulnerabilidad y los datos de configuración. • Habilidad de preparar y presentar informes. • Habilidad de producir documentación técnica. • Habilidad de identificar sistemas de infraestructura crítica con tecnología de información y comunicación que fueron diseñadas sin consideraciones de seguridad del sistema.
Educator	• Conocimiento de métodos pedagógicos, conocimientos técnicos relevantes y técnicas innovadoras en educación y formación práctica en ciberseguridad. • Conocimiento sobre el desarrollo de programas de sensibilización, educación y formación en ciberseguridad. • Conocimientos sobre certificaciones profesionales relacionadas con la ciberseguridad.	• Capacidad de analizar la educación y formación en ciberseguridad. • Capacidad de definir, diseñar y desplegar programas de educación, formación, sensibilización y consultoría en ciberseguridad. • Capacidad de monitorizar, evaluar e informar la efectividad de la capacitación en función de KPIs.	• Habilidad de usar los medios e instrumentos educativos adecuados para mejorar la cultura, los KSA de ciberseguridad en la organización. • Habilidad de fomentar la importancia de la ciberseguridad y la consolida en la organización. • Habilidad de facilitar, ayudar y ofrecer orientación y capacitación para certificaciones profesionales de ciberseguridad utilizando diversos recursos de capacitación.

Tabla 6. Perfiles de ciberseguridad y sus respectivos KSA (II/IV)

Perfiles	Knowledge	Skills	Abilities
Cybersecurity Auditor	• Conocimiento de leyes, regulaciones, políticas y ética en lo que respecta a la seguridad cibernética y la privacidad. • Conocimiento de aspectos como: Pentesting, revisión de diseño e implementación de medidas de seguridad. • Conocimiento de diversos marcos de trabajo para el control de la seguridad (ISO, NIST, etc.). • Conocimiento amplio en certificaciones y frameworks relacionados con ciberseguridad.	• Capacidad de proporcionar una revisión independiente o interna de los controles de seguridad y los sistemas de información. • Capacidad de probar la seguridad y la eficacia de los componentes individuales de las defensas. • Capacidad de proporcionar una descripción pgeneral del proceso de auditoría. • Capacidad de analizar / investigar cualquier brecha o problema de seguridad. • Capacidad de evaluar los sistemas, controles y políticas de seguridad interna.	• Habilidad de monitorizar las normas y metodologías de evaluación de conformidad. • Habilidad de desarrollar un plan de auditoría que describa el esquema, las normas, la metodología, los procedimientos y las pruebas de auditoría que se seguirán. • Habilidad de ejecutar el plan de auditoría, recopilar todas las pruebas / mediciones.
Cybersecurity Risk Manager	• Conocimiento de los conceptos y protocolos de redes informáticas y metodologías de seguridad de redes. • Conocimiento de los procesos de gestión de riesgos (por ejemplo, métodos para evaluar y mitigar el riesgo). • Conocimiento de las posibles vulnerabilidades de ciberseguridad de las tecnologías de la industria. • Conocimiento de competencias cibernéticas como una forma de desarrollar capacidades.	• Capacidad de discernir las necesidades de protección (es decir, controles de seguridad) de los sistemas y redes de información. • Capacidad de aplicar los principios de ciberseguridad y privacidad a los requisitos organizacionales (relevantes a la confidencialidad, integridad, disponibilidad, autenticación, no repudio).	• Habilidad de analizar objetivamente datos e información para formar una visión general del riesgo. • Habilidad de digerir información detallada para determinar tendencias. • Habilidad de comunicarse de manera efectiva a nivel ejecutivo. • Habilidad de ser ágil y reaccionar a los cambios en el entorno empresarial.
Threat Intelligence Analyst	• Conocimiento de conceptos, terminología y funcionamiento de una amplia gama de medios de comunicación (redes informáticas y telefónicas, satélite, fibra, inalámbrica). • Conocimiento de tácticas internas para anticipar y / o emular capacidades y acciones de amenazas. • Conocimiento de las formas en que los objetivos o amenazas utilizan Internet. • Conocimiento de lo que constituye una "amenaza" para una red y / o un sistema.	• Capacidad de identificar amenazas cibernéticas que pueden poner en peligro los intereses de la organización y / o socios. • Capacidad de proporcionar comprensión de los sistemas objetivo o de amenazas a través de la identificación y análisis de vínculos de relaciones físicas, funcionales o de comportamiento. • Capacidad de realización de investigaciones no atribuibles e investigaciones utilizando deep web. • Capacidad de definir y caracterizar todos los aspectos pertinentes del entorno operativo.	• Habilidad de pensar como un actor de amenazas. • Habilidad de comunicar información, conceptos o ideas complejos de manera segura y bien organizada a través de medios verbales, escritos y / o visuales. • Habilidad de obtener de forma precisa y completa todos los datos utilizados en productos de inteligencia, evaluación y / o planificación. • Habilidad de articular claramente los requisitos de inteligencia en preguntas de investigación bien formuladas y variables de seguimiento de datos para fines de seguimiento de consultas.

Tabla 7. Perfiles de ciberseguridad y sus respectivos KSA (IV/IV)

Perfiles	Knowledge	Skills	Abilities
Incident Responder	• Conocimiento de los conceptos y protocolos de redes informáticas y metodologías de seguridad de redes. • Conocimiento de las categorías de incidentes, respuestas a incidentes y plazos para las respuestas. • Conocimiento de metodologías de respuesta y manejo de incidentes. • Conocimiento de los modelos de servicios en la nube y cómo esos modelos pueden limitar la respuesta a incidentes.	• Capacidad de identificar, capturar, contener y reportar *malware*. • Capacidad de coordinar y proporcionar soporte técnico experto a los técnicos de ciberdefensa de toda la empresa para resolver incidentes de ciberdefensa. • Capacidad de preservar la integridad de la evidencia de acuerdo con procedimientos operativos estándar. • Capacidad de proteger las comunicaciones de red.	• Habilidad de diseñar respuesta a incidentes para modelos de servicios en la nube. • Habilidad de aplicar técnicas para detectar intrusiones basadas en host y en red mediante tecnologías de detección de intrusiones.
Digital Forensics Investigator	• Conocimiento de leyes, regulaciones, políticas y ética en lo que respecta a la seguridad cibernética y la privacidad. • Conocimiento de tipos de datos forenses digitales y cómo reconocerlos. • Conocimiento de la ciencia forense desplegable. • Conocimiento de tácticas, técnicas y procedimientos anti-forenses. • Conocimiento de aplicaciones de soporte y configuración de diseño de laboratorio forense (por ejemplo, VMWare, Wireshark).	• Capacidad de identificar y extraer datos de interés forense en diversos medios (es decir, análisis forense de medios). • Capacidad de configurar una estación de trabajo forense. • Capacidad de uso de conjuntos de herramientas forenses (por ejemplo, EnCase, Sleuthkit, FTK). • Capacidad de uso de máquinas virtuales. (por ejemplo, Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop / Server, Amazon Elastic Compute Cloud, etc.	• Habilidad de descifrar colecciones de datos digitales. • Habilidad de realizar análisis forenses en y para entornos Windows y Unix / Linux. • Habilidad de explicar y presentar evidencia digital de una manera simple, directa y fácil de entender para personas sin conocimientos técnicos.
Penetration Tester	• Conocimiento de leyes, regulaciones, políticas y ética en lo que respecta a la seguridad cibernética y la privacidad. • Conocimiento de métodos y procesos de prueba y evaluación de sistemas. • Conocimiento sobre herramientas, técnicas y metodologías de pruebas de penetración. • Conocimiento técnico de hardware y software, incluidos (entre otros) routers, firewalls y server systems.	• Capacidad de realización de eventos de prueba. • Capacidad de diseñar una estructura de análisis de datos (es decir, los tipos de datos que debe generar una prueba y cómo analizar esos datos). • Capacidad de determinar un nivel apropiado de rigor de prueba para un sistema dado. • Capacidad de desarrollo de escenarios de prueba basados en operaciones. • Capacidad de hacer pruebas de integración de sistemas.	• Habilidad de analizar datos de prueba. • Habilidad de recopilar, verificar y validar datos de prueba. • Habilidad de traducir datos y resultados de pruebas en conclusiones evaluativas. • Habilidad de aplicar los principios de ciberseguridad y privacidad a los requisitos de la organización (relevantes a la confidencialidad, integridad, disponibilidad, autenticación).

Tabla 8. Perfiles de ciberseguridad y sus respectivos KSA (III/IV)

Los perfiles descritos anteriormente son los que ENISA 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.

6.3_ Aplicación en la industria de la ciberseguridad o empresas (públicas y privadas)

Relevancia: al tener la descripción de los perfiles, la organización puede evaluar la relevancia de esas funciones. Por ejemplo, los conocimientos de un arquitecto de ciberseguridad serán posiblemente poco interesantes para la mayoría de las pymes, mientras que algunas otras funciones pueden parecer relevantes, pero no estar incluidas en las actividades diarias de la organización. El *Framework* permite a la organización definir el alcance de los roles de ciberseguridad.

Capacidad: si se definen las funciones relevantes, la organización puede evaluar su capacidad para realizarlas. Al tener una descripción clara de los KSA necesarios, resulta más fácil tomar decisiones sobre la capacitación, *outsourcing* y evaluación de la fuerza laboral.

Gestión: si el *Framework* está estructurado de la misma manera que cualquier sistema típico de gestión de talento, puede integrarse directamente en el sistema y ser utilizado por la organización.

6.4_ Aplicación en instituciones educativas (academia)

Evaluar: la granularidad de los KSA permite a las instituciones educativas y proveedores de capacitación revisar sus planes de estudio de manera estructurada y sistemática. El *Framework* se puede considerar como un instrumento importante de referencia.

Mejorar: se puede hacer basándose en el ejercicio de evaluación. Esto es especialmente importante teniendo en cuenta las necesidades emergentes de los profesionales. El *Framework* podría identificar incoherencias a una etapa temprana, proporcionando a la academia la previsión para mejorar y desarrollar aún más sus planes de estudio.

Enfoque: la educación proporcionada por las universidades puede diferir en la forma en que se enfocan en las competencias básicas. Algunas pueden estar más enfocadas en temas tecnológicos específicos, algunas en derecho, otras en finanzas, etc. Al tener un *Framework* integrado para trabajar, pueden mapear sus competencias básicas en varios bloques temáticos. Esto permite a la institución desarrollar internamente los programas específicos más eficaces en torno a las principales competencias.

La credibilidad de esta herramienta dependerá de la capacidad que tengan las organizaciones de comprender y comunicar que la finalidad con la que se desarrolló este *Framework* es definir no solo las habilidades actuales necesarias para proteger las organizaciones, sino también incluir tendencias en los *skills* emergentes requeridos, que responden a la velocidad de cambio de la tecnología.

Así mismo, las organizaciones deben hacer un ejercicio de autoevaluación que les permita conocer realmente qué componentes de este *Framework* 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_ 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.

Durante la reciente pandemia de COVID-19 la industria de la ciberseguridad en España ha demostrado su nivel de resiliencia, y su capacidad de apoyar a ciudadanos y empresas en tiempos de crisis. La rápida adopción de tecnologías no ha sido opcional, y por lo tanto el ecosistema de ciberseguridad tiene la obligación de buscar maneras para proteger la vida de los ciudadanos. Esa tenacidad y determinación deben estar impresas en todas las iniciativas y proyectos que se aborden para fortalecer el talento de ciberseguridad en España.

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.

Uno de los desafíos más visibles que se han querido abordar durante la ejecución del proyecto es comprender mejor los matices de la brecha de talento en ciberseguridad que continúa siendo una de las mayores dolencias para las organizaciones españolas, tanto públicas como privadas. Conjuntamente, como una parte central en la ejecución de cada una de las fases del diagnóstico, se han desarrollado una serie de temas (que por su relevancia en la coyuntura de ciberseguridad han demandado una mayor profundización y nivel de detalle[45]), mediante sesiones participativas con los agentes más relevantes de la industria de ciberseguridad española, como lo son empresas de ciberseguridad, expertos en ciberseguridad en entidades públicas y privadas, miembros activos de grupos de investigación y profesores de ciberseguridad, reclutadores para grandes multinacionales que entienden la dinámica del talento al interior de las empresas, y otras organizaciones que de una u otra manera denotan conocimiento tácito en cuanto a la gestión del talento de ciberseguridad.

Todo ello para establecer un escenario común de intervención que refleje no solo el estado actual del talento de ciberseguridad en España, sino el camino que debe establecerse para incrementar, tanto la cantidad como calidad de los trabajadores (nuevos y existentes) en un contexto de cambio acelerado y de necesidad de formación permanente.

La digitalización acelerada sufrida en los últimos meses ha transforma-

45 Las temáticas son: caracterización de la oferta, demanda de talento de ciberseguridad, contratación y reciclaje de perfiles hacia la ciberseguridad, gestión y retención del talento de ciberseguridad, formación autodidacta y presencia femenina.

do no solo las estructuras y modelos de negocio, sino la forma en la que el talento humano de la organización debe ser gestionado en el entorno digital. Por ello, este apartado comienza describiendo un conjunto de recomendaciones generales que deberían incorporar las organizaciones para avanzar en la gestión del talento digital.

De esta forma, será posible establecer recomendaciones específicas orientadas a la gestión del talento de ciberseguridad, como resultado del presente trabajo. 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_Generales de gestión de talento digital

El proceso de transformación digital en el que están inmersas las organizaciones ha impactado con fuerza en todas las áreas de las organizaciones, especialmente en la de Recursos Humanos. El talento es ahora más importante que hace unos años y el éxito o fracaso en su gestión puede marcar la evolución de las organizaciones.

Sin embargo, en este nuevo contexto, las reglas han cambiado. La aceleración sin precedentes en la digitalización de empresas, ciudadanos y profesionales también ha impactado en los recursos humanos, que ahora deben responder no solo a la gestión actual y figura del talento, sino a cómo se está abordando el ciclo completo del talento: detección y atracción de talento, *onboarding* en la organización, crecimiento profesional y *offboarding* final. Así, a medida que las organizaciones se digitalizan, el conocimiento que se necesita para desarrollar el trabajo muta de una forma muy rápida, quedándose obsoleto en un periodo muy corto de tiempo. Tanto es así que, según la OCDE, en España un 30% de los empleos sufrirán una profunda transformación, siendo un 22%, aquellos que presentan ya un alto riesgo de transformación.

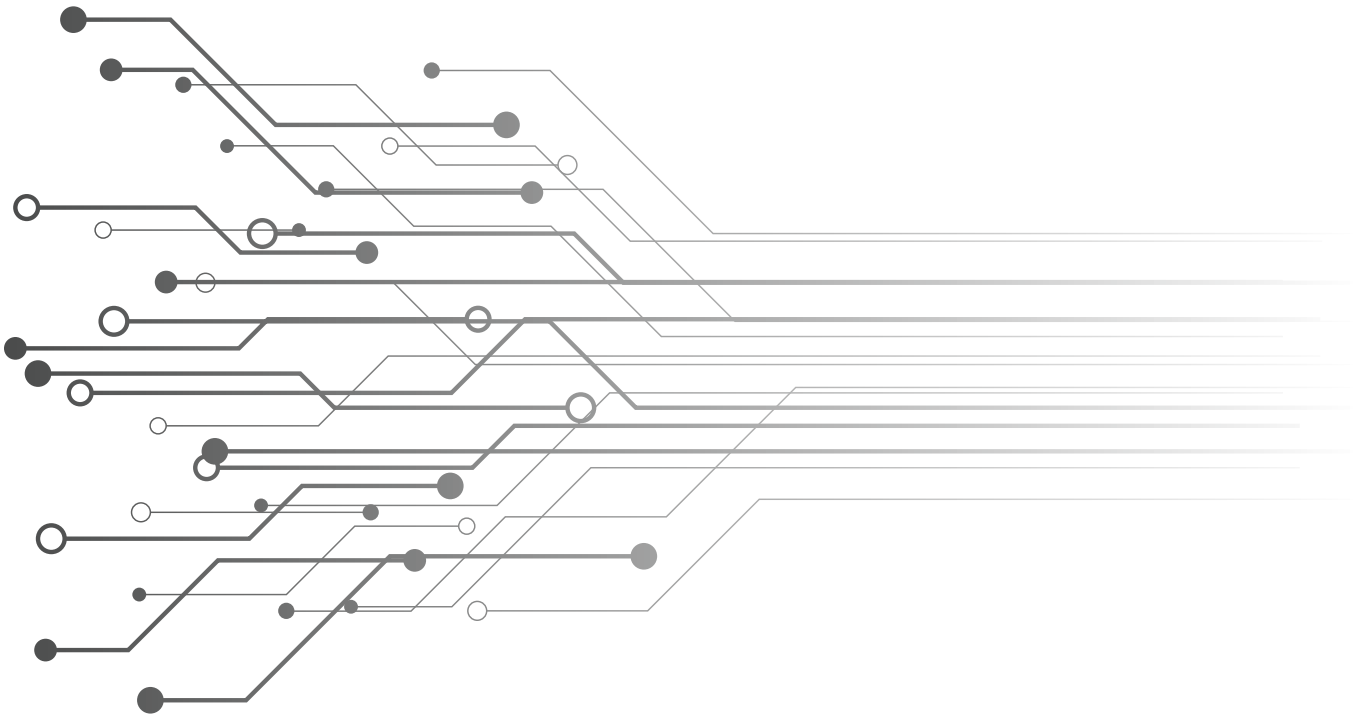
En este sentido, tras el análisis realizado, se presentan a continuación un conjunto de recomendaciones que inciden en los diferentes bloques del ciclo de

vida del talento segmentados en función del área dentro del ciclo de vida del talento donde pertenecen, 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 9. 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. La operativización de las mismas se recogerá en el capítulo de plan de acción.



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 (*offline y online*) 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.
· Asímismo, 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 solo 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 mismos 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 en la fuga del 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_Específicas de gestión del 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.

Para el sector público.

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 del 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.

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 del 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 del 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 al 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.

ANEXOS

ANEXO I. DETALLE DE FORMACIONES PROFESIONALES SUPERIORES QUE DAN ACCESO AL CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD

Título de Técnico Superior en Administración de Sistemas Informáticos en Red

En qué consiste el título de Técnico Superior:

Configurar, administrar y mantener sistemas informáticos, garantizando la funcionalidad, la integridad de los recursos y servicios del sistema, con la calidad exigida y cumpliendo la reglamentación vigente. Este profesional será capaz de:

- Administrar sistemas operativos de servidor, instalando y configurando el software, en condiciones de calidad para asegurar el funcionamiento del sistema.
- Administrar servicios de red (web, mensajería electrónica y transferencia de archivos, entre otros) instalando y configurando el software, en condiciones de calidad.
- Implantar y gestionar bases de datos instalando y administrando el software de gestión en condiciones de calidad, según las características de la explotación.
- Evaluar el rendimiento de los dispositivos hardware identificando posibilidades de mejoras según las necesidades de funcionamiento.
- Determinar la infraestructura de redes telemáticas elaborando esquemas y seleccionando equipos y elementos.
- Integrar equipos de comunicaciones en infraestructuras de redes telemáticas, determinando la configuración para asegurar su conectividad.
- Administrar usuarios de acuerdo a las especificaciones de explotación para garantizar los accesos y la disponibilidad de los recursos del sistema.
- Diagnosticar las disfunciones del sistema y adoptar las medidas correctivas para restablecer su funcionalidad.
- Gestionar y/o realizar el mantenimiento de los recursos de su área (programando y verificando su cumplimiento), en función de las cargas de trabajo y el plan de mantenimiento.

Plan de formación:

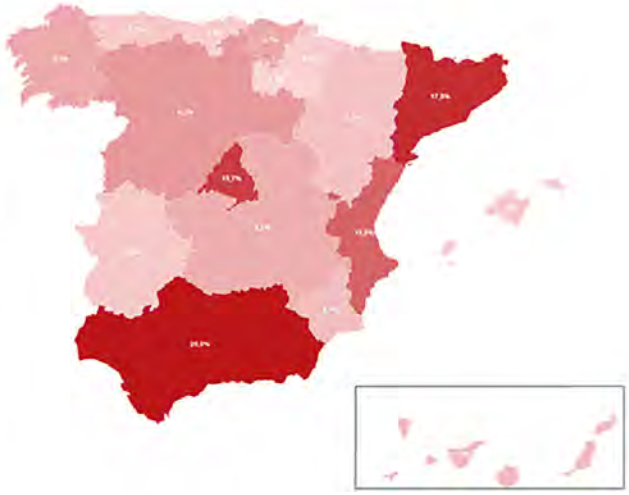
- Implantación de sistemas operativos.
- Planificación y administración de redes.
- Fundamentos de hardware.
- Gestión de bases de datos.
- Lenguajes de marcas y sistemas de gestión de información.
- Administración de sistemas operativos.
- Servicios de red e Internet.
- Implantación de aplicaciones web.
- Administración de sistemas gestores de bases de datos.
- Seguridad y alta disponibilidad.
- Proyecto de administración de sistemas informáticos en red.
- Formación y orientación laboral.
- Empresa e iniciativa emprendedora.
- Formación en centros de trabajo.

Perfiles profesionales:

- Técnica / técnico en administración de sistemas.
- Responsable de informática.
- Técnica / técnico en servicios de Internet.
- Técnica / técnico en servicios de mensajería electrónica.
- Personal de apoyo y soporte técnico.
- Técnica / técnico en teleasistencia.
- Técnica / técnico en administración de base de datos.
- Técnica / técnico de redes.
- Supervisor / supervisora de sistemas.
- Técnica / técnico en servicios de comunicaciones.
- Técnica / técnico en entornos web.

Fuente: Ministerio de Educación y Formación Profesional

Centros privados y públicos de FP dónde se imparte este título		
Andalucía	20,0%	89
Aragón	2,2%	10
Cantabria	1,1%	5
Castilla y León	6,3%	28
Castilla-La Mancha	4,3%	19
Cataluña	17,5%	78
Ceuta	0,2%	1
Comunidad de Madrid	15,7%	70
Comunidad Valenciana	11,9%	53
Extremadura	1,6%	7
Galicia	4,7%	21
Islas Baleares	1,3%	6
Islas Canarias	2,7%	12
La Rioja	0,4%	2
Melilla	0,2%	1
Murcia	2,7%	12
Navarra	0,9%	4
País Vasco	4,7%	21
Principado de Asturias	1,6%	7



Fuente: Ministerio de Educación y Formación Profesional

- Se registran un total de 12.876 demandantes de empleo, de los cuales, 6.800 son parados. Por el contrario, en los últimos doce meses se han hecho un total de 13.402 contratos acumulados a un total de 7.691 demandantes de empleo con esta titulación. En abril de 2021 se registran 1.068 contratos a 921 personas.
- De los 1.068 contratos que se han hecho en abril de 2021 a demandantes titulados, se aprecia que no se les contrata exclusivamente como técnicos en operaciones/superiores en admin de sistemas informáticos en red.
- Respecto a la diferencia de género en técnicos con esta titulación, se ajusta con la diferencia de contratados con este título. Por lo tanto, teniendo en cuenta los datos de abril de 2021, no se aprecia discriminación por sexos en el mercado para técnicos que cuentan con este título.

Diferencia de género

Título de Técnico Superior en Desarrollo de Aplicaciones Multiplataforma

En qué consiste el título de Técnico Superior:

- Configurar y explotar sistemas informáticos, adaptando la configuración lógica del sistema según las necesidades de uso y los criterios establecidos.
- Aplicar técnicas y procedimientos relacionados con la seguridad en sistemas, servicios y aplicaciones, cumpliendo el plan de seguridad.
- Gestionar bases de datos, interpretando su diseño lógico y verificando integridad, consistencia, seguridad y accesibilidad de los datos.
- Gestionar entornos de desarrollo adaptando su configuración en cada caso para permitir el desarrollo y despliegue de aplicaciones.
- Desarrollar aplicaciones multiplataforma con acceso a bases de datos utilizando lenguajes, librerías y herramientas adecuados a las especificaciones.
- Integrar contenidos gráficos y componentes multimedia en aplicaciones multiplataforma, empleando herramientas específicas y cumpliendo los requerimientos establecidos.
- Desarrollar interfaces gráficos de usuario interactivos y con la usabilidad adecuada, empleando componentes visuales estándar o implementando componentes visuales específicos.
- Desarrollar aplicaciones para teléfonos, PDA y otros dispositivos móviles empleando técnicas y entornos de desarrollo específicos.
- Desarrollar aplicaciones multiproceso y multihilo empleando librerías y técnicas de programación específicas.
- Participar en la implantación de sistemas ERP-CRM evaluando la utilidad de cada uno de sus módulos.
- Gestionar la información almacenada en sistemas ERP-CRM garantizando su integridad.

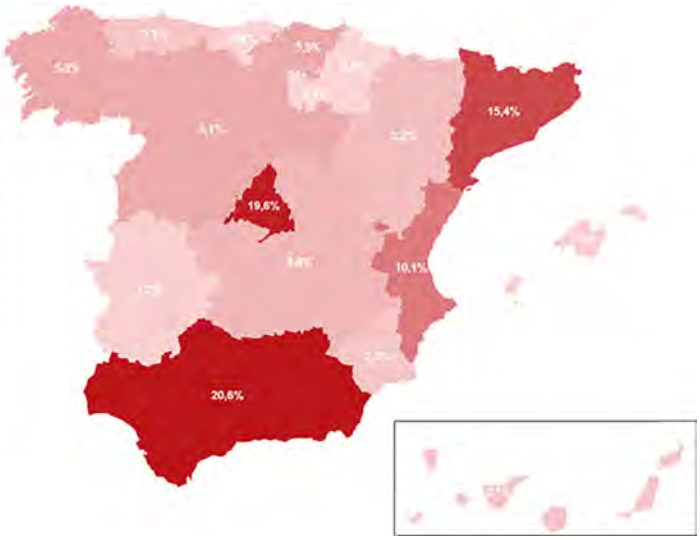
Plan de formación:

- Sistemas informáticos.
- Bases de Datos.
- Programación.
- Lenguajes de marcas y sistemas de gestión de información.
- Entornos de desarrollo.
- Acceso a datos.
- Desarrollo de interfaces.
- Programación multimedia y dispositivos móviles.
- Programación de servicios y procesos.
- Sistemas de gestión empresarial.
- Proyecto de desarrollo de aplicaciones multiplataforma.
- Formación y orientación laboral.
- Empresa e iniciativa emprendedora.
- Formación en centros de trabajo.

Perfiles profesionales:

- Desarrollando aplicaciones informáticas para la gestión empresarial y de negocio.
- Desarrollando aplicaciones de propósito general.
- Desarrollando aplicaciones en el ámbito del entretenimiento y la informática móvil.

Centros privados y públicos de FP dónde se imparte este titulo		
Andalucía	20,6%	98
Aragón	3,2%	15
Asturias	2,3%	11
Cantabria	0,8%	4
Castilla y León	5,1%	24
Castilla-La Mancha	3,8%	18
Cataluña	15,4%	73
Comunidad de Madrid	19,6%	93
Comunidad Valenciana	10,1%	48
Extremadura	1,3%	6
Galicia	5,3%	25
Islas Baleares	1,3%	6
Islas Canarias	2,1%	10
La Rioja	0,8%	4
Murcia	2,3%	11
Navarra	0,6%	3
País Vasco	5,5%	26



- Se registran un total de 16.168 demandantes de empleo, de los cuales, 8.644 son parados. Por el contrario, en los últimos doce meses se han hecho un total de 14.118 contratos acumulados a un total de 7.754 demandantes de empleo con esta titulación. En abril de 2021 se registran 1.244 contratos a 1.064 personas.
- De los 1.244 contratos que se han hecho en abril de 2021 a demandantes titulados, se aprecia que no se les contrata principalmente en su sector.
- Respecto a la diferencia de género en técnicos con esta titulación, se ajusta con la diferencia de contratados con este título. Por lo tanto, teniendo en cuenta los datos de abril de 2021, no se aprecia prácticamente discriminación por sexos en el mercado para técnicos que cuentan con este título.

Fuente: Servicio Público de Empleo Estatal. Abril 2021

Diferencia de género

Título de Técnico Superior en Desarrollo de Aplicaciones Web

En qué consiste el título de Técnico Superior:

Desarrollar, implantar, y mantener aplicaciones web, con independencia del modelo empleado y utilizando tecnologías específicas, garantizando el acceso a los datos de forma segura y cumpliendo los criterios de accesibilidad, usabilidad y calidad exigidas en los estándares establecidos.

Este profesional será capaz de:

- Configurar y explotar sistemas informáticos, adaptando la configuración lógica del sistema según las necesidades de uso y los criterios establecidos.
- Aplicar técnicas y procedimientos relacionados con la seguridad en sistemas, servicios y aplicaciones, cumpliendo el plan de seguridad.
- Gestionar servidores de aplicaciones adaptando su configuración en cada caso para permitir el despliegue de aplicaciones web.
- Gestionar bases de datos, interpretando su diseño lógico y verificando integridad, consistencia, seguridad y accesibilidad de los datos.
- Desarrollar aplicaciones web con acceso a bases de datos utilizando lenguajes, objetos de acceso y herramientas de mapeo adecuados a las especificaciones.
- Integrar contenidos en la lógica de una aplicación web, desarrollando componentes de acceso a datos adecuados a las especificaciones.
- Desarrollar interfaces en aplicaciones web de acuerdo con un manual de estilo, utilizando lenguajes de marcas y estándares web.
- Desarrollar componentes multimedia para su integración en aplicaciones web, empleando herramientas específicas y siguiendo las especificaciones establecidas.
- Integrar componentes multimedia en el interface de una aplicación web, realizando el análisis de interactividad, accesibilidad y usabilidad de la aplicación.
- Desarrollar e integrar componentes software en el entorno del servidor web, empleando herramientas y lenguajes específicos, para cumplir las especificaciones de la aplicación.
- Desarrollar servicios para integrar sus funciones en otras aplicaciones web, asegurando su funcionalidad.
- Integrar servicios y contenidos distribuidos en aplicaciones web, asegurando su funcionalidad.

Plan de formación:

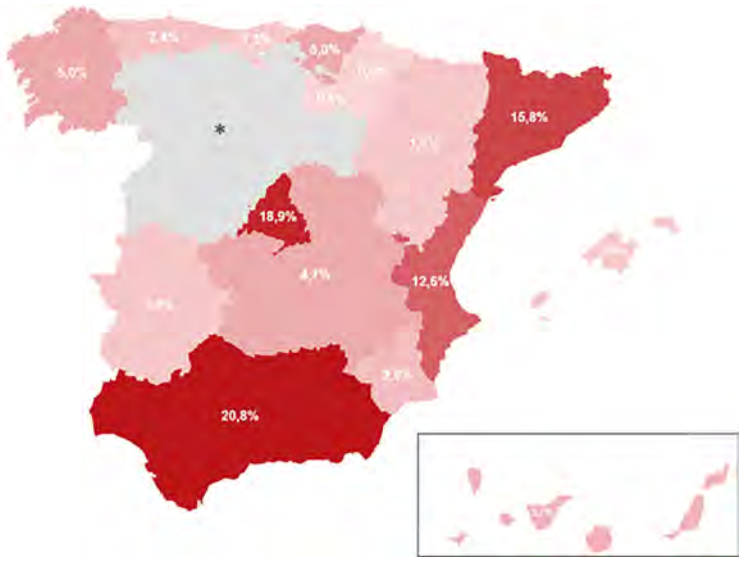
- Sistemas informáticos.
- Bases de datos.
- Programación.
- Lenguajes de marcas y sistemas de gestión de información.
- Entornos de desarrollo.
- Desarrollo web en entorno cliente.
- Desarrollo web en entorno servidor.
- Despliegue de aplicaciones web.
- Diseño de interfaces WEB.
- Proyecto de desarrollo de aplicaciones web
- Formación y orientación laboral.
- Empresa e iniciativa emprendedora.
- Formación en centros de trabajo.

Perfiles profesionales:

- Programador / programadora Web.
- Programador / programadora Multimedia.
- Desarrollador / desarrolladora de aplicaciones en entornos Web.

Centros privados y públicos de FP dónde se imparte este título		
Andalucía	20,8%	79
Aragón	1,8%	7
Asturias	2,4%	9
Cantabria	1,3%	5
Castilla-La Mancha	4,7%	18
Cataluña	15,8%	60
Ceuta	0,3%	1
Comunidad de Madrid	18,9%	72
Comunidad Valenciana	12,6%	48
Extremadura	1,8%	7
Galicia	5,0%	19
Islas Baleares	1,6%	6
Islas Canarias	3,7%	14
La Rioja	0,5%	2
Melilla	0,3%	1
Murcia	2,9%	11
Navarra	0,5%	2
País Vasco	5,0%	19

*Nota aclaratoria: Este título se impartirá en 16 centros privados y públicos de Castilla y León en el curso 2021/2022. A fecha de julio 2021 no aparece en el listado definitivo del Ministerio de Educación y Formación Profesional.



- Se registran un total de 1.628 demandantes de empleo, de los cuales, 1.019 son parados. Por el contrario, en los últimos doce meses se han hecho un total de 1.732 contratos acumulados a un total de 1.232 demandantes de empleo con esta titulación. En abril de 2021 se registran 139 contratos a 129 personas.
- De los 139 contratos que se han hecho en abril de 2021 a demandantes titulados, se aprecia que a la mayoría efectivamente se les contrata principalmente en su sector.
- Respecto a la diferencia de género en técnicos con esta titulación, se ajusta a grandes rasgos con la diferencia de contratados con este título. Por lo tanto, teniendo en cuenta los datos de abril de 2021, se aprecia una ligera diferencia en el mercado por sexos para técnicos que cuentan con este título.

Fuente: Servicio Público de Empleo Estatal. Abril 2021.

Diferencia de género

Título de Técnico Superior en Sistemas de Telecomunicaciones e Informáticos

En qué consiste el título de Técnico Superior:

- Desarrollar proyectos de instalaciones o sistemas de telecomunicaciones obteniendo datos y características para la elaboración de informes y especificaciones.
- Calcular los parámetros de equipos, elementos e instalaciones, cumpliendo la normativa vigente y los requerimientos del cliente.
- Configurar instalaciones y sistemas de telecomunicación, con las especificaciones y las prescripciones reglamentarias.
- Planificar el montaje de instalaciones y sistemas de telecomunicaciones según documentación técnica y condiciones de obra.
- Realizar el lanzamiento del montaje de las instalaciones partiendo del programa de montaje y del plan general de obra.
- Supervisar y/o ejecutar los procesos de montaje de las instalaciones y sistemas, verificando su adecuación a las condiciones de obra y controlando su avance para cumplir con los objetivos de la empresa.
- Planificar el mantenimiento a partir de la normativa, condiciones de la instalación y recomendaciones de los fabricantes.
- Supervisar y/o ejecutar los procesos de mantenimiento de las instalaciones, controlando los tiempos y la calidad de los resultados.
- Realizar la puesta en servicio de las instalaciones y equipos de telecomunicaciones, supervisando el cumplimiento de los requerimientos y asegurando las condiciones de calidad y seguridad.

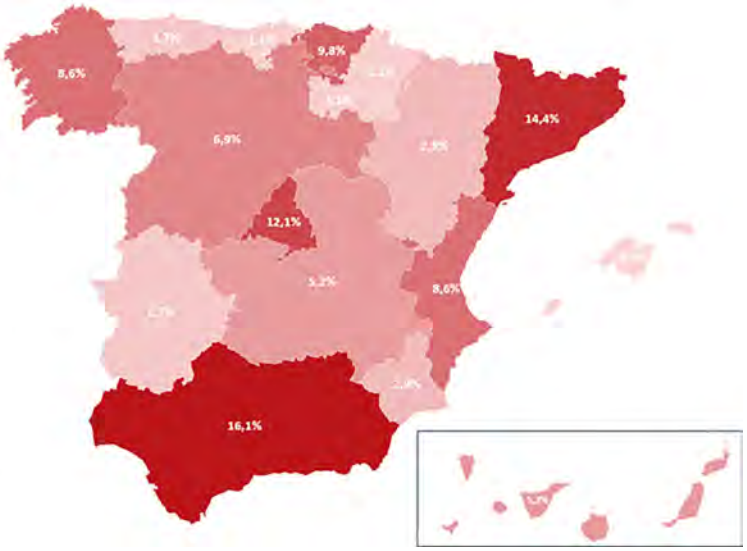
Plan de formación:

- Configuración de infraestructuras de sistemas de telecomunicaciones.
- Elementos de sistemas de telecomunicaciones.
- Sistemas informáticos y redes locales.
- Técnicas y procesos en infraestructuras de telecomunicaciones.
- Sistemas de producción audiovisual.
- Redes telemáticas.
- Sistemas de radiocomunicaciones.
- Sistemas integrados y hogar digital.
- Gestión de proyectos de instalaciones de telecomunicaciones.
- Sistemas de telefonía fija y móvil.
- Proyecto de sistemas de telecomunicaciones e informáticos.
- Formación y orientación laboral.
- Empresa e iniciativa emprendedora.
- Formación en centros de trabajo.

Perfiles profesionales:

- Ayudante de proyectista en instalaciones de telecomunicaciones para viviendas y edificios.
- Especialista en instalación, integración y mantenimiento de equipos y sistemas de telecomunicación.
- Jefe de obra en instalaciones de telecomunicaciones.
- Técnica / técnico en supervisión, instalación, verificación y control de equipos de sistemas de radio y televisión en estudios de producción y sistemas de producción audiovisual.
- Técnica / técnico en supervisión, instalación, mantenimiento, verificación y control de equipos de sistemas de radiodifusión.
- Técnica / técnico en supervisión, instalación, mantenimiento, verificación y control de equipos de sistemas de seguridad electrónica y circuitos cerrados de televisión.
- Técnica / técnico en supervisión, instalación, mantener, verificación y control en redes locales y sistemas telemáticos
- Técnica / técnico en supervisión, instalación, mantenimiento, verificación y control en sistemas de radioenlaces.
- Especialista en integración, instalación y mantenimiento de equipos y sistemas informáticos.

Centros privados y públicos de FP dónde se imparte este título		
Andalucía	16,1%	28
Aragón	2,9%	5
Asturias	1,7%	3
Cantabria	1,1%	2
Castilla y León	6,9%	12
Castilla-La Mancha	5,2%	9
Cataluña	14,4%	25
Comunidad de Madrid	12,1%	21
Comunidad Valenciana	8,6%	15
Extremadura	1,7%	3
Galicia	8,6%	15
Islas Baleares	0,6%	1
Islas Canarias	5,2%	9
La Rioja	1,1%	2
Murcia	2,9%	5
Navarra	1,1%	2
País Vasco	9,8%	17



- Se registran un total de 8.800 demandantes de empleo, de los cuales, 4.199 son parados. Por el contrario, en los últimos doce meses se han hecho un total de 9.928 contratos acumulados a un total de 5.277 demandantes de empleo con esta titulación. En abril de 2021 se registran 834 contratos a 703 personas.
- De los 834 contratos que se han hecho en abril de 2021 a demandantes titulados, se aprecia que no se les contrata principalmente en su sector.
- Respecto a la diferencia de género en técnicos con esta titulación, se ajusta a grandes rasgos con la diferencia de contratados con este título. Por lo tanto, teniendo en cuenta los datos de abril de 2021, no se aprecia ninguna diferencia en el mercado por sexos para técnicos que cuentan con este título.

Diferencia de género

Título de Técnico Superior en Mantenimiento Electrónico

En qué consiste el título de Técnico Superior:

- Configurar circuitos electrónicos reconociendo su estructura en bloques.
- Calcular parámetros de circuitos electrónicos analógicos y digitales identificando los valores de las etapas de entrada-salida y de acondicionamiento y tratamiento de señal.
- Verificar el funcionamiento de circuitos analógicos y de electrónica digital microprogramables utilizando equipos de medida y sistemas software de análisis y configuración.
- Elaborar el presupuesto del mantenimiento, cotejando los aspectos técnicos y económicos para ofrecer la mejor solución.
- Organizar y gestionar las intervenciones para el mantenimiento correctivo de acuerdo al nivel de servicio y optimizando los recursos humanos y materiales.
- Gestionar el suministro y almacenamiento de los materiales y equipos, definiendo la logística asociada y controlando existencias.
- Desarrollar las intervenciones de mantenimiento atendiendo a la documentación técnica y condiciones de los equipos o sistemas.
- Realizar el diagnóstico de las disfunciones o averías en los equipos o sistemas, a partir de los síntomas detectados, información aportada por el usuario, información técnica e historial de la instalación.
- Supervisar y/o ejecutar los procesos de mantenimiento preventivo, correctivo y predictivo, controlando los tiempos y la calidad de los resultados.
- Realizar la puesta en servicio de los equipos y sistemas electrónicos, asegurando su funcionamiento dentro de los parámetros técnicos de aceptación y asegurando las condiciones de calidad y seguridad.

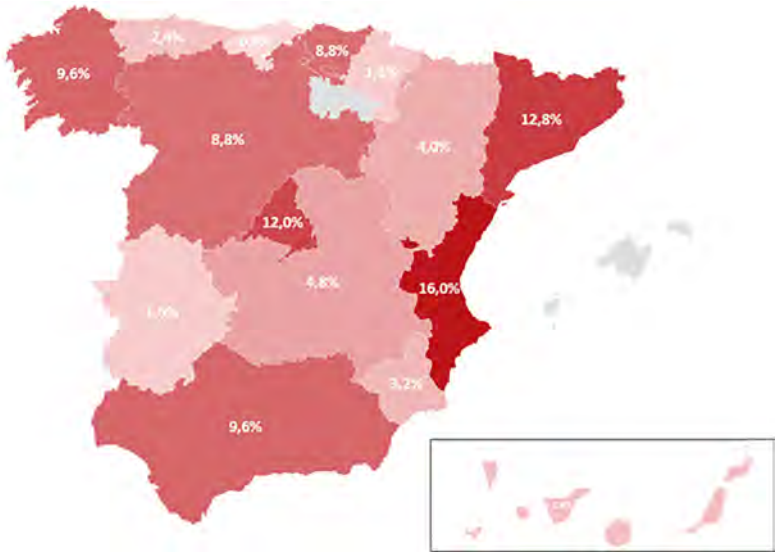
Plan de formación:

- Circuitos electrónicos analógicos.
- Equipos microprogramables.
- Mantenimiento de equipos de radiocomunicaciones.
- Mantenimiento de equipos de voz y datos.
- Mantenimiento de equipos de electrónica industrial.
- Mantenimiento de equipos de audio.
- Mantenimiento de equipos de vídeo.
- Técnicas y procesos de montaje y mantenimiento de equipos electrónicos.
- Infraestructuras y desarrollo del mantenimiento electrónico.
- Proyecto de mantenimiento electrónico.
- Formación y orientación laboral.
- Empresa e iniciativa emprendedora.
- Formación en centros de trabajo

Perfiles profesionales:

- Técnica / técnico en supervisión y verificación de equipos de sistemas de radio y televisión y sistemas de producción audiovisual.
- Técnica / técnico en reparación y mantenimiento de sistemas de radio y televisión de sistemas de producción audiovisual y de radiodifusión.
- Técnica / técnico en supervisión y verificación de equipos de sistemas de radiodifusión.
- Técnica / técnico en supervisión y verificación de equipos de sistemas domóticos, inmóticos y de seguridad electrónica.
- Técnica / técnico en reparación y mantenimiento de sistemas domóticos, inmóticos y de seguridad electrónica.
- Técnica / técnico en supervisión y verificación en redes locales y sistemas telemáticos
- Técnica / técnico en reparación y mantenimiento de equipos de redes locales y sistemas telemáticos.
- Técnica / técnico en supervisión, verificación y control en sistemas de radioenlaces.
- Técnica / técnico en reparación y mantenimiento de equipos profesionales de audio, de vídeo y de equipos industriales

Centros privados y públicos de FP dónde se imparte este título		
Andalucía	9,6%	12
Aragón	4,0%	5
Asturias	2,4%	3
Cantabria	0,8%	1
Castilla y León	8,8%	11
Castilla-La Mancha	4,8%	6
Cataluña	12,8%	16
Ceuta	1,6%	2
Comunidad de Madrid	12,0%	15
Comunidad Valenciana	16,0%	20
Extremadura	1,6%	2
Galicia	9,6%	12
Islas Canarias	2,4%	3
Murcia	3,2%	4
Navarra	1,6%	2
País Vasco	8,8%	11

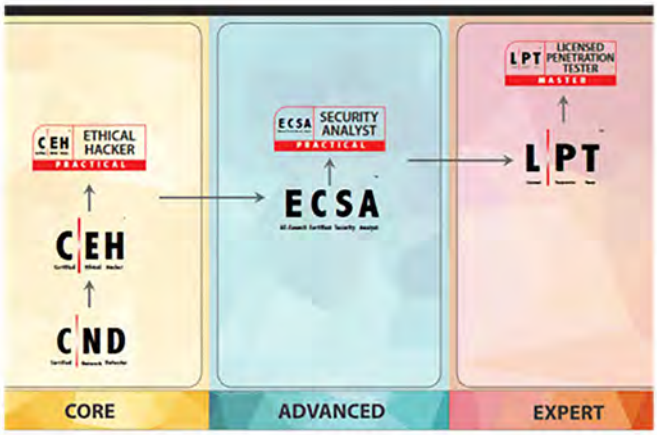


- Se registran un total de 12.611 demandantes de empleo, de los cuales, 5.046 son parados. Por el contrario, en los últimos doce meses se han hecho un total de 11.466 contratos acumulados a un total de 5.766 demandantes de empleo con esta titulación. En abril de 2021 se registran 926 contratos a 755 personas.
- De los 926 contratos que se han hecho en abril de 2021 a demandantes titulados, se aprecia que a la mayoría efectivamente se les contrata principalmente en su sector.
- Respecto a la diferencia de género en técnicos con esta titulación, se ajusta a grandes rasgos con la diferencia de contratados con este título. Por lo tanto, teniendo en cuenta los datos de abril de 2021, no se aprecia apenas diferencia en el mercado por sexos para técnicos que cuentan con este título.

Diferencia de género

ANEXO 2. CARACTERÍSTICAS DE LAS CERTIFICACIONES DE CIBERSEGURIDAD MÁS RELEVANTES

EC-Council Certificado Hacker Ético (CEH)



El CEH es una calificación avanzada de pruebas de penetración que evalúa la capacidad del candidato para buscar e identificar posibles riesgos de seguridad dentro de la infraestructura de redes e informáticas de una organización. El CEH es uno de los cursos fundamentales ofrecidos por EC-Council y es un buen punto de partida antes de decidirse por el examen del Analista de Seguridad Certificado - EC-Council Certified Security Analyst (ESCA).

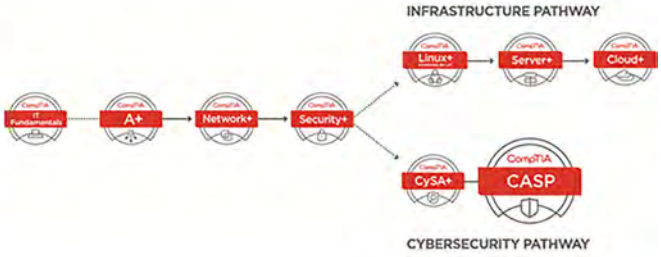
- Requisitos previos: Los candidatos deben asistir a la capacitación oficial o tener al menos dos años de experiencia relacionada con la seguridad de la información.
- Examen: El examen CEH contiene 125 preguntas y dura cuatro horas. Se debe sacar un 70% para superar la prueba.

Existen muchos roles de seguridad donde se requieren certificaciones de tipo CEH. La CEH enseña habilidades ventajosas con pruebas prácticas. Es una buena certificación para los profesionales de la seguridad de la información y los administradores de red que buscan una introducción al hacking ético y las pruebas de penetración.

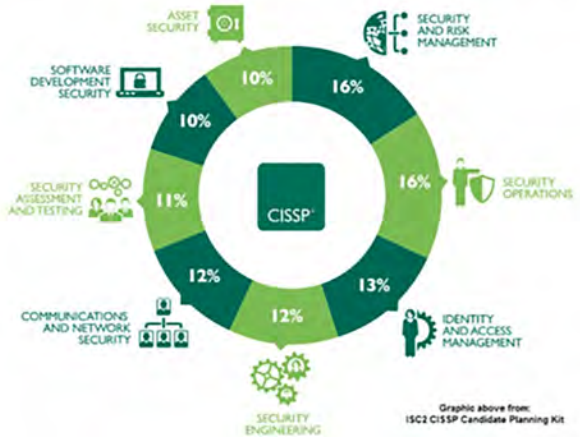
CompTIA Security+ (SY0-401)

La certificación CompTIA Security+ es una certificación popular, independiente del proveedor, que es un buen punto de partida para los profesionales de la seguridad de la información. La certificación Security+ está dirigida a profesionales de seguridad de nivel inicial y ofrece información generalizada para ayudar a los candidatos a desarrollar una comprensión fundamental de la seguridad de la información. El examen Security+ presenta seis dominios útiles para los aspirantes a profesionales de la seguridad de la información.

- Requisitos previos: Se recomienda disponer de la certificación de CompTIA Network+ y dos años de experiencia en administración de sistemas con un enfoque de seguridad.
- Examen: CompTIA Security+ SY0-401 tiene un máximo de 90 preguntas y dura 90 minutos. La puntuación para aprobar es del 75% en una escala de 100-900.



(ISC)² Certified Information Systems Security Professional (CISSP)



El CISSP es una calificación muy útil para conocer el grado de madurez de los empleados en cuanto a seguridad digital. Las habilidades que se adquieren durante este curso son fundamentales para cualquier persona que necesite diseñar e implementar sistemas de seguridad de la información en el puesto de trabajo. El CISSP mide objetivamente las habilidades de los candidatos. Esta es la razón por la cual la certificación tiene tanto valor entre los profesionales de seguridad TI.

El CISSP está reconocido a nivel mundial.

- Requisitos previos: Se debe contar con al menos cinco años de experiencia en un campo relacionado con el tema del examen CISSP. También se debe tener conocimiento de al menos dos de los ocho dominios en el material de estudio o cuerpo de conocimiento común (CBK). Los candidatos sin la experiencia laboral requerida pueden satisfacer el requisito con un año de experiencia laboral y un título universitario de cuatro años, o una credencial aprobada de la vía de prerrequisito del CISSP. Otra opción para quienes no tienen la experiencia laboral adecuada es hacer el examen y obtener una designación de Asociado de (ISC)². Los candidatos tendrán seis años para obtener la experiencia laboral requerida para el CISSP.
- Examen CISSP: El examen tiene 250 preguntas de opción múltiple y dura seis horas. Para aprobar, son necesarios 700 de 1000 puntos, o lo que es lo mismo, el 70% es la puntuación.

(ISACA) Certified Information Security Manager (CISM)

El CISM está orientado a personas que buscan un puesto de gerencia en el que la seguridad de la información, la garantía y la gestión de riesgos formen parte de sus responsabilidades laborales. Cubre los principios de administración de seguridad que son tanto prácticos como vitales para la capacidad del candidato para llevar a cabo sus tareas en el rol de un administrador de seguridad de sistemas de información.

- Requisitos previos: Los candidatos que buscan esta certificación deben contar con un mínimo de cinco años de experiencia laboral en el campo de la seguridad de la información, con al menos tres años en el puesto de gerente de seguridad de la información. Esto debe ser verificado antes de que los candidatos puedan realizar el examen.
- Examen CISM: El examen CISM consiste en 200 preguntas y dura cuatro horas. La puntuación oscila entre 200 y 800, y la puntuación mínima para aprobar es de 450.

A medida que la demanda de profesionales de gestión de la seguridad de la información sigue aumentando, también aumenta la demanda de los profesionales certificados en CISM. Los roles gerenciales en la seguridad de la información también son publicitados más ampliamente por las compañías corporativas que buscan retener gerentes de seguridad de la información capacitados.

ISACA

	CISA	CISM	CRISC	CGEIT
Career Path	Lead IT Auditor	Chief (Information) Security Officer (CSO / CISO)	Chief Risk Officer (CRO)	Chief Information Officer (CIO)
Focus	IT Audit	Information Security	Risk Management	IT Governance
Work Performed	Provide assurance by conducting audits and assessments of information systems	Oversee, direct and manage information security activities	Identify, evaluate and manage risk through the development, implementation and maintenance of information systems controls	Define, establish, maintain and manage a framework of IT governance
Requirements	Submit verified evidence of a minimum of 5 years of verifiable IS audit, control or security experience (substitutions available)	Submit verified evidence of a minimum of 5 years of information security management work experience (covering 3 of the 4 job practice domains	Submit verified evidence of a minimum of 3 years of risk and information systems controls experience (covering 3 of the 5 job practice domains)	Submit verified evidence of the 5 years experience requirements as defined by the CGEIT Job Practice
Additional requirements	• Adhere to the ISACA Code of Professional Ethics • Comply with the CGEIT Continuing Education Policy			

(ISC)² Certified Cloud Security Professional (CCSP)

Una de las principales razones por las que los profesionales de seguridad se certifican con el CCSP es para demostrar que están bien informados sobre la seguridad cloud y todas las consideraciones de seguridad relacionadas con cloud. Los entornos en la nube están llenos de retos de seguridad que cambian a diario, por lo que obtener el CCSP es vital para mostrar que se está bien informado sobre las consideraciones de seguridad necesarias que son parte integrante de la computación cloud.

- Requisitos previos: Los candidatos deben contar con un mínimo de cinco años de experiencia en TI, de los cuales tres años deben estar relacionados con la seguridad de la información. También deben contar con un año de experiencia en al menos una de las seis áreas del Common Knowledge (CBK) del CCSP.
- Examen CCSP: El examen CCSP consiste de 125 preguntas y dura cuatro horas. La puntuación para aprobar es de 700 de 1000 puntos.

Esta certificación ayuda a los candidatos a demostrar competencia en seguridad de datos en la nube, arquitectura y diseño Cloud, así como en las operaciones diarias, consideraciones de seguridad de aplicaciones y mucho más. Esta certificación es especialmente útil para quien busque un puesto de trabajo en un ambiente basado en cloud.

CCSP Certified Cloud Security Professional

GIAC Security Essentials (GSEC)

Global Information Assurance Certification (GIAC) es el proveedor y desarrollador líder de certificaciones de ciberseguridad y es reconocido mundialmente por líderes gubernamentales, militares y de la industria. GIAC prueba y valida la capacidad de los profesionales en áreas tales como administración de seguridad, análisis forense, administración, auditorías, seguridad de software y mejores prácticas legales.

La certificación GIAC Security Essentials (GSEC) está diseñada para candidatos que desean demostrar habilidades en roles de sistemas de TI y tareas de seguridad de la información. El GSEC es una certificación especialmente codiciada. Enseña las mejores prácticas y métodos de seguridad generales para aplicaciones del mundo real.

- Prerrequisitos: Ninguno
- Examen GSEC: Examen GIAC Security Essentials (GSEC) es un examen de cinco horas con 180 preguntas. Se debe obtener una puntuación de 73% para aprobar.

GIAC SECURITY ESSENTIALS CERTIFICATION
GSEC

ANEXO 3. ANÁLISIS DE TAXONOMÍAS DE CIBERSEGURIDAD

Definición de taxonomía / Estudio de perfiles

A pesar de ser una industria relativamente nueva, en comparación a las de otros sectores, la ciberseguridad es una disciplina en evolución que se ha venido expandiendo considerablemente en los últimos años. La definición y categorización de perfiles, roles de trabajo y tareas asociadas ha ido incrementándose, y cobran mucha relevancia los conocimientos, capacidades y habilidades (KSA, por sus siglas en ingles) que permiten ejecutar eficientemente las tareas y el buen desempeño en el rol de trabajo.

Hay diferentes taxonomías a nivel internacional para perfiles de ciberseguridad, pero son pocas las que periódicamente se revisan o se amplían. Las diferentes estructuras, alcance, procedimientos, y las bases descriptivas utilizadas son el trabajo de diferentes organizaciones del sector público y privado que componen la cadena de valor de ciberseguridad, cuyos aportes constructivos mejoran la calidad y utilidad general de estos marcos de trabajo.

Para realizar una definición de perfiles de ciberseguridad que tenga coherencia con las características y particularidades del mercado europeo, se han analizado los siguientes *frameworks* como punto de partida para definir una estructura de referencia que detalle la naturaleza interdisciplinaria del trabajo en ciberseguridad.

Frameworks considerados.

European Cybersecurity Skills Framework (ECSF) Profiles

La Agencia de la unión europea para la ciberseguridad, ENISA[21], es la agencia dedicada a lograr un nivel común de ciberseguridad en toda Europa. Establecida en 2004 y reforzada por la Ley de Ciberseguridad de la UE, ENISA contribuye a la política de ciberseguridad de la UE, mejora la confiabilidad de los productos, servicios y procesos TIC con esquemas de certificación de ciberseguridad, coopera con los estados miembros y los organismos de la UE, y ayuda a Europa a prepararse para los retos de ciberseguridad del mañana. A través de compartir conocimiento, desarrollar capacidades y sensibilizar, la agencia trabaja con *stakeholders* clave para fortalecer la confianza en la economía conectada, impulsar la resiliencia de la infraestructura y, en última instancia, mantener la seguridad digital de la sociedad y los ciudadanos europeos.

46 https://www.enisa.europa.eu/

Para ENISA, el desarrollo de un *Framework* europeo de capacidades o *skills* en ciberseguridad es un paso fundamental hacia el futuro digital de Europa. Esta iniciativa tendría en cuenta las necesidades de la UE y cada uno de sus estados miembros, y el propósito de su desarrollo es 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, de manera que se pueda combatir una de las problemáticas más visibles de la industria: la brecha entre oferta y demanda de talento. Además, ayudaría a facilitar aún más el reconocimiento de *skills* relacionados con la ciberseguridad y respaldaría el diseño de programas de formación para el desarrollo de capacidades y carreras exitosas. En consecuencia, el ECSF apoyaría el empleo y la empleabilidad en puestos relacionados con la ciberseguridad.

Con esta finalidad, ENISA ha formado un grupo de trabajo designado al *European Cybersecurity Skills Framework* (ECSF) para reunir, a un grupo multidisciplinario de expertos con el objetivo de promover la armonización en el ecosistema de educación, capacitación y desarrollo de la fuerza laboral de ciberseguridad, promoviendo un lenguaje común europeo en el contexto de *skills* en ciberseguridad.

De esta manera, el alcance de este grupo de trabajo es asesorar y ayudar a ENISA en el desarrollo de un *Framework* que permita una comprensión común de los roles, competencias, conocimientos, capacidades y habilidades utilizadas por las personas, empleadores y los proveedores de formación en los estados miembros de la UE. Además, también podría crear conciencia identificando las brechas en el panorama actual de ciberseguridad que se pueden abordar con la creación de dicho marco de trabajo europeo.

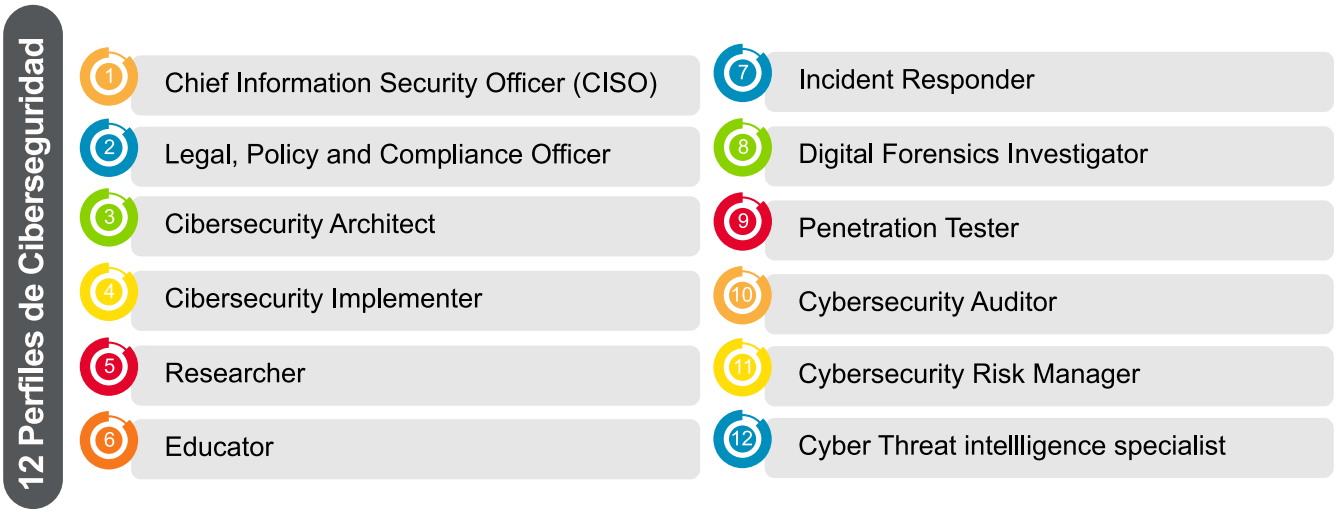


Figura 1 European Cybersecurity Skills Framework (ECSF) Profiles

Los perfiles que refleja el ECSF se describen mediante connotaciones o títulos alternativos observados en el mercado, una descripción general, tareas, funciones, conocimientos, capacidades clave y competencias. Estos perfiles proporcionan idealmente un lenguaje común y compartido

en Europa, se ajustan a las particulares del mercado, y se ponen a disposición para uso de múltiples *stakeholders*, por ejemplo, organizaciones del sector TIC, academias y otros proveedores de capacitación, asociaciones, profesionales, departamentos de recursos humanos, formuladores de políticas, entre otros.

Este *Framework* reconoce que los perfiles ECSF no son únicos, son más una descripción simple de un rol genérico para una amplia usabilidad. Por lo tanto, en la práctica, un trabajo de ciberseguridad puede constar de varios roles del ECSF y / o partes de estos roles.

European E-Competence Framework.

Este marco proporciona una referencia de 40 competencias requeridas y aplicadas en puestos de trabajo de las TIC. Al igual que otros *Frameworks* de su tipo, utiliza un lenguaje común para competencias, habilidades y niveles de capacidad que se pueden entender en todos los ámbitos en Europa.

Denominado comúnmente como e-CF, fue creado para su aplicación en empresas de servicios, usuarios y proveedores de tecnología, directores y departamentos de recursos humanos, así como también en instituciones educativas y organismos de formación, incluidos educación superior, e incluso para observadores del mercado y formuladores de políticas y otras organizaciones de los sectores público y privado.

Foco en Competencias.

El e-CF fue creado como una herramienta para apoyar el entendimiento mutuo en el sector y proporcionar transparencia del lenguaje a través de la articulación de las competencias requeridas y desplegadas por los profesionales de las TIC (incluidos tanto los profesionales como los *managers*).

La esencia de este trabajo, como su nombre indica, se encuentra en comprender las competencias como un componente de los roles de trabajo, más no como un sustituto de los roles ya definidos. En este sentido el *Framework* invita a pensar en las competencias como algo duradero en el tiempo (a pesar del rápido cambio de las tecnologías), que requieren de mantenerlas actualizas aproximadamente cada 3 años para mantener su relevancia frente al mercado. Estas competencias idealmente empoderan a los profesionales, en vez de limitarlos (a veces por las mismas dinámicas en los procesos en las compañías). Además,

se presentan en 4 dimensiones. Las *e-competences* en las dimensiones 1 y 2 se presentan desde la perspectiva de la organización en lugar de la perspectiva del individuo. La dimensión 3, que define los niveles de competencia relacionados con el *European Qualifications Framework* (EQF), es un puente entre las competencias organizacionales e individuales. Finalmente la dimensión 4, indica los conocimientos y habilidades que se relacionan con las competencias digitales.

Dimension 1 5 e-CF areas (A – E)	**Dimension 2** 40 e-Competences identified	**Dimension 3** e-Competence proficiency levels e-1 to e-5, related to EQF levels 3–8				
		e-1	e-2	e-3	e-4	e-5
A. PLAN	A.1. IS and Business Strategy Alignment				■	■
	A.2. Service Level Management			■	■	
	A.3. Business Plan Development			■	■	■
B. BUILD	B.1. Application Development	■	■	■		
	B.2. Component Integration		■	■	■	
	B.3. Testing	■	■	■	■	
C. RUN	C.1. User Support	■	■	■		
	C.2. Change Support		■	■		
	C.3. Service Delivery	■	■	■		
D. ENABLE	D.1. Information Security Strategy Development				■	■
	D.2. ICT Quality Strategy Development				■	■
	D.3. Education and Training Provision		■	■		
E. MANAGE	E.1. Forecast Development			■	■	
	E.2. Project and Portfolio Management		■	■	■	■
	E.3. Risk Management		■	■	■	

Figura 2 European Compenteces Framework (EQF)

Este marco define para cada una de las competencias el área dentro de la organización donde encaja mejor, una descripción genérica, los niveles de competencia relacionados con el (EQF), así como también los conocimientos y capacidades que debe evidenciar la persona.

En la siguiente imagen se muestra el ejemplo para la competencia de

Dimension 1 e-Comp. area	**B. BUILD**				
Dimension 2 e-Competence: Title + generic description	**B.3. Testing** Constructs and executes systematic test procedures for ICT systems or customer usability requirements to establish compliance with design specifications. Ensures that new or revised components or systems perform to expectation. Ensures meeting of internal, external, national and international standards; including health and safety, usability, performance, reliability or compatibility. Produces documents and reports to evidence certification requirements.				
Dimension 3 e-Competence proficiency levels e-1 to e-5, related to EQF levels 3 to 8	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
	Performs simple tests in strict compliance with detailed instructions.	Organises test programmes and builds scripts to stress test potential vulnerabilities. Records and reports outcomes providing analysis of results.	Exploits specialist knowledge to supervise complex testing programmes. Ensures tests and results are documented to provide input to subsequent process owners such as designers, users or maintainers. Accountable for compliance with testing procedures including a documented audit trail.	Exploits wide ranging specialist knowledge to create a process for the entire testing activity, including the establishment of internal standard of practices. Provides expert guidance and advice to the testing team.	–
Dimension 4 Knowledge examples *Knows/aware of/ familiar with*	K1 techniques, infrastructure and tools to be used in the testing process K2 the lifecycle of a testing process K3 the different sorts of tests (functional, integration, performance, usability, stress etc.) K4 national and international standards defining quality criteria for testing K5 web, cloud and mobile technologies and environmental requirements				
Skills examples *Is able to*	S1 create and manage a test plan S2 manage and evaluate the test process S3 design tests of ICT systems S4 prepare and conduct tests of ICT systems S5 report and document tests and results				

Figura 3. Ejemplo de competencia para testing. Fuente: ECF

El e-CF es un componente de gran relevancia en la estrategia de la Unión Europea sobre '*e-Skills for the 21st Century*'. Se promueve como una herramienta muy útil para impulsar las habilidades digitales y el reconocimiento de competencias y cualificaciones en todos los países y fomentar el profesionalismo de las TIC en Europa.

Cybersecurity Workforce Framework (NICE).

Este *Framework* sirve como un recurso de referencia fundamental para describir e intercambiar información sobre el trabajo de ciberseguridad, y los conocimientos, capacidades y habilidades (KSA) necesarios para llevar a cabo las tareas que pueden fortalecer la postura de ciberseguridad de una organización. El marco mejora la comunicación sobre la manera de identificar, contratar, formar y retener personas con talento en el campo de la ciberseguridad por medio de un léxico común y uniforme que clasifica y describe el trabajo en materia de ciberseguridad. Finalmente, sirve de referencia para que las organizaciones puedan preparar publicaciones o recursos adicionales que satisfagan sus necesidades de definir u ofrecer orientación sobre diferentes aspectos de la formación, planificación, capacitación y educación del personal de ciberseguridad.

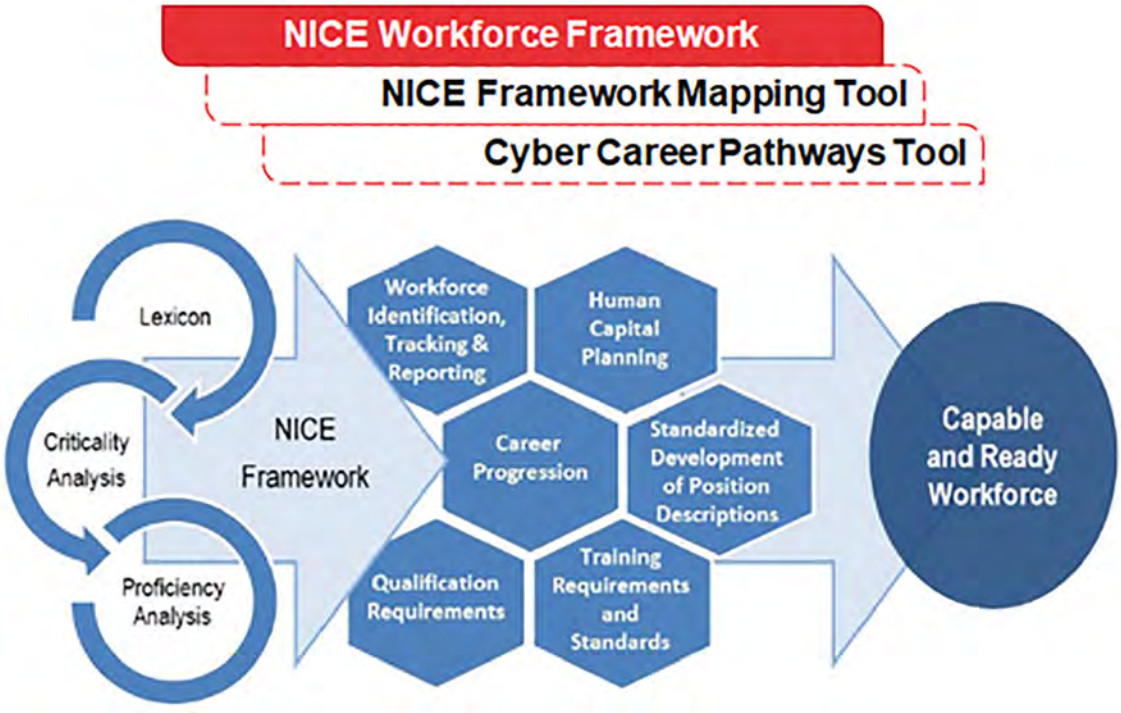


Figura 4. Cybersecurity Workforce Framework (NICE).

NICE además incorpora herramientas adicionales como el NICE *Framework Mapping Tool* que permiten a las organizaciones y profesionales navegar de una manera intuitiva y amigable todo el contenido del marco.

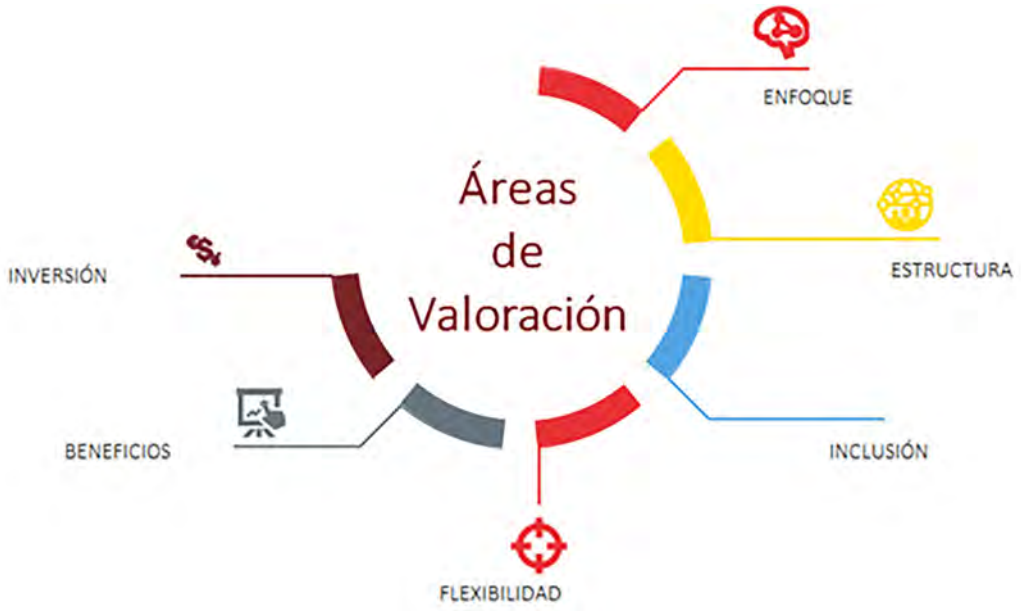


Figura 5. Áreas de valoración del Cybersecurity Workforce Framework (NICE).

Como parte del diagnóstico del talento en ciberseguridad, y para poder analizar el *Framework* de una manera más amplia, se han establecido unas áreas de valoración que nos ayuden a evaluar el contenido de esta herramienta.

Este marco es ampliamente abordado por organizaciones multinacionales, como JPMorgan, para la gestión del talento y un mejor diseño de sus estrategias de recursos humanos.

Áreas de valoración.

Enfoque: el Framework se basa en el lenguaje común para describir el trabajo en ciberseguridad entre los diferentes niveles jerárquicos de las organizaciones, logrando interoperabilidad y simplicidad, en un tema bastante complejo. Habilita la comunicación en los temas más críticos, de tal forma que es comprensible para todos los *stakeholders*.

Estructura: aborda un total de (7) categorías, (33) áreas de especialidad, (52) roles de trabajo, y una combinación de indicadores de capacidad en el proceso de formación de la fuerza laboral. Particularmente este *Framework* cuenta con funcionalidades, como el Mapping Tool y Cyber Career Pathways Tool, que permiten una mejor experiencia de uso y resultados. Esto es un indicativo de la robustez y de la alta probabilidad de que bajo esta herramienta, un profesional se desempeñe con éxito en roles de ciberseguridad.

Inclusión: herramienta donde confluyen múltiples actores, entre los más destacados, estudiantes, educadores, empleadores, profesionales, proveedores de capacitación y formuladores de políticas. Adicionalmente, es de gran atractivo para organizaciones de distinta tipología: grandes organizaciones, pymes, *start-ups*; y a través de diferentes verticales.

Flexibilidad: está diseñado para hacer uso de categorías (análisis, investigación, etc.) dependiendo de las necesidades de la fuerza laboral de cada organización. Es fundamental la combinación que permite a las empresas entre diferentes competencias (*Knowledge* + *skills*) que describen el sujeto, y las tareas a realizar con esas competencias (describen el trabajo). Esto permite comprender mejor los diferentes roles y finalmente poder diseñar mejores estrategias en la gestión del talento.

Beneficios: los beneficios de este *Framework* se pueden asociar con el objetivo de la estrategia nacional de ciberseguridad de identificar, reclutar, desarrollar y retener el talento de ciberseguridad. Más específicamente ayuda a explorar e identificar roles de trabajo, KSA (*Knowledge, Skills and Abilities*), y tareas valoradas por los empleadores, como identificar brechas críticas. También apoya al diseño de carreras y planes de estudios, a estudiantes y solicitantes de empleo en el diseño de su camino hacia un trabajo en ciberseguridad, entre otros.

Inversión: conocer de manera precisa los recursos asignados al proyecto NICE es complejo, sin embargo, se conoce que los recursos asignados para el gestor del *Framework*, es decir, CISA, alcanzan los 1.7 billones de dólares

En la siguiente imagen se muestra el ejemplo para el perfil de *Threat Analyst:*

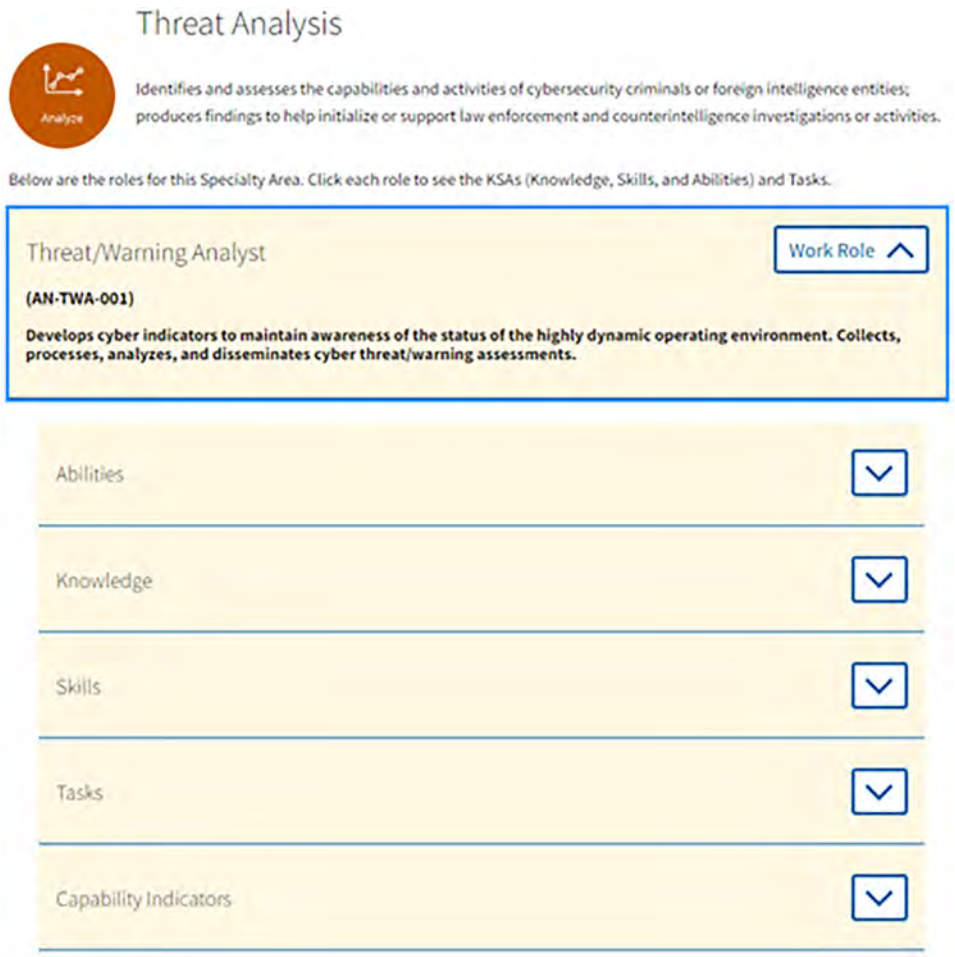


Figura 6. Ejemplo de perfil de perfil de Threat Analyst siguiendo el marco NICE

Para los diferentes *stakeholders* es posible acceder a la descripción de los diferentes perfiles, así como a las múltiples aptitudes que se esperan de un candidato que aspire a desempeñarse satisfactoriamente en una posición determinada.

Además del amplio contenido sobre KSA, también es importante notas que la herramienta proporciona, como indicadores de capacidad. Esto es definido como nivel básico, intermedio o avanzado, y describe para cada uno de los perfiles, el entrenamiento, la educación, capacitación o certificaciones que el candidato debe evidenciar para poder demostrar realmente que tiene las competencias para ejercer el trabajo.

Además de ayudar a recopilar datos de los empleados y su desempeño frente a ciertos roles definidos, se espera que este *Framework* sea un mecanismo que ayude a generar un mejor ajuste en los empleados dentro de las organizaciones, en base a sus capacidades, y finalmente que se puedan realizar planes de aprendizaje presupuestados de una manera más eficiente.

Career Framework for Security Professionals

Este *framework* implementado para los profesionales en posiciones gubernamentales en UK, busca fundamentalmente transformar la forma en que el gobierno aborda la problemática de la seguridad nacional al ser una guía esencial para respaldar el desarrollo, construir experiencia y apoyar más carreras a través del gobierno. Es un indicativo de cómo la fuerza laboral en ciberseguridad es una comunidad diversa de más de 11.500 profesionales que desarrollan y aportan conocimientos para gestionar y reducir los riesgos.

Los principales beneficios que aporta este *framework* son:

- Ayuda a los profesionales de la seguridad a identificar las necesidades de aprendizaje y proporciona un enfoque estructurado para la formación y el desarrollo.
- Dentro de la gestión de este *framework* se contempla darle más formalidad a la profesión, esto incluye aprendizaje vinculado a mentores de la industria y acreditación profesional.
- Ha sido clave para atraer, desarrollar y retener profesionales altamente cualificados en seguridad que necesita UK.

- Brinda un sentido real de pertenencia al usar un lenguaje común en todas las especialidades técnicas para eliminar barreras, reducir el trabajo en silos e inspirar a las personas a verse a sí mismas como parte de una comunidad más amplia y diversa.

En definitiva, el *Framework* se puede utilizar como base para abordar los planes de carrera para los profesionales, planificar cómo el personal puede acceder a las oportunidades de aprendizaje y desarrollo, y las descripciones de funciones pueden usarse para formar la base de las descripciones de los puestos de trabajo.

Especialidades y familias de roles de Ciberseguridad.

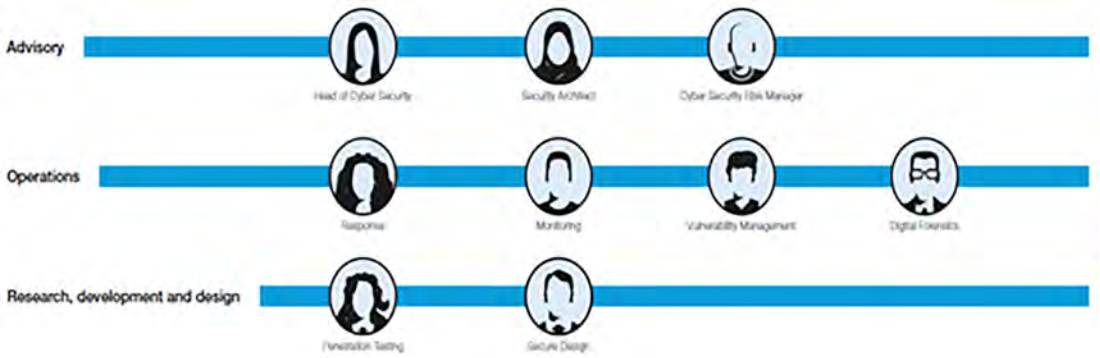


Figura 7. Especialidades y familias de roles de ciberseguridad según el Career Framework for Security Professionals.

El *Career Framework for Security Professionals* incluye 9 familias de roles y 25 roles en ciberseguridad, y los roles a su vez tienen niveles jerárquicos: *Associate, lead y principal.*

Además de esto, indica trayectorias profesionales por cada rol, con rutas indicativas de entrada y de salida hacia otros roles y especialidades y promoviendo el movimiento horizontal para los profesionales (fundamental para el reciclaje del talento desde la misma industria). Asimismo, a través de la funcionalidad *Grade to Role Mapping*, es un indicativo de los grados relacionados con los roles en ciberseguridad, por ejemplo, incluye grados del servicio civil y grados militares.

Un factor diferenciador podría ser que incluye ejemplos de perfiles reales de profesionales en el ámbito de la ciberseguridad, y cómo se han movido horizontalmente.

Finalmente, se podría afirmar que este marco es ideal para para generar coherencia entre las descripciones de los roles y los niveles de capacidad. Esto impulsa las trayectorias profesionales, guía el desarrollo, y con el tiempo se lograrán las acreditaciones asociadas. Se considera una herramienta clave para las áreas de RR.HH., proporcionando los criterios a utilizar en todo el proceso de *recruiting*.

European Skills, Competences, Qualifications and Occupations (ESCO).

ESCO es la clasificación europea multilingüe de habilidades, competencias, cualificaciones y ocupaciones y funciona como un diccionario, describiendo, identificando y clasificando ocupaciones profesionales y habilidades relevantes para el mercado laboral y la educación y formación de la UE. Estos conceptos y las relaciones entre ellos pueden entenderse mediante sistemas electrónicos, lo que permite que diferentes plataformas en línea utilicen la ESCO para servicios, como vincular a los solicitantes de empleo con puestos de trabajo en función de sus habilidades, sugerir capacitaciones a las personas que desean hacer *reskilling* o *upskilling*, etc.

ESCO proporciona descripciones de 2942 ocupaciones y 13.485 habilidades relacionadas con estas ocupaciones, traducidas a 27 idiomas (todos los idiomas oficiales de la UE más islandés, noruego y árabe).

El objetivo de ESCO es apoyar la movilidad laboral en Europa y, por lo tanto, un mercado laboral más integrado y eficiente, ofreciendo un 'lenguaje común' sobre ocupaciones y habilidades que puedan ser utilizadas por diferentes partes interesadas en temas de empleo y educación y formación.

The Cybersecurity Body of Knowledge (CyBoK).

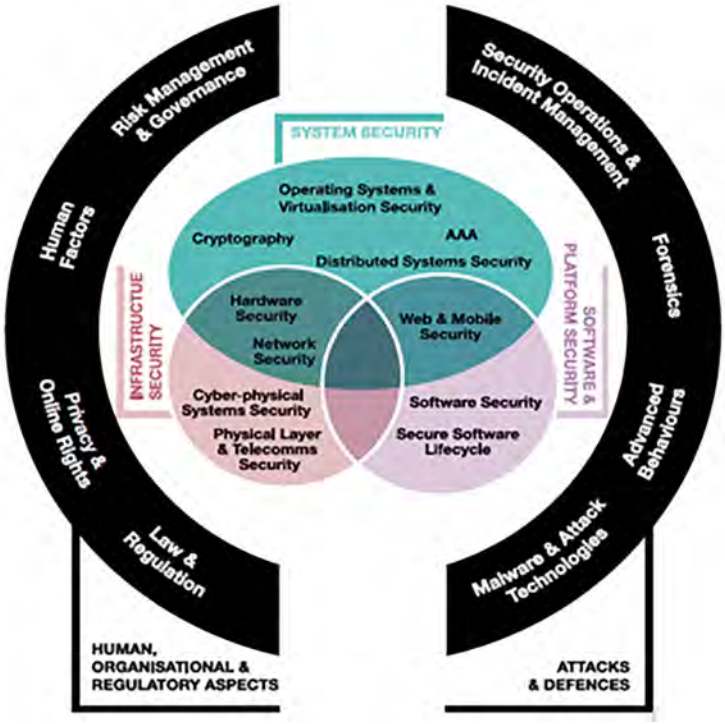


Figura 8. The Cybersecurity Body of Knowledge (CyBoK).

El CyBoK es un recurso único desarrollado en UK, que proporciona por primera vez un 'cuerpo de conocimiento' subyacente que abarca la amplitud y profundidad de la ciberseguridad.

El objetivo principal del proyecto es codificar el conocimiento en ciberseguridad que sustenta la profesión. Además, el proyecto permite el desarrollo de trayectorias profesionales y planes de estudio para la educación. Cuenta con 19 áreas de conocimiento y la versión 1.0 de CyBoK se publicó el 31 de octubre de 2019 y se lanzó formalmente en enero de 2020. La siguiente fase del proyecto se extendió hasta marzo de 2021 y se centra en la difusión y aplicación de CyBoK.

Para el Centro Nacional de Ciberseguridad en UK (NCSC), el CyBoK es una guía patrocinada que destila el conocimiento de los principales expertos en ciberseguridad del mundo. Reconocen que no es una lectura sencilla, pero a través de ese intercambio de conocimientos, se alcanza el fortalecimiento conjunto. De igual forma, se busca motivar a otros a usar CyBoK para ayudar en el diseño de materiales de cursos de ciberseguridad en educación, capacitación y profesionalización.

El CyBoK es un recurso que promueve la narrativa alrededor de la ciberseguridad y por ende es una base esencial como estándar de desarrollo del talento. Sin embargo, el CyBoK en sí no define perfiles de ciberseguridad, ni los conocimientos o capacidades que los profesionales deben tener, más sí menciona para la parte de material de formación o entrenamiento, sitios disponibles en internet de manera gratuita. Entre ellos, se encuentra el *Trustworthy Software Foundation*, que proporciona una biblioteca de recursos de materiales de concientización y orientación dirigida a quienes enseñan principios de *software* confiable, quienes buscan aprender sobre *software* confiable y quienes desean asegurarse de que el *software* que utilizan sea confiable. Los recursos disponibles incluyen una mezcla de documentos, videos, animaciones y estudios de casos. Además, también hace referencia al *US National Institute of Standards and Technology* (NIST) y al *Framework NICE*, donde lo describe como el marco que proporciona los recursos en materia de conocimientos, capacidades y habilidades (KSA) así las tareas para una serie de roles en ciberseguridad.

Cybersecurity Curricula 2017 by Association for Computing Machinery (ACM) en colaboración con IEEE Computer Society (IEEE-CS), Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC) y The International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8).

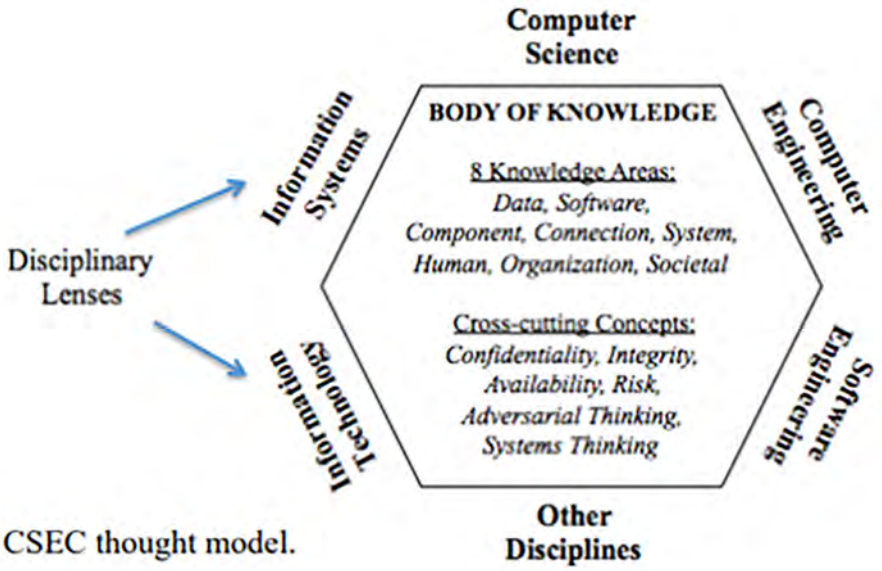


Figura 9. CSEC Thought model

Hay una alta demanda de talento, y es inmediata y creciente. Con el fin de desarrollar el talento requerido, los departamentos académicos de todo el espectro de disciplinas informáticas están lanzando iniciativas para establecer nuevos programas de ciberseguridad o cursos y contenido dentro de los programas existentes. Ya sea que desarrollen programas completamente nuevos, definan nuevas concentraciones dentro de los programas existentes o aumenten el contenido de cursos existente, estas instituciones necesitan orientación curricular basada en una visión integral del campo de la ciberseguridad, las demandas específicas de la disciplina base y la relación entre el plan de estudios y *frameworks* de la fuerza laboral en ciberseguridad.

En agosto de 2015, la (ACM) reconoció esta necesidad urgente y tomó medidas para reunir un Grupo de Trabajo Conjunto (*Joint Task Force*) sobre educación en ciberseguridad (CSEC2017) con otras sociedades de computación profesionales y científicas para desarrollar una guía curricular integral en educación en ciberseguridad.

Visión de CSEC2017: el volumen curricular de CSEC2017 será el principal recurso de contenido curricular integral de ciberseguridad para instituciones académicas globales que buscan desarrollar una amplia gama de ofertas de ciberseguridad a nivel possecundario.

Misión de CSEC2017: la misión tiene dos partes:

- Desarrollar una guía curricular integral y flexible en educación en ciberseguridad que respaldará el desarrollo de programas futuros y los esfuerzos educativos asociados en el nivel possecundario.
- Producir un volumen curricular que estructura la disciplina de ciberseguridad y brinda orientación a las instituciones que buscan desarrollar o modificar una amplia gama de programas, concentraciones y / o cursos en lugar de un documento prescriptivo para respaldar un solo tipo de programa.

Este modelo muestra unas áreas de conocimiento que sirven como la estructura organizativa básica para el contenido de ciberseguridad. Cada área de conocimiento se compone de conocimientos críticos de gran importancia dentro y a través de múltiples disciplinas basadas en la computación. Las áreas de conocimiento están estructuradas como cubos flexibles en el *thought model* para permitir la expansión y contracción del contenido según sea necesario.

Skills Framework version 2.4, Chartered Institute of Information Security (CIISec).

Figura 10. Skills Framework version 2.4, Chartered Institute of Information Security (CIISec).

El *Skills Framework* de CIISec describe la gama de competencias que se esperan de los profesionales de seguridad de la información y aseguramiento de la información en el desempeño efectivo de sus funciones. Fue desarrollado a través de la colaboración entre organizaciones del sector público y privado y académicos y líderes de seguridad de renombre mundial. Este marco define las habilidades y capacidades que se esperan de los profesionales de la seguridad en la aplicación práctica y no solo una evaluación de sus conocimientos.

A continuación, se muestra a manera de ejemplo específico para la sección *Information Security Governance and Management,* donde detalla los principios bajo los cuales se rige este tipo de rol y las diferentes capacidades que la persona debería tener teniendo en cuenta los diferentes niveles.

SECTION A Security Discipline: Information Security Governance and Management		
Skills Group	Principles	Example Skills
A1 – Governance	Directs, oversees, designs, implements or operates within the set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage Cyber and Information Security at an enterprise level, supporting an organisation's immediate and future regulatory, legal, risk, environmental and operational requirements and ensuring compliance with those requirements.	**Level 1:** Can describe the principles of Information Security Governance. Can list the potential impacts that occur where poor Information Governance has been observed.
		Level 2: Can explain the basic principles of Information Security Governance and how it applies within an organisation.
		Level 3: Understands local (organisation or project) Information Security Governance processes. Undertakes Information Security Governance tasks under supervision. Recognises and addresses non-compliance and makes recommendations for change.
		Level 4: Contributes to the development, revision or implementation of Information Security Governance processes.
		Level 5: Leads the development, revision or implementation of Information Security Governance processes.
		Level 6: Responsible for the development, revision and implementation of Information Security Governance processes across a range of clients or within a large corporate organisation.

Esta herramienta describe cerca de 35 perfiles y está organizado en diferentes secciones. Los profesionales de ciberseguridad requieren una combinación de habilidades técnicas, conocimiento específico, inteligencia social, además de poder demostrar que son confiables y resilientes. La complejidad multidisciplinar de la profesión une las ciencias físicas y de la computación, las matemáticas, la economía, el derecho y la psicología. Idealmente, el marco aborda una amplia gama de *skills* en todas esas áreas relevantes.

National Infocomm Competency Framework.

Este marco de competencias (NICF) fue desarrollado como un esfuerzo conjunto entre *SkillsFuture Singapore* (SSG), *Infocomm Media Development Authority* (IMDA) y *stakeholders* estratégicos en el sector (TIC). NICF se actualizó por última vez en 2014 y, hasta la fecha, se han identificado 631 estándares de competencia para 334 puestos de trabajo.

SkillsFuture Singapore también tiene iniciativas con compañías de la industria de tecnología donde introducen o lanzan programas de manera conjunta para aportar a la formación y entrenamiento de profesionales. Un ejemplo de esto lo han hecho con IBM en septiembre de 2020, mediante una iniciativa que busca entrenar a 800 profesionales que se encuentran en nivel intermedio de su carrera.

Los recursos que tiene a disposición los organizan para individuos, empleadores, proveedores de entrenamiento, sin embargo, no ha sido posible identificar en el sitio oficial web una taxonomía clara que defina perfiles para ciberseguridad. Por el contrario, es una plataforma con diversos

recursos para desarrollar una generación de profesionales en Singapore de líderes empresariales, apoyando la adquisición de competencias y experiencias.

The Proposal for a European Cybersecurity Taxonomy by European Commission Joint Research Centre (JRC).

En septiembre de 2018, la Comisión propuso un reglamento por el que se crea un centro europeo de competencia industrial, tecnológica y de investigación en ciberseguridad con una red de centros nacionales de coordinación. La misión general del Centro de Competencia y la Red (CCCN) es ayudar a la Unión Europea a retener y desarrollar las capacidades tecnológicas e industriales de ciberseguridad necesarias para asegurar su mercado único digital. Esto va de la mano con el objetivo clave de aumentar la competitividad de la industria de la ciberseguridad y convertir la ciberseguridad en una ventaja competitiva de otras industrias europeas.

En este contexto, se publicó la primera versión de la taxonomía propuesta con el objetivo de alinear las terminologías, definiciones y dominios de ciberseguridad. La taxonomía se utilizó luego para la categorización y el mapeo de los centros de ciberseguridad de la UE existentes (por ejemplo, organizaciones de investigación, laboratorios, asociaciones, instituciones académicas, grupos, centros operativos, etc., de acuerdo con su experiencia en ciberseguridad en dominios específicos). Con base en este primer análisis, también se realizó una encuesta en la que participaron más de 600 instituciones y registraron su experiencia en ciberseguridad.

Esta taxonomía parte de la base de que la ciberseguridad es una disciplina compleja y multifacética y por ende debe agruparse en múltiples dimensiones. Así, intenta capturar no solo los dominios de investigación centrales y tradicionales, sino también sectores y aplicaciones. Las 3 dimensiones son:

- Dominios de investigación: representan áreas de conocimiento relacionadas con diferentes aspectos de la ciberseguridad. Dada la naturaleza multidisciplinar de la ciberseguridad, dichos dominios están destinados a cubrir diferentes áreas, incluidos los aspectos humanos, legales, éticos y tecnológicos.
- Sectores: para resaltar la necesidad de considerar diferentes requisitos y desafíos de ciberseguridad (desde una perspectiva humana, legal y ética) en escenarios como el energético, el transporte o el sector financiero.
- Tecnologías y los casos de uso: representan los habilitadores tecnológicos para potenciar el desarrollo de los diferentes sectores. Están relacionados con dominios de ciberseguridad que abarcan aspectos tecnológicos.

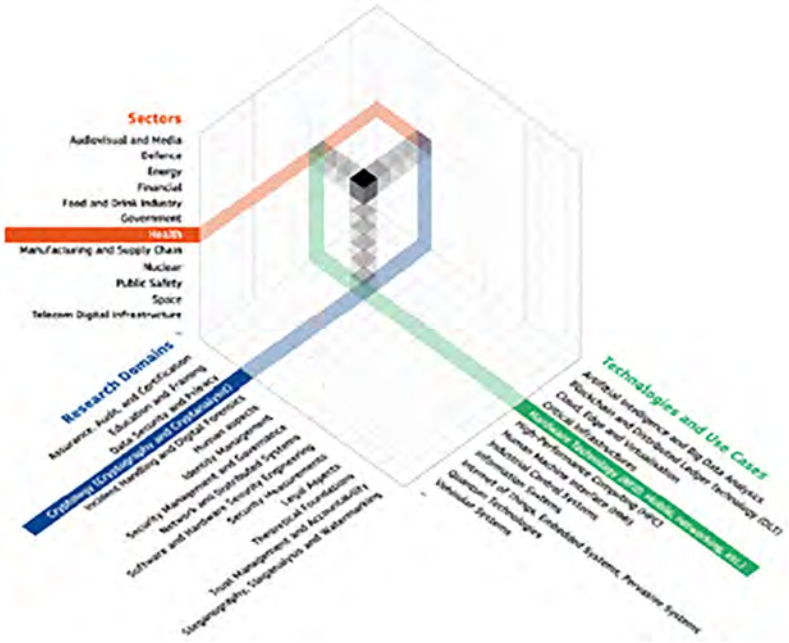


Figura 11. Propuesta de la European Commission Joint Research Centre (JRC).

Se espera que esta taxonomía tridimensional permita garantizar una alineación con el panorama regulador europeo, asegurar su exhaustividad (fusionando los subdominios necesarios para resaltar diferentes clasificaciones y evitar la redundancia en términos y definiciones.

The SPARTA Cybersecurity Skills Framework (SPARTA CSF).

Este proyecto es financiado por la Comisión Europea y cuenta con 44 *partners* de 14 países diferentes. SPARTA designa sus esfuerzos para analizar el estado del conocimiento sobre la gestión de competencias, revisando las mejores prácticas y proponiendo el camino a seguir con el desarrollo de un marco de competencias en ciberseguridad basado en la UE. Se ha descubierto que la taxonomía de dominios de ciberseguridad del *Joint Research Centre* (JRC) y la Iniciativa Nacional para la Educación en Ciberseguridad (NICE) son los puntos de partida más razonables, ya que proporcionan una estructura integral y flexible para incorporar las realidades específicas de la UE y el panorama de habilidades emergentes.

Este marco, se basa en la estructura del NICE *Framework*, modificado con especificaciones para la UE, y consolidado con la taxonomía del JRC. Así uno de los objetivos fundamentales de SPARTA es preparar una clasificación práctica utilizable para:

- Describir programas educativos dentro y fuera de la UE en el ámbito de la ciberseguridad.
- Identificar las brechas en el desarrollo de la fuerza laboral: qué áreas de conocimiento están presentes y cuáles carecen de programas educativos.
- Proporcionar una herramienta práctica para los planificadores de la

educación sobre cómo comprender las brechas existentes y cómo modificar los programas educativos para responder a estas brechas.

- Proporcionar herramientas para la discusión de los conocimientos y habilidades (KSA) que se requerirán con la aparición de nuevos retos y nuevas tecnologías.

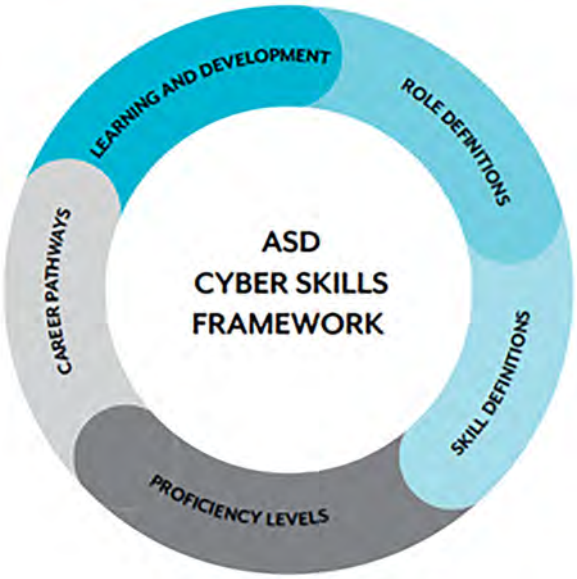
JRC taxonomy subdomains	NICE Framework						
Subdomains	Securely provision (SP)	Operate and Maintain (OM)	Oversee and Govern (OV)	Protect and Defend (PR)	Analyze (AN)	Collect and Operate (CO)	Investigate (IN)
Assurance, Audit, and Certification	X		X	X			
Data Security and Privacy	X	X	X				
Education and Training			X				
Operational Incident Handling and Digital Forensics							X
Human Aspects	X		X	X	X	X	

Figura 12. Consolidación de los subdominios de la taxonomía del Joint Research Centre con las áreas de especialidad del Framework NICE mework NICE

La tabla muestra la forma en la que se consolida o se fusionan los subdominios de la taxonomía del *Joint Research Centre* con las áreas de especialidad del *Framework NICE.*

Australian Signals Directorate (ASD) Cyber Skills Framework.

Este *Framework* de habilidades de ciberseguridad define los roles y capacidades que son esenciales para las misiones cibernéticas y que pueden usarse, tanto en contextos de seguridad como ofensivos. El marco permite la contratación de especialistas de ciberseguridad, proporciona una vía de desarrollo para el personal actual y futuro y alinea el conocimiento, habilidades y los atributos con los estándares de la industria nacional e internacional. Este marco es relevante para el gobierno, la industria y la academia en general, y puede implementarse y usarse como una herramienta para comprender y perfilar las habilidades de ciberseguridad en cualquier organización.



Los fundamentos del ASD Cyber Skills Framework se construyen sobre los siguientes elementos centrales.

- 9 definiciones de roles de ciberseguridad.
- 9 definiciones de capacidades y *skills*.
- 6 niveles de competencia.
- 4 trayectorias profesionales.
- 1 ruta de aprendizaje y desarrollo.

Los 9 roles se agrupan a su vez en 4 disciplinas.

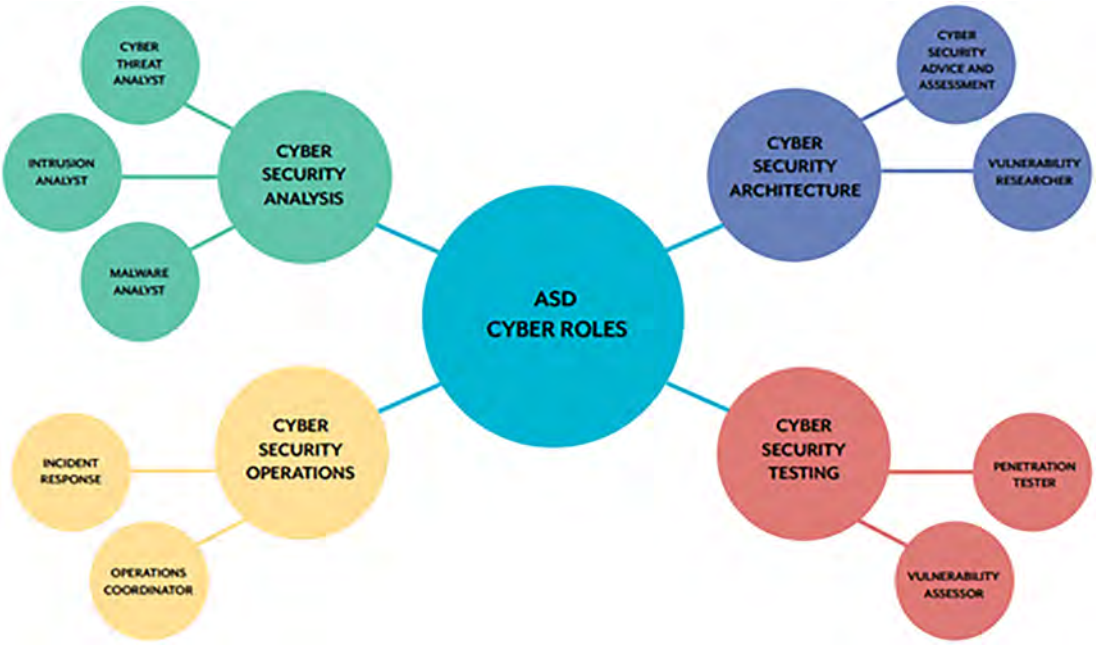


Figura 13. Agrupación de los roles con disciplinas en el modelo ASD Cyber Skills Framework

Se han definido nueve capacidades básicas que se utilizan para agrupar las habilidades relacionadas en el *Framework*. Las capacidades y la herramienta utilizada como referencia es el *CIISec Skills Framework*, descrito anteriormente.

Para comprender cómo usar y aplicar correctamente esta herramienta, cada función definida tiene las capacidades requeridas y las habilidades asociadas enumeradas. El nivel de competencia requerido para realizar esa habilidad para ese rol se define contra el nivel de ASD usando los indicadores a la derecha.

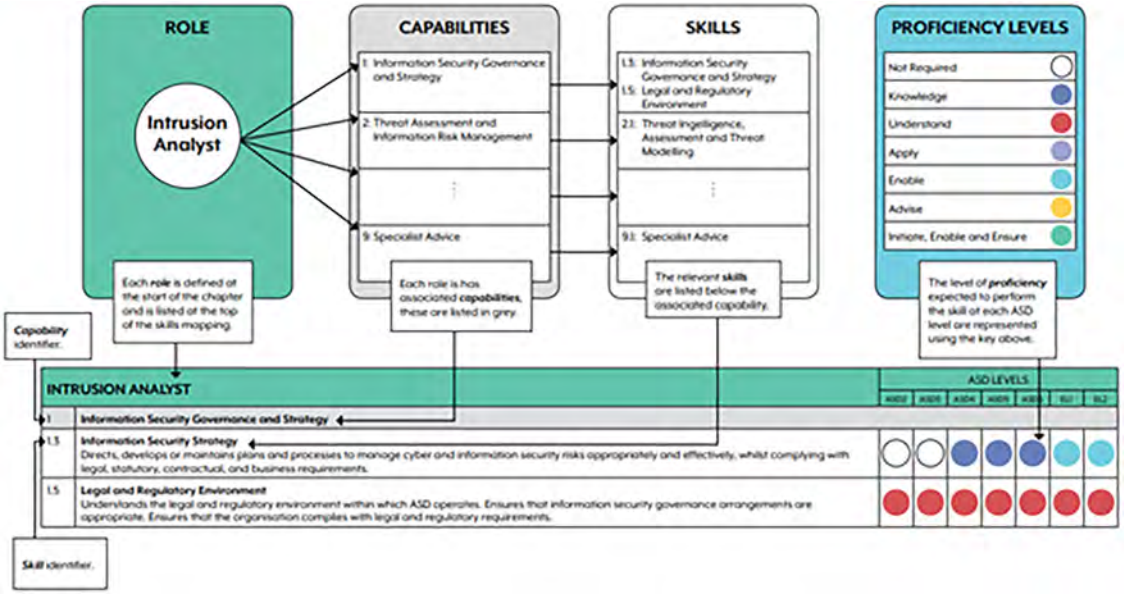


Figura 14. Racional para entender y aplicar correctamente la herramienta de ASD Cyber Skills Framework

Hay una notable similitud en la estructura de este *Framework* con el desarrollado por NICE en EE.UU, ya que en ambos casos se logra definir de manera amplia y detallada el trabajo en ciberseguridad. Pero, además este marco, logra integrar elementos de otros marcos desarrollados por CIISec y *Digital Career Pathways* que están más orientados al desarrollo del talento en los profesionales. Las definiciones que logran un lenguaje común entre los *stakeholders* es lo que realmente aporta valor y permite un mejor entendimiento de la fuerza laboral en ciberseguridad.

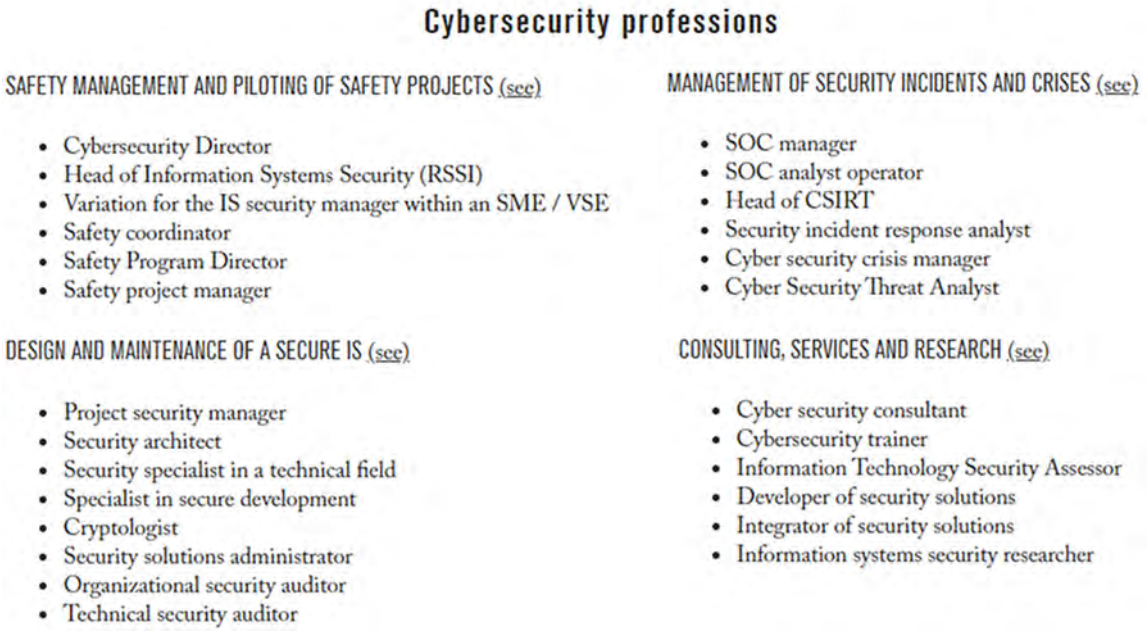
Panorama des métiers de la cyber sécurité by ANSSI.

El panorama de las profesiones de la ciberseguridad tiene como objetivo orientar a las empresas en su política de contratación, apoyar a los responsables de la formación y animar a los estudiantes o empleados a la reconversión (reciclaje hacia posiciones de ciberseguridad). Ofrece una visión clara y compartida de los distintos oficios del sector para estructurar el mercado laboral de la ciberseguridad.

El propósito de esta herramienta es un trabajo de exploración, caracterización y puesta en común en torno a las profesiones, establecidas o

emergentes, que constituyen el amplio y variado campo de la seguridad digital. Profundizar en las profesiones, misiones, habilidades, áreas de intervención y las tendencias de desarrollo, son todas las dimensiones sobre las que es necesario tratar de consolidar visiones compartidas para agilizar e impulsar un mercado laboral de la ciberseguridad en auge.

La lista de ocupaciones actualizada es un esfuerzo conjunto del ámbito público y privado, organizaciones de diferentes tamaños, la comunidad educativa y otros organismos. Cabe resaltar que al igual que en otros marcos, la definición de perfiles es compleja y en muchos casos puede haber inconsistencias o variaciones de una organización a otra. Por eso, el objeto de este panorama no es definir un estándar, sino más bien desarrollar un inventario compartido a quienes deseen usar esta herramienta. A continuación, se aprecian algunas de estas ocupaciones:



Cybersecurity professions

SAFETY MANAGEMENT AND PILOTING OF SAFETY PROJECTS (see)

- Cybersecurity Director
- Head of Information Systems Security (RSSI)
- Variation for the IS security manager within an SME / VSE
- Safety coordinator
- Safety Program Director
- Safety project manager

MANAGEMENT OF SECURITY INCIDENTS AND CRISES (see)

- SOC manager
- SOC analyst operator
- Head of CSIRT
- Security incident response analyst
- Cyber security crisis manager
- Cyber Security Threat Analyst

DESIGN AND MAINTENANCE OF A SECURE IS (see)

- Project security manager
- Security architect
- Security specialist in a technical field
- Specialist in secure development
- Cryptologist
- Security solutions administrator
- Organizational security auditor
- Technical security auditor

CONSULTING, SERVICES AND RESEARCH (see)

- Cyber security consultant
- Cybersecurity trainer
- Information Technology Security Assessor
- Developer of security solutions
- Integrator of security solutions
- Information systems security researcher

El panorama ofrece en francés una descripción más detallada de cada una de estas profesiones de la ciberseguridad.

Cyber security skills in the UK labor market, Department for Digital, Culture, Media, and Sport and Ipsos Mori.

Esta investigación explora la naturaleza y el alcance de las brechas de habilidades de ciberseguridad (personas que carecen de las habilidades adecuadas) y la escasez de habilidades (falta de personas disponibles para trabajar en puestos de trabajo de ciberseguridad) utilizando una combinación de:

- Encuestas representativas con empresas del sector cibernético y la población en general que tiene relevancia en UK (empresas, organizaciones benéficas y organizaciones del sector público). El foco especial está en las empresas.
- Investigación cualitativa con proveedores de formación, empresas

de ciberseguridad y grandes organizaciones de diversos sectores.

- Un análisis secundario de las ofertas de trabajo de ciberseguridad en la base de datos de *Burning Glass Technologies*.

Este reporte refleja de manera estadística un panorama claro del mercado laboral en ciberseguridad en UK. Desde el lado de la demanda explora las personas que cubren la ciberseguridad en todas las organizaciones, incluidos los títulos de sus puestos, las trayectorias profesionales en el puesto y las calificaciones que poseen. Basado en encuestas a las empresas, han pedido a las organizaciones participantes que elijan al miembro del personal más responsable de su seguridad cibernética para completar la encuesta. Estas personas no son necesariamente ciberprofesionales y la encuesta explora hasta qué punto esos roles se etiquetan formalmente como roles de ciberseguridad.

Este informe muestra de manera acertada como está estructurado el mercado laboral de ciberseguridad, además de reflejar, por ejemplo, las certificaciones o acreditaciones que están siendo más visibles entre los profesionales. Además de esto, analiza el mercado laboral desde la óptica de la diversidad, para ver desde el punto de vista de género, grupo étnico u otros colectivos con capacidades especiales, cómo estos grupos poco representados en la industria han venido jugando un rol cada vez más importante para las organizaciones y la industria en general.

Algunos de los datos de este reporte indican que el 95% de las grandes empresas consideran la ciberseguridad una alta prioridad. Los hallazgos también muestran que la gran mayoría de organizaciones fuera de la industria de la ciberseguridad no sienten que necesitan habilidades técnicas avanzadas. Por lo tanto, es probable que la demanda actual de tales habilidades se concentre entre las organizaciones más grandes y de la misma industria.

A continuación, se presenta una tabla de análisis con los *Frameworks* que se consideran de mayor relevancia para la industria de la ciberseguridad a nivel europeo.

Framework	Enfoque / Estructura	Claridad en la Definición de Perfiles / Beneficios	Grupos que impacta	Flexibilidad / Facilidad de Implementación	Compatibilidad con Otras Taxonomías
European Cybersecurity Skills Framework (ECSF) Profiles	Los perfiles que refleja el ECSF se describen mediante connotaciones o títulos alternativos observados en el mercado, una descripción general, tareas, funciones, conocimientos, capacidades clave y competencias, y se ponen a disposición para uso de múltiples stakeholders.	El ECSF actualmente cuenta con 12 perfiles asociados a la ciberseguridad. Estos perfiles vienen enumerados para facilitar la referenciación a un rol en particular. La estructura define, entre otras cosas: propósito del rol, misión, tareas, aportes, y naturalmente las capacidades.	• Organizaciones del sector TIC • Academia y otros proveedores de capacitación • Asociaciones • Profesionales • Departamentos de recursos humanos • Formuladores de políticas	ENISA ha formado un grupo multidisciplinario de expertos con el objetivo de promover la armonización en el ecosistema y cadena de valor de la ciberseguridad, todo alrededor del contexto de las capacidades. Esto permite abordar de manera inclusiva puntos relevantes tanto para las empresas como las intituciones educativas.	No menciona otras taxonomías, sin embargo, destaca que el grupo de trabajo designado para el desarrollo de este marco es altamente diverso. Incluye perfiles académicos, miembros de importantes organismos como OTAN (grupo de ciberdefensa), multinacionales del sector privado como P&G, lo cual denota un caracter integral en su enfoque.
European E-Competence Framework	Este marco proporciona una referencia de 40 competencias requeridas y aplicadas en puestos de trabajo de las TIC. Utiliza un lenguaje común para competencias, habilidades y niveles de capacidad que se pueden entender en todos los ámbitos en Europa.	El e-Competence framework denota que una competencia puede ser un componente de un rol de un puesto de trabajo, más no un sustituto del puesto de trabajo en sí. Las competencias no representan el contenido completo de un puesto de trabajo y se pueden agregar al contenido esencial del perfil de trabajo. Por otra parte, e-Competence tiene un documento separado para indicar 30 perfiles en el sector TIC que conecta luego con estas competencias.	• Administración pública. • Empresas privadas (incluidas pymes). • Empresas del sector TIC. • Profesionales de ciberseguridad en todos los sectores. • Instituciones educativas. • Proveedores de certificación. • Formuladores de políticas. • Población en general.	Este framework de competencias se ha desarrollado y desplegado en diferentes talleres donde han participado expertos del sector TIC a nivel internacional, así como expertos en RRHH. En estos espacios y en diferentes ediciones se logrado consolidar el feedback de diferentes stakeholders para lanzar una guía de uso para la aplicación del framework que facilita su implementación.	No menciona otras taxonomías pero sí articula el contenido con otros trabajos desarrollados dentro del marco ecomptecenes EU y el Comité Europe de Normalización (CEN).
Cybersecurity Workforce Framework (NICE)	Este Framework sirve como un recurso de referencia fundamental para describir e intercambiar información sobre el trabajo de ciberseguridad, y los (KSAs) necesarios para llevar a cabo las tareas que pueden fortalecer la postura de ciberseguridad de una organización. Mejora la comunicación sobre la manera de identificar, contratar, formar y retener personas con talento por medio de un léxico común y uniforme que clasifica roles.	Aborda un total de (7) categorías, (33) áreas de especialidad, (52) roles de trabajo, y una combinación de indicadores de capacidad en el proceso de formación de la fuerza laboral. Particularmente este Framework cuenta con funcionalidades como el Mapping Tool y Cyber Career Pathways Tool, que permiten una mejor experiencia de uso y resultados.	• Administración pública. • Empresas privadas (incluidas pymes). • Empresas del sector TIC. • Profesionales de ciberseguridad en todos los sectores. • Instituciones educativas. • Educadores. • Proveedores de certificación. • Formuladores de políticas. • Reclutadores o áreas de RRHH.	Está diseñado para hacer uso de las 7 categorías dependiendo de las necesidades de la fuerza laboral de cada organización. Es fundamental la combinación que permite a las empresas entre diferentes competencias (Knowledge + skills) que describen el sujeto, y las tareas a realizar con esas competencias (describen el trabajo). Esto permite comprender mejor los diferentes roles y finalmente poder diseñar mejores estrategias en la gestión del talento.	Al ser un proyecto único en su clase, que se viene revisando con los diferentes stakeholders que involucra, este framework no menciona otras taxonomías. Incluso, en la misma oficina de gestión de personal de EE.UU. Han generado un memorando para establecer procedimientos e implementar la estructura de códigos del framework NICE. Esto indica que otros organismos se están adaptando a los parámetros del framework.

A continuación, se presenta una tabla de análisis con los *Frameworks* que se consideran de mayor relevancia para la industria de la ciberseguridad a nivel europeo.

Framework	Enfoque / Estructura	Claridad en la Definición de Perfiles / Beneficios	Grupos que Impacta	Flexibilidad / Facilidad de Implementación	Compatibilidad con Otras Taxonomías
The Sparta Cybersecurity Skills Framework (SPARTA CSF)	Sparta es una nueva red (44 partners en 14 países) de competencia en ciberseguridad, respaldada por el programa H2020 de la UE. El trabajo se basa encontrar soluciones y maneras de gestionar situaciones a través de una red de personas con diferentes skills, intereses, cultura y trayectorias. El framework de skills es un trabajo realizado que hace parte del bloque de training y awareness en ciberseguridad.	La definición de perfiles está basada en el Framework NICE con el argumento de que esta herramienta proporciona el mejor ejemplo de las características distintivas necesarias para permitir un uso viable de las categorías de roles al tratar cuestiones estratégicas relacionadas con el desarrollo de habilidades en ciberseguridad.	• Profesionales de ciberseguridad. • Academia. • Administración pública. • Empresas privadas.	El framework describe cómo el uso y los beneficios varía con base en por ejemplo una institución educativa o una empresa. Se ha llevado una fase de validación donde han puesto a prueba la usabilidad del framework en diversos grupos de interés lo que indica el amplio alcance que tiene.	Sparta ha realizado un exhaustivo estudio de diferentes marcos de capacidades tanto a nivel europeo como fuera de la UE. Esto indica que han analizado desde diferentes perspectivas la definición de perfiles y los respectivos conocimientos y skills para posteriormente consolidar bajo su propia metodología, adaptando este framework a la casuística de la UE.
The Proposal for a European Cybersecurity Taxonomy by European Commission Joint Research Centre (JRC)	El Joint Research Centre llevó a cabo un análisis exhaustivo de las clasificaciones de investigación del dominio de la ciberseguridad existentes y trató de fusionarlas en un esquema de clasificación integral que define el dominio de la ciberseguridad con respecto al panorama de la UE, evitando la redundancia de términos, definiciones y dominios.	El (JRC) desarrollo una taxonomía empleando una matriz tridimensional: • Dominios de ciberseguridad / investigación (14): Aspectos tecnológicos sin aplicación específica. • Sectores / Industrias (15): Desafíos por sectores o industrias. • Aplicaciones y tecnologías (17): Tecnologías que requieren protección como IoT, Cloud, etc.	Se enfoca en categorizar la experiencia de las organizaciones considerando las 3 dimensiones. Esto se traduce a la experiencia ya bien sea específica o genérica que puedan tener los usuarios. • Organizaciones de investigación. • Laboratorios. • Asociaciones. • Instituciones académicas. • Centros de operación.	Se considera un framework completo que cubre casi todos los aspectos de la ciberseguridad, pero de igual forma se pueden agregar elementos al framework si es necesario.	La taxonomía definida es reconocida por Sparta y múltiples stakeholders de la UE.
Australian Signals Directorate (ASD) Cyber Skills Framework	Este Framework de habilidades de ciberseguridad define los roles y capacidades que son esenciales para las misiones cibernéticas y que pueden usarse tanto en contextos de seguridad como ofensivos. El marco permite la contratación de especialistas de ciberseguridad, proporciona una vía de desarrollo para el personal actual y futuro y alinea el conocimiento, habilidades y los atributos con los estándares de la industria nacional e internacional.	Los cimientos de este marco en cuando a la definición de roles es: • 9 definiciones de roles de ciberseguridad. • 9 definiciones de capacidades y habilidades. • 6 niveles de competencia. • 4 planes de carrera. • 1 plan de desarrollo y aprendizaje.	• Administración pública. • Profesionales de ciberseguridad. • Academia. • Organizaciones privadas.	Está diseñado para ser utilizado como un documento guía y sus diferentes elementos se pueden implementar según sea necesario para cumplir con las metas y objetivos de las organizaciones y la fuerza laboral.	Este framework introduce adicionalmente elementos de otros trabajos realizados en ciberseguridad o en el sector TIC: • National Initiative for Cybersecurity Education (NICE). • Australian Defense Force (ADF) professional framework. • The global skills and competency framework for a digital world (SFIA).

La tabla de análisis busca expresar el contenido de los diferentes *Frameworks* analizados desde la óptica de los siguientes criterios de evaluación:

- **Enfoque / estructura**: conceptos más importantes en los que se enfoca el *Framework* y la claridad y la lógica con la que está organizado el marco de trabajo.
- **Claridad en la definición de perfiles /beneficios**: forma en la que están ilustrados los diferentes perfiles de ciberseguridad, y los conocimientos, capacidades y habilidades (KSA) que están asociados a esos perfiles. Considera el beneficio o aporte que genera el uso de la herramienta a los diferentes grupos a los que está dirigido.
- **Grupos a los que impacta**: los diferentes actores o grupos de distinta tipología que se benefician del *Framework*. Es vital, entender que las necesidades del 'target' pasa por haber involucrado en la fase de diseño y desarrollo a diferentes *stakeholders* de la industria de la ciberseguridad de manera que validaran el proceso y así poder garantizar unos mejores resultados.
- **Flexibilidad / facilidad de implementación**: determina si el *Framework* se adapta a las necesidades de cada uno de los grupos a los que se dirige. Idealmente los marcos de trabajo deben proveer una estructura que potencie el talento de las personas de una manera eficiente y clara.
- **Compatibilidad con otras taxonomías**: determina si el trabajo realizado ha sido abordado de manera inclusiva con las aportaciones que han realizado otras taxonomías y de esta manera, se busca dar continuidad de manera homogénea a una taxonomía de la que se puedan beneficiar diferentes organizaciones a nivel global. Esto cobra importante relevancia al tratarse de una industria que se puede beneficiar de ecosistemas de confianza y del trabajo conjunto, y que por la naturaleza del avance digital, es altamente descentralizada.

Definición de un modelo de caracterización de los perfiles de ciberseguridad en España.

Los diferentes marcos de trabajo o *Frameworks* en el cuadro de análisis representan toda una aproximación razonable acerca de los perfiles de ciberseguridad y las diferentes competencias que los individuos deben ostentar para poder desempeñarse con éxito en roles de ciberseguridad. Ahora bien, es importante reconocer que la ciberseguridad no es estática y está constantemente en evolución y los diferentes *frameworks* no son del todo exhaustivos, sino que están sujetos a modificaciones, actualizaciones y revisiones, lo cual obedece a una realidad digital que evoluciona a un considerable ritmo.

La propuesta para la definición de una taxonomía en España debería considerar el mejor '*approach*' a lograr interiorizar las mejores prácticas

o beneficios del trabajo realizado por otras instituciones e idealmente debe buscar la manera de consolidar una estructura homogénea que sea válida en la mayoría de los grupos de trabajo o *stakeholders* de la industria. Por esta razón, después de abordar los diferentes *Frameworks* que se han incluido como referencia en este estudio, se ha establecido que se puede implementar una taxonomía para España de amplio alcance teniendo presente el *European Cybersecurity Skills Framework* (ECSF) *Profiles* de ENISA.

A pesar de que una buena gestión de talento depende en gran medida de que los marcos de trabajo sean ampliamente conocidos y aceptados por diferentes organismos, no se debe ignorar que no hay evidencia que indique que alguno de los *frameworks* que se han analizado sea ampliamente aceptado en la UE. Si bien es cierto que el *Framework* NICE es ampliamente conocido y aceptado por múltiples instituciones y compañías en EE. UU, estableciendo que el alcance y adaptación a las condiciones del mercado en Europa son aún una preocupación. Por otra parte, a pesar de que existen varios documentos que hacen referencia a las competencias y capacidades en ciberseguridad, no hay ciertamente una clasificación europea estandarizada, y 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.

El ECSF *Framework* de ENISA, además de ser un trabajo que se está actualmente realizando y revisando por 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, tiene una definición de perfiles basada las necesidades de la UE y cada uno de sus estados miembros.

Además, se enfoca 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 analizar el estado del conocimiento sobre la manera en que se está gestionando el talento y los *skills* en ciberseguridad. Otro punto de alta relevancia es que se espera que el ECSF esté alineado con otros trabajos de la UE, como el e-Competences *Framework*, y esto, sin duda, sería un reflejo de la coherencia y rigurosidad con la que se está llevando a cabo el proceso.

El ECSF se ha identificado como un modelo completo y altamente práctico que consideraría una lista de tareas que deben necesariamente realizarse en el campo de la ciberseguridad en casi todas las organizaciones. Esas tareas están asociadas a los KSA que se deben tener para poder realizar dichas tareas. De esta manera, este *Framework* modela y articula de manera integral los roles, tareas, conocimientos, capacidades y habilidades clave en el campo de la ciberseguridad. En este sentido, se espera que este sea un recurso práctico y aplicable para la gestión y planificación de la fuerza laboral. Los objetivos de la imple-

mentación de este marco deben aportar fundamentalmente:

- Una estructura de referencia que categoriza y describe la naturaleza interdisciplinaria del trabajo de ciberseguridad y los (KSA) necesarios para completar tareas que pueden fortalecer las estrategias de ciberseguridad implementadas por una determinada organización.
- Una guía para identificar, reclutar, desarrollar y retener talentos en ciberseguridad en todo el tejido productivo.
- Una fuente de referencia sobre diferentes aspectos del desarrollo, planificación, capacitación y educación de la fuerza laboral en ciberseguridad, describiendo programas formativos dentro y fuera de la UE.
- Identificar brechas en el desarrollo de la fuerza laboral, específicamente en las áreas de conocimiento más apremiantes y demandadas de la ciberseguridad.
- Apoyar a las instituciones educativas para identificar y comprender brechas existentes, y cómo modificar los programas educativos para responder a estas brechas.

Consideraciones para la implementación de una taxonomía basada en ENISA.

- Mientras que la UE ha demostrado ser un referente que lidera temas de GDPR, está ligeramente rezagada en el desarrollo de un enfoque integral para definir un conjunto de roles, tareas y *skills* relevantes para proteger a las organizaciones en el campo de la ciberseguridad.
- Debido a las diferencias legislativas y a los detalles específicos que rigen en cada país de la UE, la implementación debe respetar las especificidades de la UE, lo que permite un uso y adopción mayoritariamente aceptada dentro del entorno de la UE.
- Cualquier definición debe considerar el desarrollo extremadamente rápido de la ciberseguridad y la aparición de *skills* emergentes, y esto implica el riesgo de perder relevancia si no se revisa periódicamente a través de procesos que involucren a los agentes más relevantes de la industria. El trabajo realizado debe estudiar cuidadosamente las fuentes más importantes que estén generando información que podría ser utilizada para fines de revisión y actualización del modelo de taxonomía.
- El ECSF *Framework* respeta la integridad de otros trabajos realizados alrededor de la ciberseguridad. Idealmente habrá propuestas y revisiones periódicas que permitan desarrollar y validar la relevancia y aplicabilidad de otras investigaciones al entorno europeo.

En base a estas consideraciones, se recomienda que todo el detalle de los perfiles de ciberseguridad, tareas, conocimientos, capacidades y habilidades se consulte en el *European Cybersecurity Skills Framework* de

ENISA. El objetivo de ENISA ha sido lograr un nivel común de ciberseguridad en toda Europa, aprovechando fortalezas y descubriendo deficiencias en la industria, lo cual demuestra un trabajo holístico del que se pueden beneficiar las organizaciones en España.

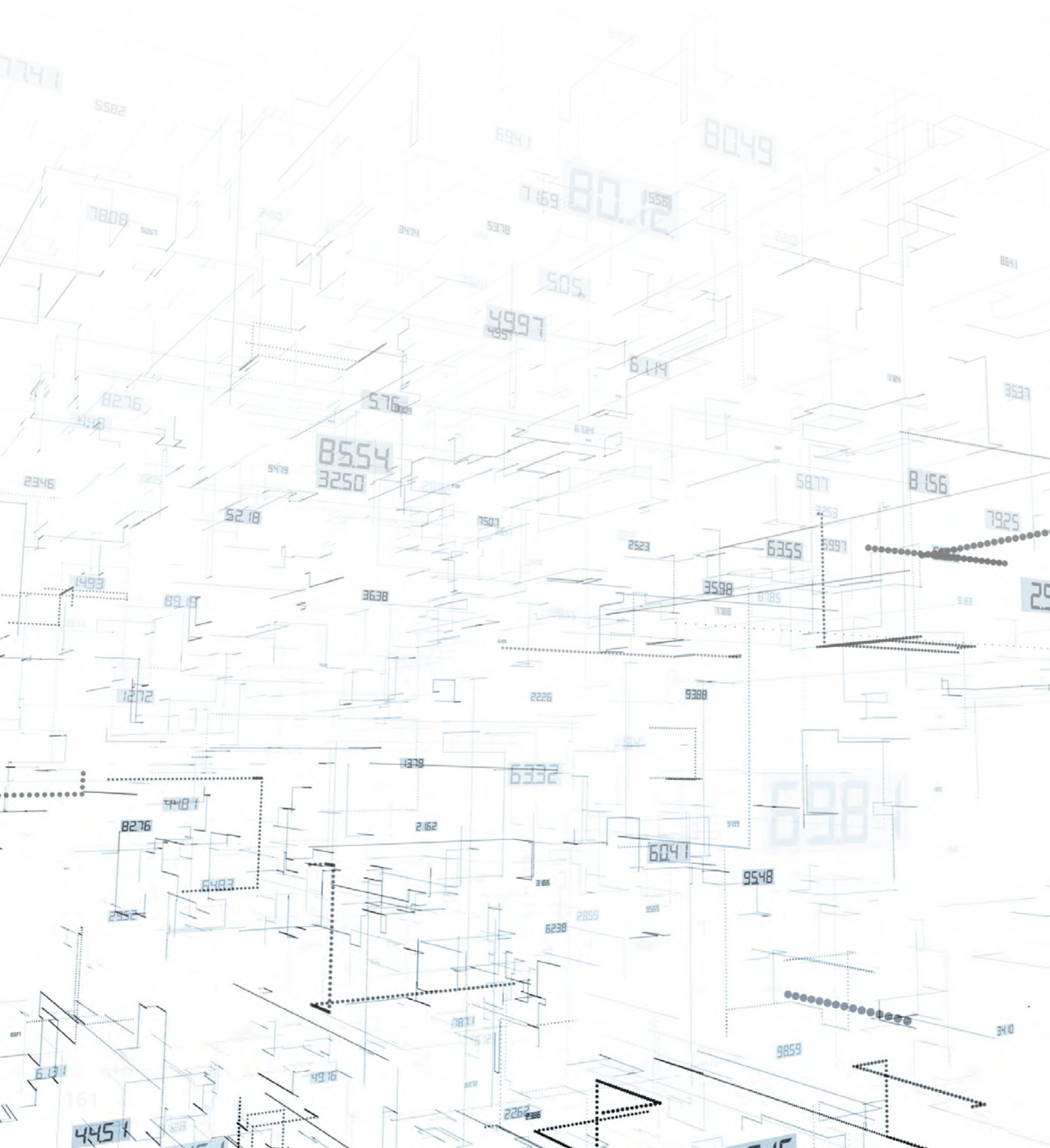
Una de las recomendaciones que derivan del análisis realizado es que las organizaciones en España que hagan uso de los recursos del ECSF *Framework* o la misma ENISA, deberían primeramente vincular aún más esos *skills* a los roles reconocidos en el mercado laboral nacional y a las particularidades y necesidades específicas de las empresas españolas. Esto idealmente permite diseñar estrategias y planes de formación y de carrera más ajustados y personalizados para que los profesionales agreguen valor de una manera más ágil a las organizaciones.

De manera idónea el uso de un *Framework* promueve el fortalecimiento de la industria en general, y de hecho todos los países necesitan una fuerza laboral integrada de ciberseguridad capaz de satisfacer las necesidades de todo su ecosistema digital. Esto requiere de personas con conocimientos y experiencia, y con la capacidad de diseñar, desarrollar, implementar y mantener estrategias de ciberseguridad para contrarrestar amenazas.

De esta manera, el desarrollo de una taxonomía que sirva a este propósito debe ser concebido con la participación del gobierno, sector privado, academia y los mismos ciudadanos. Más aún, los modelos de gobernanza son claves, ya que el avance es probablemente más rápido cuando el conocimiento y la experiencia se comparten, reutilizan o mejoran, en lugar de reinventarlos. Reutilizar y adaptar las mejores prácticas a necesidades específicas a nivel nacional puede ser un camino eficaz para la gestión del talento en ciberseguridad.

ANEXO 4. BENCHMARK INTERNACIONAL DE GESTIÓN DE TALENTO EN CIBERSEGURIDAD.

El benchmark es una presentación aparte en formato PowerPoint que será entregado junto con el presente estudio.



ÍNDICE DE FIGURAS

Figura 1. Objetivos del proyecto	15
Figura 2. Estructura de fases del trabajo de diagnóstico de talento de ciberseguridad en España	15
Figura 3. Tamaño de mercado de la seguridad (en M€). Fuente: Security Spending Guide IDC 2021	18
Figura 4. Tamaño de mercado por grupo de tecnología. Fuente: Security Spending Guide IDC 2021	19
Figura 5. Tamaño de mercado por categorías de tecnología. Fuente: Security Spending Guide IDC 2021	20
Figura 6. CAGR top 6 detalle de tecnologías. Fuente: Security Spending Guide IDC 2021	20
Figura 7. Gasto en ciberseguridad en mediana y gran empresa (M€). Fuente: Security Spending Guide IDC 2021	21
Figura 8. Gasto en ciberseguridad en gran empresa. Fuente: Security Spending Guide IDC 2021	21
Figura 9. Tamaño de mercado de la ciberseguridad por sectores – Fuente: Security Spending Guide IDC 2021	22
Figura 10. Tamaño de mercado de la ciberseguridad por subsectores – Fuente: Security Spending Guide IDC 2021	23
Figura 11. Tendencia de canales a 2024. Fuente: IDC Consumer Survey	24
Figura 12. Beneficios de la convergencia IT/OT para las empresas. Fuente: IDC	30
Figura 13. Ecosistema de la ciberseguridad en España – elaboración propia basada en mapa del sistema de valor de INCIBE publicada en abril 2015	34
Figura 14. Distribución geográfica de la oferta de Masters en ciberseguridad en España. Fuente: elaboración propia	40
Figura 15. ¿Una persona formada de manera autodidacta tiene las mismas competencias, habilidades y conocimiento que otra que disponga formación reglada?	51
Figura 16. ¿Por qué considera que no es así?	51
Figura 17. Aspectos valorados por el mercado de ciberseguridad en la oferta de talento	52
Figura 18. Grado de importancia de los requisitos que debería cumplir una persona que se quiera dedicar a la ciberseguridad	53
Figura 19. Hándicaps que las empresas se encuentran a la hora de contratar talento en ciberseguridad	54
Figura 20. Certificaciones demandadas de manera prioritaria	54
Figura 21. ¿Cómo ha adquirido los conocimientos y competencias en seguridad?	55
Figura 22. Opciones preferidas para desarrollar competencias y conocimientos de manera autodidacta	57
Figura 23. Modalidades de impartir formación universitaria en ciberseguridad	58
Figura 24. Iniciativas que ayudarían a incrementar la presencia de mujeres en posiciones de ciberseguridad	59
Figura 25. ¿Tiene claro qué habilidades, itinerario formativo y cualificación debe tener para dedicarse a la ciberseguridad?	60
Figura 26. ¿A qué cree que se debe que no conozca el itinerario formativo y de capacitación requerido?	61

Figura 27. Proyecciones de estimación de la demanda de talento en ciberseguridad en España 68
Figura 28. Características de los programas actuales de formación en ciberseguridad 70
Figura 29. Principales requerimientos asociados la formación. Percepción de la demanda. 70
Figura 30. Necesidades específicas de formación consideradas por las organizaciones para alinear oferta y demanda de talento en ciberseguridad 71
Figura 31. Acciones para el impulso del talento de la ciberseguridad por parte del sector TIC / Ciberseguridad 72
Figura 32. Presencia femenina en la industria de ciberseguridad 73
Figura 33. Existencia de políticas flexibles en la industria de la ciberseguridad 74
Figura 34. Presencia femenina en función del perfil considerado 75
Figura 35. Existencia de planes de refuerzo para la contratación de mujeres en la industria de ciberseguridad 75
Figura 36. Existencia de departamentos de seguridad en las organizaciones 77
Figura 37. Rotación de personal de los equipos de ciberseguridad en la empresa española 77
Figura 38. Principales factores para la rotación del talento de ciberseguridad en España. 78
Figura 39. Escala salarial en la que se distribuye la muestra consultada 79
Figura 40. Talento reciclado de otras áreas de la organización 79
Figura 41. Porcentaje de posiciones abiertas de ciberseguridad que se cubren con reciclaje interno 80
Figura 42. Principales conocimientos demandados para los perfiles de ciberseguridad 80
Figura 43. Presencia de perfiles transversales con conocimientos en ciberseguridad en la empresa española 81
Figura 44. Principales efectos negativos de la escasez de talento de ciberseguridad en las empresas 82
Figura 45. Factores limitantes de la capacidad de las empresas para mejorar sus capacidades de seguridad de TI. Fuente: IDC European Security Survey, June 2020, n=702, n= 50 (Spain) 84
Figura 46. Principales acciones llevadas a cabo por las empresas para mitigar la fuga de talento 85
Figura 47. Dificultad de incorporar perfiles de seguridad en modo subcontratación 86
Figura 48. Porcentaje de contrataciones de talento procedente de FP 86
Figura 49. Importancia del título universitario en posiciones de entry level en ciberseguridad 87
Figura 50. Ejecución de programas de sensibilización y formación en ciberseguridad en la empresa 88
Figura 51. Tipología de perfiles de ciberseguridad que demanda la empresa española. 89
Figura 52. Principales industrias de las que se contrata talento de ciberseguridad 89
Figura 53. Análisis de los factores de atracción y retención de talento en Startups 90

Figura 54. Importancia de los factores con relación a la retención de talento en un startup 91
Figura 55. Principales barreras encontradas en el proceso de recruiting de talento de ciberseguridad en las empresas 92
Figura 56. Tiempo medio para cubrir una posición de ciberseguridad en la empresa española 93
Figura 57. Salario actual para las posiciones de ciberseguridad en España 94
Figura 58. Perfiles más complicados de incorporar en el ámbito de la ciberseguridad 94
Figura 59. Grupos de impacto de las actuaciones analizadas. Fuente: propia 100

ÍNDICE DE TABLAS

Tabla 1. Grados oficiales en ciberseguridad.	39
Tabla 2. Proyecciones de oferta de talento en ciberseguridad en España.	49
Tabla 3. Principales vías para adquirir conocimiento y competencias en ciberseguridad	56
Tabla 4. Perfiles de ciberseguridad del ECSF Framework	112
Tabla 5. Perfiles de ciberseguridad y sus respectivos KSA (I/IV)	113
Tabla 6. Perfiles de ciberseguridad y sus respectivos KSA (II/IV)	114
Tabla 7. Perfiles de ciberseguridad y sus respectivos KSA (III/IV)	114
Tabla 8. Perfiles de ciberseguridad y sus respectivos KSA (IV/IV)	115
Tabla 9. Encuadre de las recomendaciones en las diferentes etapas del ciclo de gestión del talento. Fuente: propia	120

8_ COLABORADORES

La elaboración del estudio ha contado con una amplia variedad de metodologías de análisis que ha permitido **incorporar la visión de todos los actores del ecosistema nacional** de ciberseguridad, buscando contrastar el con el sector todas las cuestiones abordadas.

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

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
SECRETARÍA GENERAL DE FORMACIÓN PROFESIONAL

MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL
SERVICIO PÚBLICO DE EMPLEO ESTATAL
SEPE

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS EXTERIORES, UNIÓN EUROPEA Y COOPERACIÓN

EXPERTOS

crue Universidades Españolas

FORO NACIONAL DE CIBERSEGURIDAD

RENIC
Red de Excelencia Nacional de Investigación en Ciberseguridad

edipe
ASOCIACIÓN ESPAÑOLA DE DIRECCIÓN Y DESARROLLO DE PERSONAS

asociación española directores recursos humanos

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
SPAIN

FUNDACIÓN BORREDÁ
al servicio de la seguridad

Revista SIC
ciberseguridad, seguridad de la información y privacidad

COLABORADORES

CCN centro criptológico nacional

DSN

Fundación Estatal PARA LA FORMACIÓN EN EL EMPLEO

INSTITUTO NACIONAL DE LAS CUALIFICACIONES

MCCE

OCC OFICINA DE COORDINACIÓN DE CIBERSEGURIDAD

aeiciberseguridad Agrupación Empresarial Innovadora CIBERSEGURIDAD y Tecnologías Avanzadas

Ametic LA VOZ DE LA INDUSTRIA DIGITAL

CEOE Empresas Españolas

CEPYME CONFEDERACIÓN ESPAÑOLA DE LA PEQUEÑA Y MEDIANA EMPRESA

conetic Confederación Española de Empresas de Tecnologías de la Información, Comunicaciones y Electrónica.

Fundación GOODJOB

isms forum INTERNATIONAL INFORMATION SECURITY COMMUNITY

grupo social ONCE

AENOR Confía

ISACA Madrid Chapter

C1B3R WALL

GUARDIA CIVIL

/RootedCON