Punto de partida al Modelo de gestión y seguimiento del TALENTO en ciberseguridad en España

Visión conjunta de la industria, sector académico e investigador y profesionales del sector

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL

Índice

Índice de figuras

Índice de tablas

1 Antecedentes

La proliferación de nuevas amenazas, con un grado de sofisticación elevado y creciente, conduce a la necesidad de incorporar profesionales expertos en ciberseguridad en distintos tipos de organizaciones.

La actual complejidad de los sistemas de información y su grado de interconexión suponen una vulnerabilidad susceptible de ser explotada por ciberataques, cada vez más frecuentes y complejos. Es necesario identificar cuáles son las posibles brechas en la seguridad y moverse en una situación de equilibrio entre la confianza, la transparencia y la privacidad y, para realizar esa identificación y la consiguiente defensa, se precisan profesionales con una dotación de competencias específica.

En 2020 la Unión Europea tendrá una carencia de 825.000 profesionales tecnológicos

Sin embargo, la oferta disponible de profesionales expertos y preparados para asumir estos retos no ha crecido al mismo ritmo que la demanda de los mismos y los periodos de formación requeridos implican que esta carencia, cuantificada por la Comisión Europea en 825.000 profesionales para 2020 en el conjunto de la Unión Europea, continuará aumentando durante los próximos años si no se inician las medidas necesarias para paliarla [0].

Todas las fuentes consultadas coinciden en este diagnóstico y el esperable agravamiento de la situación, así como en el hecho de que se trata de un fenómeno global. A pesar de que la tendencia parece clara, no hay acuerdo en las cifras manejadas por los diferentes actores. Así, mientras el 2015 (ISC)2 Global Information Security Workforce Study [1] realizado por (ISC)2 (International Information Systems Security Certification Consortium) cifra la carencia mundial de especialistas en ciberseguridad en 1,5 millones para 2020, Michael Brown, CEO de Symantec, señala que en 2019 habrá seis millones de puestos de trabajo relacionados con la ciberseguridad, de los cuales un millón y medio quedará sin cubrir [2]. Por su parte, la Universidad de Stanford, a través de su programa Peninsula Press [3], señala que 209.000 puestos de trabajo en este ámbito están actualmente sin cubrir en Estados Unidos.

Como conclusión, existe un entorno de sistemas más abiertos, complejos e interconectados y, por tanto, más vulnerable. En ese contexto, aumenta la frecuencia y la sofisticación de los ciberataques y, además, hay una carencia de profesionales especializados. Todas las previsiones apuntan a que dicha situación se agravará en los próximos años.

Este es el punto de partida necesario para la definición de un modelo global de gestión y seguimiento del talento[1] que abarque:

- Aparición de talento, es decir, orientación desde una etapa temprana de personas hacia la adquisición de competencias técnicas que propicien el interés hacia la ciberseguridad aprovechando el atractivo que supone un sector en auge y con un enorme crecimiento.
- Identificación del talento, lo que implica búsqueda de profesionales en desarrollo en el ámbito de la ciberseguridad de forma que se facilite su acercamiento a las organizaciones que los necesitan.

1. En el contexto de este documento nos referimos al talento como la nominalización de la capacidad que tienen determinadas personas para comprender y desempeñar actividades relacionadas con la ciberseguridad.

1 Antecedentes

- Atracción de talento, de forma que los profesionales vean el entorno empresarial, investigador o académico nacional lo suficientemente atractivo como para querer desarrollar su carrera en él.
- Retención del talento, con el objetivo de que los profesionales ya formados puedan desarrollar su carrera profesional en el ámbito nacional a través de la generación de ofertas que puedan competir en atractivo con las disponibles en otros países para los profesionales formados.

La preocupación por la ciberseguridad y la necesidad de cubrir los puestos de trabajo especializados con profesionales es compartida por todos los Gobiernos de los países más desarrollados. En consecuencia, las distintas estrategias nacionales de ciberseguridad están contemplando la falta de profesionales cualificados y la necesidad de abordar la gestión del talento.

A continuación, se enumeran algunas iniciativas destacables por su énfasis en las estrategias encaminadas a atraer talento hacia el terreno de la ciberseguridad:

- NICCS-National Initiative for Cybersecurity Careers and Studies [4]: Iniciativa del Department of Homeland Security estadounidense que proporciona recursos educativos y profesionales de ciberseguridad. Entre sus recursos, destaca el *Interactive National Cybersecurity Workforce Framework*, que identifica los principales perfiles en ciberseguridad y relaciona los conocimientos y habilidades asociados a ellos, así como cursos donde los profesionales pueden adquirir esas habilidades. A pesar de que su alcance es estadounidense, muchos de los recursos informativos pueden ser aprovechados en España.
- Department of Homeland Security's Task Force on CyberSkills [5]: En 2012 formula una serie de propuestas y recomendaciones con objeto de facilitar la captación y retención del talento en seguridad cibernética para el propio Department of Homeland Security, así como para elevar la capacidad general del país para desarrollar profesionales con las habilidades avanzadas necesarias para proteger la información.
- Israel National Cyber Bureau [6]: Iniciativa de ciberseguridad en Israel muy centrada en la seguridad institucional que, al mismo tiempo, establece alianzas con centros universitarios especializados en ciberseguridad como la Universidad Ben Gurion.
- Cybersecurity Strategy of the European Union [7]: Desarrollada en 2013 por la Comisión Europea bajo el nombre *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, aborda el problema de la escasez de profesionales y las posibles vías para su solución.
- Roadmap for NIS education programmes in Europe [8]: Se trata de un informe de ENISA que recopila escenarios de educación en seguridad de la información en Europa.

1 Antecedentes

- Cybersecurity Education snapshot for workforce development in the EU [9]: Informe publicado en septiembre de 2015 en el entorno del Grupo de Trabajo 3 de la Network and Information Security de la Unión Europea, ofrece un diagnóstico del panorama educativo en ciberseguridad en la UE, a la vez que proporciona oportunidades y recomendaciones.
- Cyber career connection [10]: Programa de Responsabilidad Social Corporativa de Symantec en colaboración con **Npower** y **YearUp**. Conecta las necesidades de la industria (300.000 puestos en ciberseguridad) con colectivos en riesgo de exclusión (jóvenes adultos en el caso de YearUp y jóvenes y veteranos en el caso de Npower). Su ámbito espacial se ciñe a algunas áreas de Estados Unidos.
- SAPROMIL (Sistema de Aprovechamiento de Capacidades Profesionales del Personal Militar) [11]: Programa de incorporación del personal militar español a otros ámbitos laborales implementado en colaboración con las distintas administraciones públicas y con el sector privado. A través de un sistema de segmentación de perfiles profesionales / áreas funcionales / categorías, las empresas pueden consultar los CV de los profesionales más interesantes.

Todas las iniciativas señaladas coinciden en la escasez actual de profesionales, la importancia de atraer talento hacia la ciberseguridad y la necesidad de implicar, en este objetivo común, tanto a organizaciones empresariales como a organizaciones educativas.

En el momento de la elaboración de este documento, no hay constancia de la existencia de un estudio exhaustivo de la situación de la ciberseguridad en España, por lo que éste mismo podría ser considerado como punto de partida para su realización.

Existe la necesidad de atraer talento hacia la ciberseguridad, implicando tanto a organizaciones empresariales como a organizaciones educativas

2 Objeto

El objeto del presente documento es establecer un punto de partida que sirva para la definición de un Modelo de gestión y seguimiento del talento en ciberseguridad en España, que contribuya a satisfacer la demanda de profesionales cualificados tanto en la actualidad como en el futuro.

El documento recoge una propuesta de líneas generales de actuación, como un intento de conocer mejor las necesidades y demandas del mercado, y como una forma de aumentar la oferta disponible de profesionales suficientemente cualificados. No obstante, cada una de esas líneas deberá ser desarrollada en planes específicos, cuya ejecución e implementación se desarrollará durante el periodo 2016 - 2018.

La solución propuesta es de medio y largo plazo debido a que, la falta de profesionales, impide una solución rápida por la vía del trasvase de personas ya formadas y procedentes de otras actividades. La Oficina Nacional de Auditoría de Reino Unido ha advertido que podría llevar 20 años cubrir la falta de profesionales cualificados en ciberseguridad. Por ello, este modelo de gestión pretende revertir la tendencia actual, fidelizando a los profesionales ya existentes al mismo tiempo que se identifica talento aún no plenamente operativo y se atrae el interés por parte de personas que se encuentren en etapas más primarias de su formación. Para ello, es preciso presentar la ciberseguridad como un ámbito de trabajo atractivo y demandado para la población que se encuentre en etapas del ciclo educativo donde aún no se hayan definido opciones profesionales futuras.

El documento recoge líneas generales de actuación propuestas como una forma de aumentar la oferta disponible de profesionales

3 Actores

Bajo este epígrafe se incluyen a los distintos actores que, bien desde la perspectiva de usuarios o bien desde la de proveedores de talento específico, denotan interés con respecto a las actividades relacionadas con la ciberseguridad.

Los generadores institucionales de competencias específicas son los centros educativos y, singularmente, las Universidades. Estas competencias son adquiridas por personas con talento específico para la actividad y que, contando con la suficiente motivación, complementan mediante una búsqueda activa de información, es decir, mediante la capacidad para funcionar en forma autodidacta. Finalmente, la persona dotada de las competencias requeridas se incorpora al mercado laboral, representado por las empresas y los centros de investigación, o bien se incorpora al mercado como emprendedor o freelance. El sector académico e investigador juega un doble papel en el modelo. Por un lado, imparte formación de carácter avanzado. Por otro lado, participa como elemento de simbiosis entre la academia y la realidad empresarial que permita afrontar nuevos retos. Todo ello, contando con la Administración como facilitador y regulador del entorno.

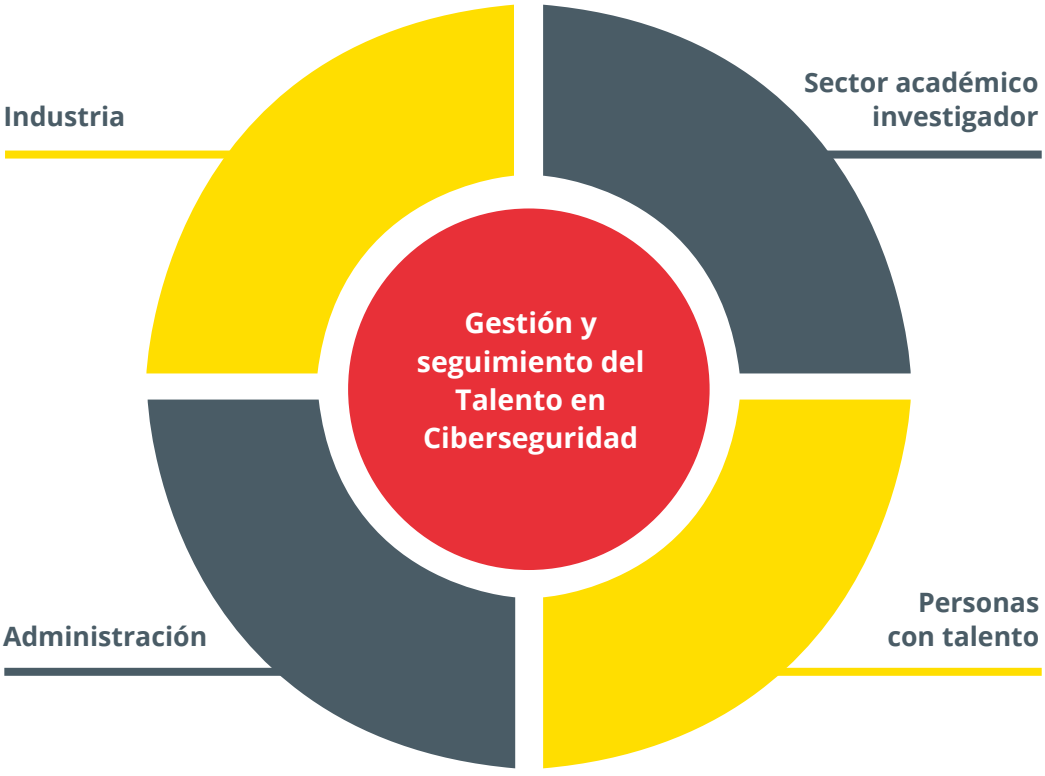


Figura 1: Actores del modelo de gestión y seguimiento del talento en ciberseguridad.

3 Actores

3.1 Industria

Se considera bajo este apartado a cualquier empresa que necesite incorporar perfiles especializados en ciberseguridad. El requerimiento de estos perfiles no se limita a empresas tecnológicas, y los perfiles requeridos no siempre son estrictamente técnicos.

INCIBE lidera el Polo tecnológico en ciberseguridad, formado por un conglomerado de entidades públicas y privadas *pure players* en ciberseguridad. El objetivo del Polo tecnológico es la promoción de la industria de la ciberseguridad española, a través de medidas encaminadas a aumentar la competitividad en el sector, potenciar el mercado interior y promover la internacionalización de la Industria en ciberseguridad española. En este contexto, es fundamental para estas entidades altamente especializadas dotarse del mejor talento que contribuya al aumento de la competitividad del sector.

Cualquier empresa que necesite incorporar perfiles especializados en ciberseguridad

La necesidad de contratación de profesionales de la seguridad va más allá de las empresas consideradas *pure players*. En general, las grandes organizaciones, especialmente aquellas en las que un fallo en su funcionamiento pueda tener mayor impacto, son conscientes del problema y de la necesidad de profesionales especializados. Otras empresas de menor tamaño y que no responden a este perfil, aún consideran que su actividad no las convierte en interesantes para un atacante y, por tanto, han tomado medidas básicas o carecen completamente de ellas. La actitud de muchas de ellas suele seguir siendo reactiva, minimizando el número de profesionales dedicados a la ciberseguridad. Una mayor concienciación del impacto que puede tener en el negocio este tipo de acciones ayudaría a ver la ciberseguridad no como una carga, sino como una necesidad en sí misma dentro del modelo de negocio de la empresa.

Las empresas demandan perfiles más amplios de lo estrictamente técnico y, además de requerir unas sólidas bases en ciberseguridad, precisan de personal con conocimientos de inglés y otras competencias transversales, como la comunicación o el trabajo en equipo, básicas para trabajar integrados en equipos multidisciplinares. Al mismo tiempo, buscan personas comprometidas con la empresa.

3.2 Sector académico e investigador

Las Universidades y los Centros de Formación que imparten estudios en ciberseguridad o en el ámbito de ésta, así como los investigadores asociados a dichas entidades y a Centros Tecnológicos y Centros de Investigación, representan otro participante necesario en cualquier modelo de gestión del talento en ciberseguridad, ya que son al mismo tiempo demandantes de talento y generadores del mismo, constituyendo una de las vías de acceso profesional al sector.

Es de destacar el hecho de que, en el terreno de la ciberseguridad, es muy frecuente que exista una elevada carga de autoaprendizaje, al igual que sucede en otras disciplinas

3 Actores

El sector académico e investigador es a su vez demandante y generador de talento en ciberseguridad

técnicas que están en sus primeros estadios de desarrollo. La rápida evolución de la ciberseguridad dificulta garantizar la actualización permanente de una oferta formativa tradicional. Esta circunstancia, unida al coste habitualmente asociado a la formación especializada, provoca que la opción de la autoformación sea muy habitual entre los jóvenes y profesionales. En algunas ocasiones, ese autoaprendizaje se sustenta también sobre actividades propias del sector académico como la oferta disponible gratuitamente a través de internet de cursos MOOC (*Massive Open Online Courses*) mientras que, en otros casos, se trata de búsqueda de información compartida en foros especializados.

Otra fuente de formación no estrictamente reglada en los currículos docentes, es la certificación ofrecida por los fabricantes en sus propios productos. Este tipo de formación es difícil que se vea incluida en programas académicos, aunque sí que es muy apreciada por las empresas, debido a la utilización directa que de dichos productos hacen en sus soluciones.

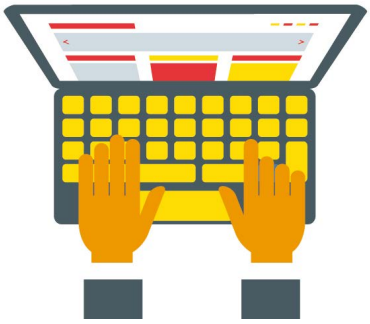
3.3 Personas con talento

Genéricamente, se considera que tienen talento, a aquellas personas que han mostrado un elevado potencial en ciberseguridad y disponen de conocimientos y competencias en la materia, que pueden encontrarse en grados de desarrollo diferentes (maduros o más incipientes).

La demanda más generalizada dentro de este colectivo, se refiere al acceso a puestos de trabajo y proyectos nacionales e internacionales acordes a su nivel de conocimientos, remunerados de manera competitiva y flexibles (que les permitan compatibilizar estudios, trabajo, teletrabajo, etc.).

Perciben una diferencia importante entre los niveles salariales disponibles en España y los que se pueden conseguir en el extranjero. Esto conduce a que, personas con talento en ciberseguridad y que dominen al menos un idioma extranjero, puedan ser reclutadas para cubrir ofertas de trabajo fuera de España, agravándose la situación de carencia de profesionales.

Personas con talento en ciberseguridad y que dominen al menos un idioma extranjero pueden ser reclutadas fuera de España y agravar así la situación de carencia



3 Actores

3.4 Administración

La Administración juega un papel fundamental en cualquier proyecto que involucre distintos sectores económicos y grupos sociales. Como consecuencia, es necesaria su participación en la definición de un modelo de gestión del talento en ciberseguridad, ya que su actuación, además de relacionarse con la normativa y regulación aplicable en materia de ciberseguridad, se relaciona con la demanda actual para cubrir sus propias necesidades.

Es la encargada de legislar y crear el marco regulador del entorno en el que se van a mover el resto de los actores definiendo, por tanto, los límites de actuación y señalando, qué puede o no ser considerado como delito.

Actúa como dinamizadora del sector, sentando las bases para que se pueda crear una oferta formativa adecuada y proporcionando o canalizando ayudas y colaboraciones con otros estamentos o entidades internacionales, que permitan el desarrollo de proyectos industriales y de investigación.

Al mismo tiempo es demandante de talento ya que, además de proteger los propios intereses públicos, necesita identificar y captar al mejor talento a fin de asegurar el cumplimiento de la legislación vigente y la adaptación de ésta a la evolución tecnológica de sistemas y tendencias relacionadas con la ciberseguridad, en un entorno dinámico y constantemente cambiante.

La Administración actúa como dinamizadora del sector y es, al mismo tiempo, demandante de talento

4 Metodología

La metodología seguida para la elaboración del presente documento, como punto de partida para la definición posterior de un Modelo de gestión y seguimiento del talento en ciberseguridad en España, consta de cuatro fases.

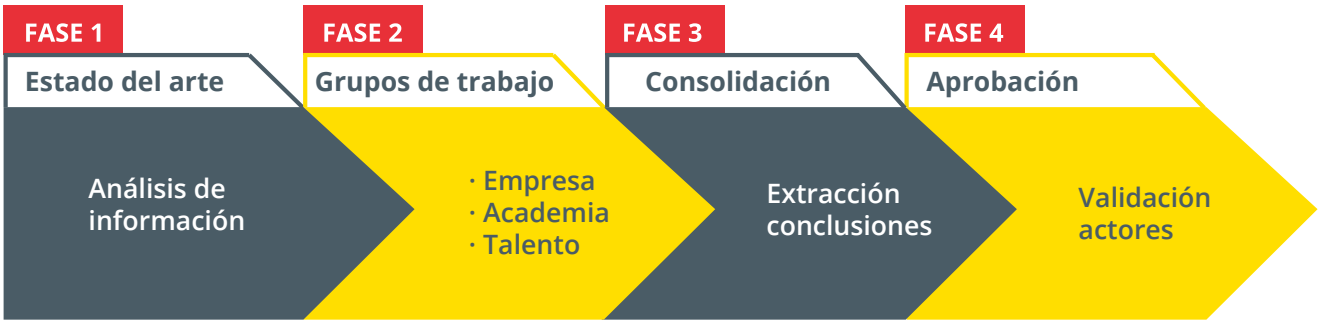


Figura 2: Metodología seguida para la elaboración del Punto de partida al Modelo de gestión y seguimiento del talento en ciberseguridad en España.

FASE 1 Estado del arte

En la fase inicial, se consultaron múltiples fuentes documentales dirigidas al establecimiento de un diagnóstico y a la búsqueda de soluciones aplicadas por países que hubieran percibido la misma falta de profesionales expertos en ciberseguridad.

Esta fase llevó a analizar distintas estrategias de ciberseguridad, en su parte relacionada con la gestión de talento específico, así como al análisis de la oferta formativa nacional e internacional, información relativa a tipos de certificaciones, sus requerimientos y consideración en el mercado, badges digitales como instrumentos de acreditación de competencias, perfiles competenciales de los profesionales de ciberseguridad y de otras familias profesionales cercanas como potencial fuente de reclutamiento.

Como resultado de esta fase, se estableció un borrador de diagnóstico inicial del mercado del talento de la ciberseguridad en España, que se compartió con los diferentes actores en la Fase 2, y que se describe en el [apartado 5 Diagnóstico inicial] del presente documento. Este diagnóstico no debe ser tomado como definitivo, sino servir como punto de partida para la elaboración de un estudio más exhaustivo.

4 Metodología

FASE 2

Grupos de trabajo

Con objeto de validar la información obtenida como fruto de la Fase 1, así como detectar las necesidades particulares de cada uno de los públicos objetivo, se establecieron grupos de trabajo con cada uno de los actores identificados.

Se realizaron un total de cuatro grupos de trabajo entre los meses de octubre y noviembre de 2015:

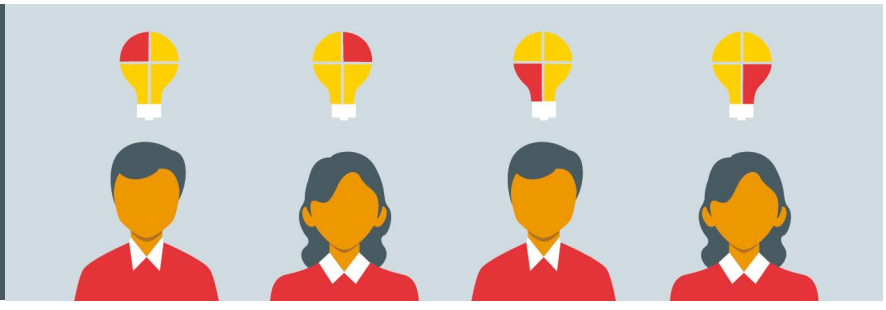
1. Grupo de trabajo con empresas del Polo Tecnológico Nacional en Ciberseguridad.
2. Grupo de trabajo con empresas participantes en el Foro Empleo y Talento en Ciberseguridad de CyberCamp, en la que participaron conjuntamente representantes de las áreas técnicas y de negocio con responsables del área de Recursos Humanos.
3. Grupo de trabajo con universidades y centros formativos participantes en el Education & Research Corner de CyberCamp y en el programa de becas de estudios de especialización en ciberseguridad INCIBE.
4. Grupo de trabajo con personas con talento en ciberseguridad, detectadas en los retos de CyberCamp.

En cada una de las reuniones se siguió el siguiente modelo de trabajo:

- Presentación de iniciativas internacionales de gestión del talento en ciberseguridad (INCIBE).
- Presentación del diagnóstico inicial del panorama nacional en la gestión del talento en ciberseguridad (INCIBE).
- Problemas y necesidades de los actores (ACTORES).
- Debate (TODOS).

Como resultado de esta fase, se validó y concretó el diagnósticon inicial del mercado del talento de la ciberseguridad en España que se presenta en el [apartado 5 Diagnóstico inicial] del presente documento y se recogieron problemáticas y sugerencias, que han sido tenidas en cuenta para la elaboración de las conclusiones y recomendaciones, así como para la propuesta de acciones que se detallan en el [apartado 6 Conclusiones y recomendaciones].

En esta fase dos, se establecieron grupos de trabajo con cada uno de los actores identificados



4 Metodología

FASE 3

Consolidación

La fase de consolidación consistió en cruzar las referencias obtenidas de distintas fuentes para su validación y para establecer las líneas generales, así como para la elaboración del presente documento.

FASE 4

Aprobación

El documento resultado de la Fase 3 ha sido circulado entre los diferentes actores de interés (industria, sector académico e investigador, Administración y talento), que han enriquecido el documento con sus aportaciones

Las líneas generales identificadas en este informe han de desarrollarse en programas específicos a ser realizados durante el periodo 2016 - 2018.

Las líneas generales identificadas en este informe han de desarrollarse en programas específicos a ser realizados durante el periodo 2016 - 2018

5 Diagnóstico inicial

Fruto del trabajo de análisis del estado del arte y de las aportaciones de los participantes en los grupos de trabajo, se ha llegado a un diagnóstico que permite terner una visión preliminar de cómo es el mercado del talento en ciberseguridad en España. Este diagnóstico se debe tomar como punto de partida para la elaboración de un estudio más exhaustivo, que aporte una visión más aproximada de la realidad del mercado.

Para dibujar el diagnóstico se establece un escenario (que hace referencia a la situación actual así como a la esperable en el corto plazo), unos limitadores (que se refieren a aquellas condiciones que representan o pueden llegar a constituir un obstáculo) y unos potenciadores (que serían factores que podrían contribuir a mejorar la situación).

Esquemáticamente, el diagnóstico para España vendría perfilado del siguiente modo.

Escenario

- Aumento de la formación en ciberseguridad.
- Aumento de los profesionales en ciberseguridad.
- Aumento de las ofertas de empleo tecnológicas.
- 94% de empleo en el sector TIC.
- Muchos puestos de ciberseguridad quedan sin ser cubiertos.
- Escasez de competencias de los profesionales de la ciberseguridad.
- Aumento de las certificaciones de ciberseguridad.

Limitadores

- Formación inadecuada:
  - Faltan mecanismos que adapten idustria-investigaciónción-academia.
  - Falta formación multidisciplinar.
  - Falta una metodología clara.
- Profesión de la ciberseguridad no definida.
- Falta formación continua para profesionales de la ciberseguridad.
- Fuga de talentos fuera de España en busca de mejores condiciones.

Potenciadores

- Formación/sensibilización desde el inicio (edad temprana).
- Interés creciente en la ciberseguridad como materia de investigación.
- La Seguridad Digital es una de las tendencias clave del mercado.
- Apuestas de los Gobiernos por la ciberseguridad.
- El emprendimiendo puede ser una alternativa.

Figura 3: Diagnóstico esquemático del mercado del talento en ciberseguridad en España.

5 Diagnóstico inicial

5.1 Escenario

5.1.1 Aumento de la oferta formativa en ciberseguridad y mayor número de personas formadas

El aumento de la oferta formativa en ciberseguridad durante los últimos años es evidente en nuestro país, así como en países del entorno. Mientras que la presencia de programas o asignaturas específicos en seguridad era anecdótica hace tan sólo unos años, en el curso académico 2014/15 se han identificado 83 programas de posgrado sobre Seguridad y Fiabilidad, de los que 26 llevan el título de Master en Ciberseguridad. Son datos del *Libro Blanco para el diseño de las titulaciones universitarias en el marco de la Economía Digital* [12]. Esta tendencia al aumento de la oferta formativa es compartida en todo el ámbito de la Unión Europea.

Relacionado con ello, están saliendo al mercado un número cada vez mayor de personas formadas en la materia, procedentes no solo del sector académico sino también del investigador, susceptibles de convertirse en profesionales de la ciberseguridad. El informe *Cybersecurity Education snapshot for workforce development in the EU* [9] menciona específicamente un aumento de profesionales de la ciberseguridad en los últimos años, de acuerdo con análisis realizados en Estados Unidos y Reino Unido.

En su compromiso con la generación de talento en ciberseguridad en España, INCIBE ha lanzado en 2015 el *Programa de apoyo a estudios de especialización en ciberseguridad*, que tiene por objetivo contribuir a la formación de expertos en ciberseguridad a través de la distribución de fondos destinados a sufragar parcialmente las matrículas de los alumnos. Un total de 25 programas de formación en ciberseguridad han resultado beneficiarios de las ayudas.

Los organismos nacionales e internacionales que expiden certificaciones profesionales relacionadas con formación en ciberseguridad proveen de información acerca de la constante profesionalización del sector. Así, de acuerdo con el informe *Digital Economy Outlook* [13] de la OCDE de 2015, el (ISC)2 (entidad que expide una amplia gama de certificaciones en ciberseguridad) habría certificado a finales del año 2013 a un total de 95.781 personas en el mundo, habiéndose cuadruplicado en una década.

También ha proliferado la oferta de una formación online más abierta y flexible para adaptarse a las necesidades de los usuarios. Los MOOC (Massive Open Online Courses) se posicionan como un elemento clave en la difusión de contenidos especializados. INCIBE, a través de su plataforma de formación online [2], proporciona una oferta formativa avanzada de ciberseguridad gratuita con el objeto de generar una masa crítica de profesionales altamente cualificados en la materia.

2. Plataforma de formación online de INCIBE: https://formacion-online.incibe.es

5 Diagnóstico inicial

Los programas de formación para el empleo llevados a cabo por distintas Administraciones y los certificados de profesionalidad, regulados por el Real Decreto 34/2008, de las cualificaciones profesionales del Catálogo Nacional de Cualificaciones Profesionales, también están contribuyendo al aumento de personas formadas en aspectos relacionados con la ciberseguridad. Partiendo de unos conocimientos esenciales en TI y con la formación adecuada, estas personas pueden desempeñar trabajos muy específicos en este ámbito.

A día de hoy, no se ha identificado la existencia de carreras universitarias específicas en seguridad informática.

5.1.2 Aumento de ofertas de empleo para titulaciones tecnológicas

Se aprecia, en general, un aumento de las ofertas de empleo en España para titulaciones tecnológicas, de acuerdo con el informe *Infoempleo Adecco 2015 de Titulaciones con más salidas profesionales* [14]. Según dicho informe, la Ingeniería Informática es la segunda titulación más demandada (por detrás de Administración y Dirección de Empresas), con el 2,9% de las ofertas de empleo de nuestro país, porcentaje que asciende al 6,8% si nos centramos en las ofertas que especifican una titulación universitaria. En el año anterior, la Ingeniería Informática ocupaba el cuarto puesto en el mismo ranking.

La creciente importancia y visibilidad de los riesgos de seguridad y privacidad ha incrementado las oportunidades profesionales para expertos en estas áreas. La demanda de profesionales en seguridad a lo largo de la última década se ha caracterizado por un aumento continuado, al igual que ocurre con los profesionales de privacidad. Esta información se refleja en el informe *Digital Economy Outlook* [13] de la OCDE de 2015. Por su parte, la consultora Burning Glass, refleja que en EEUU la demanda de puestos en ciberseguridad creció un 91% en el periodo 2010-2014, mientras que el del global de IT en el mismo periodo fue de un 28%, tres veces inferior [15].

5.1.3 Empleo en el sector TIC

Los datos del *Estudio Nacional sobre la Situación Laboral de los Profesionales del Sector de Tecnologías de la Información* (2015) [16], elaborado por el Consejo General de Colegios Profesionales de Ingeniería Informática, sugieren que existe una elevada tasa de empleo en el sector TIC. Así, el propio informe reconoce que se puede hablar de pleno empleo entre los profesionales del sector de las tecnologías de la información, pues sólo el 5,9% estaba desempleado en 2014.

La importancia de la ciberseguridad queda manifiesta, entre otras cosas, en el hecho de que el Observatorio de las Ocupaciones del Servicio Público de Empleo Estatal (SEPE) incluye específicamente, como nuevo grupo profesional, el de "Especialistas en Ciberseguridad" en su informe *Los perfiles de la oferta de empleo 2014* [17]. En él,

5 Diagnóstico inicial

el Servicio Público de Empleo Estatal configura cómo es el perfil básico de la persona desempleada y de la persona contratada perteneciente al grupo ocupacional (2729), en el que están incluidos los especialistas en ciberseguridad.

Según los datos recogidos en el propio informe, aunque la ciberseguridad es una ocupación cada vez más demandada, existen en el mercado demandantes de empleo en este sector que no se encuentran trabajando.

Habría que considerar especialmente a los egresados que finalizaron sus estudios y no han sido absorbidos por el mercado de trabajo. A pesar de manifestarse un cierto repunte en las contrataciones, la demanda existente de este tipo de profesionales no se ve del todo cubierta, debido a las razones que se indican en el punto que se describe a continuación.

5.1.4 Puestos de ciberseguridad sin cubrir y falta de competencias del profesional

La descripción del escenario se completa con un volumen importante de puestos de ciberseguridad que quedan sin ser cubiertos, en parte motivado por la falta generalizada de profesionales en el ámbito de las TIC y en particular por la escasez de competencias del profesional de la ciberseguridad. Este punto ha sido específicamente confirmado por los participantes de los grupos de trabajo. Como dato ilustrativo, según un estudio realizado por ISACA (Information Systems Audit and Control Association) y RSA Conference, entre profesionales de ciberseguridad que trabajan en empresas de Europa, América y Asia, el 59% de los encuestados piensan que la mitad o menos de los candidatos para puestos de ciberseguridad están cualificados. El mismo estudio indica que más de la mitad de las empresas emplean al menos tres meses para cubrir vacantes en seguridad, y un 28% adicional se demora hasta seis meses. Un 9% reporta no haber sido capaz de realizar la contratación [18].

Esta falta podría llegar a ser en parte cubierta con la incorporación de profesionales extranjeros que ayudaran a consolidar y potenciar el sector de la ciberseguridad, facilitando de forma indirecta el interés y la atracción de talento a este sector.

En España, considerando el ámbito profesional de la Tecnología de la Información (y no específicamente el de expertos en ciberseguridad), el informe del Ministerio de Empleo y Seguridad Social *PAFET VII: Perfiles profesionales más demandados en el ámbito de los contenidos digitales en España 2012-2017* señala que *se prevé que existirán en 2015 hasta 700.000 puestos vacantes en el ámbito TIC que no podrán ser cubiertos por falta de la formación adecuada* [19].

5 Diagnóstico inicial

La falta de adaptación de las competencias del empleado a las necesidades del puesto se aprecia especialmente en los puestos de nivel más elevado. Para un 75% de las empresas, la habilidad en la que más se manifiesta el gap es la capacidad para comprender el negocio [18] .

La escasez de competencias puede estar conectada al hecho de que la ciberseguridad, como profesión, no está aún bien definida. Sólo recientemente ha empezado a tratarse de forma separada dentro de la especialidad TIC por algunos organismos públicos y, pese a ello, todavía no existe una definición clara y universalmente aceptada del concepto mismo de ciberseguridad.

El conocimiento es uno de los ejes del talento, pero no el único. El profesional debe tener habilidades tales como la iniciativa, creatividad, comunicación, capacidad de liderazgo, orientación al cliente, motivación y trabajo en equipo, para poder integrarse exitosamente en la dinámica empresarial.

Un hecho adicional a destacar, es el bajo índice de mujeres profesionales en el entorno de la ciberseguridad, que coincide con el existente en el sector TIC en general, en el que representan solo el 30% del total de trabajadores de TI. Según el informe *Women active in the ICT sector* de la Comisión Europea [20], únicamente un 2,9% de las mujeres realizan estudios de grado en TIC y únicamente 4 de cada 1.000 continúan trabajando en el sector. La necesidad de aumentar el atractivo de la profesión desde las etapas formativas, desvinculando de su imagen como una profesión principalmente de hombres, así como una mayor conciliación laboral y familiar, pueden ayudar a paliar en parte este aspecto.

5.1.5 Aumento de las certificaciones de ciberseguridad

La creciente demanda de certificaciones es un hecho. Las titulaciones académicas pueden acreditar una formación básica pero, en un ambiente de evolución muy rápida, es difícil que puedan acreditar la actualización de conocimientos o competencias muy específicas. Éste es el terreno en el que se desenvuelven las certificaciones, posicionándose como un elemento fundamental a la hora de modelar las competencias de los profesionales.

El valor de las certificaciones es muy diverso y su validez dependerá del crédito que merezca su emisor en el mercado. En ocasiones, se ha criticado el papel de las certificaciones como fuente de negocio para las entidades emisoras, más que como vía de acreditación de conocimientos. Asumido este punto, una certificación otorgada por un emisor acreditado, debería garantizar la posesión y actualización de conocimientos específicos y reaccionar con rapidez a las nuevas demandas del mercado.

5 Diagnóstico inicial

Algunas voces críticas con las certificaciones de ciberseguridad mencionan los siguientes puntos negativos:

- Alto precio de las certificaciones y limitado impacto real una vez obtenidas.
- Exigencia de renovaciones periódicas.
- Excesivo volumen de certificaciones.
- Riesgo de obsolescencia por volubilidad de la tecnología.
- Desigual valoración de las certificaciones en el sector.

La estrategia de la UE *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* [7] propone el desarrollo de una hoja de ruta para la creación de un NIS Driving License como un programa de certificación voluntaria para promover la mejora de la capacidad y la competencia de los profesionales. ENISA (European Union Agency for Network and Information Security), Agencia de la Unión Europea para la Seguridad de las Redes y la Información, ha liderado los trabajos, a través de un proceso de consulta a las partes interesadas, para identificar los gaps entre la oferta formativa existente y las necesidades de formación. El objetivo es proponer escenarios para reducir las brechas, así como proporcionar pautas y buenas prácticas para las organizaciones de todos los Estados miembros.

El valor de las certificaciones es muy diverso y su validez dependerá del crédito que merezca su emisor en el mercado

5.2 Limitadores

5.2.1 Formación inadecuada al puesto de trabajo

En este contexto, ante la imposibilidad de seleccionar los perfiles deseados, las organizaciones están optando por reclutar a profesionales que, en ocasiones, presentan carencias en competencias y/o conocimientos. Las empresas participantes en los grupos de trabajo están de acuerdo en reconocer las problemáticas asociadas a esta política.

5 Diagnóstico inicial

Las organizaciones buscan formas de cobertura incompleta, es decir, contratando a profesionales que no presentan todas las competencias requeridas, y por ello, se aprecia una brecha entre los requerimientos de las empresas y las características de los candidatos / empleados. A pesar de la creciente oferta formativa, esta brecha continua aumentando, dado que la oferta de profesionales crece a menor ritmo que la demanda de estos perfiles expertos.

La principal razón que justifica esta brecha deriva de la propia dinámica del sector, en constante evolución. Los mecanismos para la certificación y actualización de los programas académicos son, a menudo, más lentos que la velocidad a la que evoluciona la tecnología relacionada con las ciberamenazas.

La oferta de profesionales crece a menor ritmo que la demanda de estos perfiles expertos

Un dato ilustrativo: la proporción de descargas de malware desconocido, de acuerdo con el *2015 Check Point Annual Security Report,* [21] ha pasado de 2,2 por hora en 2013 a 106 por hora en 2014. Para hacer frente a estas amenazas, la adquisición de nuevos conocimientos debería realizarse a una velocidad que, en el momento actual, las instituciones educativas tradicionales no están en condiciones de proveer mediante programas que sigan los canales estandarizados para su oficialización y actualización. Los programas académicos proporcionan a los alumnos un punto de partida para adquirir unos conocimientos básicos en amplios aspectos relacionados con el bien a proteger, pero es difícil que sean capaces de satisfacer las necesidades de un mercado de trabajo dinámico. Para ello, es necesario que existan programas de formación especializada, que se configuren a través de un diálogo directo entre la industria y el sector académico e investigador y que permitan adquirir conocimientos en las últimas tendencias o tecnologías. A partir de ahí, las certificaciones en aspectos de muy alta especialización, pueden terminar por completar las necesidades demandadas.

El sector investigador puede desempeñar un papel importante para ayudar a acercar el sector académico a la realidad de la empresa a través de la formación avanzada de profesionales y el asesoramiento para la creación de los itinerarios formativos adecuados.

De manera complementaria, la dificultad en el diseño de los contenidos formativos que deben formar parte del currículo académico en ciberseguridad es una realidad. El informe *Cybersecurity Education snapshot for workforce development in the EU* [9] apunta para la Unión Europea que no existe suficiente formación de carácter multidisciplinar que combine formación técnica en ciberseguridad con otra complementaria y necesaria para la práctica profesional: privacidad, entorno legal y regulatorio, aspectos económicos, usabilidad, etc.

Según refleja el informe del proyecto *Mapa de Enseñanza de la Seguridad de la Información* [22] en España no se encuentran programas de Máster que profundicen en temáticas actuales; como técnicas de hacking, informática forense, *exploits*, seguridad web, ciberseguridad, etc.
Un factor clave es la falta, aún existente, de un nivel de inglés adecuado, lo que tiene un gran impacto en el mundo de la seguridad informática, ya que muchos de los materiales

5 Diagnóstico inicial

No existe suficiente formación de carácter multidisciplinar que combine formación técnica en ciberseguridad con otra complementaria y necesaria para la práctica profesional

educativos se encuentran en ese idioma. Según el informe *EPI 2015* [23] elaborado por Education First, España se sitúa en 2015 en el puesto 23 de 70 países, descendiendo tres puestos respecto al año anterior. Un refuerzo en su desarrollo desde las etapas tempranas de formación es, por tanto, indispensable.

Otro factor que ayuda a explicar el desajuste entre las necesidades de la empresa y la capacitación del candidato se encuentra en la dificultad para adquirir experiencia práctica previa. En ocasiones, durante las etapas de formación, los jóvenes utilizan software libre para la adquisición de competencias, mientras que las empresas demandan experiencia en software propietario. En la práctica, la utilización de este tipo de software propietario acarrea un coste difícilmente asumible por los jóvenes.

La inexistencia de una metodología clara para enseñar ciberseguridad se posiciona como otro aspecto crítico. Las diferencias de enfoque varían desde el académico tradicional hasta la organización de retos o desafíos en ciberseguridad basados en ejercicios prácticos de detección y respuesta a intrusiones. Estos ejercicios son utilizados como forma de aprendizaje por los jóvenes talentos y, al mismo tiempo, como vía de identificación de talento por parte de las empresas.

Por último, no debe concluirse que la necesidad de formación especializada en ciberseguridad afecta exclusivamente a los perfiles más técnicos. El mercado irá demandando perfiles cada vez más especializados en ciberseguridad en el campo operativo, jurídico y actuarial.

5.2.2 Profesión de ciberseguridad no definida

La falta de una metodología clara y compartida de enseñanza de la ciberseguridad y la escasez de competencias profesionales entre los perfiles se explica, entre otras razones, por la inexistencia de una definición precisa de la profesión de ciberseguridad, con una identificación clara de perfiles, competencias y conocimientos.

5.2.3 Formación continua para profesionales

Dada la rápida evolución tecnológica del mercado, es imprescindible un proceso de formación continua para mantener vigentes los conocimientos del profesional en ejercicio. Si bien existen mecanismos coordinados por distintas Administraciones, que permiten la actualización o reciclado para el empleo, éstos se suelen referir a conocimientos básicos o generales, pero no a aquellos avanzados o última generación. No existe, por tanto, en la actualidad, un mecanismo estandarizado que permita la actualización de conocimientos avanzados, más allá de la autoformación y de la formación ad hoc proporcionada por la empresa a sus empleados.

5 Diagnóstico inicial

En particular, se aprecia esta circunstancia cuando se trata de situaciones de formación de emergencia en ciberseguridad, para su puesta en marcha ante nuevas y urgentes necesidades derivadas de la aparición de nuevos ataques. Esta necesidad es compartida por muchas áreas distintas relacionadas con la tecnología.

Algunas grandes empresas, cuyo volumen de plantilla les permite tener una masa crítica de profesionales, han optado por elaborar un currículo formativo adaptado a sus necesidades y desarrollado en la propia empresa, ya que no encuentran en el mercado una formación tan específica.

5.2.4 Fuga de talentos

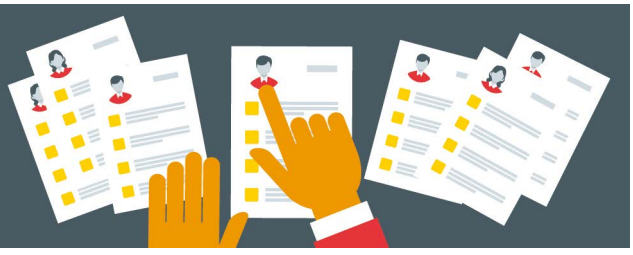
Uno de los limitadores más graves es la fuga de talentos fuera de España en busca de proyectos profesionales atractivos y salarios competitivos. El talento se ve atraído por aspiraciones internacionales y, en este terreno, las grandes empresas cuentan con la ventaja de disponer de planes de movilidad internacional, permitiéndoles una capacidad de retención no accesible a otras de menor tamaño o con una menor implantación internacional, o fórmulas de trabajo flexible que incluyen, por ejemplo, la prestación de servicios desde España a empresas ubicadas en otros países.

Otro aspecto que pesa a la hora de decidir trabajar fuera de España es la posibilidad de aprender de la mano de los mejores. Esta motivación inspira a muchos jóvenes talentos a establecerse en núcleos tecnológicos como Silicon Valley.

Estas circunstancias, unidas a la atractiva remuneración que el profesional de la ciberseguridad percibe fuera de España, están contribuyendo a que se contemple favorablemente la opción de desarrollar la carrera profesional en el extranjero.

La cuestión salarial fue ampliamente discutida en los grupos de trabajo, con la conclusión mayoritaria de que los salarios del profesional de la ciberseguridad en España no estaban al nivel de la importancia estratégica que dicha figura debería tener en los organigramas empresariales. Así, el informe *Los perfiles de la oferta de empleo 2014* [17] del Servicio Público de Empleo Estatal (SEPE) sitúa el salario medio del especialista en ciberseguridad en el rango 17-33 mil €/año (el dato se obtiene del análisis de una muestra de 59 ofertas publicadas en internet).

El valor de las certificaciones es muy diverso y su validez dependerá del crédito que merezca su emisor en el mercado



5 Diagnóstico inicial

5.3 Potenciadores

5.3.1 Estimulación temprana del talento

Si bien las formaciones superiores y certificaciones permiten acreditar competencias específicas en profesionales ya en ejercicio o próximos a estarlo, es necesario también garantizar un flujo de entrada de nuevos talentos en potencia. Sin embargo, una encuesta realizada por Raytheon y la National Cybersecurity Alliance (NCSA) [24] muestra que un 70% de los jóvenes europeos afirma, que ningún profesor u orientador educativo les mencionó nunca la ciberseguridad como una posible carrera profesional.

Desde 2014, INCIBE impulsa el programa "Espacios de Ciberseguridad", consistente en impartir charlas gratuitas sobre ciberseguridad dirigidas a estudiantes de secundaria que están empezando a definir su carrera profesional

Se están empezando a poner en marcha programas centrados en formar y sensibilizar en ciberseguridad desde una edad temprana. Dichos programas se promueven en el entorno de la Unión Europea con el objetivo de concienciar a los más jóvenes sobre la importancia de la ciberseguridad y bajo la coordinación de ENISA.

La ampliación de las ciberamenazas, en forma de distintos tipos de delincuencia informática dirigida hacia los más jóvenes, ha contribuido a un creciente interés en torno a estos programas y a su alusión en distintas fases de la educación primaria y secundaria. A pesar de ello, se hace necesario su tratamiento de manera más formal mediante la introducción, acorde al nivel educativo, de conceptos relacionados con la seguridad en asignaturas ya existentes o con la creación de otras nuevas específicamente en esta materia.

Desde 2014, INCIBE está impulsando el programa "Espacios de Ciberseguridad", consistente en impartir charlas gratuitas sobre ciberseguridad, dirigidas a estudiantes de secundaria que están empezando a definir su carrera profesional. El objetivo es que los adolescentes sean capaces de adquirir conocimientos avanzados en ciberseguridad para así estimular la generación de talento. A partir de 2015 se ha incluido a los profesores en la iniciativa, para que sean ellos quienes introduzcan a sus alumnos de secundaria o FP en el mundo de la ciberseguridad.

5.3.2 Importancia estratégica de la ciberseguridad

Hay un interés creciente en la ciberseguridad como materia de investigación, interés al que pueden haber contribuido tanto los esfuerzos patrocinados desde múltiples ámbitos institucionales en la evaluación de la formación y entrenamiento en ciberseguridad, como en la imagen social del hacker[3] y su atractivo para estudiantes de distintos niveles.

3. Aunque la RAE define hacker como "pirata informático", en la comunidad de la ciberseguridad se hace una distinción entre "hacker de sombrero blanco" como aquel profesional con muy altos conocimientos en seguridad informática que protege los sistemas frente a vulnerabilidades, en contraposición al "hacker de sombrero negro" que lo que busca es romper la seguridad con fines maliciosos. Es con esta connotación de "sombrero blanco" con la que se utiliza el término hacker en este documento.

5 Diagnóstico inicial

En 2013, el Gobierno de España publica la *Estrategia Nacional de Ciberseguridad [25]* con el fin de dar respuesta al enorme desafío que supone la preservación del ciberespacio de los riesgos y amenazas que se ciernen sobre él. La Estrategia menciona expresamente como uno de sus seis objetivos la capacitación, definida como *alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de la ciberseguridad.*

En el terreno laboral, crece el número de organizaciones que facilitan formación en ciberseguridad a sus miembros o empleados y aparecen iniciativas dirigidas desde los Estados, a fin de garantizar la seguridad digital que, en la actualidad, aparece como una tendencia clave del mercado.

En 2014, una encuesta de la OCDE sobre economía digital concluyó que los gobiernos identificaban la seguridad como la segunda prioridad, y la privacidad como la tercera, de entre 31 posibles áreas de prioridad. Solo en 2014 la cuantía de registros con información personal robados ascendió a 1.000 millones de dólares.

Sin embargo, se debe seguir concienciando a la sociedad en su conjunto (empresas, instituciones, formadores y público en general), sobre la importancia de la ciberseguridad en un mundo cada vez más digital y tecnológicamente complejo y conectado. Solo así se podrá valorar adecuadamente la profesión de la ciberseguridad y a los profesionales que la desarrollan.

5.3.3 Emprendimiento en ciberseguridad

A partir de los análisis realizados por INCIBE, el colectivo de emprendedores ofrece tanto servicios como productos de ciberseguridad, y suelen presentar un perfil profesional y de experiencia elevado.

Por último, la posibilidad de emprendimiento en el terreno de la ciberseguridad puede permitir cubrir la distancia entre la gran organización internacional (con fuertes equipos especializados y la posibilidad de una carrera profesional atractiva) y las Pymes, que necesitan cubrir sus requerimientos, pero no disponen de tales opciones ni de una masa crítica que les permita la contratación de especialistas a tiempo completo. La provisión de servicios externos desde organizaciones especializadas puede permitir la cobertura de tal necesidad.

El emprendimiento en ciberseguridad es una cuestión de especial interés para INCIBE, que está apostando por iniciativas de estímulo. Mediante acciones coordinadas de esfuerzos, INCIBE está aportando recursos, capacidades técnicas y personal cualificado para contribuir a generar un ecosistema que favorezca oportunidades, innovación y emprendimiento en este ámbito. Reflejo de ello es la Aceleradora de Start Ups cuya primera edición tuvo lugar en 2015, en la que se seleccionaron 5 empresas que, a la fecha de elaboración del presente informe, son ya una realidad, y el Programa de Ciberemprende, puesto en marcha con el objetivo de crear una comunidad de emprendimiento y estímulo de proyectos de ciberseguridad.

6 Conclusiones y recomendaciones

A partir del diagnóstico dibujado en el epígrafe anterior, se extraen una serie de conclusiones y recomendaciones, que inspiran una propuesta de acciones enumeradas en la [Tabla 2: Propuesta de acciones]. La primera de esas propuestas, es la realización de un estudio detallado sobre la situación de la ciberseguridad en España en todos sus aspectos, académico, industrial, profesional y de conocimiento por la sociedad. Dicho estudio proporcionará una visión más completa y aproximada a la realidad, que permitirá corroborar o matizar las conclusiones y recomendaciones, así como adaptar o ampliar el resto de acciones propuestas. El desarrollo y ejecución de las acciones requerirá del diseño de planes específicos de actuación a lo largo del periodo 2016 - 2018.

Las conclusiones y recomendaciones obtenidas del diagnóstico inicial, se estructuran en torno a las siguientes fases:

- Generación de talento.
- Identificación de talento.
- Captación de talento.
- Retención del talento.
- Gestión del talento.

6.1 Generación de talento

La generación de futuros talentos en ciberseguridad pasa necesariamente por la estimulación de vocaciones desde la infancia y adolescencia temprana. La utilización de técnicas de gamificación para la formación en conceptos y detección de habilidades del menor, que estimulen la orientación hacia estudios relacionados con las TIC y su posterior especialización en ciberseguridad, podrían ser elementos determinantes en la creación de talento.

INCIBE, a través de las jornadas de "Espacios de Ciberseguridad", está contribuyendo a la difusión y formación en conceptos de ciberseguridad a estudiantes de secundaria. De esta forma, además de formarles, se les pone en conocimiento de una alternativa más, dentro del conjunto de posibles salidas profesionales.

La generación de futuros talentos en ciberseguridad pasa necesariamente por la estimulación de vocaciones desde la infancia y adolescencia temprana

Así mismo, se pueden desarrollar actividades orientadas a fomentar el deseo de niños y adolescentes de convertirse en expertos en ciberseguridad, los denominados "hackers de sombrero blanco", en cualquiera de sus múltiples vertientes (técnica, operativa, jurídica, etc.). Aprovechando la atractiva imagen social de éstos, y cultivando mediante dichas actividades las cualidades necesarias para conseguirlo, como la curiosidad, perseverancia, independencia, capacidad para descomponer situaciones complejas y ganas de aprender, se contribuirá a difundir la profesión de especialista en ciberseguridad y a conocer la realidad de un trabajo, a la vez atractivo y desconocido. Atractivo por lo que supone la posibilidad de trabajar en el mundo TIC con tecnología punta y con la necesidad de tener los conocimientos continuamente actualizados, en un entorno cada vez más complejo y demandante de este tipo de perfiles, y a la vez desconocido, por la falta de una definición clara de la profesión.

6 Conclusiones y recomendaciones

Se hace indispensable la adecuación de los programas formativos o la creación de otros nuevos específicos

De manera más específica, los adolescentes y jóvenes que se encuentran próximos a la elección de estudios o inserción laboral, y que manifiestan habilidad e interés por el área de la Tecnología de la Información, demandan una orientación académica y profesional sobre las opciones disponibles para desarrollarse profesionalmente en el mundo de la ciberseguridad: estudios, programas de becas o ayudas, certificaciones, eventos, retos, autoempleo, posibilidad de emprendimiento y la investigación. Esta orientación, que es clave para encauzar el talento hacia el máximo potencial, ya se está realizando desde hace unos años para otros ámbitos profesionales, a través de salones o eventos especializados, y sería conveniente incluir también en ellos la ciberseguridad.

En estos salones se organizan diferentes espacios donde se muestra la oferta formativa, actividades relacionadas con las salidas profesionales explicadas directamente por técnicos, además de talleres sobre otros temas transversales, como la realización de presentaciones, entrevistas o la confección del curriculum, entre otros.

Una Formación Profesional (FP) en ciberseguridad, puede constituir una vía complementaria al catálogo formativo existente para acercar el talento técnico y las necesidades de empresas.

La Universidad y, en general, el sector académico e investigador, deben seguir jugando un papel predominante en la generación de talento. Se hace indispensable la adecuación de los programas formativos, o la creación de otros nuevos específicos, para acercar de la mejor forma posible la oferta a la necesidad real del mercado. Se deben impulsar fórmulas de apoyo a estudiantes 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.

La generación de profesionales altamente especializados en ciberseguridad dentro del ecosistema investigador permite cubrir la propia demanda de dicho ecosistema, así como permitir el trasvase o transferencia de profesionales al sector empresarial o industrial de forma temporal o permanente, a través de spin-off, emprendimiento, colaboraciones, o bien de forma directa, siendo en último término el sector de la ciberseguridad nacional el gran beneficiario de esta promoción de talento.

En este sentido, y adecuándolos a cada nivel formativo, se deben tener en cuenta no solamente los aspectos técnicos, sino también aquellos relacionados con habilidades transversales (conocidas también como “soft skills”), tales como la comunicación o el trabajo en equipo. La consideración de valores éticos en el mundo de la ciberseguridad y el hacking debe acompañar cualquier actuación orientada a proporcionar formación e inspiración a los futuros profesionales.

6 Conclusiones y recomendaciones

6.2 Identificación de talento

En España existen diferentes fuentes desde las que identificar el talento en ciberseguridad en estados iniciales. Algunas de ellas son, por ejemplo, las competiciones de ciberseguridad, las universidades y centros de formación, los equipos de investigación y los eventos especializados. INCIBE está interviniendo directamente en algunas de estas actuaciones de identificación de talento: organización de eventos y retos de ciberseguridad, lanzamiento de cursos en formato MOOC, otorgamiento de becas de estudios de especialización en ciberseguridad, impulso de una red de centros de excelencia en I+D+I en ciberseguridad, aceleración de *Start-Ups* de ciberseguridad, etc.

El primer paso para la gestión del talento y el acercamiento del mismo a las empresas, consiste en una correcta identificación de las personas con potencial. Para ello, resulta imprescindible la coordinación de dicha identificación desde las distintas fuentes y tenerlo en cuenta para la construcción de una base de datos con los mejores talentos en ciberseguridad (no solo del talento residente en España, sino también de aquel que se encuentra trabajando o estudiando en el extranjero). Esta base de datos, y siempre que exista una viabilidad y cobertura legal para ello, podría llegar a ser consultada por reclutadores: empresas y centros de investigación principalmente.

6.3 Captación de talento

Las fórmulas habituales de selección de recursos humanos pueden no ser las más efectivas para captar el talento en ciberseguridad. Los miembros del grupo de trabajo de talento, participantes en la Fase 2 del modelo, coinciden en que los requisitos de los puestos de trabajo publicados por las empresas suelen incluir filtros previos de titulación, certificaciones y experiencia previa, excesivos para las condiciones laborales ofertadas. Por su parte, las empresas manifiestan que, con frecuencia, los técnicos seleccionados no reúnen las competencias demandadas por el reclutador.

Se deben establecer mecanismos de captación eficaces que permitan a empresas, universidades, investigadores y reclutadores en general, identificar el talento real en los procesos de selección

En este contexto, se deben establecer mecanismos de captación eficaces que permitan a empresas, universidades, investigadores y reclutadores en general, identificar el talento real en los procesos de selección, para cubrir sus programas o sus puestos de trabajo y, una vez identificado, interactuar de manera libre.

Los mecanismos para la captación del talento, deben adaptarse a los espacios específicos del sector, que en el caso de la ciberseguridad, se concentran en torno a competiciones y retos donde los participantes ponen a prueba sus habilidades. La celebración de este tipo de eventos es un fenómeno en auge tanto en España como en Estados Unidos y en los países de nuestro entorno. A nivel europeo, se celebra anualmente el European Cyber Security Challenge, competición que tiene por objetivo determinar qué país tiene los mejores talentos cibernéticos, a través de la resolución de pruebas prácticas de alta complejidad.

En el contexto actual no se deben excluir los talentos extranjeros de las actuaciones impulsadas para captar talento en ciberseguridad.

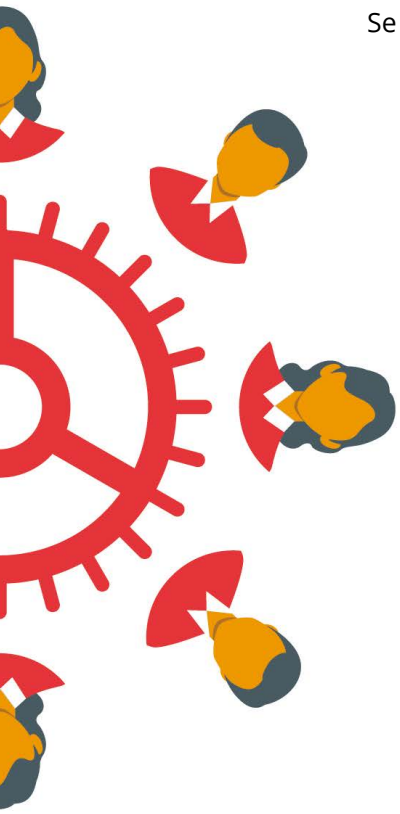
6 Conclusiones y recomendaciones

6.4 Retención del talento

Es necesario implementar prácticas eficaces que contribuyan a paliar la fuga de talentos fuera de España y a recuperar los profesionales que han emigrado

Es necesario implementar prácticas eficaces que contribuyan a paliar la fuga de talentos fuera de España, y a recuperar los profesionales que han emigrado.

Este problema del éxodo o fuga del talento se da, tanto en el mundo de la empresa, como en el de la investigación. Para cualquiera de ellos, podrían aplicarse diversos y efectivos mecanismos que permitirían la retención del talento, y que formarían parte de las políticas de cada empresa o centro investigador. Además de la propia "marca" y su relevancia en el sector, mecanismos eficaces de retención pueden ser: la oferta de proyectos profesionales interesantes, el reconocimiento y prestigio, tanto empresarial, como social, sin olvidar una acorde remuneración económica. En este punto, los reclutadores son responsables de garantizar unas condiciones interesantes para retener, e incluso recuperar, el talento. También son necesarias políticas nacionales, bien coordinadas desde la administración, bien a través de iniciativas público-privadas, que pongan el foco en potenciar e impulsar iniciativas para que el sector de la ciberseguridad nacional sea un universo atractivo para los profesionales nacionales, así como polo de atracción de talento especializado internacional.



Se debe avanzar en varias vías:

- **Sensibilizar a las empresas sobre 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. En este punto, se aprecian diferencias en el grado de concienciación entre empresas grandes, internacionales y con sistemas abiertos (más conscientes, en general, del valor del profesional de la ciberseguridad) y empresas pequeñas y medianas.

- **Estudiar el fenómeno de los expertos en ciberseguridad españoles que están trabajando fuera de nuestras fronteras**. En concreto, es interesante el establecimiento de medidas que permitan cuantificarlos, identificarlos, conocer y entender sus necesidades y motivos de marcha, para así estudiar posibles formas de contacto que permitan formular políticas de repatriación y recuperación del talento. Este estudio es la base para la formulación de medidas que permitan frenar la emigración y retener efectivamente el talento.

- **Replantear políticas y líneas de investigación nacionales** de forma que el resultado de las mismas permita la solución a los problemas y necesidades actuales de los usuarios e industria, así como adelantarse a las tendencias futuras del mercado. Dichas políticas deberían facilitar el trasvase de conocimiento y tecnología entre la industria y grupos de investigación,

6 Conclusiones y recomendaciones

impulsando el acercamiento entre ambos sectores. Se conseguiría así, crear un entorno más atractivo para el talento investigador, con la posibilidad de trabajar en líneas punteras de investigación, de emprender o de incorporarse en una empresa nacional, incentivando de esta forma la retención y atracción del mismo.

- **Buscar mecanismos que contribuyan a que las empresas y centros de investigación difundan su marca** como actores relevantes en el sector de la ciberseguridad, pasando a convertirse así en atrayentes y retenedores de talento.

6.5 Gestión del talento

Dentro de este sub-epígrafe, se incluyen una serie de actuaciones de carácter más transversal, que abarcan todos los estados anteriores. Las conclusiones y recomendaciones en este punto son las siguientes.

La implementación de un modelo para la gestión y seguimiento del talento en ciberseguridad en España requiere la identificación de unos indicadores claros que permitan medir el nivel de efectividad de las medidas, así como el establecimiento de itinerarios acordes al nivel de madurez de las personas con talento. Para ello, el primer paso es la construcción de una base de datos que recoja las personas con talento identificadas en las diferentes iniciativas lanzadas por INCIBE y otros actores (ver [apartado 6.2 Identificación de talento]). El diseño de un plan de impactos personalizado y dirigido a cada público objetivo permitirá lanzar mensajes adaptados al estado de madurez de las personas con talento, acercarles a iniciativas interesantes y conectar oferta y demanda. La elaboración de un plan racional de comunicaciones vía correo electrónico tiene el doble objetivo de orientar itinerarios de desarrollo para cada sujeto, así como informarles sobre actividades profesionales de interés en su carrera. En última instancia, se debe avanzar hacia un modelo en el que los reclutadores (empresas y centros de investigación, principalmente) puedan acceder y consultar la base de datos e interactuar libremente con el talento.

CyberCamp es el gran evento de la ciberseguridad que, en su edición de 2015, reunió a más de 10.000 personas de manera presencial y otras 12.000 online. CyberCamp debe ser el punto de encuentro donde confluyan todas las iniciativas de gestión del talento lanzadas o coordinadas desde INCIBE. Se posiciona como el foro perfecto para permitir la conexión entre los diferentes actores, promoviendo la participación de aquellos interesados en el diseño de las actividades a realizar, de forma que puedan utilizar CyberCamp como punto de identificación y captación de talento.

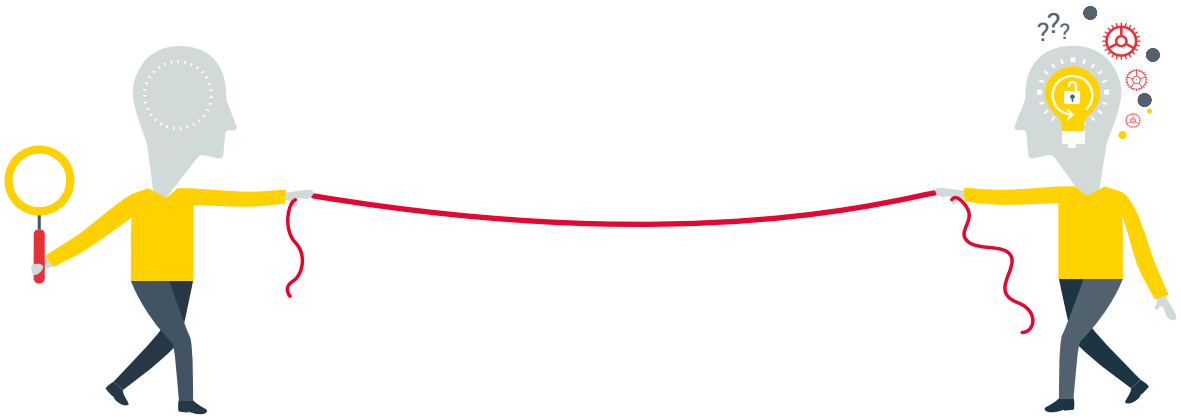
La falta de un itinerario en ciberseguridad definido, aconseja el lanzamiento de acciones de asesoramiento a los jóvenes sobre posibles trayectorias educativas y profesionales.

6 Conclusiones y recomendaciones

CyberCamp debe ser el punto de encuentro donde confluyan todas las iniciativas de gestión del talento

En este sentido, un proyecto de *mentoring* puede resultar atractivo y útil. Se trata de un modelo donde expertos en activo, procedentes del mundo empresarial y académico, pueden compartir sus experiencias con jóvenes con talento en ciberseguridad con menos experiencia, y servirles de apoyo y orientación tanto en aspectos técnicos ,como en cuestiones de carácter general.

En la misma línea de otros países que han realizado el esfuerzo de identificar perfiles competenciales relativos a la ciberseguridad, se debe avanzar hacia un modelo de definición de los perfiles válido para España como paso previo para la identificación de las competencias y conocimientos necesarios. Para ello, se pueden tomar como punto de partida modelos ya existentes y definidos en las políticas de ciberseguridad de otros países. Se hace necesario disponer de un diagnóstico realista de la situación actual en España, que permita un análisis comparativo de competencias en ciberseguridad demandadas con respecto a estudios ofertados. Para ello, es imprescindible contar con una visión conjunta de la empresa, centros de investigación, la Universidad / sector educativo en general y los propios profesionales del sector, de cara a definir esos perfiles competenciales que permitan un mayor acercamiento entre oferta y demanda.



La implementación de un sistema de reconocimiento y acreditación de conocimientos y competencias, tipo *badges* digitales, puede contribuir a que los interesados quieran dar a conocer sus competencias en el mercado. Se les dotaría así de una mayor visibilidad hacia el resto de actores del ecosistema de la ciberseguridad, facilitando su interacción con ellos, al mismo tiempo que éstos podrían comprobar y verificar de una forma fehaciente las competencias mostradas.

De forma paralela a la definición de los perfiles profesionales, se debe avanzar hacia el establecimiento de una 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.

6 Conclusiones y recomendaciones

6.6 Propuestas de acciones

Fruto de las conclusiones y recomendaciones identificadas en los apartados anteriores, se propone la puesta en marcha de una serie de acciones que contribuyan a solventar la falta de profesionales especializados en ciberseguridad.

A0

Diagnóstico de situación de la ciberseguridad en España

Realización de un estudio exhaustivo que permita la obtención de un diagnóstico del panorama de la ciberseguridad en España y en el que se tenga en cuenta el punto de vista de los diferentes actores que en él intervienen (Industria, Sector Académico e Investigador, Administración y Profesionales). Como consecuencia de dicho diagnóstico, se obtendrán conclusiones y recomendaciones que permitirán la elaboración de un catálogo de acciones a poner en marcha. Dicho catálogo podrá ampliar o modificar, tanto en número como en forma, las acciones incluidas en esta propuesta.

A1

Contenidos "Pequeños hackers"[4]

Creación o fomento de contenidos audiovisuales, juegos, concursos, charlas, películas, series de TV, dirigidos a niños y preadolescentes con el objetivo de estimular el deseo de convertirse en hackers u otros expertos en seguridad y cultivar las cualidades necesarias para poder llegar a ser un profesional, como curiosidad, perseverancia, independencia, capacidad para descomponer situaciones complejas y ganas de aprender.

En este punto, se puede contar con figuras públicas de peso en el mundo de la ciberseguridad, el patrocinio de series de TV o películas, así como aprovechar sinergias con los canales de INCIBE abiertos a los menores (OSI Menores).

4. Para las acciones A1 y A2 se utiliza el término "hacker" como genérico, por el carácter aspiracional que la profesión puede tener entre el colectivo de menores y adolescentes. Se incluyen en el alcance de las acciones, no obstante, aspectos referentes a otras profesiones enmarcadas en el sector de la ciberseguridad, no exclusivamente las competencias de los hackers en sentido estricto.

6 Conclusiones y recomendaciones

A2	**Contenidos "Conviértete en hacker"**	Creación o fomento de contenidos multimedia dirigidos a adolescentes y jóvenes con el objetivo de que conozcan el día a día de un profesional experto en distintos ámbitos de la ciberseguridad y puedan orientar sus pasos académicos y profesionales, incluyendo información sobre los perfiles profesionales de la ciberseguridad, estudios, certificaciones, eventos, retos, empleo, autoempleo, investigación, etc. Consideración de valores éticos en el mundo de la ciberseguridad y el hacking. También en este punto es interesante recurrir a fórmulas y canales que permitan maximizar la difusión, tales como los salones de estudios, así como aprovechar sinergias con otras iniciativas de INCIBE ("Jornadas Espacios de Ciberseguridad" para alumnos y profesores, MOOC, CyberCamp, European Challenge y Becas INCIBE).
A3	**Ciberseguridad en la Formación Profesional**	Avanzar hacia un modelo de Formación Profesional de Ciberseguridad, estudiando el estado del arte e identificando cómo satisfacer las necesidades de las empresas.
A4	**Base de Datos de Talento en Ciberseguridad**	Construcción de una base de datos con los talentos en ciberseguridad identificados mediante las iniciativas lanzadas por INCIBE y otros actores, como CyberCamp, Becas INCIBE, retos, eventos, MOOC, competiciones y otros. Establecimiento de mecanismos de detección del talento para el mantenimiento actualizado de la misma.

6 Conclusiones y recomendaciones

Todos los datos serán almacenados con el consentimiento del interesado y cumpliendo estrictamente la normativa fijada por la LOPD. Esta base de datos, y siempre que exista una viabilidad y cobertura legal para ello, podría llegar a ser consultada por reclutadores: empresas y centros de investigación principalmente.

A5 **Apoyo a eventos de ciberseguridad**

Apoyo a la identificación del talento en eventos que incluyan total o parcialmente aspectos relacionados con la ciberseguridad.
El apoyo se realizará a través de:

1) Celebración de retos y pruebas enfocadas a la detección del talento en ciberseguridad (CTF, wargames, hackathons, etc.) y su atracción hacia CyberCamp.
2) Presentación de trabajos, CFP, como resultado de investigación teórica y práctica.
3) Impulso de acciones que permitan a los reclutadores la interacción directa con los jóvenes participantes en los eventos, como canal de detección del talento.
4) Visibilidad a los participantes destacados en los eventos a través de vídeos, reportajes u otros canales, que permitan a las empresas conocer a los mejores talentos. Esta visibilidad se realizará siempre bajo la voluntad de los interesados y cumpliendo estrictamente la normativa fijada por la LOPD.

A6 **Repatriación del talento en ciberseguridad**

Estudio del fenómeno de los expertos en ciberseguridad expatriados, cuantificándolos y determinando sus necesidades con vistas a la formulación de futuras políticas de re-captación y prevención de fuga de futuros talentos.

6 Conclusiones y recomendaciones

A7	**Plan de impactos personalizado para cada público objetivo y explotación de la BBDD**	Sobre la base de la Base de Datos (acción A4), envío de mensajes adaptados al estado de madurez de las personas con talento, acercarles a iniciativas interesantes y conectar oferta y demanda. En un estadio más avanzado, permitir a las empresas acceder a la BBDD de Talento. Tanto el envío de mensajes como el acceso a la BBDD de Talento, se realizará siguiendo estrictamente la normativa fijada por la LOPD.
A8	**Mentoring en ciberseguridad**	Plataforma o mecanismo que ponga en contacto personas con interés en la ciberseguridad (estudiantes o profesionales), con un experto en activo que les pueda proporcionar orientación académica y profesional, así como apoyo en cuestiones de carácter más general.
A9	**Perfiles de ciberseguridad**	Definición del marco de referencia de profesionales del sector de la ciberseguridad y confianza digital que identifique las ocupaciones, conocimientos, habilidades, competencias y cualificaciones. Publicación online del catálogo.
A10	**Badges digitales**	Implantación de un sistema de acreditación y reconocimiento de competencias para los talentos detectados a través de cursos MOOC, retos, hackathones, jornadas, eventos, etc. mediante identificativos digitales específicos emitidos por INCIBE.

6 Conclusiones y recomendaciones

		Posibilidad de publicación de los credenciales obtenidos, lo que aumentará la visibilidad de sus titulares frente al resto de actores y facilitará la validación y verificación de los mismos.
A11	**Profesión de la ciberseguridad**	Avanzar hacia el 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.
A12	**Ayudas para la realización de estudios de especialización en ciberseguridad**	Programa de becas de estudios de especialización en ciberseguridad.
A13	**Ayudas para la excelencia de los equipos de investigación avanzada en ciberseguridad**	Programa de ayudas para fortalecer y mejorar las capacidades de los equipos de investigación avanzada en ciberseguridad nacionales, promoviendo la contratación de investigadores (doctorandos y doctores) al mismo tiempo que permite generar y retener el talento especializado en ciberseguridad.

Tabla 2: Propuesta de acciones
Las actuaciones serán llevadas a cabo a lo largo del periodo 2016 - 2018

7 Próximos pasos: puesta en marcha del modelo

La puesta en marcha del modelo exige la actuación coordinada de todos los actores, así como la definición de unos indicadores de impacto claros. Esquemáticamente, la ejecución de las actuaciones identificadas seguirá el siguiente planteamiento temporal.

Figura 4: Planteamiento temporal para la ejecución de las actuaciones indentificadas.

8 Referencias

[0] European Commission, «Grand Coalition for Digital Jobs» March 2015. [En línea]. Available: https://ec.europa.eu/digital-single-market/en/blog/here-how-we-will-improve-digital-skills-and-create-more-jobs-europe-0. [Último acceso: Diciembre 2016].

[1] ISC)2 International Information Systems Security Certification Consortium, «(ISC)² Global Information Security Workforce Study,» 2015. [En línea]. Available: https://www.isc2cares.org/IndustryResearch/GISWS/. [Último acceso: Noviembre 2015].

[2] Symantec, «NASSCOM Partners with Security Leader Symantec for Building Cyber Security Skills in India,» 18 June 2015. [En línea]. Available: https://www.symantec.com/en/aa/about/news/release/article.jsp?prid=20150618_01. [Último acceso: Enero 2016]

[3] A. Setalvad, «Demand to fill cybersecurity jobs booming,» 31 March 2015. [En línea]. Available: http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/. [Último acceso: Enero 2016].

[4] NICCS, National Initiative for Cybersecurity Careers and Studies, «Framework Specialty Areas,» Department of Homeland Security, EEUU, [En línea]. Available: https://niccs.us-cert.gov/training/tc/framework/specialty-areas. [Último acceso: Enero 2016].

[5] Homeland Security Advisory Council, «Cyberskills Task Force Report,» 2012. [En línea]. Available: https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf. [Último acceso: abril 2016].

[6] Prime Minister's Office, Israel, «Bureau's Activities,» Prime Minister's Office, Israel, 2013. [En línea]. Available: http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/Activities.aspx. [Último acceso: Enero 2016].

[7] European Commission, «EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive,» February 2013. [En línea]. Available: https://ec.europa.eu/digital-single-market/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security [Último acceso: Enero 2016].

[8] European Union Agency for Network and Information Security (ENISA), «Roadmap for NIS education programmes in Europe,» 31 Octubre 2014. [En línea]. Available: https://www.enisa.europa.eu/publications/roadmap-for-nis-education-programmes-in-europe. [Último acceso: Abril 2016].

[9] M. H. (. D.-E. Claire Vishik (Intel), «Cybersecurity Education snapshot for workforce development in the EU,» September 2015. [En línea]. Available: https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/cybersecurity-education-snapshot-for-workforce-development-in-the-eu/view. [Último acceso: Enero 2016].

[10] SYMANTEC, «CYBER CAREER CONNECTION,» SYMANTEC, 2014. [En línea]. Available: http://www.symantec.com/corporate_responsibility/topic.jsp?id=cyber_career_connection. [Último acceso: Enero 2016].

[11] Ministerio de Defensa, «SAPROMIL, Sistema de Aprovechamiento de Capacidades Profesionales del Personal Militar,» 2013. [En línea]. Available: http://www.sapromil.es/. [Último acceso: Enero 2016].

[12] Ministerio de Industria, Energía y Turismo, «El Gobierno presenta el Libro Blanco para el diseño de las titulaciones universitarias en el marco de la Economía Digital,» 2015. [En línea]. Available: http://www.agendadigital.gob.es/agenda-digital/noticias/Paginas/presentacion-libro-blanco.aspx. [Último acceso: Enero 2016].

8 Referencias

[13] OCDE, OECD Digital Economy Outlook 2015, Paris: OECD Publishing, 2015.

[14] Adecco, «VI Informe Spring Professional sobre Titulaciones con más salidas profesionales,» 18 Junio 2015. [En línea]. Available: http://www.adecco.es/_data/NotasPrensa/pdf/676.pdf. [Último acceso: Enero 2016].

[15] Burning Glass, «Cybersecurity Jobs, 2015,» 2015. [En línea]. Available: http://burning-glass.com/research/cybersecurity/. [Último acceso: Marzo 2016].

[16] CCII Consejo General de Colegios Profesionales de Ingeniería en Informática, «Presentación del Estudio Nacional sobre la Situación Laboral de los Profesionales del Sector TI,» Abril 2015. [En línea]. Available: http://www.ccii.es/noticias/243-presentacion-del-estudio-nacional-sobre-la-situacion-laboral-de-los-profesionales-del-sector-ti [Último acceso: Enero 2016].

[17] SEPE, Servicio Público de Empleo Estatal, «Los perfiles de la oferta de empleo,» Mayo 2014. [En línea]. Available: https://www.sepe.es/indicePerfiles/indicePerfiles.do?idioma=es. [Último acceso: Marzo 2016].

[18] ISACA and RSA Conference, «STATE OF CYBERSECURITY: IMPLICATIONS FOR 2015,» December 2015. [En línea]. Available: http://www.isaca.org/cyber/pages/state-of-cybersecurity-implications-for-2015.aspx.

[19] FTI - AMETIC, «PAFET VII. Perfiles Profesionales más demandados en el ámbito de los Contenidos Digitales en España 2012 - 2017. Profesionales TIC,» 2012. [En línea]. Available: http://ametic.es/es/publicaciones/pafet-vii-perfiles-profesionales-m%C3%A1s-demandados-en-el-%C3%A1mbito-de-los-contenidos. [Último acceso: Enero 2016].

[20] European Commission, Directorate-General for Communications Networks, Content and Technology, «Women active in the ICT sector,» 2013. [En línea]. Available: http://bookshop.europa.eu/is-bin/INTERSHOP.enfinity/WFS/EU-Bookshop-Site/en_GB/-/EUR/ViewPublication-Start?PublicationKey=KK0113433

[21] Check Point, «THREATS ARE ON THE RISE. KNOW YOUR LANDSCAPE.,» 2015. [En línea]. Available: https://www.checkpoint.com/resources/2015securityreport/.

[22] J. R. -. M. Ambite, «Proyecto MESI: Mapa de Enseñanza de la Seguridad de la Información,» Junio 2015. [En línea]. Available: http://www.criptored.upm.es/mesi/proyectomesi.htm.

[23] Education First, «El ranking mundial más grande según su dominio del inglés,» 2015. [En línea]. Available: http://www.ef.com.es/epi/.

[24] Raytheon and National Cyber Security Alliance (NCSA), «Now Hiring: Cyber Defenders Needed - A new survey details the growing talent gap in cybersecurity,» October 2015. [En línea]. Available: http://www.raytheoncyber.com/news/feature/now_hiring.html.

[25] Gobierno de España, «Estrategia de ciberseguridad nacional,» 2013. [En línea]. Available: http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf. [Último acceso: 25 abril 2016].

INSTITUTO NACIONAL DE CIBERSEGURIDAD