EDITORES:

Manuel A. Serrano - Eduardo Fernández-Medina

Cristina Alcaraz - Noemí de Castro - Guillermo Calvo

Actas de las VI Jornadas Nacionales
(JNIC2021 LIVE)

INVESTIGACIÓN EN ciber segu ridad

Ediciones de la Universidad
de Castilla-La Mancha

Investigación en Ciberseguridad

Actas de las VI Jornadas Nacionales (JNIC2021 LIVE)

Online 9-10 de junio de 2021
Universidad de Castilla-La Mancha

Investigación en Ciberseguridad

Actas de las VI Jornadas Nacionales (JNIC2021 LIVE)

Online 9-10 de junio de 2021
Universidad de Castilla-La Mancha

Editores:
Manuel A. Serrano,
Eduardo Fernández-Medina,
Cristina Alcaraz
Noemí de Castro
Guillermo Calvo

Ediciones de la Universidad
de Castilla-La Mancha

Cuenca, 2021




Edita: Ediciones de la Universidad de Castilla-La Mancha

Colección JORNADAS Y CONGRESOS n.º 34

Esta editorial es miembro de la UNE, lo que garantiza la difusión y comercialización de sus publicaciones a nivel nacional e internacional.

I.S.B.N.: 978-84-9044-463-4
D.O.I.: http://doi.org/10.18239/jornadas_2021.34.00

Hecho en España (U.E.) – *Made in Spain (E.U.)*

Bienvenida del Comité Organizador

Tras la parada provocada por la pandemia en 2020, las VI Jornadas Nacionales de Investigación en Ciberseguridad (JNIC) vuelven el 9 y 10 de Junio del 2021 con energías renovadas, y por primera vez en su historia, en un formato 100% online. Esta edición de las JNIC es organizada por los grupos GSyA y Alarcos de la Universidad de Castilla-La Mancha en Ciudad Real, y con la activa colaboración del comité ejecutivo, de los presidentes de los distintos comités de programa y del Instituto Nacional de Ciberseguridad (INCIBE). Continúa de este modo la senda de consolidación de unas jornadas que se celebraron por primera vez en León en 2015 y le siguieron Granada, Madrid, San Sebastián y Cáceres, consecutivamente hasta 2019, y que, en condiciones normales se habrían celebrado en Ciudad Real en 2020.

Estas jornadas se han convertido en un foro de encuentro de los actores más relevantes en el ámbito de la ciberseguridad en España. En ellas, no sólo se presentan algunos de los trabajos científicos punteros en las diversas áreas de ciberseguridad, sino que se presta especial atención a la formación e innovación educativa en materia de ciberseguridad, y también a la conexión con la industria, a través de propuestas de transferencia de tecnología. Tanto es así que, este año se presentan en el Programa de Transferencia algunas modificaciones sobre su funcionamiento y desarrollo que han sido diseñadas con la intención de mejorarlo y hacerlo más valioso para toda la comunidad investigadora en ciberseguridad.

Además de lo anterior, en las JNIC estarán presentes excepcionales ponentes (Soledad Antelada, del Lawrence Berkeley National Laboratory, Ramsés Gallego, de Micro Focus y Mónica Mateos, del Mando Conjunto de Ciberdefensa) mediante tres charlas invitadas y se desarrollarán dos mesas redondas. Éstas contarán con la participación de las organizaciones más relevantes en el panorama industrial, social y de emprendimiento en relación con la ciberseguridad, analizando y debatiendo el papel que está tomando la ciberseguridad en distintos ámbitos relevantes.

En esta edición de JNIC se han establecido tres modalidades de contribuciones de investigación, los clásicos artículos largos de investigación original, los artículos cortos con investigación en un estado más preliminar, y resúmenes extendidos de publicaciones muy relevantes y de alto impacto en materia de ciberseguridad publicados entre los años 2019 y 2021. En el caso de contribuciones de formación e innovación educativa, y también de transferencias se han considerado solamente artículos largos. Se han recibido para su valoración un total de 86

contribuciones organizadas en 26, 27 y 33 artículos largos, cortos y resúmenes ya publicados, de los que los respectivos comités de programa han aceptado 21, 19 y 27, respectivamente. En total se ha contado con una ratio de aceptación del 77%. Estas cifras indican una participación en las jornadas que continúa creciendo, y una madurez del sector español de la ciberseguridad que ya cuenta con un volumen importante de publicaciones de alto impacto.

El formato online de esta edición de las jornadas nos ha motivado a organizar las jornadas de modo más compacto, distinguiendo por primera vez entre actividades plenarias (charlas invitadas, mesas redondas, sesión de formación e innovación educativa, sesión de transferencia de tecnología, junto a inauguración y clausura) y sesiones paralelas de presentación de artículos científicos. En concreto, se han organizado 10 sesiones de presentación de artículos científicos en dos líneas paralelas, sobre las siguientes temáticas: detección de intrusos y gestión de anomalías (I y II), ciberataques e inteligencia de amenazas, análisis forense y cibercrimen, ciberseguridad industrial, inteligencia artificial y ciberseguridad, gobierno y riesgo, tecnologías emergentes y entrenamiento, criptografía, y finalmente privacidad.

En esta edición de las jornadas se han organizado dos números especiales de revistas con elevado factor de impacto para que los artículos científicos mejor valorados por el comité de programa científico puedan enviar versiones extendidas de dichos artículos. Adicionalmente, se han otorgado premios al mejor artículo en cada una de las categorías. En el marco de las JNIC también hemos contado con la participación de la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC), impulsando la ciberseguridad a través de la entrega de los premios al *Mejor Trabajo Fin de Máster en Ciberseguridad* y a la *Mejor Tesis Doctoral en Ciberseguridad*. También se ha querido acercar a los jóvenes talentos en ciberseguridad a las JNIC, a través de un CTF (Capture The Flag) organizado por la Universidad de Extremadura y patrocinado por Viewnext.

Desde el equipo que hemos organizado las JNIC2021 queremos agradecer a todas aquellas personas y entidades que han hecho posible su celebración, comenzando por los autores de los distintos trabajos enviados y los asistentes a las jornadas, los tres ponentes invitados, las personas y organizaciones que han participado en las dos mesas redondas, los integrantes de los distintos comités de programa por sus interesantes comentarios en los procesos de revisión y por su colaboración durante las fases de discusión y debate interno, los presidentes de las sesiones, la Universidad de Extremadura por organizar el CTF y la empresa Viewnext por patrocinarlo, los técnicos del área TIC de la UCLM por el apoyo con la plataforma de comunicación, los voluntarios de la UCLM y al resto de organizaciones y entidades patrocinadoras, entre las que se encuentra la Escuela Superior de Informática, el Departamento de Tecnologías y Sistemas de Información y el Instituto de Tecnologías y Sistemas de Información, todos ellos de la Universidad de Castilla-La Mancha, la red RENIC, las cátedras (Telefónica e Indra) y aulas (Avanttic y Alpinia) de la Escuela Superior de Informática, la empresa Cojali, y muy especialmente por su apoyo y contribución al propio INCIBE.

Manuel A. Serrano, Eduardo Fernández-Medina
Presidentes del Comité Organizador
Cristina Alcaraz
Presidenta del Comité de Programa Científico
Noemí de Castro
Presidenta del Comité de Programa de Formación e Innovación Educativa
Guillermo Calvo Flores
Presidente del Comité de Transferencia Tecnológica

Índice General

Comité Ejecutivo

Juan Díez González	INCIBE
Luis Javier García Villalba	Universidad de Complutense de Madrid
Eduardo Fernández-Medina Patón	Universidad de Castilla-La Mancha
Guillermo Suárez-Tangil	IMDEA Networks Institute
Andrés Caro Lindo	Universidad de Extremadura
Pedro García Teodoro	Universidad de Granada. Representante de red RENIC
Noemí de Castro García	Universidad de León
Rafael María Estepa Alonso	Universidad de Sevilla
Pedro Peris López	Universidad Carlos III de Madrid

Comité Organizador

Presidentes del Comité Organizador

Eduardo Fernández-Medina Patón	Universidad de Castilla-la Mancha
Manuel Ángel Serrano Martín	Universidad de Castilla-la Mancha

Finanzas

David García Rosado	Universidad de Castilla-la Mancha
Luis Enrique Sánchez Crespo	Universidad de Castilla-la Mancha

Actas

Antonio Santos-Olmo Parra	Universidad de Castilla-la Mancha

Difusión

Julio Moreno García-Nieto	Universidad de Castilla-la Mancha
José Antonio Cruz Lemus	Universidad de Castilla-la Mancha
María A Moraga de la Rubia	Universidad de Castilla-la Mancha

Webmaster

Aurelio José Horneros Cano	Universidad de Castilla-la Mancha

Logística y Organización

Ignacio García-Rodriguez de Guzmán	Universidad de Castilla-la Mancha
Ismael Caballero Muñoz-Reja	Universidad de Castilla-la Mancha
Gregoria Romero Grande	Universidad de Castilla-la Mancha
Natalia Sanchez Pinilla	Universidad de Castilla-la Mancha

Comité de Programa Científico

Presidenta

Cristina Alcaraz Tello	Universidad de Málaga

Miembros

Aitana Alonso Nogueira	INCIBE
Marcos Arjona Fernández	ElevenPaths
Ana Ayerbe Fernández-Cuesta	Tecnalia
Marta Beltrán Pardo	Universidad Rey Juan Carlos
Carlos Blanco Bueno	Universidad de Cantabria
Jorge Blasco Alís	Royal Holloway, University of London
Pino Caballero-Gil	Universidad de La Laguna
Andrés Caro Lindo	Universidad de Extremadura
Jordi Castellà Roca	Universitat Rovira i Virgili
José M. de Fuentes García-Romero de Tejada	Universidad Carlos III de Madrid
Jesús Esteban Díaz Verdejo	Universidad de Granada
Josep Lluis Ferrer Gomila	Universitat de les Illes Balears
Dario Fiore	IMDEA Software Institute
David García Rosado	Universidad de Castilla-La Mancha
Pedro García Teodoro	Universidad de Granada
Luis Javier García Villalba	Universidad Complutense de Madrid
Iñaki Garitano Garitano	Mondragon Unibertsitatea
Félix Gómez Mármol	Universidad de Murcia
Lorena González Manzano	Universidad Carlos III de Madrid
María Isabel González Vasco	Universidad Rey Juan Carlos I
Julio César Hernández Castro	University of Kent
Luis Hernández Encinas	CSIC
Jorge López Hernández-Ardieta	Banco Santander
Javier López Muñoz	Universidad de Málaga
Rafael Martínez Gasca	Universidad de Sevilla
Gregorio Martínez Pérez	Universidad de Murcia

David Megías Jiménez	Universitat Oberta de Cataluña
Luis Panizo Alonso	Universidad de León
Fernando Pérez González	Universidad de Vigo
Aljosa Pasic	ATOS
Ricardo J. Rodríguez	Universidad de Zaragoza
Fernando Román Muñoz	Universidad Complutense de Madrid
Luis Enrique Sánchez Crespo	Universidad de Castilla-La Mancha
José Soler	Technical University of Denmark-DTU
Miguel Soriano Ibáñez	Universidad Politécnica de Cataluña
Victor A. Villagrá González	Universidad Politécnica de Madrid
Urko Zurutuza Ortega	Mondragon Unibertsitatea
Lilian Adkinson Orellana	Gradiant
Juan Hernández Serrano	Universitat Politécnica de Cataluña

Comité de Programa de Formación e Innovación Educativa

Presidenta

Noemí De Castro García	Universidad de León

Miembros

Adriana Suárez Corona	Universidad de León
Raquel Poy Castro	Universidad de León
José Carlos Sancho Núñez	Universidad de Extremadura
Isaac Agudo Ruiz	Universidad de Málaga
Ana Isabel González-Tablas Ferreres	Universidad Carlos III de Madrid
Xavier Larriva	Universidad Politécnica de Madrid
Ana Lucila Sandoval Orozco	Universidad Complutense de Madrid
Lorena González Manzano	Universidad Carlos III de Madrid
María Isabel González Vasco	Universidad Rey Juan Carlos
David García Rosado	Universidad de Castilla - La Mancha
Sara García Bécares	INCIBE

Comité de Transferencia Tecnológica

Presidente

Guillermo Calvo Flores	INCIBE

Miembros

José Luis González Sánchez	COMPUTAEX
Marcos Arjona Fernández	ElevenPaths
Victor Villagrá González	Universidad Politécnica de Madrid
Luis Enrique Sánchez Crespo	Universidad de Castilla – La Mancha

http://doi.org/10.18239/jornadas_2021.34.63

Selección de competencias en ciberseguridad para la formación en la industria de defensa

Rafael Estepa
Universidad de Sevilla
ORCID: 0000-0001-8505-1920
rafaestepa@us.es

José María de Fuentes
Univ. Carlos III de Madrid
ORCID: 0000-0002-4023-3197
josemaria.defuentes@uc3m.es

Lorena González-Manzano
Univ. Carlos III de Madrid
ORCID:0000-0002-3490-621X
lorena.gonzalez@uc3m.es

Antonio Estepa
Universidad de Sevilla
ORCID: 0000-0003-1841-3973
aestepa@us.es

Jaime Domínguez
Universidad de Sevilla
ORCID: 0000-0002-0491-7911
jaime@us.es

Daniel Segovia-Vargas
Univ. Carlos III de Madrid
ORCID: 0000-0001-7811-3791
dansevar@ing.uc3m.es

Resumen- **En el contexto de la defensa escasean los profesionales capacitados en ciberseguridad, siendo aconsejable impulsar programas de formación específicos para la industria de este sector. Este es uno de los objetivos del proyecto europeo ASSETS+. En este trabajo presentamos uno de sus resultados preliminares: una lista de competencias que los profesionales de ciberseguridad deberían poseer para satisfacer las necesidades formativas de la industria de defensa europea. Para la realización de este listado, se ha seguido una metodología basada en dos fases. En primer lugar, se identifican aquellas tecnologías de ciberseguridad útiles para el sector de defensa mediante el análisis de múltiples fuentes de datos. En segundo lugar, se realiza una adaptación del listado de competencias en ciberseguridad del NIST (NICE) a aquellas aplicables a los perfiles de trabajo en la industria de la defensa, así como a las tecnologías identificadas en la fase 1. El resultado es una relación de competencias de tipo transversal, técnicas o exclusivas del sector de defensa que debería ser central en el diseño de futuros cursos de formación especializados.**

***Index Terms*- formación ciberseguridad, competencias ciberseguridad, ciberseguridad en defensa**

Tipo de contribución: *Formación innovación*

I. Introducción

Nuevos dominios tecnológicos tales como la inteligencia artificial, robótica o ciberseguridad están revolucionando el tradicional mundo de la defensa. En particular, el ciberespacio resulta de especial interés por constituir (junto a tierra, mar, aire, y espacio) un dominio de batalla donde se llevan a cabo multitud de operaciones en misiones 'no públicas'. Éstas se articulan habitualmente a través de grupos de atacantes patrocinados por Estados, como son las amenazas persistentes avanzadas, o incluso cuerpos especiales del Ejército que operan libremente en el ciberespacio mientras que intentan evitar que los adversarios lo hagan [1].

La importancia de la ciberseguridad dentro de la defensa se ve potenciada por el riesgo que supone la captura de información sensible militar (con la consiguiente pérdida de ventaja frente al adversario), ya se produzca en el ejército o en un subcontratista (denominado Defence Industrial Base - DIB-). Este riesgo se ha incrementado en los últimos años debido a la masiva incorporación de las TIC en productos y servicios militares, introduciendo nuevas vulnerabilidades que pueden ser explotadas por el adversario. No en vano, ciertas amenazas avanzadas (como las APT, por sus siglas en inglés *Advanced Persistent Threats*) ya han sido especialmente dirigidas para atacar este sector. Por todo ello, [2] es deseable que la DIB tenga, al menos, las competencias mínimas necesarias para proteger la información sensible, tal y como establece la norma NIST 800.171 para la DIB de Estados Unidos. Adicionalmente, sería muy deseable que los productos software y hardware producidos por la DIB cumplieran las buenas prácticas y los estándares de ciberseguridad descritos por los reguladores. Por lo tanto, una formación adecuada en este sentido forma parte de las necesidades esenciales de la industria.

La actual panorámica educativa actual adolece de algunos problemas. En primer lugar, el escaso número de trabajadores con las competencias y experiencia necesaria para desarrollar ciertas tareas de ciberseguridad provoca un mercado laboral desequilibrado y comporta inherentes debilidades en la seguridad de las organizaciones (en especial el sector DIB). En segundo lugar, la mayoría de los estudiantes están altamente especializados o fragmentados en 'sub-campos' (p.ej., forense, *hacking*, operaciones, auditoría). Para el acceso a cursos de especialización normalmente se exige como prerrequisito la formación en ingenierías TIC, lo que excluye a la mayoría de la fuerza del mercado laboral. Además, los programas educativos especializados en ciberseguridad orientada a defensa son escasos en la Unión Europea y, en no pocas ocasiones, utilizan tecnologías que no están completamente actualizadas. Actualmente es posible encontrar tres tipos de programas de formación en ciberseguridad: (a) programas de certificaciones internacionales en campos específicos de ciberseguridad (p.ej., ISC2, ISACA), (b) programas de postgrado de orientación más generalista (p.ej., Másteres Universitarios, normalmente como títulos de especialización de un grado en el ámbito TIC), y (c) formación en instituciones públicas de defensa (p.ej., policía, militar, …), donde se cubren algunos aspectos muy específicos de la ciberseguridad (p.ej. el ámbito forense). Animamos a los lectores interesados a profundizar en el diseño de currículos en ciberseguridad a leer el tutorial [3], que revisa las principales aproximaciones en el mundo académico y de la industria.

Por ello, uno de los retos a los que se enfrentan los países es la incorporación al sector DIB de personal técnico formado en estos dominios tecnológicos, en general, y en ciberseguridad, en particular. Esta necesidad ha sido identificada y está siendo actualmente atendida por un proyecto Erasmus+ denominado ASSETS+ [3], en el que se encuentran incursos los autores del presente trabajo.

La definición de los cursos requiere de la selección de aquellas competencias relacionadas con ciberseguridad que permitan afrontar con éxito temas y tecnologías de interés en la industria de defensa. En este artículo se presenta un primer resultado del citado proyecto: un listado de competencias que sirvan de base para la elaboración de futuros programas formativos para profesionales de la defensa.

Organización del artículo. La Sección II introduce los conceptos previos. La Sección III describe la metodología empleada. La Sección IV muestra la lista de competencias identificada. Finalmente, la Sección V describe las conclusiones y líneas de trabajo futuro.

II. Terminología y Marcos de referencia

La palabra *tecnología* se refiere a *métodos, sistemas y dispositivos, resultado de conocimiento científico, utilizados para propósitos prácticos* (diccionario Collins). Guiados por esta definición, en el proceso de diseño de cursos de formación será necesario examinar fuentes de información de distintos dominios (mercado, reguladores, academia/investigación, defensa) con la finalidad de identificar y clasificar tecnologías de ciberseguridad que puedan resultar clave en el dominio de la defensa. Sin embargo, realizar una clasificación o taxonomía en ciberseguridad es un reto debido a la falta de homogeneidad en la terminología empleada en conceptos similares a lo largo del tiempo por parte de diferentes actores. De esta forma, en ambientes académicos se emplean términos ligados a las áreas de formación. Por ejemplo, en [5] se revisan más de 100 artículos educativos en el campo de la ciberseguridad agrupados en las siguientes áreas: desarrollo seguro de software (incluyendo ingeniería inversa), monitorización y seguridad en red, ciberataques, malware, seguridad ofensiva y explotación, aspectos humanos, incluyendo privacidad, ingeniería social, legislación y ética e impacto social, criptografía y autenticación y autorización. Estas áreas podrían suponer una primera clasificación basada en temas que forman parte de los cursos de formación actuales. Sin embargo, en el ámbito de la investigación se emplea otra terminología diferente, basada en áreas y palabras clave de los artículos de investigación, que difieren según la revista y autor. Finalmente, en el ámbito de la industria, se suelen emplear términos y clasificaciones basadas en el uso de tecnologías de ciberseguridad, habitualmente cambiantes en el tiempo. Entendemos que las empresas DIB son quien, en última instancia, deben especificar los requisitos y tareas a realizar por los alumnos que reciban los cursos de formación específicos. Por ello, resulta conveniente ofrecer una taxonomía de las tecnologías de ciberseguridad basada en su aplicación en la industria como paso previo a la selección de aquellas que resulten de interés al mundo de la defensa.

Dado que los organismos de normalización y regulación proporcionan referencias de utilidad internacionalmente aceptadas, tanto en el ámbito de las taxonomías de ciberseguridad como en la definición de competencias y terminología, revisaremos a continuación los principales marcos encontrados.

A. Taxonomías en ciberseguridad

Existen distintos marcos conceptuales que agrupan o clasifican controles o procedimientos de ciberseguridad que permiten cubrir las necesidades de la industria. Uno de estos modelos, especialmente relevante en el ámbito de defensa, es el definido por NIST como Cybersecurity Maturity Model Certification (CMMC) [2]. Su objetivo es que aquellas empresas e instituciones (universidades o centros de investigación) que trabajan para el Ministerio de Defensa de EE.UU (unas 300.000) puedan acreditar un nivel de seguridad que les posibilite tener información sensible como contratos federales o información controlada no clasificada. Así, CMMC permite certificar a empresas en función del nivel de cumplimiento de los controles o buenas prácticas que utilicen. Las prácticas descritas en CMMC se agrupan en 17 dominios de capacidades diferentes (p.e.: *Access control, Incident Response, Awareness and Training, Recovery, Identification and Authentication*, etc.) que en sí podría suponer una posible taxonomía en el campo de la ciberseguridad.

Una posible crítica al modelo del CMMC es que se centra mucho en la protección del control de acceso la información (26 prácticas), auditorías (14 prácticas), respuesta a incidentes (13 prácticas) y proyección de comunicaciones y sistemas (27 prácticas). Por ello, un marco de referencia alternativo podría ser el descrito por NIST en su *Framework for Improving Critical Infrastructure Cybersecurity* (CSF) [6]. CSF define 260 controles o buenas prácticas para infraestructuras críticas agrupados en una taxonomía de 23 categorías que pertenecen a una de las 5 funcionalidades básicas de la ciberseguridad: identificar, proteger, detectar, respuesta y recuperación. En cualquier caso, ambas normas tienen una serie de limitaciones para nuestro trabajo: (I) La aplicación de dominios de seguridad (17 en CMMC) o categorías (23 en CSF) resulta difusa para la definición de tecnologías, mientras que el uso de dos niveles (prácticas en CMMC o subcategorías en CSF) ofrece un nivel de granularidad excesivo (entre 72-172 con CMMC y 260 en CSF). (II) Se basan en buenas prácticas bien conocidas para bastionar o reforzar sistemas, pero de manera generalista y no centrada en la industria de defensa.

B. Marcos de referencia en educación en ciberseguridad

Hay dos grandes marcos de referencia internacionales en formación para ciberseguridad: el ACM *cybersecurity Curricula Guideline* [7] y el propuesto por el NIST en 2020 denominado *National Initiative for Cybersecurity Education* (NICE) [7]. El primero está pensado para el diseño de Grados en ciberseguridad dentro del mundo académico, y divide los contenidos en 8 grandes áreas de conocimiento sobre las que define unidades de conocimiento, tópicos y resultados del aprendizaje. El segundo, sin embargo, define las competencias y conocimientos a adquirir por un alumno para realizar distintas tareas en el campo de la ciberseguridad, lo que facilita el diseño de cursos en función de las tareas que se

buscan para un perfil de trabajo determinado. Dado nuestro enfoque a la industria, y la facilidad que ofrece NICE para trasladar en áreas de conocimiento de otros marcos como el de ACM, adoptaremos NICE como marco de referencia. De dicho marco tomaremos las siguientes definiciones:

- Tarea (*Task*): actividad dirigida a conseguir los objetivos de la organización. La definición de la tarea debe realizarse en el lenguaje corporativo y debe incluir el trabajo que debe ser completado (ej. resolución de problemas de hardware). En la definición no se debe incluir el objetivo, sino la tarea.
- Competencia (*Skill*): es la capacidad para realizar una acción observable. En relación con una tarea, la competencia es la demostración de la pericia para realizarla (ej. reconocer alertas de un sistema de detección de intrusiones). La descripción de una competencia debería incluir qué puede hacer una persona gracias a ella. Hay que señalar que las competencias pueden ser específicas de ciberseguridad o transversales.
- Conocimiento (*Knowledge*) un conjunto de conceptos dentro de la memoria que pueden ser recuperados (ej. conocimiento de fuentes de diseminación de información sobre vulnerabilidades).

El marco de referencia NICE permite asociar competencias a tareas concretas que forman la base de perfiles de trabajo. El uso de perfiles de trabajo facilita a los empleadores la definición de puestos demandados y permite extraer las competencias y conocimientos a incluir en los cursos de formación.

Para nuestro propósito, el nivel de granularidad de NICE resulta muy elevado, pues define 377 competencias (algunas transversales) asociadas a 54 perfiles de trabajo diferentes en ciberseguridad pertenecientes a 32 áreas de especialidad. No obstante, el ámbito de la defensa tiene sus propios roles de trabajo que no están incluidos, por lo que no puede utilizarse este marco directamente para satisfacer nuestro objetivo, pero sí podemos aprovechar las listas de competencias y conocimientos asociados a una tarea concreta.

Aunque en Europa existe una clasificación genérica de competencias, cualificaciones y ocupaciones (ESCO [13]), su empleo en la ciberseguridad resultaría muy difícil ya que se centra básicamente en competencias TIC y transversales.

III. METODOLOGÍA EMPLEADA

Para confeccionar una lista de competencias en ciberseguridad necesarias para el desarrollo de la labor de la DIB se propone una metodología en dos fases secuenciales (Ilustración 1):

1. Identificar una lista de tecnologías de interés del DIB. Para ello, partiendo de una búsqueda documental, se elaborará una taxonomía de tecnologías de ciberseguridad, así como una lista de aplicaciones en defensa de la Ciberseguridad. La relación entre ambas listas y la realización de encuestas a empresas DIB ofrecerán el resultado final de las tecnologías en ciberseguridad de mayor interés en el ámbito de la defensa. Se fija como objetivo un nivel de granularidad intermedio, de entre 20 y 30 tecnologías.
2. Partiendo del resultado anterior, se buscará un conjunto de competencias dentro del marco de NICE relacionadas con dichas tecnologías. El resultado final será un conjunto de competencias agrupadas en: (I) competencias técnicas en ciberseguridad, (II) competencias transversales, aplicables a cualquier campo y (III) competencias en técnicas con potencial ofensivo (defensa) en ciberseguridad.

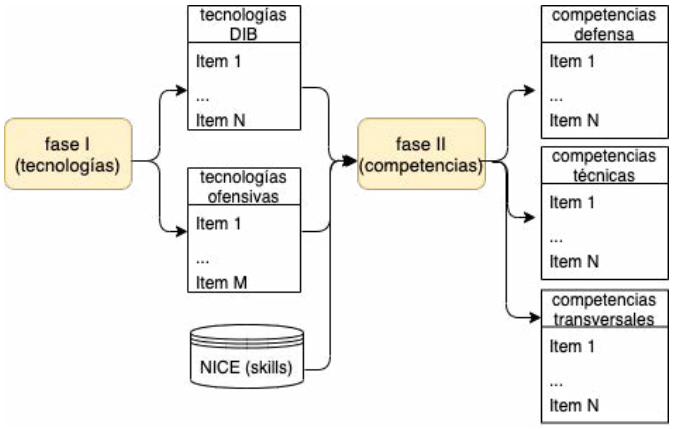

Ilustración 1- Etapas y resultados en la metodología

A continuación, se describe la metodología seguida en cada una de las dos fases anteriores.

A. Fase 1: Identificación de Tecnologías en ciberseguridad de interés en defensa

Las actividades desarrolladas en esta primera fase se descomponen en los siguientes pasos reflejados en la Ilustración 2:

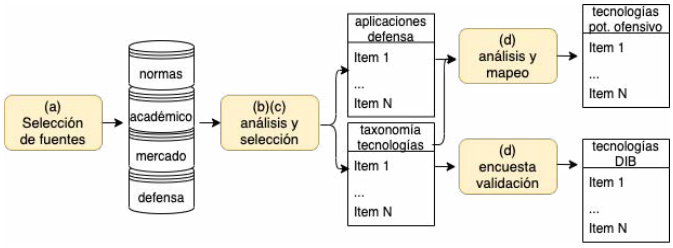

Ilustración 2. Pasos de la fase 1

a) Selección de fuentes de información: se identificaron fuentes para clasificar tecnologías desde distintas perspectivas: industria/mercado, academia/investigación, reguladores, y defensa. La metodología seguida en cada tipo de fuente y los resultados más relevantes han sido:

- Industria y Mercado: búsqueda en Google de los términos: *"market", "cybersecurity technology", "cybersecurity technologies", "cybersecurity technologies classification", "cybersecurity market"*.
- Reguladores: Se han buscado las publicaciones del NIST (principal actor a nivel internacional en ciberseguridad) y en otros organismos similares internacionales como MITRE (en concreto las técnicas y tácticas de la matriz ATT&CK).
- Academia / Investigación: búsquedas en Scopus y Google Scholar con los términos: *"cybersecurity technologies", "cybersecurity classification", "cybertechnologies", "cyber-technologies", "cybersecurity trends", "cybersecurity education"*. También se incluyeron búsquedas de las contribuciones en el *track* de ciberseguridad de la conferencia MILCOM 2018-2019.

• Defensa / Militar: búsquedas en Google, Google Scholar y Scopus sobre los términos: *"cyberwar", "cyberspace", "cyber-warfare", "cyberdefense", "cyber operations", "cybersecurity military", "cybercommand"*. Igualmente se consideró la revista "*Cyberdefense review*" editada por la academia de West Point.

b) Definición de una taxonomía: Tomando como clasificación de partida la única encontrada en el informe sobre ciberseguridad en 18 países europeos [9], se mezcló con la ofrecida por [10] realizada tras el análisis de los productos y servicios de 3.500 empresas de ciberseguridad internacionales. Luego se utilizaron las clasificaciones extraídas de los marcos descritos en la Sección II, de las que se excluyeron las tecnologías ya presentes y se unificaron por analogía de conceptos. Tras ello se utilizaron las fuentes de la academia y defensa para incorporar aquellas tecnologías que no estaban presentes. La clasificación de tecnologías anterior ha sido enlazada con el marco CSF, y a su vez se han buscado empresas europeas que las utilicen gracias a ECSO *market radar.*

c) Búsqueda de aplicaciones de ciberseguridad para defensa. Todos los documentos recopilados relacionados con defensa y Ejército, fueron transformados de PDF a texto plano utilizando la librería *poppler* a fin de automatizar las búsquedas de artículos y párrafos que tuvieran los siguientes términos: *"cyber" and "defense", "war", "warfare", "applications", "military", "technique", "mission", "operations"*. Los párrafos con frases encontradas fueron analizados a fin de encontrar las distintas aplicaciones. Se creó una lista inicial con las aplicaciones encontradas y de ella se filtraron sólo las entradas más referenciadas. A la lista final se añadió una aplicación adicional relacionada con la protección de información sensible en manos de las empresas que forman la DIB.

d) Selección de las tecnologías más apropiadas para la defensa. Para ello se han realizado los siguientes pasos:
- Evaluación de la utilidad de cada una de las tecnologías en cada una de las aplicaciones en defensa, puntuando de 0 a 10 a juicio de experto.
- Validación mediante una encuesta realizada a industrias de defensa españolas del consorcio ASSETs+. En concreto, se ha preguntado: (I) la relevancia de la tecnología para su empresa y para el ámbito de la defensa, (II) la facilidad para encontrar expertos en dicha tecnología y (III) el grado de madurez de la empresa en dicha tecnología. Las posibles respuestas iban de 1 (poco) a 3 puntos (mucho)
- Filtrado de las tecnologías: se han considerado relevantes las tecnologías que cumplan con las siguientes restricciones: (a) que exista alguna empresa europea con productos, (b) que la facilidad para encontrar expertos sea inferior a 2,3 puntos sobre 3 y (c) que sea relevante para la empresa (más de 1,5 puntos sobre 3) o bien que sea aplicable al 50% o más de las aplicaciones encontradas.

B. Selección de competencias

Esta parte se selecciona un subconjunto de competencias de entre las 377 definidas en NICE. Con respecto a la granularidad, se fija como objetivo conseguir una lista final con no más de 40 competencias.

La metodología seguida se representa en la Ilustración 3.

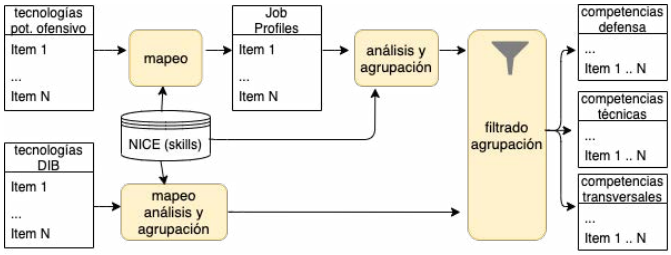

Ilustración 3. Pasos en la fase 2

A continuación, se describen los pasos principales seguidos:

a) Se han relacionado las competencias NICE con su aplicación a las tecnologías con propósito defensivo seleccionadas en el paso anterior. Se eliminaron duplicados y se filtraron las competencias transversales.

b) Se reduce la granularidad de forma iterativa, uniendo competencias similares y seleccionando las competencias con mayor prevalencia (asociadas a más tecnologías). Tras ello se verifica la coherencia de la selección (debe haber al menos una competencia representativa por cada tecnología) y se realiza una nueva iteración, hasta llegar a la lista final de competencias técnicas.

c) Las competencias transversales han sido agrupadas por similitud de conceptos y prevalencia en un proceso similar al anterior. El resultado final ha sido completado con 3 competencias propuestas por el Foro económico mundial (*World Economic Forum)*.

d) Las tecnologías con potencial ofensivo han sido relacionadas con los perfiles de trabajo que presentan mayor afinidad. Para ello, se extraen las competencias asociadas, filtrando las transversales, los duplicados y las ya presentes en las listas anteriores. Las competencias resultantes han sido reducidas en un proceso iterativo similar al descrito para las competencias técnicas hasta llegar a la lista final.

IV. RESULTADOS

En esta sección se presentarán los resultados de aplicar la metodología descrita. A fin de mantener la información lo más fielmente posible a las referencias utilizadas, los resultados procedentes de NICE se presentarán en inglés. Los resultados de la búsqueda de información fueron un total de 135 artículos (50% del campo defensa/Militar y 50% de Academia /investigación), 2 libros y 3 informes de mercado. Estos documentos forman el corpus que sirve de base para realizar los análisis del presente trabajo. Tan sólo en el informe de mercado [10] encontramos una clasificación de tecnologías en ciberseguridad, que, junto con [11] sirvieron de punto de partida.

En la tabla I se especifica la clasificación final realizada para las tecnologías de ciberseguridad, donde en torno al 60% han sido obtenidas de las fuentes de industria/mercado, el

30% conforme a los marcos CMMC y CSF y el 10% de defensa e investigación.

Tabla I
LISTA DE LAS TECNOLOGÍAS EN CIBERSEGURIDAD

ID	Tecnología	Descripción
1	Identificación & Autenticación	Asegurar que una característica declarada por una entidad es correcta. [12]
2	Autorización & Control de acceso	La concesión de derechos, que incluye la concesión de acceso en función de los derechos de acceso. [13]
3	Cortafuegos	Conjunto de técnicas para proteger activamente una red, como cortafuegos o protecciones DDoS
4	*Cyber range*	Un conjunto de activos y capacidades que se pueden integrar en los niveles de clasificación y controles apropiados para realizar investigación, desarrollo, demostración, prueba o evaluación de capacidades militares apoyadas en o para capacitar al personal militar durante las operaciones. [14]
5	Cifrado	Cifrado de datos dentro o en el sistema final de origen, y el descifrado correspondiente se produce dentro o en el sistema final de destino. [15]
6	Certificación	Procesos para certificar la identidad o un atributo de un sistema o servicio.
7	Seguridad en *endpoint*	Los sistemas de seguridad *endpoint* protegen las computadoras y otros dispositivos en una red o en la nube de las amenazas de ciberseguridad. La seguridad de los *endpoints* ha evolucionado desde el software antivirus tradicional hasta proporcionar una protección integral contra malware sofisticado y amenazas de día cero en constante evolución. [16]
8	Seguridad móvil & IoT	Conjunto de técnicas para proteger los dispositivos por pocos recursos.
9	Seguridad en la nube y virtualización	Conjunto de técnicas relacionadas con la protección del entorno de la nube y los entornos virtualizados.
10	Gestión de vulnerabilidades	Proceso de identificación, evaluación y corrección de vulnerabilidades, definido como "Debilidad en un sistema de información, procedimientos de seguridad del sistema, controles internos o implementación que podrían ser explotados o desencadenados por una fuente de amenaza". [17]
11	Análisis de malware	Adquirir datos confidenciales desensamblando y analizando el diseño de un componente del sistema. [18]
12	Seguridad hardware	Conjunto de protecciones físicas aplicadas para asegurar la correcta ejecución y funcionamiento de un dispositivo.
13	Intrusion Prevention/Detection Systems (IDS/IPS)	Productos de hardware o software que recopilan y analizan información de diversas áreas dentro de una computadora o una red para identificar posibles brechas de seguridad, que incluyen tanto intrusiones como mal uso. [19]
14	Inteligencia de ciberamenazas	Actividades que utilizan todas las fuentes de "inteligencia" en apoyo de la ciberseguridad para trazar las ciberamenazas, recopilar las intenciones de ataque y las posibilidades de los adversarios potenciales, para analizar y comunicar, e identificar, localizar y asignar la fuente de los ciberataques.. [23]
15	*Honeypots*	Un sistema (por ejemplo, un servidor web) o un recurso del sistema (por ejemplo, un archivo en un servidor) que está diseñado para ser atractivo para los posibles atacantes e intrusos, como la miel es atractiva para los osos. [43]
16	Operaciones de seguridad	Conjunto de tecnologías disponibles en un Centro de operaciones de seguridad, que según McAfee, "es una función centralizada dentro de una organización que emplea personas, procesos y tecnología para monitorear y mejorar continuamente la postura de seguridad de una organización mientras previene, detecta, analiza y responde a incidentes de ciberseguridad ". [25]
17	Evaluación & Gestión de riesgo	El proceso de identificar, evaluar y responder al riesgo. [24]
18	Aseguramiento y cumplimiento	Cumplimiento con, y capacidad para demostrar el cumplimiento a los requisitos obligatorios definidos por las leyes y reglamentos, así como a los requisitos voluntarios resultantes de las obligaciones contractuales y las políticas internas. [25]
19	Desarrollo seguro de software	Proceso de desarrollo de software que considera los problemas relacionados con la seguridad desde el primer paso.
20	Análisis forense	La práctica de recopilar, retener y analizar datos relacionados con el ordenador con fines de investigación de una manera que mantenga la integridad de los datos.. [26]
21	Protección DoS	Implementaciones para protegerse contra ataques de denegación de servicio.
22	Ciber resiliencia	El proceso para asegurar que la recuperación de las operaciones esté asegurada en caso de que ocurra algún incidente inesperado o no deseado que sea capaz de afectar negativamente la continuidad de las funciones comerciales esenciales y los elementos de apoyo. [27]
23	Inteligencia de fuentes abiertas (OSINT)/ Inteligencia privada (PRIVINT)	Inteligencia a partir de información pública / privada que se recopila, explota y se informa para abordar un requisito de inteligencia específico. [27]
24	Test de penetración / *Red Teaming*	Conjunto de herramientas y técnicas enfocadas en atacar un dispositivo, servicio o host para identificar debilidades y protegerlo posteriormente.

Cada tecnología ha sido clasificada de acuerdo con el propósito o finalidad de la misma conforme al marco CSF. Los resultados se muestran en la tabla II.

Tabla II
AGRUPACIÓN DE LAS TECNOLOGÍAS SEGÚN SU FINALIDAD

Propósito		ID
Defensivo	Proteger	1 -12
	Detectar	13 - 16
	Identificar	17 – 19
	Responder	20 – 21
	Recuperar	22
Ofensivo		23 - 24

Así mismo, se ha buscado en *ECSO market radar* el número de empresas de la Unión Europea que presentan productos o servicios relacionados con dicha tecnología. Los resultados se muestran en la columna "Empresas EU" de la tabla III.

A. Selección de aplicaciones

Continuando con la metodología presentada, se han identificado las siguientes aplicaciones de ciberseguridad para la defensa:

- A1: Colaboración de la Base Industrial de Defensa (DIB): DIB proporciona una mayor seguridad para el Departamento de defensa. Un contratista de DIB puede proteger los contratos y controlar la información a un nivel acorde con el riesgo, contabilizando los flujos de información hacia sus subcontratistas en una cadena de suministro de varios niveles [2].
- A2: Concienciación y formación en ciberseguridad: se corresponde con el uso de las plataformas de formación para formar al eslabón más débil de la cadena de ciberseguridad, el usuario; proporcionando guías para una buena conducta y mejorando el uso de la información por parte del personal militar. Así, se persigue aumentar la eficiencia operacional.
- A3: Seguridad de las operaciones (OPSEC): es el proceso de ayudar en la identificación de acciones que puedan ser observadas y recogidas por los adversarios. También persigue determinar los indicadores que los adversarios podrían obtener e interpretar para adquirir información crítica y, si fuese apropiado, seleccionar y ejecutar medidas OPSEC que eliminen y reduzcan el riesgo a niveles aceptables [20].
- A4: Operaciones ciber (CO): se corresponde con las capacidades del ciberespacio cuyo propósito es la de conseguir los objetivos en o a través del ciberespacio. Se pueden clasificar en Operaciones Ciber (OCO) y Operaciones Defensivas (DCO) [21].
- A5: Operaciones de apoyo a la información militar (MISO): son las acciones especialmente relacionadas con el uso de capacidades asociadas a la información del ciberespacio durante las operaciones militares, para influir, interrumpir, corromper o usurpar la toma de decisiones de adversarios y adversarios potenciales.
- A6: Soporte de comando y control: son las decisiones que ofrecen soporte de comando y control (inteligencia, vigilancia, adquisición de objetivos, reconocimiento).
- A7: Comunicaciones seguras (COMSEC): se utilizan para proteger tráfico clasificado y no clasificado en redes de comunicación militar, incluyendo voz, vídeo y datos [22].
- A8: Actividades de enfrentamiento ciber-electrónicos (CEWA): combinan los enfrentamientos ciber y electrónicos en un mismo contexto para respaldar, habilitar, proteger y recopilar las capacidades que operan dentro del espectro electromagnético (EMS), incluidas las capacidades del ciberespacio.

Finalmente se ha procedido con el filtrado de las tecnologías con mayor interés para el ámbito de la defensa conforme se estableció en la metodología para la Fase 1 apartado d). Las 19 tecnologías seleccionadas (color negro en la tabla III) cumplen las restricciones de filtrado y siempre hay al menos una tecnología por cada clase del CSF.

Tabla III
MÉTRICAS DE LAS TECNOLOGÍAS

ID Tecnología	Empresas EU	Aplicaciones defensa	Encuesta DIB	
			Mercado Laboral	Relevancia Empresa
1	8	7	1,6	1,8
2	8	7	1,6	1,8
3	8	5	2,6	2
4	9	4	1,8	2,2
5	10	7	1,6	1,8
6	5	4	1,6	1,8
7	9	5	2,2	1,6
8	12	2	2,4	2,2
9	8	2	2	1
10	15	4	1,6	1,8
11	5	3	1,8	1,2
12	12	3	1,8	1,8
13	14	5	1,8	1,6
14	17	7	1,4	1,6
15	6	2	1,4	0,8
16	14	7	1,6	1,4
17	10	4	1,8	2
18	13	4	2,4	2,2
19	9	3	1,8	2,2
20	14	2	1,4	1,6
21	6	5	2	1,6
22	9	7	1,6	1,6
23	1	7	1,4	1,4
24	4	4	1,2	1,2

B. Selección de competencias

La vinculación de dichas tecnologías con las competencias de NICE ofreció un promedio de 11 competencias por tecnología. Tras el proceso de reducción de granularidad y filtrado, en la tabla IV se muestra el listado de competencias técnicas (indicando en cada una el código y descripción de dicha competencia según NICE).

Tabla IV
LISTADO DE COMPETENCIAS TÉCNICAS

Código	*Descripción*
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
S0357	Skill to anticipate new security threats.
S0124	Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution.
S0371	Skill to respond and take local actions in response to threat sharing alerts from service providers.

Código	*Descripción*
S0077	Skill in securing network communications.
S0178	Skill in analyzing essential network data (e.g., router configuration files, routing protocols), network traffic capacity and performance characteristics.
S0185	Skill in applying analytical methods typically employed to support planning and to justify recommended strategies and courses of action.
S0221	Skill in extracting information from packet captures.
S0006	Skill in applying confidentiality, integrity, and availability principles.
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
S0040	Skill in implementing, maintaining, and improving established network security practices.
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
S0096	Skill in reading and interpreting signatures (e.g., snort).
S0156	Skill in performing packet-level analysis.
S0173	Skill in using security event correlation tools.
S0202	Skill in data mining techniques (e.g., searching file systems) and analysis.
S0258	Skill in recognizing and interpreting malicious network activity in traffic.
S0269	Skill in researching vulnerabilities and exploits utilized in traffic.
S0288	Skill in using multiple analytic tools, databases, and techniques (e.g., Analyst's Notebook, A-Space, Anchory, M3, divergent/convergent thinking, link charts, matrices, etc.).
S0007	Skill in applying host/network access controls (e.g., access control list).
S0010	Skill in conducting capabilities and requirements analysis.
S0015	Skill in conducting test event and secure test plan design (e. g. unit, integration, system, acceptance)
S0018	Skill in creating policies that reflect system security objectives.
S0020	Skill in developing and deploying signatures.
S0031	Skill in developing and applying security system access controls.
S0032	Skill in developing, testing, and implementing network infrastructure contingency and recovery plans.
S0036	Skill in evaluating the adequacy of security designs.
S0063	Skill in collecting data from a variety of cyber defense resources.
S0084	Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).
S0087	Skill in deep analysis of captured malicious code (e.g., malware forensics).
S0089	Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]) and verifying the integrity of all files.
S0093	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures.
S0120	Skill in reviewing logs to identify evidence of past intrusions.
S0138	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).
S0164	Skill in assessing the application of cryptographic standards.
S0195	Skill in conducting research using all available sources (including deep web)
S0197	Skill in conducting social network analysis, buddy list analysis, and/or cookie analysis.
S0270	Skill in reverse engineering (e.g., hex editing, binary packaging utilities, debugging, and strings analysis) to identify function and ownership of remote tools.
S0317	Skill to compare indicators/observables with requirements.
S0064	Skill in developing and executing technical training programs and curricula.

Por su parte, la lista de competencias transversales se muestra la tabla V. Nótese que tres de ellas no tienen identificador en NICE puesto que provienen del Foro económico mundial (señaladas como WEF en dicha tabla).

Tabla V
LISTADO DE COMPETENCIAS TRANSVERSALES

Código	*Descripción*
S0070	Skill in talking to others to convey information effectively
S0356	Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).
S0344	Skill to prepare and deliver reports, presentations and briefings, to include using visual aids or presentation technology.
S0301	Skill in writing about facts and ideas in a clear, convincing, and organized manner.
S0213	Skill in documenting and communicating complex technical and programmatic information.
S0306	Skill to analyze strategic guidance for issues requiring clarification and/or additional guidance.
S0128	Skill in using manpower and personnel IT systems.
WEF	Skill in Conflict Management
WEF	Skill in Critical Thinking
WEF	Skill in Complex problem solving

Por último, para las competencias en defensa se consideraron tres perfiles profesionales definidos en NICE, a saber: *Exploitation analyst, Cyber Intel Planner, Cyber Ops Planner, Cyber Operator*. De esta forma, la lista de competencias asociadas a defensa se refleja en la tabla VI.

Tabla VI
LISTADO DE COMPETENCIAS DE DEFENSA

Código	*Descripción*
S0182	Skill in analyzing target communications internals and externals collected from wireless LANs.
S0242	Skill in interpreting vulnerability scanner results to identify vulnerabilities.
S0252	Skill in processing collected data for follow-on analysis.
S0255	Skill in providing real-time, actionable geolocation information utilizing target infrastructures.
S0293	Skill in using tools, techniques, and procedures to remotely exploit and establish persistence on a target.
S0295	Skill in using various open-source data collection tools (online trade, DNS, mail, etc.).
S0218	Skill in evaluating information for reliability, validity, and relevance.
S0309	Skill to anticipate key target or threat activities which are likely to prompt a leadership decision.
S0209	Skill in developing and executing comprehensive cyber operations assessment programs for assessing and validating operational performance characteristics.
S0360	Skill to analyze and assess internal and external partner cyber operations capabilities and tools.

V. Conclusiones y líneas de avance

En este trabajo se ha presentado una lista de competencias que puede ser utilizada para la planificación de cursos de ciberseguridad en el ámbito de la defensa. La metodología empleada utiliza una revisión exhaustiva de diversas fuentes documentales y marcos de referencia internacionales. Estos resultados preliminares se corresponden con la ejecución en curso del proyecto europeo ASSETS+, enmarcado en la iniciativa Erasmus+.

Los siguientes pasos consisten en la definición de perfiles de cursos de formación, que serán realizados en consonancia con la industria de defensa. Dichos cursos deberán considerar no sólo las competencias, sino los conocimientos y las dependencias entre ellos.

Agradecimientos

Este trabajo ha sido parcialmente financiado por el proyecto ASSETS+ [3] en el ámbito de la iniciativa Erasmus+; por el proyecto CAVTIONS-CM-UC3M, co-financiado por la Comunidad de Madrid (CAM) y la Universidad Carlos III de Madrid; por el MINECO, proyecto ODIO/COW(PID2019-111429RB-C21); por la CAM, proyecto CYNAMON-CM(P2018/TCS-4566), co-financiado con fondos europeos ESF y FEDER; y por el Programa de Excelencia para Investigadores de la Universidad Carlos III de Madrid.

Referencias

[1] Departamento de defensa EE.UU., “Cybersecurity Maturity Model Certification, version 1.02,” Enero 2020. Disponible en: https://www.acq.osd.mil/cmmc/draft.html [Accedido el 5 mayo 2021]

[2] Mouheb, D., Abbas, S., & Merabti, M.. “Cybersecurity curriculum design: A survey” en Transactions on Edutainment XV (pp. 93-107) .Springer, Berlin, Heidelberg. 2020

[3] Proyecto “Alliance for strategic skill addressing emerging technologies in Defense (ASSETs+)”. Disponible en https://assets-plus.eu [Accedido el 5 de mayo 2021]

[4] Švábenský, V., Vykopal, J., & Čeleda, P. “What are cybersecurity education papers about? a systematic literature review of sigcse and iticse conferences” en Proceedings of the 51st ACM Technical Symposium on Computer Science Education (pp. 2-8). 2020

[5] ACM “Cybersecurity curriula guidelines 2017”. Disponible en: https://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017_web.pdf [Accedido el 5 de mayo de 2021].

[6] NIST Cybersecurity Framework (CSF). Disponible en: https://www.nist.gov/cyberframework [Accedido el 5 de mayo de 2021]

[7] NIST.SP.181r1. “Workforce Framework for Cybersecurity (NICE Framework)”. Disponible en https://doi.org/10.6028/NIST.SP.800-181r1 2020. [Accedido el 5 de mayo de 2021]

[8] Clasificación europea de capacidades/competencias, cualificaciones y ocupaciones. (ESCO). Disponible en: https://ec.europa.eu/esco/portal/skill [Accedido el 5 de mayo de 2021]

[9] Cybersecurity Technologies & Market - Focus on Europe - 2017-2022. Disponible: https://homelandsecurityresearch.com/reports/cybersecurity-technologies-market-focus-europe/ [Accedido el 5 de mayo de 2021]

[10] Momentum Cybersecurity Group. “Momentum Cyberscape 2021”. Disponible en https://momentumcyber.com/docs/CYBERscape.pdf [Accedido el 5 de mayo 2021].

[11] ISO/IEC.. ISO/IEC 27000: 2014 (E) Information technology—Security techniques—Information security management systems—Overview and vocabulary. 2014.

[12] Reihe, I.. IEC 7498 ISO/IEC 7498-1: 1994-11. Information technology–Open Systems Interconnection–Basic Reference Model: The Basic Model ISO, 7498-2. 1994

[13] Damodaran, S. K., & Smith, K.. CRIS “Cyber Range Lexicon, Version 1.0 (No. MIT-LL-59-0001)”. MASSACHUSETTS INST OF TECH LEXINGTON LINCOLN LAB. 2015

[14] ISO 7498-2:1989. Information processing systems — Open Systems Interconnection — Basic Reference Model. 1989

[15] McAffee, “What Is Endpoint Security? Disponible en https://www.mcafee.com/enterprise/es-es/security-awareness/endpoint.html [Accedido el 5 de mayo de 2021]

[16] NIST, S.. 800-53: 2013. Security and Privacy Controls for Federal Information Systems and Organizations. 2013.

[17] SANS. “Glossary of Security Terms” Disponible en https://www.sans.org/security-resources/glossary-of-terms/ .[Accedido el 5 de mayo de 2021]

[18] US Committee on National Security Systems “National Information Assurance. (IA) glossary”. Tech. Rep. 4009, 2010. Disponible en https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf [Accedido el 5 de mayo de 2021]

[19] U.S. Department of Energy. Office of Scientific and Technical Information. “Differences Between OPSEC and Security Awareness.” Disponible en https://www.osti.gov/servlets/purl/1367112 .[Accedido el 5 de mayo de 2021].

[20] M. Karamanetal. “Institutional Cybersecurity from Military Perspective“. International Journal of Information Security Science, Vol.5, No.1. 2016.

[21] Azgomi, Mohammad Abdollahi, et al. "Introduction to the special issue on secure communications." Telecommunication Systems vol 69. 2018:

[22] OTAN. Tech Repport ACST–Strategy-CyberSecurity-001 "Cyber Security Strategy for Defence". Editado por COS STRAT. 2014

[23] “What Is a Security Operations Center (SOC)?”. McAfee. https://www.mcafee.com/enterprise/es-es/security-awareness/operations/what-is-soc.html

[24] ISACA, Cybersecurity Glossary, 2014. https://www.isaca.org/resources/glossary

[25] NIST, S. (2004). 800-61. Computer security incident handling guide, 800-61.

[26] ISO-18028-1:2006. Information technology — Security techniques — IT network security. 2006

[27] Josh Huff, OSINT: Open Source Intelligence. Disponible en https://www.coursehero.com/file/71790416/summit-archive-1533737204pdf/ . [Accedido el 5 de mayo de 2021]

.