Capítulo octavo

Capacitación profesional y formación especializada en ciberseguridad

Óscar Pastor Acosta
Gerente de Seguridad
Isdefe

José Javier Martínez Herráiz
Director de la Cátedra Amaranto de Seguridad Digital
Universidad de Alcalá de Henares

Resumen

En el presente capítulo se abordará uno de los aspectos donde mayor puede llegar a ser la colaboración público-privada en materia de ciberseguridad y ciberdefensa: la necesidad de capacitar de manera adecuada a los profesionales especialistas en esta materia. Veremos cómo esta necesidad es casi un imperativo, el de la colaboración, al continuar aumentando la brecha entre la necesidad de profesionales y la oferta de los mismos.

Empezaremos, precisamente, analizando esta escasez de profesionales en todo el mundo y las cotas de preocupación que está alcanzando, tanto a nivel de los Estados y sus políticas nacionales como en el sector privado.

Continuaremos estudiando las iniciativas procedentes de organismos públicos en lo que respecta a la formación, certificación y acreditación de conocimientos en ciberseguridad, terminando con las procedentes del sector privado, en este caso, más centradas en la importancia de las certificaciones como garantía y aseguramiento de calidad y nivel.

El presente análisis no pretende hacer una descripción y búsqueda exhaustiva ni una descripción pormenorizada de todas las iniciativas en esta temática, sino centrarse en aquellas que nos parecen más relevantes y significativas. Quedan, manifiestamente, también fuera del mismo las innumerables iniciativas académicas, tanto públicas como privadas.

Palabras clave

ciberseguridad, ciberdefensa, formación, capacitación, certificación, habilidades, conocimientos, competencias, talento, escasez, profesional, pública, privada.

Abstract

In this chapter, it will be addressed one aspect which can become the greatest public-private collaboration landscape on cyber security and cyber defence: the need to adequately train specialized professionals in this field. We will see how this need is almost an imperative, that of collaboration, because the gap between the need for professionals and the offer of them continues to increase.

We will begin precisely analyzing the shortage of professionals worldwide and the dimensions of concern which it is achieving, both at governmental and national policies level and to private sector.

We will continue studying the initiatives from public agencies with regard to training, certification and accreditation of knowledge on cybersecurity, ending with those from the private sector, in this case, more focused on the importance of certifications as security and quality assurance and level.

This analysis is not intended to provide a description and exhaustive search or a detailed description of all initiatives in this area but focus on those that seem more relevant and significant. The uncountable academic initiatives, both public and private, are, obviously, also outside of this analysis.

Keywords

Cyber security, cyber defence, education, training, certification, skills, abilities, knowledge, talent, shortage, professional, public, private.

Introducción

Parece claro y reconocido que las tecnologías de la información y las comunicaciones están llamadas a convertirse en la columna vertebral de la economía europea.

La Comisión Europea, en su Estrategia para el Mercado Único Digital de Europa de 2015, lo reconoce como un objetivo prioritario dentro de sus políticas[1]:

«La economía mundial se está convirtiendo rápidamente en digital. Las tecnologías de la información y la comunicación (TIC) ya no son un sector específico, sino el fundamento de todos los sistemas económicos innovadores modernos. Internet y las tecnologías digitales están transformando la vida que llevamos y la forma en que trabajamos (como personas, en las empresas y en nuestras comunidades) cuanto más se integran en todos los sectores de nuestra economía y nuestra sociedad».

En numerosos párrafos de dicho documento se muestra la preocupación por la seguridad digital y se insiste en la necesidad de «Reforzar la confianza y la seguridad en los servicios digitales y en el tratamiento de los datos personales», citando iniciativas ya en marcha como la Estrategia de Ciberseguridad de la Unión Europea, la Agenda Europea de Seguridad o la adopción de la Directiva sobre Seguridad de las Redes y de la Información.

Pues bien, en este contexto, se destaca que «En el primer semestre de 2016 la Comisión iniciará la creación de una asociación entre los sectores público y privado en materia de ciberseguridad en el ámbito de las tecnologías y soluciones de seguridad de la red en línea», incluyéndolo como punto de la «Hoja de ruta para la realización del mercado único digital» y, por lo que respecta a cualificaciones digitales, se resalta que: «La demanda de empleados con cualificaciones digitales crece en torno a un 4 % anual. La escasez de profesionales de las TIC en la Unión Europea podría alcanzar los 825.000 puestos vacantes de aquí a 2020 si no se adoptan medidas firmes». Entre esas medidas de apoyo que se proponen se menciona a la iniciativa de la Unión Europea: la «Gran Coalición para el empleo digital».

Ya en 2006, en la Declaración de Salónica, adoptada en la Conferencia Europea sobre Cibercapacidades de 1 de octubre de ese año, se identificaron tres mensajes clave, el segundo de los cuales decía: «En segundo lugar, es necesario realizar grandes esfuerzos para mejorar la cooperación a largo plazo entre los sectores público y privado, a fin de garantizar un marco transpa-

[1] Comisión Europea, «Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones: una Estrategia para el Mercado Único Digital de Europa, COM(2015) 192 final», 2015, http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015DC0192&rid=1

rente que vincule la formación básica en cibercapacidades, la formación profesional, la enseñanza superior y el desarrollo profesional»[2].

Surge así como algo reconocido, importante y crítico, la llamada brecha entre la necesidad y demanda de profesionales especializados en ciberseguridad y la escasez de los mismos.

A estudiar la evolución que esta brecha ha tenido en los últimos cinco o seis años dedicaremos el primer punto de este capítulo, analizando diferentes informes tanto públicos como privados y procedentes de diferentes países del mundo occidental (Estados Unidos, el Reino Unido y la Unión Europea). El principal objetivo del capítulo es mostrar la unánime opinión en la acuciante necesidad de profesionales tanto en el ámbito público como en el privado y algunas propuestas para intentar paliarla mediante la colaboración público-privada en materia de formación.

Volviendo a la Conferencia Europea sobre Cibercapacidades anteriormente citada, podemos encontrar la siguiente recomendación: «La experiencia de integrar certificaciones de cibercapacidades del sector de las TIC en el marco nacional de cualificaciones, como se ha hecho por primera vez en el Reino Unido y en algunos nuevos Estados miembros, proporciona casos interesantes que deberían analizarse y compartirse con los demás Estados miembros».

Más recientemente, en 2015, el grupo de trabajo *European Cybersecurity Industry Leaders* (*ECIL*) remitía un informe a M. Günther H. Oettinger —*European Commissioner for Digital Economy and Society*— titulado «Recommendations on Cybersecurity for Europe»[3], en el que se puede encontrar como recomendación: «La certificación de profesionales de ciberseguridad trabajando en infraestructuras críticas con sistemas *ICS/SCADA*». Recomendación que puede ser perfectamente extrapolada a cualquier otro ámbito relacionado con la ciberseguridad y la ciberdefensa.

En esta línea de recomendaciones ampliamente aceptadas en materia de certificaciones profesionales podemos encontrar numerosa información sobre los beneficios de las acreditaciones y certificaciones, tanto para los profesionales de la ciberseguridad como para los empleadores de estos profesionales.

---

[2] Comisión de las Comunidades Europeas, «Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones: cibercapacidades para el siglo XXI: fomento de la competitividad, el crecimiento y el empleo, COM(2007) 496 final», 2007, http://www.cdiex.org/documentos/documento_121.pdf

[3] *European Cybersecurity Industrial Leaders* (*ECIL*), «Recommendations on Cybersecurity for Europe», 25 de enero de 2016, http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=13326

Incluso en estudios de un marcado corte académico como puede ser el de ACM del año 2013 «Toward Curricular Guidelines for Cybersecurity»[4], se concluye en la necesidad de certificar y acreditar a profesionales en ciberseguridad mediante la necesaria colaboración público-privada.

Al estudio y análisis de iniciativas para la formación y certificación profesional en ciberseguridad es a lo que dedicaremos los dos siguiente apartados de este capítulo. Primero trataremos las iniciativas de organismos públicos y por último, las privadas.

El objetivo en ambos epígrafes es el de presentar los diferentes trabajos que se están llevando a cabo para tratar de «acoplar» lo más ajustadamente posible distintos esquemas de certificación profesional con los esquemas de competencias en el ámbito de la ciberseguridad en los que se está trabajando desde hace tiempo. Las iniciativas públicas analizadas han sido estadounidenses, británicas y, por supuesto, españolas.

En la parte de iniciativas privadas, nos centramos en aquellas más ampliamente difundidas y con más prestigio a nivel internacional. El objetivo ha sido el de analizar las más recientes propuestas de estas organizaciones y, siempre, vinculadas directamente al profesional de la ciberseguridad. No se incluyen aquellas propuestas de certificaciones que, si bien pudieran estar relacionadas con aspectos de seguridad digital, no forman, estrictamente, parte central de lo que se entiende por ciberseguridad.

Escasez de profesionales en ciberseguridad

Desde hace años podemos encontrar en estudios, análisis y artículos de opinión la afirmación reiterada de que no hay suficiente personal con los conocimientos y habilidades en ciberseguridad necesarios para desempeñar con éxito las responsabilidades que empresas y departamentos gubernamentales necesitan y demandan. Es un consenso a nivel mundial que dicha escasez de profesionales de la ciberseguridad tendrá implicaciones negativas en la seguridad nacional, impactando gravemente tanto en entidades del sector público como del privado.

Ya en 2010, un informe[5] de la Comisión sobre Ciberseguridad para la 44ª Presidencia (de los Estados Unidos) elaborado por el *CSIS* (*Center for Stra-*

[4] Andrew Mcgettrick y Association for Computing Machinery (ACM). «Towards Curricular Guidelines for Cybersecurity - Report of a Workshop on Cybersecurity Education and Training», 30 de agosto de 2013, https://www.acm.org/education/TowardCurricularGuidelines-Cybersec.pdf

[5] Karen Evans y Franklin Reeder. «A Human Capital Crisis in Cybersecurity», Technical Proficiency Matters (1800 K Street, NW, Washington, DC 20006: CSIS Center for Strategic and International Studies - Commission on Cybersecurity for the 44th Presidency, noviembre de 2010), https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/101111_Evans_HumanCapital_Web.pdf

tegic and International Studies) abordaba el tema en profundidad, apuntando que un elemento crítico de una estrategia de ciberseguridad robusta es disponer de profesionales adecuados, a todos los niveles, para construir y dotar de personal a las defensas frente a las ciberamenazas, y precisamente esa era el área identificada como más débil. Se identificaba el problema tanto en cantidad como en calidad, sobre todo cuando se buscaban profesionales con muy altas competencias en *red teaming* (entendido como un proceso diseñado para detectar vulnerabilidades de la red y del sistema y examinar la seguridad mediante la adopción de una enfoque similar al de un atacante que quiera acceder a la red/sistema/datos, también se le conoce como «*hacking* ético»[6]). La escasez de personal técnico altamente cualificado no solo afectaba a la operación y soporte de sistemas ya desplegados, sino que la carencia era todavía más acuciante en personal que pudiera diseñar sistemas robustos, desarrollar código seguro y crear herramientas sofisticadas para prevenir, detectar, mitigar y reconstruir los impactos en los sistemas atacados.

En julio de ese mismo año 2010, en una entrevista[7] a varios analistas de ciberseguridad conducida por Jim Gosler, científico de la *NSA* (*National Security Agency*) y fundador de la Oficina de Tecnología de la Información Clandestina de la *CIA* (*Central Intelligence Agency*), se afirmaba que en los Estados Unidos tan solo unas mil personas disponían de las habilidades necesarias para defender los sistemas informáticos complejos contra los ciberataques. Sin embargo, ese mismo grupo de analistas afirmaba que se precisaban entre veinte y treinta veces la cantidad disponible.

Según un informe[8] de 2012, producido por el Grupo de Trabajo «CyberSkills» del *DHS* (*Department of Homeland Security*) estadounidense, el número de profesionales con conocimientos prácticos y habilidades suficientemente avanzadas en ciberseguridad era tan limitado que las empresas proveedoras del Gobierno y las agencias federales competían «fieramente» entre ellas, así como con el sector privado, por contratarlos. Entre las recomendaciones del Grupo de Trabajo se incluían:

- Desarrollar escenarios de entrenamiento que permitan evaluar los perfiles de ciberseguridad críticos.
- Diseñar un proceso de contratación preciso y eficaz, y hacer que las vacantes de ciberseguridad críticas sean atractivas para los empleados federales.

[6] Chris Peake. «Red Teaming: The Art of Ethical Hacking» (SANS Institute - InfoSec Reading Room, 16 de julio de 2003), https://www.sans.org/reading-room/whitepapers/auditing/red-teaming-art-ethical-hacking-1272

[7] Jim Gosler. Cyberwarrior Shortage Threatens US Security, NPR Morning Edition, 29 de julio de 2010, http://www.npr.org/templates/story/story.php?storyId=128574055

[8] Homeland Security Advisory Council, «CyberSkills Task Force Report» (US Department of Homeland Security, otoño de 2012), https://www.dhs.gov/sites/default/files/publications/HSAC %20CyberSkills %20Report %20- %20Final.pdf

– Lanzar una iniciativa importante y sostenida para mejorar las oportunidades para que los veteranos estadounidenses puedan ser adiestrados y contratados en puestos de ciberseguridad críticos.
– Especificar las habilidades críticas y el nivel de competencia para toda la contratación relacionada con la ciberseguridad.
– Establecer un programa piloto de «CiberReservistas» para garantizar que expertos avanzados en ciberseguridad fuera del Gobierno sean conocidos y estén disponibles en caso de necesidad.

En febrero de 2013, el interventor general del Reino Unido, en su informe «The UK cyber security strategy: Landscape review»[9], advierte de que la brecha existente entre la disponibilidad de personal con las habilidades y conocimientos en ciberseguridad y la necesidad de los mismos sigue creciendo: «las conversaciones con el Gobierno, la academia y los representantes de las empresas privadas confirman que el Reino Unido carece de las suficientes habilidades técnicas y que la provisión de graduados y profesionales no cubrirá la demanda necesaria», poniendo de manifiesto que el número de profesionales de ciberseguridad no ha seguido el ritmo creciente de la ciberamenazas a las que se enfrenta la nación. Añade que la falta de personal con competencias en ciberseguridad podría persistir durante muchos años: «podría llevar hasta veinte años el poder hacer frente a la falta de competencias en todos los niveles educativos», afirmando que grupos de criminales se están aprovechando de este déficit de cualificaciones, dando una cifra del coste de la ciberdelincuencia para el Reino Unido que estaría entre £18.000 millones y £27.000 millones al año.

Asimismo, en octubre de 2014, un comité parlamentario especial en la Cámara de los Lores del Reino Unido predijo una escasez mundial de «no menos de dos millones de profesionales de seguridad cibernética»[10] para el año 2017.

Otra prueba de la escasez de talento en ciberseguridad aparece en el informe[11] de septiembre de 2013 de la Oficina de Responsabilidad Gubernamental de los Estados Unidos (*GAO, Government Accountability Office*), en el que se mostraba una tasa de vacantes del 22 % en puestos de trabajo dentro de la Oficina de Ciberseguridad y las Comunicaciones de la Dirección General de Programación y Protección del Departamento de Seguridad Nacional (*DHS, Department of Homeland Security*).

[9] Comptroller and Auditor General, «The UK Cyber Security Strategy: Landscape Review» (London: National Audit Office, 5 de febrero de 2013), http://www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/

[10] Lewis Morgan. «Global Shortage of Two Million Cyber Security Professionals by 2017», *IT Governance Blog*, 30 de octubre de 2014, http://www.itgovernance.co.uk/blog/global-shortage-of-two-million-cyber-security-professionals-by-2017/

[11] GAO, «GAO-13-742 - DHS Recruiting and Hiring: DHS Is Generally Filling Mission-Critical Positions, but Could Better Track Costs of Coordinated Recruiting Efforts», Report to Congressional Requesters (United States Government Accountability Office, septiembre de 2013), http://www.gao.gov/products/GAO-13-742

En enero del año 2016, un informe[12] del Servicio de Investigación del Congreso de los Estados Unidos analiza la mano de obra de ciberseguridad en los Departamentos de Defensa y de Seguridad Nacional, reconociendo que desarrollar y mantener una fuerza de trabajo robusta en ciberseguridad dentro de las Agencias Federales se ha convertido en un desafío continuo. Así, según recoge el mencionado informe, aunque la Administración Obama había creado una prioridad para todas las agencias gubernamentales con el objeto de reducir a la mitad, a fínales de 2013, el déficit en los puestos de ciberseguridad, que había detectado un grupo de trabajo del Consejo Federal de Directores de Capital Humano, según un informe[13] de la *GAO*, de enero de 2015, los esfuerzos necesarios para cerrar las carencias de profesionales de ciberseguridad en las Agencias Federales se encontraban en un estado de madurez muy inicial.

El 12 de julio de 2016, la Oficina de Administración y Presupuesto (*OMB, Office of Management and Budget*) de los Estados Unidos publica la Estrategia Federal para la Fuerza Laboral de Ciberseguridad[14], que incluye acciones para ayudar al Gobierno Federal en las siguientes áreas:

- Identificar las necesidades del personal de seguridad cibernética.
- Ampliar los recursos humanos de ciberseguridad a través de la educación y la formación.
- Reclutar y contratar talentos altamente cualificados.
- Retener y desarrollar talentos altamente cualificados.

Dentro de las instituciones del sector privado, la disponibilidad de profesionales de la ciberseguridad ha sido abordada en profundidad en las diferentes ediciones del Estudio Global sobre Personal de Seguridad de la Información, de los años 2011[15], 2013[16] y 2015[17], de la organización (*ISC*)^2 (*International In-*

[12] Kathryn A. Francis y Wendy Ginsber, «The Federal Cybersecurity Workforce: Background and Congressional Oversight Issues for the Departments of Defense and Homeland Security», CRS Report (Congressional Research Service, 8 de enero de 2016), https://www.fas.org/sgp/crs/natsec/R44338.pdf

[13] GAO, «GAO-15-223, Federal Workforce: OPM and Agencies Need to Strengthen Efforts to Identify and Close Mission-Critical Skills Gaps», Report to Congressional Requesters (United States Government Accountability Office, enero de 2015), http://www.gao.gov/assets/670/668202.pdf

[14] OMB (Office of Management and Budget), *Federal Cybersecurity Workforce Strategy*, *M-16- 15*, 2016, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf

[15] Robert Ayoub. «The 2011 (ISC)^2 Global Information Security Workforce Study», Frost & Sullivan Market Survey [(ISC)^2, 2011], https://www.isc2.org/uploadedFiles/Industry_Resources/FS_WP_ISC %20Study_020811_MLW_Web.pdf

[16] Michael SUBY. «The 2013 (ISC)^2 Global Information Security Workforce Study», Frost & Sullivan Market Study [(ISC)^2, 2013], https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf

[17] Michael SUBY y Frank DICKSON. «The 2015 (ISC)^2 Global Information Security Workforce Study», A Frost & Sullivan White Paper [(ISC)^2, 16 de abril de 2015], https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC) %C2 %B2-Global-Information-Security-Workforce-Study-2015.pdf

formation Systems Security Certification Consortium). Así, en la última edición del estudio se indica que el déficit de mano de obra de seguridad de la información es cada vez mayor. En la encuesta del año 2015, en la que participaron casi catorce mil profesionales de la seguridad de la información de todo el mundo, el 62 % de los encuestados declaró que sus organizaciones tienen muy pocos profesionales de la ciberseguridad, lo que supone un incremento del 6 % si se compara con los que respondieron lo mismo en la encuesta del año 2013. Los cinco roles de ciberseguridad más demandados son:

- Analista de seguridad.
- Auditor de seguridad.
- Arquitecto de seguridad (de productos y de soluciones).
- Analista forense.
- Gestor de incidentes (corporativo).

Otra de las diferencias significativas en la edición de 2015 del mencionado estudio de (*ISC*)[2] aparece en las razones del déficit, dado que ahora son menos los que indican la falta de presupuesto para contratar personal, apareciendo con mayor relevancia la insuficiente oferta del mercado laboral de candidatos con el perfil profesional adecuado. Estas observaciones, y otras generadas a partir de este amplio estudio, permiten a los autores del informe estimar el déficit global en la fuerza de trabajo de ciberseguridad, que se prevé llegará a 1,5 millones en cinco años. Este déficit es la diferencia entre la previsión de la fuerza de trabajo necesaria para dar respuesta plena a las crecientes necesidades de ciberseguridad y la proyección de las restricciones en la oferta de mano de obra en este sector. Esto no implica una disminución de la contratación, sino que se prevé un aumento global de 195.000 profesionales de la ciberseguridad de la información en el año 2016, lo que supone un incremento de casi un 6 % respecto a 2014.

Estas predicciones se alinean con las realizadas por otras empresas e instituciones privadas, así Cisco en julio de 2015[18] situaba la cifra global de ofertas de trabajo de ciberseguridad no cubiertas en más de un millón. Forbes, en un artículo[19] de enero de 2016, indicaba que se espera que el mercado de la seguridad cibernética crezca a más del doble de su tamaño actual, pasando de $75.000 millones en 2015 a $170.000 millones en 2020. Por otro lado, Michael Brown, CEO de Symantec, uno de los mayores proveedores de *software* de seguridad del mundo, espera que para el año 2019 la demanda aumente a 6 millones de ofertas de trabajo a nivel mundial, con un déficit previsto de 1,5 millones[20].

---

[18] Cisco Security Advisory Services, «Mitigating the Cybersecurity Skills Shortage» (Cisco Systems, Inc, julio de 2015), http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf

[19] Steve MORGAN. «One Million Cybersecurity Job Openings In 2016», *Forbes*, 2 de enero de 2016, http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/print/

[20] Rebecca Vogel. «Closing The Cybersecurity Skills Gap», *Salus Journal* 4, n.º 2 (2016): 32.

Una encuesta realizada por Raytheon[21] en 2014 mostraba que la demanda de profesionales de la seguridad informática estaba creciendo 3,5 veces más rápido que el mercado de trabajo IT genérico, y doce veces más rápido que el mercado de trabajo total. Según ese mismo estudio, en 2013, hubo en Estados Unidos 209.749 anuncios de ofertas de trabajo de ciberseguridad y cubrir estas demandas exigió un 36 % más de tiempo de dedicación para las empresas de reclutamiento.

En 2015, ISACA y RSA[22] encuestaron a seiscientos cuarenta y nueve profesionales de todo el mundo sobre la magnitud del problema de la falta de habilidades en ciberseguridad. Los resultados mostraron que el 35 % de las organizaciones encuestadas no podían cubrir las vacantes de ciberseguridad, a pesar de que un 82 % de esas mismas organizaciones esperaban ser atacadas cibernéticamente. Además, lo que podría considerarse más preocupante es que, el 52 % de dichas organizaciones manifestó que menos de una cuarta parte de todos los candidatos disponían de las habilidades de ciberseguridad realmente necesarias para el puesto.

Finalmente, según datos del Bureau of Labor Statistics[23] de Estados Unidos, en 2015 más de 209.000 puestos de trabajo de seguridad cibernética quedaron vacantes en Estados Unidos y la demanda aumentó un 74 % durante los cinco últimos años. Además, se espera que la demanda de profesionales de ciberseguridad crezca en un 53 % hasta el año 2018.

Iniciativas de organismos públicos para la formación y certificación profesional en ciberseguridad

Entre las propuestas que incluía el ya mencionado informe[24] de la Comisión sobre Ciberseguridad para la 44ª Presidencia (de los Estados Unidos) del CSIS, estaba la de construir un sistema de certificación de alto prestigio profesional, en dos o tres áreas de especialidad, creando un organismo gubernamental para desarrollar y administrar las mencionadas certificaciones donde no se identificaba la existencia de una oferta previa de certificación profesional suficientemente rigurosa. Asimismo, ese mismo organismo público debería también desarrollar criterios para la evaluación de otros programas de certificación de forma que, usando un modelo federado, otros programas de cer-

[21] Raytheon y NCSA, «Preparing Millennials to Lead in Cyberspace» (National Cyber Security Alliance, octubre de 2014), http://www.raytheoncyber.com/news/feature/blog-cyber60-helpwanted.html

[22] ISACA y RSA Conference, «State of Cybersecurity: Implications for 2015» (ISACA, 11 de abril de 2015), http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf

[23] Ariha Setalvad. «Demand to fill cybersecurity jobs booming», *Península Press*, 31 de marzo de 2015, http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/

[24] Karen Evans y Franklin Reeder. «A Human Capital Crisis in Cybersecurity».

tificación, existentes o futuros, públicos o privados, que cumplieran con unas estrictas normas de calidad, pudieran también ser acreditados.

Asimismo, en diciembre de 2014, *ENISA* (*European Union Agency for Network and Information Security*) publicaba un informe[25] abordando la certificación de competencias de ciberseguridad para los entornos *ICS/SCADA*[26] (*Industrial Control Systems / Supervisory Control and Data Acquisition*). Entre sus recomendaciones se incluía la de crear un esquema europeo global de certificación profesional de ciberseguridad *ICS/SCADA*, así como crear un comité independiente para evaluar y aprobar las certificaciones actuales y futuras.

Según *ENISA*, las nuevas certificaciones de ciberseguridad deberían ser multinivel, para llegar a un mayor número de profesionales, así como diferentes campos de aplicación, reflejando adecuadamente el diferente conjunto de habilidades que son necesarias para los profesionales. *ENISA* proponía como ejemplo los siguientes niveles de certificación profesional:

- Nivel básico.
- Nivel avanzado.
- Nivel máster.
- Nivel gerencial.

En este contexto, son numerosas las iniciativas, muchas de ellas respaldadas por organismos y agencias gubernamentales, promoviendo esquemas de certificación de profesionales en ciberseguridad, que ayuden a salvar esta escasez de personal experto en la materia. Su principal objetivo es asegurar que los conocimientos y habilidades de los profesionales certificados garanticen de forma efectiva el cumplimiento de las misiones que dichos organismos tienen marcadas, permitiendo diferenciar en la oferta formativa de ciberseguridad aquellos programas de formación con rigor y profesionalidad de los que no la tengan, poniendo en evidencia la ineficacia de multitud de iniciativas formativas oportunistas, que surgen aprovechando la actual carencia de profesionales expertos en ciberseguridad, pero que carecen de la capacidad para conseguir que quienes las cursan realmente adquieran competencias avanzadas en ciberseguridad.

A continuación se analizarán algunas de las principales iniciativas de formación y certificación profesional en ciberseguridad, promovidos por organismos públicos de las naciones más avanzadas de nuestro entorno.

National Cybersecurity Workforce Framework

[25] Adriana Pauna. «Certification of Cyber Security Skills of ICS - Good Practices and Recommendations for Developing Harmonised Certification Schemes» (Heraklion: *ENISA*, 2014), http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714040:EN:HTML

[26] NIST, «NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security» (National Institute of Standards and Technology, junio de 2011).

En noviembre de 2011, la Iniciativa Nacional para la Educación sobre Ciberseguridad (*National Initiative for Cybersecurity Education, NICE*)[27], del estadounidense Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology*, *NIST*), dio a conocer para comentarios el Marco de Referencia para la Mano de Obra en Ciberseguridad (*National Cybersecurity Workforce Framework*)[28].

NICE es una iniciativa de colaboración público-privada, dirigida por el *NIST*, en la que participan el Gobierno, la academia y el sector privado, centrada en la educación, la formación y el desarrollo profesional de ciberseguridad. La misión de *NICE* es dinamizar y promover una red robusta y un ecosistema de educación, formación y desarrollo profesional en ciberseguridad. *NICE* cumple esta misión mediante la mencionada coordinación público-privada, partiendo de los programas de capacitación existentes que hayan demostrado su éxito, para facilitar el cambio y la innovación, promoviendo el liderazgo y la visión para aumentar el número de profesionales cualificados en ciberseguridad.

El mantenimiento y desarrollo del *National Cybersecurity Workforce Framework* actualmente es coordinado[29] por la Iniciativa Nacional para las Carreras y los Estudios de Ciberseguridad (*National Initiative for Cybersecurity Careers and Studies, NICCS*)[30], del Departamento de Seguridad Nacional (*Department of Homeland Security, DHS*), en colaboración con otros organismos públicos norteamericanos y representantes del sector privado.

La misión de *NICCS* es ser un recurso nacional para la concienciación, educación, capacitación y las carreras profesionales en ciberseguridad. *NICCS* garantiza la disponibilidad de la información de investigación y formación a través de un robusto catálogo que facilita las búsquedas, permitiendo a los usuarios encontrar programas de formación según su ubicación, método de impartición, área de especialidad o nivel de competencia. *NICCS* apoya el objetivo de *DHS* de hacer crecer la mano de obra disponible en ciberseguridad, proporcionando información acerca de ciencia, tecnología, ingeniería y matemáticas (*Science, Technology, Engineering & Mathematics*, STEM) y los programas universitarios de grado relacionados con la ciberseguridad, así como prácticas, becas, desafíos y eventos de ciberseguridad.

---

[27] NIST, «The National Initiative for Cybersecurity Education (NICE)», accedido 29 de agosto de 2016, http://csrc.nist.gov/nice/about/index.html

[28] NIST, «NICE Issues Cybersecurity Workforce Framework for Public Comment», accedido 29 de agosto de 2016, http://www.nist.gov/itl/cyberwork-110811.cfm

[29] DHS y NICCS. «National Cybersecurity Workforce Framework Slick Sheet» (National Initiative for Cybersecurity Careers and Studies (NICCS), noviembre de 2011), https://niccs.us-cert.gov/sites/default/files/documents/files/Workforce %20Framework %20Slick %20Sheet_1.pdf?trackDocs=Workforce %20Framework %20Slick %20Sheet.pdf

[30] NICCS, «National Initiative for Cybersecurity Careers and Studies», accedido 29 de agosto de 2016, https://niccs.us-cert.gov/home/about-niccs

El *National Cybersecurity Workforce Framework*[31] proporciona una forma coherente para definir y describir el trabajo de ciberseguridad en cualquier organización, pública o privada, al permitir clasificar y categorizar el marco de trabajo de ciberseguridad en virtud de las áreas de especialidad, que se agrupan en siete categorías. Dentro de cada área de especialidad, el marco define funciones estándar, así como las competencias, destrezas y habilidades (*Knowledge, Skills & Abilities, KSA*) requeridas en los profesionales de la seguridad informática que las desempeñen y los títulos de trabajo por los que habitualmente se conoce a dichos grupos de actividades profesionales.

Como ya hemos mencionado, el Marco de Referencia para la Mano de Obra en Ciberseguridad se estructura inicialmente en siete categorías, cada una compuesta por varias áreas de especialidad, en base a un extenso análisis de las tareas que agrupan a los trabajadores y que comparten funciones comunes, independientemente de los títulos de trabajo u otras condiciones laborales.

Las categorías del *Workforce Framework* y sus respectivas áreas de especialidad son las siguientes:

– Provisión de Forma Segura: que agrupa las áreas de especialidad responsables de la conceptualización, diseño y construcción segura de sistemas de tecnologías de la información (IT), es decir, responsables de algún aspecto del desarrollo de sistemas.

- Cumplimiento de seguridad de la información.
- Ingeniería de seguridad y aseguramiento del software.
- Desarrollo de sistemas.
- Planificación de los requisitos de sistemas.
- Arquitectura de seguridad de sistemas.
- Investigación y desarrollo tecnológico.
- Evaluación y prueba.

– Proteger y Defender: que incluye las áreas de especialidad responsables de la identificación, análisis y mitigación de las amenazas a los sistemas de TI o redes internas.

- Análisis de la defensa de redes informáticas.
- Apoyo a la infraestructura de la defensa de redes informáticas.
- Respuesta a incidentes.
- Evaluación y gestión de vulnerabilidades.

– Supervisión y Desarrollo: son las áreas que proporcionan liderazgo, gestión, dirección y/o desarrollo y promoción, de manera que la organiza-

[31] NICE, «The National Cybersecurity Workforce Framework» (National Initiative for Cybersecurity Careers and Studies (NICCS), 15 de mayo de 2014), https://niccs.us-cert.gov/sites/default/files/documents/files/National %20Cybersecurity %20Workforce %20Framework %20Version %201.0.pdf?trackDocs=National %20Cybersecurity %20Workforce %20Framework %20Version %201.0.pdf

ción y todos los individuos puedan conducir eficazmente los trabajos de ciberseguridad.

- Formación y entrenamiento.
- Operaciones de seguridad de sistemas de información (*Information Systems Security Officer, ISSO*).
- Asesoramiento y defensa legal.
- Gestión de programas de seguridad (*Chief Information Security Officer, CISO*).
- Planificación estratégica y desarrollo de políticas.

– Recoger y Operar: con las áreas de especialidad encargadas de las operaciones especializadas de denegación y decepción, así como de la recopilación de información de ciberseguridad que pueda ser utilizada para la elaboración de inteligencia.

- Operaciones de recolección.
- Ciberoperaciones.
- Planificación de ciberoperaciones.

– Operar y Mantener: que agrupa las áreas de especialidad responsables de la prestación de soporte, administración y mantenimiento necesarios para garantizar de forma eficaz y eficiente el funcionamiento y la seguridad del sistema de información.

- Soporte técnico y servicio al cliente.
- Administración de datos.
- Gestión del conocimiento.
- Servicios de red.
- Administración de sistemas.
- Análisis de seguridad de sistemas.

– Analizar: que incluye las áreas de especialidad responsables de la revisión y evaluación altamente especializadas de información entrante sobre ciberseguridad para determinar su utilidad para la elaboración de inteligencia.

- Inteligencia de todas las fuentes.
- Análisis de la explotación.
- Objetivos.
- Análisis de amenazas.

– Investigar: con las áreas de especialidad encargadas de la investigación de eventos de ciberseguridad y/o delitos en sistemas y redes de información, así como de las evidencias digitales.

- Forense digital.
- Investigación.

Como ya se ha indicado, dentro de cada área de especialidad, el *Workforce Framework* define las competencias, destrezas y habilidades requeridas, hasta completar un total de trescientas cincuenta y ocho, así como las tareas a desempeñar por los profesionales de esa área de la ciberseguridad, hasta un total de cuatrocientas cuarenta y cuatro tareas diferentes.

El *Workforce Framework* entiende conocimiento, destrezas y habilidades como los atributos necesarios para llevar a cabo un trabajo y, en general, se ponen de manifiesto a través de la experiencia cualificada, la educación o la formación. El conocimiento es un conjunto de información aplicada directamente a la realización de una función. La destreza es una competencia observable para llevar a cabo un acto psicomotor aprendido. La habilidad es una competencia para llevar a cabo un comportamiento observable o un comportamiento que se traduce en un producto observable. El *Workforce Framework* asocia conocimiento, destrezas y habilidades con cada área de especialidad para definir claramente las cualificaciones, educación o formación necesarias para realizar con éxito las tareas o funciones asociadas con esa especialidad.

Por tanto, el *Workforce Framework* constituye el modelo de clasificar, organizar y describir el trabajo de ciberseguridad, para proporcionar a los educadores, estudiantes, empresarios, empleados, proveedores de formación, así como a los responsables políticos, una herramienta sistemática y coherente para organizar la forma en que pensamos y hablamos sobre el trabajo de ciberseguridad y entendemos lo que se requiere para mejorar la mano de obra disponible en ciberseguridad.

Al alinear los grados universitarios, los puestos de trabajo, la formación y las certificaciones con el *Workforce Framework* se obtienen los siguientes beneficios para:

- Educadores: que pueden alinear mejor sus programas de formación con los empleos requeridos.
- Estudiantes: al graduarse con los conocimientos y competencias necesarios.
- Empleadores: al contratar sobre una oferta de candidatos mejor cualificados.
- Empleados: que pueden identificar mejor diferentes carreras profesionales y oportunidades de empleo.
- Responsables políticos: para desarrollar las políticas necesarias para promover la disponibilidad de mano de obra.

La capacitación es un componente fundamental para cualquier Marco de Referencia para la Mano de Obra, por lo que este se complementa con un Catálogo de Formación[32], mantenido por el *NICCS*, en el que se incluyen los

[32] NICCS, «Training Catalog | National Initiative for Cybersecurity Careers and Studies», accedido 30 de agosto de 2016, https://niccs.us-cert.gov/training/tc/search

cursos según las áreas de especialidad del Marco de Referencia. Esto permite, tanto a los profesionales con experiencia como a los que acaban de entrar en la profesión de la ciberseguridad, identificar rápidamente los cursos que necesitan para avanzar dentro de su área o adquirir habilidades para pasar a otra especialidad. En la actualidad, el Catálogo de Formación del *NICCS* incluye 2.885 cursos a lo largo de diferentes ubicaciones geográficas de Estados Unidos.

CESG Certified Professional Scheme

En el Reino Unido, el *CESG* (originalmente *Communications Electronics Security Group*), dependiente del *GCHQ* (*Government Communications Headquarters*), que es la autoridad nacional británica para la Seguridad de la Información, ha desarrollado un Esquema de Certificación Profesional de Ciberseguridad (*Certified Professional Scheme, CESG*)[33], para aquellos candidatos que cumplan con los requisitos de competencia y habilidad para las funciones definidas por dicho organismo.

Los objetivos del Esquema de Certificación son:

- Mejorar la concordancia entre los requisitos de experiencia avanzada en seguridad de la información del sector público y la competencia de los profesionales de ciberseguridad, ya sean empleados públicos o subcontratados.
- Alentar a los trabajadores de ciberseguridad a desarrollar las habilidades y conocimientos necesarios para ser plenamente operativos.
- Proporcionar la garantía de que los profesionales certificados cubren los requisitos de los roles de ciberseguridad definidos.
- Proporcionar definiciones más claras de los conocimientos y habilidades requeridos para los diferentes roles de seguridad de la información.

La estructura general[34] del Esquema de Certificación de Profesionales de Ciberseguridad del *CESG* consta de los siguientes elementos principales:

- Órganos asesores: procedentes de departamentos gubernamentales, la industria, la academia y el *CLAS* (*CESG Listed Advisor Scheme*).
- *CESG*: que actúa como organismo propietario y supervisor del Esquema de Certificación, seleccionando a los organismos de certificación reconocidos, definiendo los roles y competencias del esquema y desarrollando el portafolio de políticas de ciberseguridad.
- Organismos de certificación: que evalúan la competencia de los candidatos de diferentes de formas, dependiendo de las habilidades necesarias

[33] CESG, «CESG Certified Professional Scheme», 19 de mayo de 2016, https://www.cesg.gov.uk/articles/cesg-certified-professional-scheme

[34] CESG, «Guidance to CESG Certification for IA Professionals v2-1» (GCHQ, enero de 2015), https://www.cesg.gov.uk/file/701/download?token=QM1gwRoi

para cada rol. El proceso de evaluación incluirá típicamente revisión de evidencias escritas, pruebas de conocimiento, referencias, una entrevista, la recomendación de los evaluadores y la decisión final de un panel de ratificación. Cuanto más nivel de competencia implique el rol evaluado, más extensa se espera que sea la evaluación.
- Candidatos: que serían todos aquellos profesionales que quieran certificar sus competencias en ciberseguridad, solicitando la evaluación a uno de los organismos de certificación acreditados y obteniendo el certificado una vez hayan superado positivamente la evaluación.
- Empleadores de profesionales certificados: entre los que se encontrarán tanto organismos del sector público como entidades e industrias del sector privado.

Los roles[35] de seguridad de la información definidos por el *CESG* para su Esquema de Certificación son:

- Acreditador (*Accreditor*).
  - Actuará como un asesor imparcial de los riesgos a los que un sistema de información puede estar expuesto, para cumplir con los requisitos de negocio, y autorizará formalmente el sistema en nombre del Consejo de Administración.
- Asesor de Riesgos de Seguridad de la Información (*Security Information Risk Advisor*, *SIRA*).
  - Asesorará al negocio sobre la gestión de la seguridad y el riesgo de la información de forma consistente con las políticas, normas y guías gubernamentales y/o con las buenas prácticas de ciberseguridad de la industria.
- Auditor de Seguridad de la Información (*IA Auditor*).
  - Evaluará el cumplimiento de los objetivos, políticas, normas y procesos de seguridad.
- Arquitecto de Seguridad de la Información (*IA Architect*).
  - Impulsará el cambio beneficioso de la seguridad en el negocio, mediante el desarrollo o revisión de arquitecturas que mitiguen los riesgos y cumplan con las políticas de seguridad pertinentes, balanceen los riesgos de seguridad de la información y el coste de las contramedidas para protegerla, y ajusten los requisitos de negocio para la seguridad.
- Director de Seguridad TI (*IT Security Officer, ITSO*).
  - Proporcionará gobernabilidad, gestión y control de la seguridad de los sistemas de información.
- Director de Seguridad de las Comunicaciones (*Communications Security Officer, ComSO*).
  - Gestionará los sistemas criptográficos según normativa gubernamental y los procedimientos de seguridad específicos para productos de

[35] CESG, «CESG Certification for IA Professionals 5.2» (GCHQ, octubre de 2015), https://www.cesg.gov.uk/file/520/download?token=j8vebyeM

referencia. Esta función abarca a aquellos que realizan funciones similares según normativa PCI/DSS[36].
- Evaluador de Vulnerabilidades (*Penetration Tester*).
  - Evaluará de forma independiente los diferentes elementos que componen un sistema de información o producto, con el objetivo de encontrar y documentar las vulnerabilidades presentes.

Cada rol se define con tres niveles de competencia:

- Practicante (*Practitioner*): nivel de entrada al Esquema, adecuado para las personas que trabajan en las tareas rutinarias bajo supervisión y pueden no tener experiencia previa en ciberseguridad.
- Practicante Senior (*Senior Practitioner*): nivel adecuado para personas que trabajan de forma independiente en proyectos complejos y que normalmente lideran un equipo o supervisan el trabajo de otros profesionales de ciberseguridad. Suelen contribuir al éxito de un programa o varios proyectos. Tiene suficiente experiencia para manejar situaciones complejas y requiere de una supervisión mínima.
- Practicante Principal (*Lead Practitioner*): nivel apropiado para los profesionales altamente experimentados, que trabajan en los niveles superiores de una organización, prestando asesoramiento y liderazgo en temas estratégicos y complejos de ciberseguridad. Suelen participar en toda una área de un responsable senior de riesgos. Influyen en los presupuestos y en el marco de gobierno corporativo para optimizar el equilibrio entre seguridad y el resto de objetivos de la organización, asegurando que contribuye a sus objetivos estratégicos.

Los mencionados niveles, para cada uno de los roles profesionales de ciberseguridad, están alineados con los niveles de responsabilidad definidas por *SFIA* (*Skills Framework for the Information Age*)[37]. El conjunto completo de los niveles de responsabilidad[38] *SFIA* es el siguiente:

1. Seguir (*Follow*).
2. Ayudar (*Assist*).
3. Aplicar (*Apply*).
4. Permitir (*Enable*).
5. Garantizar/Aconsejar (*Ensure/Advise*).
6. Poner en marcha/Influir (*Initiate/Influence*).
7. Establecer estrategia/Inspirar, movilizar (*Set Strategy/Inspire*).

[36] PCI Security Standards Council, «PCI (industria de tarjetas de pago) - Normas de seguridad de datos - Requisitos y procedimientos de evaluación de seguridad», noviembre de 2013, https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

[37] SFIA Foundation, «Versión 6 del Marco de Competencias para la Era de la Información - Español», accedido 29 de agosto de 2016, https://www.sfia-online.org/es/reference-guide

[38] SFIA Foundation, «Responsabilidades y habilidades - Español», accedido 31 de agosto de 2016, https://www.sfia-online.org/es/how-sfia-works/responsibilities-and-skills

SFIA define cada nivel de responsabilidad en términos de autonomía, influencia, complejidad y habilidades de negocio. La mayor parte de las responsabilidades del nivel Practicante, Practicante Senior y Practicante Principal se alinean con los niveles 2, 4 y 6 de *SFIA*, respectivamente.

La línea base de entrada para la certificación es bastante alta y se espera que el candidato aporte evidencias sobre la aplicación práctica de las habilidades requeridas en el rol solicitado, por lo que disponer de una titulación relacionada, pero sin experiencia práctica, no garantiza la obtención de la certificación.

Por otro lado, para la definición de las habilidades, el *CESG* se apoya en las definidas por el Marco de Referencia[39] del *IISP* (*Institute of Information Security Professional*), pero complementándolas, en consulta con los órganos asesores, procedentes de los departamentos gubernamentales, la academia, la industria y el *CLAS*, para ayudar a la evaluación con respecto a cada uno de los cuatro niveles de habilidad definidos por *IISP*.

Los niveles de habilidad del *IISP* son:

- Nivel 1: conocimiento (*awareness*). Comprende la habilidad y su aplicación. Ha adquirido y puede demostrar conocimientos básicos asociados con la habilidad. Entiende cómo la habilidad debe ser aplicada, pero puede no tener la experiencia práctica en su aplicación.
- Nivel 2: aplicación básica (*basic application*). Comprende la habilidad y la aplica a tareas básicas bajo alguna supervisión. Ha adquirido los conocimientos básicos asociados con la habilidad, por ejemplo, ha adquirido un título académico o profesional en la habilidad. Entiende cómo deben aplicarse las habilidades. Tiene experiencia en la aplicación de la habilidad para una variedad de tareas básicas. Determina cuándo los problemas se deben escalar a un nivel más alto. Contribuye con ideas en la aplicación de la habilidad. Demuestra conocimiento de la evolución reciente de la habilidad.
- Nivel 3: aplicación competente (*skilful application*). Comprende la habilidad y la aplica a tareas complejas sin supervisión. Ha adquirido una comprensión profunda de los conocimientos asociados a la habilidad. Entiende cómo la habilidad debe ser aplicada. Tiene experiencia de la aplicación de la habilidad para una variedad de tareas complejas. Demuestra una significativa responsabilidad personal o autonomía, con poca necesidad de escalar problemas. Contribuye con ideas en la aplicación de la habilidad. Demuestra conocimiento de la evolución reciente de la habilidad. Contribuye con ideas para el desarrollo técnico y nuevas áreas de aplicación de la habilidad.

[39] Institute of Information Security Professional, «IISP Skills Framework - Version 2.0», accedido 31 de agosto de 2016, https://www.iisp.org/imis15/iisp/About_Us/Our_Skills_Framework/iispv2/Accreditation/Our_Skills_Framework.aspx?hkey=e77a6f03-9498-423e-aa7b-585381290ec4

– Nivel 4: experto (*expert*). Es una autoridad que dirige el desarrollo de la habilidad. Es un experto reconocido por sus compañeros en la habilidad. Tiene experiencia en la aplicación de las habilidades en circunstancias sin precedentes. Propone, lleva a cabo y/o conduce un trabajo innovador para mejorar la habilidad.

El Esquema de Certificación de Profesionales de Ciberseguridad del *CESG* incluye veintitrés habilidades, agrupadas en nueve secciones, según el siguiente esquema:

– Sección A: Gestión de la Seguridad de la Información.

• A1: Gobierno.
• A2: Política y Estándares.
• A3: Estrategia de Seguridad de la Información.
• A4: Innovación y Mejora en el Negocio.
• A5: Sensibilización y Capacitación en Seguridad de la Información.
• A6: Entorno Legal y Regulatorio.
• A7: Gestión de Terceras Partes.

– Sección B: Gestión de Riesgos de la Información.

• B1: Análisis de Riesgos.
• B2: Gestión de Riesgos.

– Sección C: Implementación de Sistemas Seguros.

• C1: Arquitectura de Seguridad.
• C2: Desarrollo Seguro.

– Sección D: Metodologías y Pruebas para la Seguridad de la Información.

• D1: Metodologías de Seguridad de la Información.
• D2: Pruebas de Seguridad.

– Sección E: Disciplina de Seguridad: Gestión de la Seguridad Operacional.

• E1: Gestión de Operaciones Seguras.
• E2: Operaciones Seguras y Provisión del Servicio.
• E3: Evaluación de Vulnerabilidades.

– Sección F: Disciplina de Seguridad: Gestión de Incidentes.

• F1: Gestión de Incidentes.
• F2: Investigación.
• F3: Forense.

– Sección G: Disciplina de Seguridad: Auditoría, Control y Revisión.

• G1: Auditoría y Revisión.

– Sección H: Disciplina de Seguridad: Gestión de la Continuidad del Negocio.

• H1: Planificación de la Continuidad del Negocio.

- H2: Gestión de la Continuidad del Negocio.

– Sección I: Disciplina de Seguridad: Investigación de Sistemas de Información.

- I3: Investigación Aplicada.

El *CESG* complementa cada grupo de habilidades *IISP* con una descripción de los conocimientos más relevantes para esa habilidad, así como con una declaración de lo que se espera en cada nivel de habilidad, seguido de ejemplos de comportamientos, competencias, experiencias, versatilidad, autonomía o influencia, consistentes con la declaración previa. Además, las definiciones de habilidad están destinadas a ser acumulativas, es decir, para cumplir con los requisitos en los niveles superiores se debe cumplir con los de los niveles más bajos. Sin embargo, hay que tener en cuenta que, en cambio, las definiciones de roles realizadas por el *CESG* no son acumulativas.

Como ya se ha mencionado anteriormente, la certificación es proporcionada por los organismos de certificación acreditados por el *CESG*, que actualmente son los siguientes:

– *APM Group*.
– *BCS, the Chartered Institute for IT*.
– *IISP, CREST and RHUL consortium*.

Los beneficios del Esquema de Certificación del *CESG* para los profesionales de ciberseguridad son:

– Se evaluarán y verificarán de forma independiente su experiencia y competencia profesional por los organismos de certificación aprobados por el *CESG*.
– Se avalará su capacidad de aplicar de forma eficaz los conocimientos y experiencia para ofrecer beneficios al negocio.
– La pericia en roles de ciberseguridad específicos les permitirá la diferenciación del resto de profesionales.
– Formar parte de una comunidad profesional reconocida y creciente, a partir de la cual los empleadores pueden contratar a los profesionales de ciberseguridad.
– Ser elegible para trabajar en las redes del Gobierno del Reino Unido y en los proyectos de Infraestructuras Críticas Nacionales (sujeto a las habilitaciones de seguridad).

Los beneficios del Esquema de Certificación del *CESG* para los empleadores de profesionales de ciberseguridad son:

– Tener la confianza de que los profesionales de la ciberseguridad certificados han sido evaluados de forma rigurosa e independiente.
– Saber que los profesionales certificados han demostrado su experiencia en ciberseguridad y su capacidad para aplicar las habilidades, el conocimiento y la experiencia de manera efectiva en un entorno operativo.

– Tener la confianza de que los profesionales certificados tienen los conocimientos específicos necesarios para satisfacer las necesidades de negocio.
– Poder utilizar el esquema en la propia organización, para asegurarse de que los profesionales están desarrollando su experiencia, permitiendo a los empleados propios beneficiarse de ser parte de una comunidad reconocida de profesionales de la ciberseguridad.
– Influir en sus proveedores para emplear profesionales certificados, lo que también puede ayudar a reducir los riesgos de la cadena de suministro, ofreciendo una mayor confianza en la capacidad de los proveedores para gestionar con eficacia los riesgos de la información, tanto propia como ajena.

DoD 8570.01-M

Aunque la Directiva 8570.01[40] del Departamento de Defensa de Estados Unidos (*DoD, Department of Defense*) quedó derogada por la Directiva *DoD* 8140.01[41], publicada el 11 de agosto de 2015, el manual *DoD* 8570.01-M que acompañaba a la primera de ellas sigue estando vigente mientras la nueva Directiva no desarrolle uno propio.

Como su predecesora, la Directiva *DoD* 8140.01 establece las bases para una respuesta departamental a la capacitación, cualificación y gestión de la fuerza de trabajo en seguridad de la información del *DoD*, unificándola a nivel global y estableciendo elementos específicos de mano de obra de ciberseguridad, para alinear, gestionar y estandarizar los roles de trabajo de ciberseguridad, la línea base de cualificaciones y los requisitos de capacitación del *DoD*.

Como su propio nombre indica, el manual *DoD* 8570.01-M[42] (*Information Assurance Workforce Improvement Program*) constituye un programa en el que se identifican los requisitos específicos y obligatorios establecidos por el *DoD* para la gestión de su personal de seguridad de la información. El objetivo final es mantener una fuerza de trabajo con los conocimientos y habilidades necesarias para prevenir y responder a los ciberataques contra el *DoD*, permitiendo poner a las personas más adecuadas, con las habilidades requeridas, en los puestos necesarios para proteger los sistemas de información del Departamento.

La clave es la definición e identificación de todos los puestos de trabajo de seguridad de la información, de forma que cualquier persona que cubra uno

[40] Department of Defense, «DoD Directive 8570.01. Information Assurance Training, Certification, and Workforce Management, 8570.01», 2007, http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf

[41] Department of Defense, «DoD Directive 8140.01, Cyberspace Workforce Management, DoD», vol. 8140.01, 2015, https://www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf

[42] DoD, «DoD 8570.01-M - Information Assurance Workforce Improvement Program - Incorporating Change 4, November 10, 2015» 19 de diciembre de 2005, https://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

de esos puestos pasa a formar parte de dicha fuerza de trabajo (independientemente de su especialidad). Para ello, el *DoD* establece las funciones de perfiles profesionales de seguridad de la información para todo el Departamento, estructurándolos en categorías, especialidades y niveles.

La fuerza de trabajo de ciberseguridad del *DoD* se divide en dos grandes categorías, una centrada en los aspectos técnicos y otra en las funciones de gestión, con las siguientes denominaciones:

- *Information Assurance Technical* (*IAT*).
- *Information Assurance Manager* (*IAM*).

Las especialidades son grupos de perfiles profesionales de ciberseguridad del *DoD* que realizan funciones avanzadas o especializadas, que pueden exigir el dominio de un nivel técnico o de gestión específicos. Las especialidades del *DoD* son:

- *Information Assurance System Architect and Engineer* (*IASAE*).
- *Computer Network Defense Service Provider* (*CNDSP*).

Como ya se ha mencionado previamente, tanto las categorías como las especialidades se pueden desempeñar según diferentes niveles:

- *Computing Environment* (*level I*): servidores de redes de área local y su sistema operativo, periféricos y aplicaciones.
- *Networks Environment* (*level II*): elementos responsables de la conexión entre elementos del nivel anterior, proporcionando capacidades de transferencia de datos de corto alcance, tales como redes locales o redes de campus, o la capacidad de transporte de datos de larga distancia, tales como redes de área metropolitana o extensa, redes en operaciones o redes troncales.
- *Enclave Environment* (*level III*): colección de elementos de nivel 1, conectados por una o más redes internas, bajo el control de una autoridad y política de seguridad únicas, incluyendo al personal y a la seguridad física. Los enclaves proporcionan capacidades de seguridad estándar, como la defensa perimetral, la detección y la respuesta ante incidentes o la gestión de claves, ofreciendo aplicaciones comunes tales como las de ofimática o correo electrónico. Los enclaves pueden ser específicos para una organización o una misión y la organización de los entornos computacionales que albergan se pueden realizar por proximidad física o por función, en este caso independientemente de su ubicación. Ejemplos de enclaves son las redes de área local y las aplicaciones que alojan, así como redes troncales y centros de procesamiento de datos.

Por otro lado, para definir las funciones y requisitos de los puestos de trabajo de la especialidad *CNDSP*, en lugar de utilizar los tres niveles antes referidos, el manual *DoD* 8570.01-M usa los siguientes perfiles profesionales:

- *Analyst.*
- *Infrastructure support.*

– *Incident responder.*
– *Auditor.*
– *Manager*.

El *DoD* establece que todo el personal perteneciente a la fuerza de trabajo de seguridad de la información, tanto militares como civiles o contratistas externos, tanto a tiempo parcial como a tiempo completo, debe estar plenamente cualificado para llevar a cabo adecuadamente sus funciones de seguridad.

Cada categoría y especialidad tiene unos requisitos específicos de formación y certificación establecidos por niveles. Para el cumplimiento de dichos requisitos se requerirá una combinación de capacitación formal y actividades experimentales, como formación en el puesto de trabajo y formación continua.

En lo que se refiere a la capacitación formal, el *DoD* establece una tabla de certificaciones (no propias, sino de mercado, promovidas por empresas u organismos privados), aprobadas según las diferentes categorías, especialidades y niveles, para garantizar que el personal certificado dispone de un entendimiento suficiente de los principios fundamentales de ciberseguridad y de las prácticas relacionadas con las funciones propias de la posición asignada, garantizando así que todo el personal que desempeñe funciones de seguridad de la información en el *DoD* obtenga una de las certificaciones de base necesarias según su puesto de trabajo.

Las certificaciones actualmente aprobadas en el manual *DoD* 8570.01-M según diferentes categorías, especialidades y niveles son las siguientes:

– *Information Assurance Technical* (*IAT*).

- *Level I*: *A+ CE*[43], *Network+ CE*[44], *SSCP*[45] y *CCNA-Security*[46].
- *Level II: GSEC*[47], *Security+ CE*[48], *SSCP y CCNA-Security.*

[43] CompTIA, «A+ (Plus) Certification», accedido 1 de septiembre de 2016, https://certification.comptia.org/certifications/a

[44] CompTIA, «Network+ Certification», accedido 1 de septiembre de 2016, https://certification.comptia.org/certifications/network

[45] (ISC)², «SSCP - Systems Security Certified Practitioner», accedido 1 de septiembre de 2016, https://www.isc2.org/sscp/default.aspx

[46] Cisco, «CCNA (Cisco Certified Network Associate) Security», *Cisco*, accedido 1 de septiembre de 2016, http://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-security.html

[47] GIAC, «GSEC - GIAC Security Essentials Certification», accedido 1 de septiembre de 2016, http://www.giac.org/certification/security-essentials-gsec

[48] CompTIA, «Security+ Certification», accedido 1 de septiembre de 2016, https://certification.comptia.org/certifications/security

- *Level III: CISA*[49]*, GCIH*[50]*, GCED*[51]*, CISSP*[52] *(or Associate*[53]*)* y *CASP CE*[54].

– *Information Assurance Manager* (*IAM*).

- *Level I: CAP*[55]*, GSLC*[56] *y Security+ CE.*
- *Level II: CAP, GSLC, CISM*[57]*, CISSP (or Associate)* y *CASP CE.*
- *Level III: GSLC, CISM y CISSP (or Associate).*

– Information Assurance System Architect and Engineer (IASAE).

- *Level I: CISSP (or Associate), CASP CE* y *CSSLP*[58].
- *Level II: CISSP (or Associate), CASP CE* y *CSSLP.*
- *Level III: CISSP-ISSEP*[59] y *CISSP-ISSAP*[60].

– Computer Network Defense Service Provider (CNDSP).

- *Analyst: GCIA*[61]*, GCIH, CEH*[62] y *SCYBER*[63].
- *Infrastructure Support: SSCP* y *CEH.*

---

[49] ISACA, «CISA - Certified Information Systems Auditor», accedido 1 de septiembre de 2016, http://www.isaca.org/certification/cisa-certified-information-systems-auditor/pages/default.aspx

[50] GIAC, «GCIH - GIAC Certified Incident Handler», accedido 1 de septiembre de 2016, http://www.giac.org/certification/certified-incident-handler-gcih

[51] GIAC, «GCED - GIAC Certified Enterprise Defender», accedido 1 de septiembre de 2016, http://www.giac.org/certification/certified-enterprise-defender-gced

[52] (ISC)², «CISSP - Certified Information Systems Security Professional», accedido 1 de septiembre de 2016, https://www.isc2.org/cissp/default.aspx

[53] (ISC)², «Become an Associate of (ISC)2 Prior to Obtaining Certification», accedido 1 de septiembre de 2016, https://www.isc2.org/associate/default.aspx

[54] CompTIA, «CASP - CompTIA Advanced Security Practitioner Certification», accedido 1 de septiembre de 2016, https://certification.comptia.org/certifications/comptia-advanced-security-practitioner

[55] (ISC)², «CAP - Certified Authorization Professional», accedido 1 de septiembre de 2016, https://www.isc2.org/cap/default.aspx

[56] GIAC, «GSLC - GIAC Cyber Security Leadership Certification», accedido 1 de septiembre de 2016, http://www.giac.org/certification/security-leadership-gslc

[57] ISACA, «CISM - Certified Information Security Manager», accedido 1 de septiembre de 2016, http://www.isaca.org/certification/cism-certified-information-security-manager/pages/default.aspx

[58] (ISC)², «CSSLP - Certified Secure Software Lifecycle Professional», accedido 1 de septiembre de 2016, https://www.isc2.org/csslp/default.aspx

[59] (ISC)², «CISSP-ISSEP - Information Systems Security Engineering Professional», accedido 1 de septiembre de 2016, https://www.isc2.org/issep.aspx

[60] (ISC)², «CISSP-ISSAP - Information Systems Security Architecture Professional», accedido 1 de septiembre de 2016, https://www.isc2.org/issap.aspx

[61] GIAC, «GCIA - GIAC Certified Intrusion Analyst», accedido 1 de septiembre de 2016, http://www.giac.org/certification/certified-intrusion-analyst-gcia

[62] EC-Council, «CEH - Certified Ethical Hacker», *EC-Council*, 25 de febrero de 2016, https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/.

[63] Cisco, «Cybersecurity Specialist», *Cisco*, accedido 1 de septiembre de 2016, http://www.cisco.com/c/en/us/training-events/training-certifications/certifications/specialist/security/cybersecurity.html

- *Incident Responder: GCIH, GCFA*[64]*, CSIH*[65]*, CEH* y *SCYBER.*
- *Auditor: CISA, GSNA*[66] y *CEH.*
- *Manager: CISSP-ISSMP*[67] y *CISM.*

CCN/INAP - Esquema Nacional de Certificación de Profesionales en Ciberseguridad

El 31 de enero de 2014 se publica un comunicado[68] del Centro Criptológico Nacional (CCN)[69], adscrito al Centro Nacional de Inteligencia (CNI), informando sobre su propuesta, conjuntamente con el Instituto Nacional de Administración Pública (INAP)[70] para la creación de un Esquema Nacional de Certificación de Profesionales en Ciberseguridad. Ambos organismos comparten misiones y competencias en la formación del personal de las Adminstraciones públicas en materia de seguridad de las tecnologías de la información y las comunicaciones. Como indica el comunicado, la propuesta se fundamenta en la escasez de personal con los conocimientos y habilidades en ciberseguridad necesarios para cubrir las exigencias de empresas y Adminstraciones públicas ante el incremento de las ciberamenazas.

Esta iniciativa es similar a otras desarrolladas en países de nuestro entorno y permitirá diferenciar aquellos programas de formación con rigor y profesionalidad de los que no la tengan.

La propuesta, que viene a complementar algunos de los aspectos recogidos en la Estrategia de Ciberseguridad Nacional (objetivo 5)[71] y del Esquema

---

64 GIAC, «GCFA - GIAC Certified Forensic Analyst», accedido 1 de septiembre de 2016, http://www.giac.org/certification/certified-forensic-analyst-gcfa

65 SEI (Software Engineering Institute), «CERT-Certified Computer Security Incident Handler», accedido 1 de septiembre de 2016, https://www.sei.cmu.edu/certification/opportunities/csih/

66 GIAC, «GSNA - GIAC Systems and Network Auditor», accedido 1 de septiembre de 2016, http://www.giac.org/certification/systems-network-auditor-gsna

67 (ISC)², «CISSP-ISSMP - Information Systems Security Management Professional», accedido 1 de septiembre de 2016, https://www.isc2.org/issmp/default.aspx

68 CCN (Centro Criptológico Nacional), «El CCN y el INAP apuestan por un Esquema Nacional de Certificación de Profesionales en Ciberseguridad», *Comunicados CCN-CERT*, 31 de enero de 2014, https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/1846-el-ccn-y-el-inap-apuestan-por-un-esquema-nacional-de-certificacion-de-profesionales-en-ciberseguridad.html

69 Ministerio de Defensa, Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, *BOE*, accedido 27 de mayo de 2013, https://www.boe.es/boe/dias/2004/03/19/pdfs/A12203-12204.pdf

70 Ministerio de Política Territorial y Administración Pública, Real Decreto 464/2011, de 1 de abril, por el que se aprueba el Estatuto del Instituto Nacional de Administración Pública, vol. BOE-A-2011-6872, 2011, http://www.boe.es/buscar/pdf/2011/BOE-A-2011-6872-consolidado.pdf

71 Gobierno de España, *Estrategia de Ciberseguridad Nacional*, 2013, http://www.lamoncloa.gob.es/NR/rdonlyres/680D00B8-45FA-4264-9779-1E69D4FEF99D/256935/20131332EstrategiadeCiberseguridadx.pdf

Nacional de Seguridad (artículo 15)[72], ofrecerá importantes ventajas tanto para las Administraciones públicas como para las empresas privadas y los profesionales en general. La orientación a las competencias adecuadas a las necesidades de cada organismo, el incremento de la eficiencia de las inversiones de formación y el aumento de la madurez profesional del sector son algunos de los beneficios que traería esta certificación.

El desarrollo detallado del manual de competencias, definiendo todos los conocimientos y habilidades que les serán requeridos a los diferentes perfiles/categorías profesionales del esquema, el establecimiento de mecanismos de evaluación de candidatos, la elaboración de un código de conducta profesional, la determinación de los prerrequisitos de certificación y los procesos de renovación, así como la acreditación del esquema por la Entidad Nacional de Acreditación (ENAC), según la norma UNE-EN ISO/IEC 17024[73], serían los siguientes pasos a abordar dentro del Esquema.

La estructura general del posible Esquema de Certificación de Profesionales de Ciberseguridad para España constaría de cuatro elementos principales:

- ENAC: que acreditaría el esquema de certificación según la norma UNE-EN ISO/IEC 17024.
- CCN/INAP: que actuarían conjuntamente como Organismo de Certificación del Esquema, autorizando y supervisando a las entidades de evaluación reconocidas, y emitiendo los certificados profesionales que hayan superado las pruebas de evaluación.
- Entidades de evaluación: que, una vez autorizadas por el Organismo de Certificación, llevarían a cabo las evaluaciones de los candidatos.
- Candidatos: que serían todos aquellos profesionales que quieran certificar sus competencias en ciberseguridad.

La propuesta para un Esquema de Certificación incluiría dos roles profesionales[74]:

- Ingeniero de Ciberseguridad.
- Auditor de Ciberseguridad.

Cada uno de los roles anteriores con tres categorías profesionales, según la experiencia y el nivel de competencias requeridos:

- Profesional.

---

[72] Ministerio de la Presidencia, Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, 2010, http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf

[73] International Organization for Standardization, «ISO/IEC 17024:2012 - Evaluación de la conformidad. Requisitos generales para los organismos que realizan certificación de personas» (ISO/IEC, 2012), http://www.iso.org/iso/catalogue_detail?csnumber=52993

[74] INAP, CCN y Óscar PASTOR, «Esquema de Certificación de Personas», en *VII Jornadas STIC CCN - CERT* (Madrid, 2013), https://www.ccn-cert.cni.es/privatedocs/viijornadas/742-12-opastor-ccn-isdefe-esquemadecertificaciondepersonas/file.html

– Senior.
– Principal.

Inicialmente, el manual de conocimientos y habilidades de la propuesta de Esquema de Certificación de personas incluiría noventa competencias básicas, estructuradas en cuatro dominios y once subdominios:

– Gestión de la Seguridad de la Información.

• Seguridad de la Información y Objetivos de la Organización.
• Marco Normativo.
• Cultura de Seguridad.
• Cumplimiento.
• Entidades Externas.
• Gestión de Riesgos (Análisis y Tratamiento de Riesgos).

– Seguridad en el Ciclo de Vida del Sistema.

• Obtención de Sistemas Seguros (Arquitectura de Seguridad, Diseño/Desarrollo de Sistemas y Pruebas).
• Seguridad en las Operaciones (Aplicación de Procedimientos, Configuraciones de Seguridad y Prevención de Incidentes).

– Gestión de Excepciones de Seguridad.

• Incidentes de Seguridad (Gestión y Respuesta a Incidentes de Seguridad e Investigación/Forense).
• Continuidad del Servicio (Planificación y Pruebas/Ejercicios).

– Auditoría de Seguridad.

• Auditoría de Seguridad (Planificación, Ejecución e Informe).

Los posibles beneficios de la implantación de un Esquema Nacional de Certificación de Profesionales en Ciberseguridad serían[75]:

– Para las Administraciones públicas:

• Incrementar la eficiencia de las acciones de formación en seguridad de su personal, orientándolas a competencias adecuadas para el desempeño de sus funciones.
• Aumentar el conocimiento sobre sus capacidades/necesidades de profesionales de la ciberseguridad.
• Mejorar los criterios de asignación de destinos.
• Disponer de criterios objetivos de competencia profesional en ciberseguridad para la licitación y selección de servicios con proveedores externos.
• Asegurarse, mediante la gestión y el control del esquema de certificación, que las competencias, conocimientos y habilidades de los profesio-

[75] Óscar Pastor y Javier Candau, «Propuesta para un Esquema Nacional de Certificación de Profesionales en Ciberseguridad para España», *Revista SIC*, febrero de 2014.

nales de la ciberseguridad están siempre alineadas con el cumplimiento de su misión y las correspondientes estrategias nacionales.

– Para la empresas del sector privado:

• Disponer de criterios objetivos sobre los requisitos profesionales para la licitación de servicios.
• Incrementar la eficiencia de las inversiones de formación de su personal.
• Disponer de un esquema de garantía profesional independiente y de calidad.

– Para los profesionales en general:

• Incrementar la madurez profesional del sector de la ciberseguridad.
• Mejora de las expectativas y plan de carrera profesional.

SEPE - Certificado de Profesionalidad en Seguridad Informática

El Servicio Público de Empleo Estatal (SEPE)[76] es un organismo autónomo dependiente del Ministerio de Empleo y Seguridad Social. Entre sus competencias se encuentra la de elaborar, y elevar al Ministerio para su aprobación, propuestas normativas de ámbito estatal en materia de formación para el empleo, así como gestionar los correspondientes programas de formación profesional para el empleo.

En el mes de junio del año 2011 se publica el Real Decreto 686/2011[77], por el que se establecen seis certificados de profesionalidad, siendo uno de ellos el denominado Seguridad Informática. En el anexo III[78] de dicho Real Decreto se incluyen los detalles correspondientes a la Certificación Profesional en Seguridad Informática, que se creaba a partir de dicha norma, con el código IFCT0109.

El objeto de este Certificado de Profesionalidad es acreditar personal capaz de garantizar la seguridad de los accesos y usos de la información contenida en equipos informáticos, así como del propio sistema, protegiéndose de los posibles ataques, identificando vulnerabilidades y aplicando sistemas de cifrado a las comunicaciones que se realicen hacia el exterior y en el interior de la organización.

---

[76] Ministerio de Empleo y Seguridad Social, «Servicio Público de Empleo Estatal», accedido 2 de septiembre de 2016, http://www.empleo.gob.es/es/organizacion/empleo/contenido/OM29.htm

[77] BOE, Real Decreto 686/2011, de 13 de mayo, por el que se establecen seis certificados de profesionalidad de la familia profesional Informática y comunicaciones que se incluyen en el Repertorio Nacional de Certificados de Profesionalidad, 2011, https://sede.sepe.gob.es/es/portaltrabaja/resources/pdf/normativaCertificados/RD686_2011.pdf

[78] BOE, anexo III al Real Decreto 686/2011, Certificado de Profesionalidad en Seguridad Informática, 2011, https://sede.sepe.gob.es/es/portaltrabaja/resources/pdf/especialidades/IFCT0109.pdf

Se prevé que estos profesionales desarrollen su actividad en el área de sistemas del departamento de informática de empresas públicas o privadas que utilizan equipamiento informático, desempeñando tareas de auditoría, configuración y temas relacionados con la seguridad informática, tanto por cuenta ajena como por cuenta propia. Además, se supone que aunque estarán presentes en múltiples sectores productivos, trabajarán sobre todo en el sector servicios, aunque se percibe una marcada característica de transectorialidad. Los tipos de empresas a las que prestarán sus servicios serán:

- Empresas de cualquier sector y tamaño que utilizan equipamiento informático en sus procesos de gestión.
- Empresas que prestan servicios de asistencia técnica informática.
- Empresas de externalización (*outsourcing*) de servicios.
- El Certificado está desglosado en unidades de competencia, para detallar mejor los conocimientos y habilidades que deben poseer los profesionales certificados:
- Asegurar equipos informáticos (UC0486_3).
- Auditar redes de comunicación y sistemas informáticos (UC0487_3).
- Detectar y responder ante incidentes de seguridad (UC0488_3).
- Diseñar e implementar sistemas seguros de acceso y transmisión de datos (UC0489_3).
- Gestionar servicios en el sistema informático (UC0490_3).

Se establece que una formación asociada para estos profesionales de 500 horas, desglosada en los siguientes módulos formativos:

- Seguridad en Equipos Informáticos (MF0486_3): 90 horas.
- Auditoría de Seguridad Informática (MF0487_3): 90 horas.
- Gestión de Incidentes de Seguridad Informática (MF0488_3): 90 horas.
- Sistemas Seguros de Acceso y Transmisión de datos (MF0489_3): 60 horas.
- Gestión de Servicios en el Sistema Informático (MF0490_3): 90 horas.
- Prácticas Profesionales no Laborales de Seguridad informática (MP0175): 80 horas.

Además, al tratarse de un Certificado Profesional de nivel 3, se establecen una serie de requisitos previos:

- Estar en posesión del título de Bachiller.
- Estar en posesión de un certificado de profesionalidad del mismo nivel del módulo o módulos formativos y/o del certificado de profesionalidad al que se desea acceder.
- Estar en posesión de un certificado de profesionalidad de nivel 2 de la misma familia y área profesional para el nivel 3.
- Cumplir el requisito académico de acceso a los ciclos formativos de grado superior, o bien haber superado las correspondientes pruebas de acceso reguladas por las Administraciones educativas.

- Tener superada la prueba de acceso a la universidad para mayores de 25 años y/o de 45 años.
- Tener los conocimientos formativos o profesionales suficientes que permitan cursar con aprovechamiento la formación.
- Además, las personas que no tengan experiencia laboral en el sector, deben realizar obligatoriamente el módulo de prácticas, siendo este un requisito indispensable para obtener el título oficial.

Finalmente, una vez se haya obtenido la Certificación Profesional en Seguridad Informática, el SEPE establece que los profesionales acreditados puedan ocupar la siguiente relación de puestos de trabajo:

- Programador de Aplicaciones Informáticas (Código Nacional de Ocupación 3820.1017).
- Técnico en Informática de Gestión (Código Nacional de Ocupación 3812.1014).
- Técnico en Seguridad Informática.
- Técnico en Auditoría Informática.

Iniciativas privadas de formación y certificación en ciberseguridad

Analicemos a continuación los programas de formación y certificación profesional de ciberseguridad promovidos por empresas y organizaciones privadas, líderes a nivel internacional.

ISACA-CSX (Cybersecurity Nexus)

ISACA (*Information Systems Audit and Control Association*)[79] es una de las organizaciones señeras en los ámbitos del control, la auditoría y la seguridad de los sistemas y tecnologías de la información, que desde hace casi cincenta años ayuda a los profesionales a liderar, adaptar y asegurar la confianza en un mundo digital en evolución, ofreciendo conocimiento, estándares, relaciones, acreditación y desarrollo de carreras profesionales innovadoras y de primera clase. Establecida en 1969, *ISACA* es una asociación internacional sin ánimo de lucro que cuenta con unos ciento cuarenta mil profesionales en ciento ochenta y siete países. La asociación dispone de más de doscientos diez capítulos en todo el mundo.

ISACA es la creadora de COBIT[80], un marco de negocio para gobernar la tecnología de la empresa, y promueve desde hace años el avance y la certificación de habilidades y conocimientos críticos para el negocio, a través de las

[79] ISACA, «ISACA Fact Sheet», accedido 29 de agosto de 2016, http://www.isaca.org/About-ISACA/Press-room/Documents/2016-ISACA-Fact-Sheet_pre_eng_0716.pdf

[80] Information Systems Audit and Control Association, *Cobit 5: A Business Framework for the Governance and Management of Enterprise IT* (Rolling Meadows. IL: *ISACA*, 2012).

certificaciones, de reconocido prestigio a nivel internacional, entre las que se encuentran:

- *CISA* (*Certified Information Systems Auditor*)[81].
- *CISM* (*Certified Information Security Manager*)[82].
- *CGEIT* (*Certified in the Governance of Enterprise IT*)[83].
- *CRISC* (*Certified in Risk and Information Systems Control*)[84].

En 2014, *ISACA* crea el programa Cybersecurity Nexus (*CSX*)[85] con el objetivo de ayudar a cubrir la brecha de habilidades de seguridad cibernética, surgida entre la demanda y la oferta de profesionales de este ámbito (ya analizados previamente), y así proporcionar un desarrollo para los profesionales de este sector, en cada etapa de su carrera, ayudando a las empresas a desarrollar su fuerza de trabajo cibernético. *CSX* representa el compromiso de *ISACA* para ayudar a abordar la necesidad mundial de profesionales cualificados en ciberseguridad.

El programa *CSX* se diseña para ayudar a las empresas a fortalecer sus capacidades de ciberseguridad, mediante educación, formación y certificación de su personal, haciéndoles capaces de proteger la información de sus organizaciones. Para ello, *CSX* ayuda a obtener los conocimientos y habilidades que se necesitan para llevar a cabo completamente las tareas de ciberseguridad con una orientación de formación por competencias y de certificación basada en el desempeño. *CSX* está alineado con marcos de referencia internacionales como los ya mencionados *National Cybersecurity Workforce Framework*, del *NICE/NICCS*, o *SFIA*.

El programa de acreditación *CSX*[86] ofrece varios niveles de certificación, desde el más inicial hasta el experto, según la experiencia y formación de los candidatos a obtener estas credenciales.

---

81 ISACA, «Certified Information Systems AuditorTM (CISA®) Fact Sheet», accedido 29 de agosto de 2016, http://www.isaca.org/About-ISACA/Press-room/Documents/2015-CISA-Fact-Sheet_pre_eng_1015.pdf

82 ISACA, «Certified Information Security Manager® (CISM®) Fact Sheet», accedido 29 de agosto de 2016, http://www.isaca.org/About-ISACA/Press-room/Documents/2015-CISM-Fact-Sheet_pre_eng_1015.pdf

83 ISACA, «Certified in the Governance of Enterprise IT (CGEIT) Fact Sheet», accedido 29 de agosto de 2016, http://www.isaca.org/About-ISACA/Press-room/Documents/2015-CGEIT-Fact-Sheet_pre_eng_1015.pdf

84 ISACA, «Certified in Risk and Information Systems Control (CRISC)», accedido 29 de agosto de 2016, http://www.isaca.org/About-ISACA/Press-room/Documents/2015-CRISC-Fact-Sheet_pre_eng_1015.pdf

85 ISACA, «Cybersecurity Nexus (CSX) Fact Sheet», accedido 29 de agosto de 2016, http://www.isaca.org/cyber/Documents/Cybersecurity-Nexus-Fact-Sheet_pre_Eng_0115.pdf

86 ISACA, «Cybersecurity NexusTM (CSX) General Awareness Brochure», 2016, http://www.isaca.org/cyber/Documents/CSX-General-Awareness-Brochure_Bro_Eng_0816.pdf

Cybersecurity Fundamentals Certificate

Es el nivel de entrada en el programa y se trata de un certificado basado en el conocimiento. Está diseñado para universitarios recién graduados o aquellas personas que buscan un cambio en su carrera profesional hacia el ámbito de la ciberseguridad, ya que les permite demostrar su comprensión de los conceptos básicos de la seguridad cibernética.

Los exámenes revisan los conocimientos básicos en ciberseguridad a través de cinco áreas clave:

- Conceptos de ciberseguridad.
- Principios de arquitectura de ciberseguridad.
- Ciberseguridad de las redes, sistemas, aplicaciones y datos.
- Implicaciones de seguridad en la adopción de tecnologías emergentes.
- Respuesta a incidentes.

CSX Practitioner (*CSXP*)

Se trata de la primera certificación basada en el desempeño, dentro del esquema de certificaciones *CSX*, que permite a los que la poseen demostrar su capacidad para trabajar como primera línea de respuesta ante incidentes de ciberseguridad, siguiendo procedimientos establecidos, utilizando procesos definidos y trabajando con problemas conocidos en un único sistema.

La certificación *CSXP* indica que se dispone de experiencia en la configuración de cortafuegos, la gestión de parches de seguridad y los antivirus, así como capacidad de implementar controles de seguridad comunes y realizar exploraciones y análisis de vulnerabilidades. Para cumplir con requisitos de educación profesional continua, los poseedores de la certificación *CSXP* deben demostrar anualmente habilidades prácticas en un laboratorio y volver a examinarse cada tres años (al nivel de certificación *CSX* más alto que hubieran obtenido).

CSX Specialist

El siguiente nivel en la serie de certificaciones *CSX* es *Specialist*, y permite demostrar un profundo conocimiento y habilidad en ciberseguridad. En realidad, se trata de una serie de tres certificaciones independientes que cubren los cinco dominios del Marco de Referencia de Ciberseguridad del *NIST*[87]: identificar, proteger, detectar, responder y recuperarse.

- *CSX* | *Specialist*: *Identify and Protect*. Los especialistas dentro de este dominio son capaces de analizar y estimar las ciberamenazas a diferentes niveles de la infraestructura, desde un equipo individual hasta el nivel del sistema en su globalidad, utilizando buenas prácticas y herramientas

[87] NIST, «Framework for Improving Critical Infrastructure Cybersecurity», Cybersecurity Framework (National Institute of Standards and Technology, 12 de febrero de 2014), http://www.cslawreport.com/files/2015/04/07/nist-combined-file.pdf

comúnmente aceptadas. Estos profesionales son capaces de implementar controles de ciberseguridad con el fin de proteger tanto los sistemas como las redes.
- *CSX | Specialist*: *Detect*. Estos especialistas son capaces de distinguir incidentes y eventos mediante la identificación de indicadores de compromiso de red y de sistema, estimando posibles daños y proporcionando datos necesarios a los equipos de primera respuesta.
- *CSX | Specialist: Respond and Recover*. Los especialistas dentro de este dominio son capaces de desarrollar, implementar y mantener planes de respuesta a incidentes individuales, están familiarizados con técnicas de respuesta y están capacitados para comunicar correctamente eventos e incidentes. Pueden desarrollar, implementar y mantener planes de recuperación, así como utilizar herramientas especializadas para la evaluación de la integridad y de copias de seguridad distribuidas, proporcionan la restauración del servicio y sus tareas de apoyo.

Estas certificaciones se basan en las habilidades desarrolladas en la certificación *CSXP* (puesto que es un requisito previo disponer de la certificación *CSXP* antes de obtener una de las *CSX Specialist*) y en conceptos avanzados en cada uno de los dominios. *ISACA* ofrece un curso de formación de cinco días, para cada una de las certificaciones *CSX Specialist*, diseñado para enseñar las habilidades necesarias para practicar en un nivel que combina clases teóricas con al menos el 50 % de ejercicios prácticos en un entorno de laboratorio virtual.

CSX Expert

Aunque todavía no está abierta a candidatos, la certificación *CSX Expert* constituirá el vértice más alto del programa de certificación *CSX* de *ISACA*, permitiendo demostrar una maestría profesional y técnica en ciberseguridad, que garantiza el ser capaz de identificar, analizar, responder y mitigar los incidentes de ciberseguridad más complicados, generalmente en entornos empresariales complejos, en ambientes de alto nivel de exposición a los ciberataques.

Los expertos con esta certificación están destinados a servir como fuente autorizada para todos los asuntos de ciberseguridad, dentro de la organización, y a ser los responsables en la aprobación de los controles de seguridad, de los análisis de causa raíz y de correlación, para la evaluación de impacto en el negocio. Trabajan con la alta dirección para maximizar los éxitos de ciberseguridad en la organización y para comunicar los impactos comerciales relacionados con problemas cibernéticos, sirviendo como jefes de los equipos de respuesta a incidentes y de recuperación de desastres.

Certified Information Security Manager (*CISM*).

Aunque se trata de una certificación creada con anterioridad al programa *CSX*, *ISACA* incluye *CISM* dentro de la serie de certificaciones *CSX*, al mismo

nivel que *CSX Expert*, como certificación para demostrar el máximo nivel de pericia en la gestión de la seguridad de la información. Constituye, por tanto, una ruta de certificación alternativa o complementaria a la *CSX Expert*, centrada en los aspectos más técnicos, mientras que *CISM* se centra en los de gestión, que completa la serie *CSX* para ofrecer una trayectoria curricular completa, desde el nivel inicial al experto, desde los aspectos más técnicos a los gerenciales.

La certificación *CISM* identifica a personas que entienden el negocio para gestionar, diseñar, supervisar y evaluar la seguridad de la información en la empresa. Demuestra el entendimiento de quien la ostenta sobre las relaciones entre un programa de seguridad de la información y los objetivos de negocio de la organización. Garantiza no solo la máxima pericia en la seguridad de la información, sino también un profundo conocimiento y experiencia en el desarrollo y gestión de un programa de seguridad de la información.

ISACA establece los requisitos para obtener la certificación *CISM* agrupándolos en cuatro dominios, con diferentes pesos relativos, que después son definidos y detallados en conocimientos y tareas profesionales, que representan un análisis de las prácticas profesionales que llevan a cabo en todo el mundo los gestores de seguridad de la información.

Los cuatro dominios de la certificación *CISM* son:

- Dominio 1: Gobernanza de la Seguridad de la Información (24 %).
- Dominio 2: Gestión de Riesgos de la Información y Cumplimiento (33 %).
- Dominio 3: Desarrollo y Gestión de Programas de Seguridad de la Información (25 %).
- Dominio 4: Gestión de Incidencias de Seguridad de la Información (18 %).

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

El Consorcio Internacional de Certificación de Seguridad de Sistemas de Información (*ISC*)², siguiendo su denominación original en inglés (*International Information System Security Certification Consortium*)[88], es otra de las asociaciones más veteranas y con mayor prestigio en el campo de la seguridad de la información.

(*ISC*)² es una asociación internacional, sin ánimo de lucro, centrada en inspirar un mundo cibernético seguro y protegido. (*ISC*)² ofrece un conjunto de certificaciones profesionales con un enfoque integral y estructurado a la ciberseguridad. Dispone de más de 115.000 miembros, constituyendo una robusta comunidad de profesionales certificados en ciberseguridad que están contribuyendo al avance de la industria de este sector.

[88] (ISC)², «(ISC)² Overview», accedido 5 de septiembre de 2016, https://www.isc2.org/uploadedfiles/(isc)2_public_content/(isc)2-company-overview.pdf

La certificación más conocida y demandada de (*ISC*)² es *CISSP* (*Certified Information Systems Security Professional*)[89]. Se trata de una certificación, independiente de los fabricantes de tecnología, destinada a aquellos profesionales con avanzadas y probadas competencias técnicas y de gestión, con habilidades, experiencia y credibilidad para crear, diseñar e implementar programas globales de seguridad de la información, con el objetivo de proteger a las organizaciones ante la creciente sofisticación de los ataques cibernéticos.

Entre los perfiles profesionales a los que va destinada esta certificación se encontrarían los de consultor de seguridad, gerente de seguridad, director/gerente TI, auditor de seguridad, arquitecto de seguridad, analista de seguridad, ingeniero de sistemas de seguridad, *CISO* (*Chief Information Security Officer*), director de seguridad y arquitecto de redes.

CISSP es una de las credenciales más veteranas en el campo de la seguridad de la información y cumple con los estrictos requisitos de las Norma ISO/IEC 17024, convirtiéndose en una certificación de reconocido prestigio internacional asociada a la excelencia profesional. Para ello, la certificación *CISSP* se fundamenta en un Cuerpo de Conocimiento Común (*CBK, Common Body of Knowledge*) continuamente revisado y puesto al día por (*ISC*)², para asegurar que los profesionales certificados tienen un profundo conocimiento y comprensión de las nuevas amenazas, las tecnologías, la legislación, la normativa y las buenas prácticas en ciberseguridad.

El *CISSP CBK* se desglosa en ocho dominios, cada uno de los cuales cubre diferentes tópicos o aspectos de la seguridad de la información:

– Seguridad y gestión de riesgos:

- Conceptos de confidencialidad, integridad y disponibilidad.
- Principios de gobierno de la seguridad.
- Cumplimiento.
- Aspectos legales y reglamentarios.
- Ética profesional.
- Políticas, normas, procedimientos y directrices de seguridad.

– Seguridad de activos:

- Clasificación de la información y de los activos.
- La propiedad (propietarios de datos, propietarios del sistema).
- Proteger la privacidad.
- Retención adecuada.
- Controles de seguridad de los datos.
- Requisitos de manipulación (marcas, etiquetas y almacenamiento).

[89] (ISC)², «CISSP (Certified Information Systems Security Professional) Brochure», 16 de diciembre de 2015, https://www.isc2.org/uploadedfiles/credentials_and_certifcation/cissp/cissp-information.pdf

– Ingeniería de seguridad:

- Procesos de ingeniería por medio de principios de diseño seguro.
- Conceptos fundamentales de los modelos de seguridad.
- Modelos de evaluación de la seguridad.
- Capacidades de seguridad de los sistemas de información.
- Arquitecturas de seguridad, diseños y vulnerabilidades de elementos de las soluciones.
- Vulnerabilidades de sistemas basados en la web.
- Vulnerabilidades de sistemas móviles.
- Dispositivos empotrados y vulnerabilidades de los sistemas ciberfísicos.
- Criptografía.
- Principios de diseño seguro de ubicaciones y edificios.
- Seguridad física.

– Seguridad de comunicaciones y red:

- Diseño de arquitecturas de red seguras (protocolos IP y no IP, segmentación).
- Componentes de redes seguras.
- Canales de comunicación seguros.
- Ataques de red.

– Gestión de identidades y acceso:

- Control de activos físicos y lógicos.
- Identificación y autenticación de personas y dispositivos.
- Identidad como servicio (identidad en la nube).
- Servicios de identidad de terceros (en las instalaciones).
- Ataques de control de acceso.
- Ciclo de vida del aprovisionamiento de identidades y accesos (revisión de aprovisionamiento).

– Evaluación y pruebas de seguridad:

- Estrategias de evaluación y prueba.
- Datos del proceso de seguridad (la gestión y los controles operacionales).
- Pruebas de control de la seguridad.
- Salidas de prueba (automatizado, manual).
- Vulnerabilidades de las arquitecturas de seguridad.

– Operaciones de seguridad:

- Apoyo a las investigaciones y sus requisitos.
- Actividades de gestión de registros y monitorización.
- Aprovisionamiento de los recursos.
- Conceptos fundamentales de operaciones de seguridad.
- Técnicas de protección de recursos.
- Gestión de incidentes.
- Medidas preventivas.

- Gestión de parches y vulnerabilidades.
- Procesos de gestión del cambio.
- Estrategias de recuperación.
- Procesos y planes de recuperación ante desastres.
- Planificación y ejercicios de la continuidad de negocio.
- Seguridad física.
- Consideraciones sobre la protección del personal.

– Seguridad en el desarrollo *software*:

- Seguridad en el ciclo de vida de desarrollo *software*.
- Controles de seguridad del entorno de desarrollo.
- Efectividad de la seguridad del *software*.
- Impacto en la seguridad del *software* adquirido.

Los candidatos a *CISSP* deben acreditar al menos cinco años de experiencia a tiempo completo en dos o más de los dominios anteriores. Además, deberán superar un examen de seis horas de duración, compuesto de doscientas cincuenta preguntas, de elección múltiple, debiendo obtener una calificación de 700 o más sobre un total de 1.000 puntos.

Además, para mantener la credencial, se requiere la recertificación cada tres años, para lo que se deben obtener y presentar un mínimo de 40 créditos *CPE* (*Continuing Professional Education*) cada año del ciclo de certificación de tres años y un total de 120 créditos *CPE* al final del ciclo de certificación de tres años.

Debido a la constante evolución de los diferentes aspectos que afectan a la ciberseguridad, (*ISC*)² ha evolucionado la concepción original de la certificación *CISSP*, desarrollando nuevas credenciales específicas que la complementan, que ha denominado *CISSP-Concentrations*[90], para abordar las necesidades concretas de las diferentes comunidades de profesionales de la ciberseguridad, centradas en las áreas funcionales de:

– Arquitectura.
– Ingeniería.
– Gestión.

Superar el examen de una de las *CISSP-Concentrations* demuestra una mayor capacidad y experiencia, en ese aspecto concreto, que la requerida para las credenciales *CISSP* estándar.

CISSP-ISSAP - Information Systems Security Architecture Professional

Esta credencial está destinada a profesionales certificados *CISSP* que desarrollen su trabajo en posiciones tales como arquitecto de sistemas, director

[90] (ISC)², «CISSP Concentrations», accedido 5 de septiembre de 2016, https://www.isc2.org/uploadedfiles/(isc)2_public_content/certification_programs/cissp_concentrations/concentrations-web.pdf

de informática (*CTO, Chief Technology Officer*), ingeniero de redes y sistemas, analista de negocio o jefe de ciberseguridad.

Para (*ISC*)², los arquitectos de ciberseguridad juegan un papel fundamental dentro del departamento de seguridad de la información de las organizaciones, con responsabilidad para ajustar funcionalmente las expectativas de la alta dirección y la implementación de los programas de ciberseguridad. Normalmente, estos profesionales deben desarrollar, diseñar o analizar el plan de ciberseguridad global de la organización. Aunque, por lo general, el rol que desempeñan estos profesionales puede estar estrechamente vinculado a la tecnología, su desempeño fundamental debe estar más próximo al proceso de consultoría y análisis de ciberseguridad de la información, por lo que (*ISC*)² entiende que *ISSAP* es una credencial muy apropiada para profesionales *CISSP* que trabajan como consultores independientes.

El Cuerpo de Conocimiento del *CISSP-ISSAP* se desglosa en seis dominios:

- Sistemas y Metodologías de Control de Acceso.
- Seguridad de Comunicaciones y Red.
- Criptografía.
- Análisis de la Arquitectura de Seguridad.
- Tecnologías Relacionadas con el Plan de Continuidad de Negocio y el Plan de Recuperación ante Desastres.
- Consideraciones de Seguridad Física.

Para obtener la certificación *CISSP-ISSAP*, un candidato debe demostrar dos años de experiencia profesional, a tiempo completo, en el ámbito de la arquitectura de ciberseguridad y, además, superar un examen de tres horas de duración, compuesto de ciento veinticinco preguntas, de elección múltiple, debiendo obtener una calificación de 700 o más sobre un total de 1.000 puntos.

CISSP-ISSEP - Information Systems Security Engineering Professional

(*ISC*)² desarrolló la certificación *CISSP-ISSEP* conjuntamente con la Agencia Nacional de Seguridad de Estados Unidos (*NSA, National Security Agency)*[91], con el objetivo de proporcionar una valiosa herramienta para cualquier profesional de la ingeniería de sistemas de seguridad. *ISSEP* se constituye así como una guía para la incorporación de la ciberseguridad en proyectos, aplicaciones, procesos de negocio y cualquier sistema de información. Esto responde a la urgente demanda de los profesionales de la ciberseguridad por disponer de metodologías viables y mejores prácticas, que se puedan utilizar de forma real, para integrar la seguridad en todas las facetas de las operaciones de negocio.

[91] NSA, «Mission & Strategy», accedido 5 de septiembre de 2016, https://www.nsa.gov/about/mission-strategy/

Esta credencial está destinada a profesionales certificados *CISSP* que desarrollen su trabajo en posiciones tales como ingeniero senior de sistemas, ingeniero de sistemas de seguridad de la información, director de seguridad de la información, analista de seguridad de la información o analista senior de seguridad.

El Cuerpo de Conocimiento del *CISSP-ISSEP* se desglosa en cuatro dominios:

- Ingeniería de Seguridad de Sistemas.
- Certificación y Acreditación/Marco de Referencia para la Gestión de Riesgos.
- Gestión Técnica.
- Políticas y Publicaciones del Gobierno de Estados Unidos Relacionadas con la Seguridad de la Información.

Para obtener la certificación *CISSP-ISSEP*, un candidato debe demostrar dos años de experiencia profesional, a tiempo completo, en este ámbito de la ciberseguridad y, además, superar un examen de tres horas de duración, compuesto de ciento cincuenta preguntas, de elección múltiple, debiendo obtener una calificación de 700 o más sobre un total de 1.000 puntos.

CISSP-ISSMP - Information Systems Security Management Professional

Esta credencial está destinada a profesionales certificados *CISSP* que desarrollen su trabajo en posiciones tales como director de informática, director de seguridad de la información, director de tecnología o ejecutivo senior de seguridad.

Esta certificación contiene elementos que implican profundos conocimientos de gestión, tales como gestión de proyectos, gestión de riesgos, desarrollo y puesta en práctica de un programa de concienciación sobre seguridad o la gestión de un programa de planificación de la continuidad del negocio. Para $(ISC)^2$, un profesional *CISSP-ISSMP* establece, presenta y gestiona los programas de seguridad de la información, demostrando profundas habilidades de gestión y liderazgo. Normalmente, los profesionales que ostenten la certificación *ISSMP* serán los encargados de diseñar la estructura del departamento de ciberseguridad de una empresa u organización, así como de definir los medios para apoyar a este grupo internamente. Estos profesionales disponen de una comprensión completa, avanzada y definida de la gestión de la seguridad de la información.

El Cuerpo de Conocimiento del *CISSP-ISSMP* se desglosa en cinco Dominios:

- Liderazgo y Gestión de la Seguridad.
- Gestión del Ciclo de Vida de Seguridad.
- Gestión del Cumplimiento de Seguridad.
- Gestión de Contingencias.
- Legislación, Ética y Gestión de Incidentes.

Para obtener la certificación *CISSP-ISSMP* un candidato debe demostrar dos años de experiencia profesional, a tiempo completo, en la gestión de un gran

modelo de seguridad de toda una empresa u organización y, además, superar un examen de tres horas de duración, compuesto de ciento veinticinco preguntas, de elección múltiple, debiendo obtener una calificación de 700 o más sobre un total de 1.000 puntos.

SANS/GIAC

El Instituto *SANS* (originalmente, *SysAdmin, Networking and Security Institute*)[92] es una institución privada, fundada en 1989, con sede en los Estados Unidos, cuyos programas de formación son seguidos por más de 165.000 profesionales de la seguridad informática de todo el mundo, desde auditores y administradores de sistemas hasta directores de seguridad informática.

Sus principales objetivos son:

– La investigación y recopilación de información sobre todo lo referente a seguridad informática (sistemas operativos, *routers*, *firewalls*, aplicaciones, *IDS*, etcétera). En este campo, muchos de los valiosos recursos del *SANS* son de libre acceso, entre los que cabe mencionar:

- *Internet Storm Center* (Sistema de Alerta Temprana de la Internet).
- *NewsBites* (boletín semanal de noticias).
- @RISK (boletín semanal de vulnerabilidades).
- *CIS Critical Security Controls* (clasificación de consenso de los controles de seguridad que son más eficaces en la reducción del riesgo a los ciberataques del mundo real).

– Ofrecer programas de capacitación y certificación en el ámbito de la seguridad informática.

- Más de cuatrocientos cursos, en noventa ciudades de todo el mundo, diseñados para dominar las medidas prácticas necesarias para la defensa de redes y sistemas contra las ciberamenazas más virulentas, que están siendo explotados de forma activa.
- Los cursos tienen una orientación eminentemente técnica, para que los conocimientos adquiridos puedan ser puestos en práctica de forma inmediata en los respectivos puestos de trabajo.

Por otro lado, *GIAC* (*Global Information Assurance Certification*)[93] es una entidad de certificación de seguridad de la información, especializada en la certificación técnica y práctica, que fue fundada en 1999 por el *SANS Institute*. Los primeros profesionales *GIAC* fueron certificados en el año 2000 y en la actualidad se han emitido más de 84.000 certificaciones *GIAC*.

[92] SANS, «SANS Institute: About», accedido 6 de septiembre de 2016, https://www.sans.org/about/

[93] GIAC, «About GIAC», accedido 6 de septiembre de 2016, http://www.giac.org/about

GIAC proporciona un conjunto de certificaciones de ciberseguridad, independientes de los proveedores de tecnología, vinculados a los cursos de formación impartidos por el *Instituto SANS*. Aunque están alineados, los programas de formación del *SANS* y los de certificación de *GIAC* son independientes, no siendo necesario seguir un curso de formación del *SANS* para obtener una certificación *GIAC*, ni obligatorio certificarse por *GIAC* tras haber realizado alguna capacitación con *SANS*. Esto último es solo una opción.

Así, mientras que la formación de *SANS* tiene como objetivo proporcionar a los estudiantes la mejor formación disponible, en las diferentes áreas clave de la ciberseguridad, la certificación *GIAC* está diseñada para proporcionar un punto de referencia objetivo, que permita demostrar que un individuo se encuentra con un nivel mínimo de habilidades prácticas y conocimientos para las personas que desean demostrar esta capacidad a un empleador actual o potencial.

Para obtener una de las certificaciones *GIAC* se debe superar un examen controlado por un supervisor, permitiendo además alcanzar dos niveles o *status*[94]:

- *GIAC Gold Status*: que permite demostrar un conocimiento más profundo de la materia. Requiere que los candidatos desarrollen un trabajo de investigación y escriban un informe técnico o documento detallado al respecto, bajo la supervisión de un asesor.
- *GIAC Expert Status*: que acredita como profesional del máximo nivel de conocimiento en la materia. Entre los prerrequisitos se incluyen la consecución de varias certificaciones y disponer de varios *gold status*. Los exámenes para obtener el nivel «Experto» se convocan anualmente e incluyen varias actividades prácticas, abarcando varios días de duración. Las pruebas incluyen ejercicios de ciberseguridad, individual y en grupo, presentaciones, trabajos de investigación y ensayo, así como secciones de test prácticos basados en escenarios, con el objetivo de garantizar que el candidato está listo para hacer frente a diversas amenazas de ciberseguridad, en diferentes niveles de gravedad.

GIAC ofrece más de veinte certificaciones independientes, cada una de ellas con un dominio de conocimientos y habilidades, en diferentes ámbitos de la ciberseguridad, como la administración y gestión, los aspectos legales, las auditorías, el análisis forense o la seguridad del *software*. De esta forma, *GIAC* promueve que cada profesional pueda crearse su propia hoja de ruta de certificación profesional, determinando qué certificaciones son las más adecuadas para las necesidades específicas de su entorno de trabajo o las metas de su carrera profesional.

[94] GIAC, «GIAC Certification Program Candidate's Handbook» (Global Information Assurance Certification, 2012), http://www.giac.org/pdfs/certification-candidate-handbook.pdf

Revisemos brevemente algunas de las certificaciones *GIAC* más prestigiosas.

GSEC-GIAC Security Essentials Certification

Certificación destinada para aquellos profesionales de la ciberseguridad que desean demostrar que están cualificados para llevar a cabo tareas prácticas de seguridad en sistemas de información y comunicaciones. Los candidatos deben demostrar una sólida comprensión de los diferentes aspectos que implica la seguridad de la información, más allá del dominio de la terminología y los conceptos más simples.

Para obtener la certificación, los candidatos deben superar un examen supervisado de ciento ochenta preguntas, a responder en un tiempo máximo de cinco horas, obteniendo como mínimo un 74 % de respuestas acertadas.

Las áreas de conocimiento que aborda esta certificación incluyen:

- Conceptos de redes.
- Defensa en profundidad.
- Tecnologías de seguridad de internet.
- Comunicaciones seguras.
- Seguridad en Windows.
- Seguridad en Unix/Linux.

GSLC-GIAC Cyber Security Leadership Certification

Esta certificación va destinada al personal de gestión de las organizaciones y empresas, con responsabilidades de dirección y/o supervisión de otro personal de ciberseguridad a su cargo.

Para obtener la certificación, los candidatos deben superar un examen supervisado de ciento quince preguntas, a responder en un tiempo máximo de tres horas, obteniendo como mínimo un 68 % de respuestas acertadas.

Las áreas de conocimiento que aborda esta certificación incluyen:

- Gestión de la empresa, planificación, red e instalaciones físicas.
- Conceptos IP, ataques contra la empresa y defensa en profundidad.
- Comunicaciones seguras.
- El valor de la información.
- Gestión práctica.

GCIH-GIAC Certified Incident Handler

Los gestores de incidentes de seguridad son capaces de manejarlos por medio de una profunda comprensión de las técnicas más comunes de ataque, sus vectores y sus herramientas asociadas, así como del conocimiento de los fundamentos de la defensa para prevenir y/o responder a estos ataques cuando se produzcan.

La certificación *GCIH* se centra en detectar, responder y resolver incidentes de ciberseguridad y abarca las siguientes áreas de conocimiento de la ciberseguridad:

- Pasos del proceso de gestión de incidentes.
- Detección de aplicaciones maliciosas y actividad de la red.
- Técnicas comunes de ataque para comprometer servidores.
- Detección y análisis de vulnerabilidades en redes y sistemas.
- Proceso de mejora continua mediante el descubrimiento de las causas raíz de los incidentes.

Para obtener la certificación, los candidatos deben superar un examen supervisado de ciento cincuenta preguntas, a responder en un tiempo máximo de cuatro horas, obteniendo como mínimo un 73 % de respuestas acertadas.

GCED-GIAC Certified Enterprise Defender

La certificación *GCED* está pensada para completar y profundizar, sin solapamiento, los conocimientos y habilidades de ciberseguridad acreditados por medio de la certificación *GSEC*, ya vista anteriormente. En la certificación *GCED* se evalúan habilidades y conocimientos técnicos avanzados necesarios para defender el entorno de la empresa y proteger una organización en su conjunto.

Los conocimientos, competencias y habilidades que se evalúan en esta certificación abarcan las siguientes áreas:

- Infraestructura de red defensiva.
- Análisis de paquetes.
- Test de penetración.
- Gestión de incidentes.
- Eliminación de *malware*.

Para obtener la certificación, los candidatos deben superar un examen supervisado de ciento quince preguntas, a responder en un tiempo máximo de tres horas, obteniendo como mínimo un 70 % de respuestas acertadas.

GCIA-GIAC Certified Intrusion Analyst

Los profesionales con la certificación *GCIA* disponen de los conocimientos, competencias y habilidades para configurar y supervisar los sistemas de detección de intrusos, así como para leer, interpretar y analizar el tráfico de red y los archivos de registro de eventos relacionados.

Para obtener la certificación, los candidatos deben superar un examen supervisado de ciento cincuenta preguntas, a responder en un tiempo máximo de cuatro horas, obteniendo como mínimo un 67 % de respuestas acertadas.

Las áreas de conocimiento que aborda la certificación *GCIA* incluyen:

- Fundamentos del análisis del tráfico.
- Protocolos de aplicación y análisis de tráfico.
- Sistemas de detección de intrusiones *open-source*.
- Monitorización y análisis forense del tráfico de red.

– Desafío a los sistemas de detección de intrusiones.

GCFA-GIAC Certified Forensic Analyst

Certificación destinada a los profesionales que trabajan en la seguridad de la información, informática forense, así como en la gestión y respuesta a incidentes. La certificación se centra en las habilidades y conocimientos básicos para recoger y analizar los datos de sistemas informáticos en entornos Windows y Linux.

La certificación *GCFA* acredita que los candidatos tienen los conocimientos, competencias y habilidades para llevar a cabo investigaciones formales de incidentes y gestionar el manejo de incidentes en escenarios avanzados, incluyendo intrusiones externas y/o violaciones internas del control de acceso a los datos, amenazas persistentes avanzadas (*APT, Advanced Persistent Threat*), técnicas antiforenses utilizadas por los atacantes, así como casos forenses digitales complejos.

Para obtener la certificación, los candidatos deben superar un examen supervisado de ciento quince preguntas, a responder en un tiempo máximo de tres horas, obteniendo como mínimo un 71 % de respuestas acertadas.

Las áreas de conocimiento que aborda esta certificación incluyen:

– Técnicas avanzadas de respuesta a incidentes y caza de amenazas.
– Técnicas forenses en memorias volátiles en la respuesta a incidentes.
– Técnicas forenses de detección de intrusiones.
– Análisis de la línea de tiempo.
– Detección y respuesta a incidentes a nivel de toda la empresa.
– Adversarios avanzados y detección de técnicas antiforenses.
– El desafío de la respuesta a incidentes de *APT*.

GSNA-GIAC Systems and Network Auditor

Los profesionales con la certificación *GSNA* acreditan los conocimientos, competencias y habilidades para aplicar las técnicas de análisis de riesgos más básicos y para llevar a cabo una auditoría técnica de los servicios esenciales de los sistemas de información. Esta certificación va dirigida al personal técnico responsable de la seguridad y la auditoría de los sistemas de información.

Para obtener la certificación, los candidatos deben superar un examen supervisado de ciento quince preguntas, a responder en un tiempo máximo de tres horas, obteniendo como mínimo un 73 % de respuestas acertadas.

Las áreas de conocimiento que aborda la certificación *GCIA* incluyen:

– Auditoría, evaluación de riesgos y generación de informes de forma eficaz.
– Auditoría y monitorización eficaz de la red y el perímetro.
– Auditoría de aplicaciones web.

- Auditoría y monitorización avanzada de entornos Windows.
- Auditoría y monitorización avanzada de entornos Unix.
- Ciberejercicios.

EC-Council - CEH (Certified Ethical Hacker)

International Council of E-Commerce Consultants, también conocido como *EC-Council*[95], es uno de los mayores organismos del mundo para la certificación técnica de profesionales de la seguridad cibernética. Con implantación en ciento cuarenta países, el *EC-Council* ha formado y certificado a más de 140.000 profesionales de la seguridad de la información de todo el mundo, que han influido en la visión de la ciberseguridad de un gran número de organizaciones internacionales.

La misión del *EC-Council* es validar que los profesionales de la ciberseguridad disponen de las habilidades y conocimientos necesarios, en un entorno profesional muy exigente, que les permitirá ayudar a evitar que surjan ciberconflictos. *EC-Council* se compromete a mantener el más alto nivel de imparcialidad y objetividad en sus prácticas, toma de decisiones y autoridad en todos los asuntos relacionados con la certificación.

El *EC-Council* dispone de varios programas de certificación de seguridad, con gran prestigio y reconocimiento a nivel internacional, siendo el *CEH* (*Certified Ethical Hacker*)[96], creado en 2003, el más demandado.

El propósito de la credencial *CEH* es:

- Establecer y regular las normas mínimas para la acreditación del conocimiento y dominio de las medidas de *hacking* ético por parte los profesionales especialistas en ciberseguridad.
- Acreditar al público en general que los individuos certificados cumplen o exceden los estándares profesionales mínimos.
- Reforzar el ejercicio profesional del *hacking* ético como una profesión única y autorregulada.

Una persona con la certificación *CEH* es un profesional experto, que entiende y sabe cómo buscar debilidades y vulnerabilidades en los sistemas objetivo, y utiliza los mismos conocimientos y herramientas que un *hacker* malicioso, pero de una manera legal y legítima para evaluar la postura de seguridad de un sistema de objetivo. La credencial *CEH* certifica individuos en la disciplina específica del *hacking* ético desde una perspectiva neutral de los proveedores de tecnologías de seguridad de redes.

[95] EC-Council, «About - International Council of E-Commerce Consultants», 25 de febrero de 2016, https://www.eccouncil.org/about/

[96] EC-Council, «CEH Handbook v2.0», enero de 2015, https://www.eccouncil.org/wp-content/uploads/2016/06/CEH-Handbook-v2.0.pdf

El examen *CEH* incluye los siguientes dominios de conocimiento:

– Fundamentos:

- Tecnologías de red.
- Tecnologías web.
- Tecnologías de sistemas de información.
- Protocolos de comunicaciones.
- Operaciones *malware*.
- Tecnologías móviles.
- Tecnologías de redes de telecomunicaciones.
- Copias de seguridad y archivado.

– Análisis/Evaluación:

- Análisis de datos.
- Análisis de sistemas.
- Evaluación de riesgos.
- Métodos de evaluación técnica.

– Seguridad:

- Controles de seguridad en sistemas.
- Servidores de archivos/aplicaciones.
- Cortafuegos.
- Criptografía.
- Seguridad de red.
- Seguridad física.
- Modelado de amenazas.
- Procedimientos de verificación (falsos positivos).
- Ingeniería social.
- Escaneo de vulnerabilidades.
- Implicaciones de la política de seguridad.
- Privacidad/confidencialidad.
- Biometría.
- Tecnología de acceso *wireless*.
- Redes confiables.
- Vulnerabilidades.

– Herramientas/Sistemas/Programas:

- Intrusiones basadas en red/servidor.
- Sniffers de red/*wireless* (*WireShark*, *Airsnort*).
- Mecanismos de control de acceso.
- Técnicas criptográficas.
- Lenguajes de programación.
- Lenguajes de programación de *scripts*.
- Dispositivos de protección del perímetro.
- Topologías de red.

- *Subnetting*.
- Escaneo de puerto.
- Sistema de nombres de dominio.
- *Routers/modems/switches*.
- Escáneres de vulnerabilidades.
- Gestión de vulnerabilidades y protección de sistemas.
- Sistemas operativos.
- Sistemas y programas antivirus.
- Herramientas de análisis de registros.
- Modelos de seguridad.
- Herramientas de explotación.
- Estructuras de bases de datos.

– Procedimientos/Metodología:

- Criptografía.
- Infraestructura de clave pública (*PKI*).
- Arquitectura de seguridad.
- Arquitectura orientada a servicios.
- Incidente de seguridad de la información.
- Diseño de aplicaciones en N-capas.
- Comunicaciones TCP/IP.
- Metodología de evaluaciones de seguridad.

– Regulación/Política:

- Políticas de seguridad.
- Cumplimiento de regulaciones.

– Código ético:

- Código de conducta profesional.
- Adecuación del *hacking*.

Para obtener la certificación *CEH*, un candidato deberá superar un examen de ciento veinticinco preguntas, en formato de respuestas múltiples, en un tiempo máximo de cuatro horas.

Conclusiones

Conviene precisar que las necesarias conclusiones que a continuación exponemos y desarrollamos no solamente se desprenden de la lectura del presente capítulo, que también, sino que son conclusiones y puntos para la reflexión recogidos por los autores durante su realización.

Por lo que respecta a la más que palmaria escasez de profesionales en materia de Ciberseguridad, nos hemos retrotraído a seis años atrás en el análisis de estudios e informes para evidenciar que no se trata de un problema nuevo, sino que se veía venir desde hace tiempo y, como reflejan las reseñas

más actuales, existe incluso un aumento de la brecha entre oferta y demanda de profesionales en este ámbito a pesar de los esfuerzos realizados en estos últimos cinco años.

Quisiéramos en estas conclusiones subrayar que este déficit está enmarcado en un problema más general como es la falta de ingenieros y técnicos especialistas en las tecnologías de la información y las comunicaciones (TIC), si bien agravado en el caso de la ciberseguridad y ciberdefensa.

En Europa existen actualmente dos grandes iniciativas que están ya influyendo en la configuración de las ocupaciones relacionadas con las TIC.

La primera de ellas es la publicación del estándar EN 16234-1:2016[97] que define un marco de trabajo (*eCompetence Framework: eCF*) para la definición de perfiles profesionales en TIC basado en cuarenta competencias con cinco niveles de capacidad y con un total de doscientas nueve habilidades y conocimientos asociados.

El modelo ya está siendo la referencia para los grandes actores del mundo de las certificaciones como demuestran los mapas competenciales de varias decenas de sus certificaciones[98]. La previsión es que los proveedores de formación y los entes de cualificación y certificación acaben mapeando sus productos hacia *eCF* para permitir un lenguaje común y homogéneo que conecte a formadores, empleadores y candidatos a un empleo.

Actualmente en cuanto al ámbito de la ciberseguridad se han modelado dos perfiles en *eCF* (disponibles junto a otras veintiuna ocupaciones en el documento CWA 16458-2012[99] CWA, *European ICT Professional Profiles*):

- Gerente de seguridad TIC (*ICT Security Manager*), que gestiona la política de seguridad de los sistemas de información.
- Especialista en seguridad de los sistemas de información, que asegura la implementación de dicha política de seguridad en sus distintos aspectos.

Además, la seguridad digital es un elemento competencial transversal presente en hasta otros siete perfiles como *CIO* (*Chief Information Officer*), gerente de operaciones TIC, etcétera.

---

[97] European Committee for Standardization (CEN), «e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework - EN 16234-1:2016», 6 de abril de 2016, https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT,FSP_ORG_ID:41798,1218399&cs=17B0E0F8CABCDBDDB8066A46FA937510B

[98] e-Competence Quality Label, «e-Competence Certificates», accedido 2 de noviembre de 2016, http://www.e-competence-quality.com/certification-profiles/

[99] European Committee for Standardization (CEN), «CWA 16458 - European ICT Professional Profiles», mayo de 2012, http://www.kutsekoda.ee/fwk/fb/10456179/CEN-WSICT_N0393_Final_Draft_CWA_for_formal_approval_EU_ICT_P.pdf

La otra iniciativa europea que va a requerir la alineación de todos los esquemas de cualificaciones nacionales y locales es la nueva clasificación oficial laboral europea para todos los sectores, *ESCO* (*European Skills, Competences, Qualifications and Occupations*)[100], aún pendiente de publicarse en 2017.

Esta nueva clasificación laboral va a ser de uso obligatorio para todos los servicios públicos de empleo y para los recursos europeos como el portal EURES, además de promoverse como estándar para los portales privados, y estará traducida a todos los idiomas oficiales de la Unión Europea.

En el ámbito sectorial de las TIC se ha generado un nuevo catálogo de ocupaciones con ciento diez puestos y su correspondiente descripción y lista de habilidades y conocimientos, tanto esenciales como opcionales. En el ámbito de la seguridad se distinguen los puestos de *CISO* (*Chief Information Security Officer*), administrador de seguridad TIC, consultor de seguridad TIC, gerente (*manager*) de seguridad TIC, técnico de seguridad TIC y *hacker* ético. Al igual que en *eCF*, existe una buena cantidad de otras ocupaciones con habilidades y conocimientos relacionados con la seguridad.

Actualmente estos modelos están generando importantes expectativas, pero también la necesidad de buscar su consistencia para permitir que los servicios para candidatos a empleos, reclutadores y formadores sean completos y sólidos. En ese sentido, los resultados de proyectos europeos como *eSkills Match*[101], con un sistema de ayuda en el manejo de los modelos, y *eCF Council*[102] permitirán mejorar este aspecto de forma práctica, incluyendo la conexión con el cuerpo europeo de conocimientos en TIC[103].

En todo caso, parece existir un consenso a nivel mundial de que dicha escasez de profesionales de las TIC y, en particular, de la ciberseguridad tendrá implicaciones negativas en la seguridad nacional, impactando gravemente tanto en entidades del sector público como del privado.

En este sentido, y en un ámbito nacional, es pertinente resaltar el documento y proyecto del Instituto Nacional de Ciberseguridad (INCIBE) de 2016 denominado «Punto de partida al modelo de gestión y seguimiento del talento

[100] Comisión Europea, «ESCO (European Skills, Competences, Qualifications and Occupations)», accedido 2 de noviembre de 2016, https://ec.europa.eu/esco/portal/home

[101] European Commission Directorate General for Communications Networks, Content & Technology (DG CONNECT), «Proyecto e-Skills Match», accedido 2 de noviembre de 2016, http://www.eskillsmatch.eu/

[102] eCF Council, «eCF ALLIANCE , qualifications and skills for the ICT industry», accedido 2 de noviembre de 2016, http://media.wix.com/ugd/71d4ca_273ca002273242c28d1557836c68cbcc.pdf

[103] European Commission - DG Internal Market, Industry, Entrepreneurship and SMEs, Capgemini Consulting, y Ernst & Young, «The European Foundational ICT Body of Knowledge - Version 1.0», 22 de febrero de 2015, http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=925&PortalId=0&TabId=353

en ciberseguridad en España»[104] en el que, en el apartado de «Diagnóstico inicial», se realiza una muy buena valoración de la situación en nuestro país sobre los puestos de ciberseguridad sin cubrir y la falta de competencias del profesional en este ámbito.

En dicho documento, desde su mismo subtítulo: «Visión conjunta de la industria, sector académico e investigador y profesionales del sector», se puede ver claramente otro punto de concordancia con todos los informes analizados: hay un acuerdo, tanto implícito como explícito, de la importancia de la colaboración público-privada en materia de ciberseguridad y ciberdefensa para afrontar este problema.

En cuanto a las iniciativas de organismos públicos para la formación y certificación profesional en ciberseguridad, nos hemos centrado primera y principalmente en iniciativas del mundo anglosajón (Estados Unidos y Reino Unido), por ser las más prontamente iniciadas y más completamente desarrolladas, sin olvidarnos de las últimas iniciativas europeas y españolas.

Parece claro y hay conformidad en todos los ámbitos analizados sobre los beneficios de las certificaciones y acreditaciones, tanto para los profesionales de ciberseguridad como para los empleadores de los mismos. Dichas certificaciones y acreditaciones tienen necesariamente que coincidir todo lo más posible con las necesidades y los perfiles competenciales evidenciados en los diferentes estudios existentes.

En este aspecto, y en un ámbito estrictamente nacional, es importante señalar el inicio de trabajos emanados de los Planes Derivados del Plan Nacional de Ciberseguridad de 2014, que en algunas de sus diferentes vertientes: «Plan de seguridad de los sistemas de información y telecomunicaciones que soportan las administraciones públicas», «Seguridad de los sistemas de información y telecomunicaciones que soportan las infraestructuras», «Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia», «Ciberseguridad del sector privado y la industria» o «Cultura de ciberseguridad», acometen aspectos como la «Definición, aprobación e implantación de acciones para la evaluación, homologación y certificación de profesionales de ciberseguridad, dentro del marco de las AAPP» o el «Desarrollo de un marco de conocimientos de ciberseguridad en los ámbitos técnico, operativo y jurídico» mediante la elaboración del mapa de competencias en los distintos ámbitos (técnico, operativo y jurídico) y la definición de un marco de referencia de profesionales y competencias en materia de ciberseguridad.

Queda, por tanto, evidenciado que parece conveniente la creación y lanzamiento de un Esquema Nacional de Certificación de Profesionales en Ciberseguridad, contando para su desarrollo con la mayor parte posible de los

[104] INCIBE, «Punto de partida al Modelo de gestión y seguimiento del TALENTO en ciberseguridad en España», 18 de agosto de 2016, https://www.incibe.es/sites/default/files/contenidos/notasprensa/doc/modelo_gestion_talento_incibe.pdf

actores implicados, tanto en ámbito público como privado. Todo ello con la debida seriedad y profesionalidad pero con carácter de inmediatez.

En la esfera privada, tal y como sostiene el anteriormente citado informe de INCIBE, «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. Este 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».

Por otra parte, se percibe una clara evolución en los diferentes modelos de acreditaciones y certificaciones hacia propuestas que incluyen aspectos de concienciación y formación más allá de la mera evaluación de conocimientos y experiencia en materia de ciberseguridad.

Tanto su realización como su evaluación se suelen ejecutar de manera práctica. Por un lado, la formación se realiza mediante talleres en los que se prueban los conceptos que son necesarios conocer y, por otro, los exámenes consisten en la contrastación práctica de unas habilidades y unos conocimientos sobre un caso simulado.

Bibliografía

Adriana Pauna. Certification of Cyber Security Skills of ICS - Good Practices and Recommendations for Developing Harmonised Certification Schemes. Heraklion: ENISA, 2014. http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714040:EN:HTML

Andrew McGettrick y Association for Computing Machinery (ACM). «Towards Curricular Guidelines for Cybersecurity - Report of a Workshop on Cybersecurity Education and Training», 30 de agosto de 2013. https://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf

Ariha Setalvad. «Demand to fill cybersecurity jobs booming». Peninsula Press, 31 de marzo de 2015. http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/

BOE. Anexo III al Real Decreto 686/2011, Certificado de Profesionalidad en Seguridad Informática, 2011. https://sede.sepe.gob.es/es/portaltrabaja/resources/pdf/especialidades/IFCT0109.pdf.

———. Real Decreto 686/2011, de 13 de mayo, por el que se establecen seis certificados de profesionalidad de la familia profesional informática y comunicaciones que se incluyen en el repertorio nacional de certificados de profesionalidad, 2011. https://sede.sepe.gob.es/es/portaltrabaja/resources/pdf/normativaCertificados/RD686_2011.pdf

CCN (Centro Criptológico Nacional). «El CCN y el INAP apuestan por un Esquema Nacional de Certificación de Profesionales en Ciberseguridad».

Comunicados CCN-CERT, 31 de enero de 2014. https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/1846-el-ccn-y-el-inap-apuestan-por-un-esquema-nacional-de-certificacion-de-profesionales-en-ciberseguridad.html

CESG. «CESG Certification for IA Professionals 5.2». GCHQ, octubre de 2015. https://www.cesg.gov.uk/file/520/download?token=j8vebyeM

———. «CESG Certified Professional Scheme», 19 de mayo de 2016. https://www.cesg.gov.uk/articles/cesg-certified-professional-scheme

———. «Guidance to CESG Certification for IA Professionals v2-1». GCHQ, enero de 2015. https://www.cesg.gov.uk/file/701/download?token=QM1gwRoi

Chris Peake. «Red Teaming: The Art of Ethical Hacking». SANS Institute - InfoSec Reading Room, 16 de julio de 2003. https://www.sans.org/reading-room/whitepapers/auditing/red-teaming-art-ethical-hacking-1272

CISCO. «CCNA (Cisco Certified Network Associate) Security». Cisco. Accedido 1 de septiembre de 2016. http://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-security.html

———. «Cybersecurity Specialist». Cisco. Accedido 1 de septiembre de 2016. http://www.cisco.com/c/en/us/training-events/training-certifications/certifications/specialist/security/cybersecurity.html

Cisco Security Advisory Services. «Mitigating the Cybersecurity Skills Shortage». Cisco Systems, Inc, julio de 2015. http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf

Comisión de las Comunidades Europeas. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones: Cibercapacidades para el siglo XXI: fomento de la competitividad, el crecimiento y el empleo. COM(2007) 496 final, 2007. http://www.cdiex.org/documentos/documento_121.pdf

Comisión Europea. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones: una Estrategia para el Mercado Único Digital de Europa. COM(2015) 192 final, 2015. http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015DC0192&rid=1

———. «ESCO (European Skills, Competences, Qualifications and Occupations)». Accedido 2 de noviembre de 2016. https://ec.europa.eu/esco/portal/home.

CompTIA. «A+ (Plus) Certification». Accedido 1 de septiembre de 2016. https://certification.comptia.org/certifications/a

———. «CASP - CompTIA Advanced Security Practitioner Certification». Accedido 1 de septiembre de 2016. https://certification.comptia.org/certifications/comptia-advanced-security-practitioner

———. «Network+ Certification». Accedido 1 de septiembre de 2016. https://certification.comptia.org/certifications/network

———. «Security+ Certification». Accedido 1 de septiembre de 2016. https://certification.comptia.org/certifications/security

Comptroller and Auditor General. «The UK Cyber Security Strategy: Landscape Review». London: National Audit Office, 5 de febrero de 2013. http://www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/

Department of Defense. DoD Directive 8140.01, Cyberspace Workforce Management. DoD. Vol. 8140.01, 2015. https://www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf

———. DoD Directive 8570.01. Information Assurance Training, Certification, and Workforce Management. 8570.01, 2007. http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf

DHS y NICCS. «National Cybersecurity Workforce Framework Slick Sheet». National Initiative for Cybersecurity Careers and Studies (NICCS), noviembre de 2011. https://niccs.us-cert.gov/sites/default/files/documents/files/Workforce%20Framework%20Slick%20Sheet_1.pdf?trackDocs=Workforce%20Framework %20Slick%20Sheet.pdf

DoD. «DoD 8570.01-M - Information Assurance Workforce Improvement Program - Incorporating Change 4, November 10, 2015», 19 de diciembre de 2005. https://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

EC-Council. «About - International Council of E-Commerce Consultants», 25 de febrero de 2016. https://www.eccouncil.org/about/

———. «CEH - Certified Ethical Hacker». EC-Council, 25 de febrero de 2016. https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

———. «CEH Handbook v2.0», enero de 2015. https://www.eccouncil.org/wp-content/uploads/2016/06/CEH-Handbook-v2.0.pdf

eCF Council. «eCF ALLIANCE , qualifications and skills for the ICT industry». Accedido 2 de noviembre de 2016. http://media.wix.com/ugd/71d4ca_273ca002273242c28d1557836c68cbcc.pdf

e-Competence Quality Label. «e-Competence Certificates». Accedido 2 de noviembre de 2016. http://www.e-competence-quality.com/certification-profiles/

European Commission - DG Internal Market, Industry, Entrepreneurship and SMEs, Capgemini Consulting, y Ernst & Young. «The European Foundational ICT Body of Knowledge - Version 1.0», 22 de febrero de 2015. http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=925&PortalId=0&TabId=353

European Commission Directorate General for Communications Networks, Content & Technology (DG CONNECT). «Proyecto e-Skills Match». Accedido 2 de noviembre de 2016. http://www.eskillsmatch.eu/

European Committee for Standardization (CEN). «CWA 16458 - European ICT Professional Profiles», mayo de 2012. http://www.kutsekoda.ee/fwk/fb/10456179/CEN-WSICT_N0393_Final_Draft_CWA_for_formal_approval_EU_ICT_P.pdf

———. «e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework - EN 16234-1:2016», 6 de abril de 2016. https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT,FSP_ORG_ID:41798,1218399&cs=17B0E0F8CABCDBDDB8066A46FA937510B

European Cybersecurity Industrial Leaders (ECIL). «Recommendations on Cybersecurity for Europe», 25 de enero de 2016. http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=13326

GAO. «GAO-13-742 - DHS Recruiting and Hiring: DHS Is Generally Filling Mission-Critical Positions, but Could Better Track Costs of Coordinated Recruiting Efforts». Report to Congressional Requesters. United States Government Accountability Office, septiembre de 2013. http://www.gao.gov/products/GAO-13-742

———. «GAO-15-223, Federal Workforce: OPM and Agencies Need to Strengthen Efforts to Identify and Close Mission-Critical Skills Gaps». Report to Congressional Requesters. United States Government Accountability Office, enero de 2015. http://www.gao.gov/assets/670/668202.pdf

GIAC. «About GIAC». Accedido 6 de septiembre de 2016. http://www.giac.org/about

———. «GCED - GIAC Certified Enterprise Defender». Accedido 1 de septiembre de 2016. http://www.giac.org/certification/certified-enterprise-defender-gced

———. «GCFA - GIAC Certified Forensic Analyst». Accedido 1 de septiembre de 2016. http://www.giac.org/certification/certified-forensic-analyst-gcfa

———. «GCIA - GIAC Certified Intrusion Analyst». Accedido 1 de septiembre de 2016. http://www.giac.org/certification/certified-intrusion-analyst-gcia

———. «GCIH - GIAC Certified Incident Handler». Accedido 1 de septiembre de 2016. http://www.giac.org/certification/certified-incident-handler-gcih

———. «GIAC Certification Program Candidate's Handbook». Global Information Assurance Certification, 2012. http://www.giac.org/pdfs/certification-candidate-handbook.pdf

———. «GSEC - GIAC Security Essentials Certification». Accedido 1 de septiembre de 2016. http://www.giac.org/certification/security-essentials-gsec

———. «GSLC - GIAC Cyber Security Leadership Certification». Accedido 1 de septiembre de 2016. http://www.giac.org/certification/security-leadership-gslc

———. «GSNA - GIAC Systems and Network Auditor». Accedido 1 de septiembre de 2016. http://www.giac.org/certification/systems-network-auditor-gsna

Gobierno de España. Estrategia de Ciberseguridad Nacional, 2013. http://www.lamoncloa.gob.es/NR/rdonlyres/680D00B8-45FA-4264-9779-1E69D-4FEF99D/256935/20131332EstrategiadeCiberseguridadx.pdf

Homeland Security Advisory Council. «CyberSkills Task Force Report». US Department of Homeland Security, Otoño de 2012. https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf

INAP, CCN y Óscar Pastor. «Esquema de Certificación de Personas». En VII Jornadas STIC CCN - CERT. Madrid, 2013. https://www.ccn-cert.cni.es/privatedocs/viijornadas/742-12-opastor-ccn-isdefe-esquemadecertificaciondepersonas/file.html

INCIBE. «Punto de partida al Modelo de gestión y seguimiento del TALENTO en ciberseguridad en España», 18 de agosto de 2016. https://www.incibe.es/sites/default/files/contenidos/notasprensa/doc/modelo_gestion_talento_incibe.pdf

Information Systems Audit and Control Association. Cobit 5: A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows. IL: ISACA, 2012.

Institute of Information Security Professional. «IISP Skills Framework - Version 2.0». Accedido 31 de agosto de 2016. https://www.iisp.org/imis15/iisp/About_Us/Our_Skills_Framework/iispv2/Accreditation/Our_Skills_Framework.aspx?hkey=e77a6f03-9498-423e-aa7b-585381290ec4

International Organization for Standardization. «ISO/IEC 17024:2012 - Evaluación de la conformidad. Requisitos generales para los organismos que realizan certificación de personas». ISO/IEC, 2012. http://www.iso.org/iso/catalogue_detail?csnumber=52993

ISACA. «Certified in Risk and Information Systems Control (CRISC)». Accedido 29 de agosto de 2016. http://www.isaca.org/About-ISACA/Pressroom/Documents/2015-CRISC-Fact-Sheet_pre_eng_1015.pdf

———. «Certified in the Governance of Enterprise IT (CGEIT) Fact Sheet». Accedido 29 de agosto de 2016. http://www.isaca.org/About-ISACA/Pressroom/Documents/2015-CGEIT-Fact-Sheet_pre_eng_1015.pdf

———. «Certified Information Security Manager® (CISM®) Fact Sheet». Accedido 29 de agosto de 2016. http://www.isaca.org/About-ISACA/Pressroom/Documents/2015-CISM-Fact-Sheet_pre_eng_1015.pdf

———. «Certified Information Systems Auditor™ (CISA®) Fact Sheet». Accedido 29 de agosto de 2016. http://www.isaca.org/About-ISACA/Pressroom/Documents/2015-CISA-Fact-Sheet_pre_eng_1015.pdf

———. «CISA - Certified Information Systems Auditor». Accedido 1 de septiembre de 2016. http://www.isaca.org/certification/cisa-certified-information-systems-auditor/pages/default.aspx

———. «CISM - Certified Information Security Manager». Accedido 1 de septiembre de 2016. http://www.isaca.org/certification/cism-certified-information-security-manager/pages/default.aspx

———. «Cybersecurity Nexus (CSX) Fact Sheet». Accedido 29 de agosto de 2016. http://www.isaca.org/cyber/Documents/Cybersecurity-Nexus-Fact-Sheet_pre_Eng_0115.pdf

———. «Cybersecurity Nexus™ (CSX) General Awareness Brochure», 2016. http://www.isaca.org/cyber/Documents/CSX-General-Awareness-Brochure_Bro_Eng_0816.pdf

———. «ISACA Fact Sheet». Accedido 29 de agosto de 2016. http://www.isaca.org/About-ISACA/Press-room/Documents/2016-ISACA-Fact-Sheet_pre_eng_0716.pdf

ISACA, y RSA Conference. «State of Cybersecurity: Implications for 2015». ISACA, 11 de abril de 2015. http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf

(ISC)². «Become an Associate of (ISC)² Prior to Obtaining Certification». Accedido 1 de septiembre de 2016. https://www.isc2.org/associate/default.aspx

———. «CAP - Certified Authorization Professional». Accedido 1 de septiembre de 2016. https://www.isc2.org/cap/default.aspx

———. «CISSP - Certified Information Systems Security Professional». Accedido 1 de septiembre de 2016. https://www.isc2.org/cissp/default.aspx

———. «CISSP (Certified Information Systems Security Professional) Brochure», 16 de diciembre de 2015. https://www.isc2.org/uploadedfiles/credentials_and_certifcation/cissp/cissp-information.pdf

———. «CISSP Concentrations». Accedido 5 de septiembre de 2016. https://www.isc2.org/uploadedfiles/(isc)2_public_content/certification_programs/cissp_concentrations/concentrations-web.pdf

———. «CISSP-ISSAP - Information Systems Security Architecture Professional». Accedido 1 de septiembre de 2016. https://www.isc2.org/issap.aspx

———. «CISSP-ISSEP - Information Systems Security Engineering Professional». Accedido 1 de septiembre de 2016. https://www.isc2.org/issep.aspx

———. «CISSP-ISSMP - Information Systems Security Management Professional». Accedido 1 de septiembre de 2016. https://www.isc2.org/issmp/default.aspx

———. «CSSLP - Certified Secure Software Lifecycle Professional». Accedido 1 de septiembre de 2016. https://www.isc2.org/csslp/default.aspx

———. «(ISC)² Overview». Accedido 5 de septiembre de 2016. https://www.isc2.org/uploadedfiles/(isc)2_public_content/(isc)2-company-overview.pdf

———. «SSCP - Systems Security Certified Practitioner». Accedido 1 de septiembre de 2016. https://www.isc2.org/sscp/default.aspx

Jim Gosler. Cyberwarrior Shortage Threatens U.S. Security. NPR Morning Edition, 29 de julio de 2010. http://www.npr.org/templates/story/story.php?storyId=128574055.

Karen Evans y Franklin Reeder. «A Human Capital Crisis in Cybersecurity». Technical Proficiency Matters. 1800 K Street, NW, Washington, DC 20006: CSIS Center for Strategic and International Studies - Commission on Cybersecurity for the 44th Presidency, noviembre de 2010. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/101111_Evans_HumanCapital_Web.pdf

Kathryn A. Francis y Wendy Ginsber. «The Federal Cybersecurity Workforce: Background and Congressional Oversight Issues for the Departments of Defense and Homeland Security». CRS Report. Congressional Research Service, 8 de enero de 2016. https://www.fas.org/sgp/crs/natsec/R44338.pdf

Lewis Morgan. «Global Shortage of Two Million Cyber Security Professionals by 2017». IT Governance Blog, 30 de octubre de 2014. http://www.itgovernance.co.uk/blog/global-shortage-of-two-million-cyber-security-professionals-by-2017/

Michael Suby. «The 2013 (ISC)^2 Global Information Security Workforce Study». Frost & Sullivan Market Study. (ISC)^2, 2013. https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf

Michael Suby y Frank Dickson. «The 2015 (ISC)^2 Global Information Security Workforce Study». A Frost & Sullivan White Paper. (ISC)^2, 16 de abril de 2015. https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

Ministerio de Defensa. Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional. BOE. Accedido 27 de mayo de 2013. https://www.boe.es/boe/dias/2004/03/19/pdfs/A12203-12204.pdf

Ministerio de Empleo y Seguridad Social. «Servicio Público de Empleo Estatal». Accedido 2 de septiembre de 2016. http://www.empleo.gob.es/es/organizacion/empleo/contenido/OM29.htm

Ministerio de la Presidencia. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, 2010. http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf

Ministerio de Política Territorial y Administración Pública. Real Decreto 464/2011, de 1 de abril, por el que se aprueba el Estatuto del Instituto Nacional de Administración Pública. Vol. BOE-A-2011-6872, 2011. http://www.boe.es/buscar/pdf/2011/BOE-A-2011-6872-consolidado.pdf

NICCS. «National Initiative for Cybersecurity Careers and Studies». Accedido 29 de agosto de 2016. https://niccs.us-cert.gov/home/about-niccs

———. «Training Catalog | National Initiative for Cybersecurity Careers and Studies». Accedido 30 de agosto de 2016. https://niccs.us-cert.gov/training/tc/search

NICE. «The National Cybersecurity Workforce Framework». National Initiative for Cybersecurity Careers and Studies (NICCS), 15 de mayo de 2014. https://niccs.us-cert.gov/sites/default/files/documents/files/National%20Cybersecurity%20Workforce%20Framework%20Version%201.0.pdf?trackDocs=National%20Cybersecurity%20Workforce%20Framework%20Version%201.0.pdf

NIST. «Framework for Improving Critical Infrastructure Cybersecurity». Cybersecurity Framework. National Institute of Standards and Technology, 12 de febrero de 2014. http://www.cslawreport.com/files/2015/04/07/nist-combined-file.pdf

———. «NICE Issues Cybersecurity Workforce Framework for Public Comment». Accedido 29 de agosto de 2016. http://www.nist.gov/itl/cyberwork-110811.cfm

———. «NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security». National Institute of Standards and Technology, junio de 2011

———. «The National Initiative for Cybersecurity Education (NICE)». Accedido 29 de agosto de 2016. http://csrc.nist.gov/nice/about/index.html

NSA. «Mission & Strategy». Accedido 5 de septiembre de 2016. https://www.nsa.gov/about/mission-strategy/

OMB (Office of Management and Budget). Federal Cybersecurity Workforce Strategy. M-16- 15, 2016. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf

Óscar Pastor y Javier Candau. «Propuesta para un Esquema Nacional de Certificación de Profesionales en Ciberseguridad para España». *Revista SIC*, febrero de 2014

PCI Security Standards Council. «PCI (industria de tarjetas de pago) - Normas de seguridad de datos - Requisitos y procedimientos de evaluación de seguridad», noviembre de 2013. https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

Raytheon y NCSA. «Preparing Millennials to Lead in Cyberspace». National Cyber Security Alliance, octubre de 2014. http://www.raytheoncyber.com/news/feature/blog-cyber60-helpwanted.html

Rebecca Vogel. «Closing The Cybersecurity Skills Gap». Salus Journal 4, n.º 2 (2016): 32.

Robert Ayoub. «The 2011 (ISC)² Global Information Security Workforce Study». Frost & Sullivan Market Survey. (ISC)², 2011. https://www.isc2.org/uploadedFiles/Industry_Resources/FS_WP_ISC%20Study_020811_MLW_Web.pdf

SANS. «SANS Institute: About». Accedido 6 de septiembre de 2016. https://www.sans.org/about/

SEI (Software Engineering Institute). «CERT-Certified Computer Security Incident Handler». Accedido 1 de septiembre de 2016. https://www.sei.cmu.edu/certification/opportunities/csih/

SFIA Foundation. «Responsabilidades y habilidades - Español». Página. Accedido 31 de agosto de 2016. https://www.sfia-online.org/es/how-sfia-works/responsibilities-and-skills

———. «Versión 6 del Marco de Competencias para la Era de la Información - Español». Accedido 29 de agosto de 2016. https://www.sfia-online.org/es/reference-guide

Steve Morgan. «One Million Cybersecurity Job Openings In 2016». Forbes, 2 de enero de 2016. http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/print/