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

Sesión de Formación e Innovación Educativa
http://doi.org/10.18239/jornadas_2021.34.66

Curso de Especialización en Ciberseguridad, ¿están preparados nuestros docentes?

Francisco José de Haro Olmo
Dpto. Informática.
Universidad de Almería
04120 Almería
Orcid:0000-0003-3130-0877
fdo730@inlumine.ual.es

Ángel Jesús Varela-Vaca
Dpto. Lenguajes y Sistemas Informáticos.
Universidad de Sevilla
ETS Ingeniría Informática
Orcid:0000-0001-9953-6005
ajvarela@us.es

José Antonio Álvarez Bermejo
Dpto. Informática
Universidad de Almeria
04120 Almería
Orcid:0000-0002-5815-7858
jaberme@ual.es

***Resumen*—La aparición del nuevo título de Formación Profesional, Curso de Especialización en *"Ciberseguridad en entornos de tecnologías de la información"*, establece el punto de partida sobre los conocimientos del profesorado en cuestiones de Ciberseguridad. Para ello hemos realizado un estudio sobre los conocimientos del profesorado que imparte docencia en la formación profesional, basado en la propuesta curricular en ciberseguridad de la guías *ACM/IEEE/AIS SIGSEC/IFIP Cybersecurity*, con el objetivo de proponer un itinerario formativo en Ciberseguridad para el profesorado, de forma que estén en disposición de ofrecer una mejor respuesta y mayor calidad ante el proceso de formación de los profesionales del futuro en dicha materia. En primer lugar hemos desarrollado un estudio basado cuestionarios, a través del cual se han presentado las unidades de conocimiento en materia de Ciberseguridad al profesorado de Andalucía y sobre las que han realizado la valoración de su conocimiento en dicha materia. Se presenta un análisis cuantitativo de los resultados obtenidos priorizando las necesidades formativas. Como conclusión de nuestro estudio hemos propuesto la elaboración de un itinerario formativo para el profesorado basado en las diez unidades de conocimiento.**

***Index Terms*—Ciberseguridad, Profesorado, Formación Profesional, Currícula**

Tipo de contribución: *Formación e innovación educativa*

I. Introducción

La necesidad de profesionales expertos (técnicos especialistas, ingenieros, etc.) en materia de Ciberseguridad se acrecienta día tras en el mercado laboral, donde las empresas están tomando concienciando de la necesidad de contar con personal cualificado ante los nuevos retos, problemas y amenazas emergentes ante los sistemas informáticos [2], [3], [4].

Las Cyber kill chains (cadenas de ataque) [1][5] utilizadas por los atacantes para penetrar en los sistemas son cada vez más sofisticadas, demostrando la necesidad de organizaciones y administraciones de contar con expertos en Ciberseguridad. Además, en la nueva era de la de digitalización, las nuevas tecnologías como el Robotic Process Automation (RPA), el procesamiento en la nube, Big Data, y entornos como la Industria 4.0 hace que la Ciberseguridad adquiera mayor relevancia.

A nivel universitario ya existen titulaciones en Ciberseguridad que abarcan un completo abanico de contenido para formar a los profesionales de la Ciberseguridad que el mercado laboral está demandando. Sin embargo, no se consigue cubrir todos los perfiles requeridos en materia de Ciberseguridad [6]. Estos nuevos perfiles profesiones relacionadas con la Ciberseguridad, se encuentran a todos los niveles de formación y especialización, con distintos niveles de cualificación entre los que los profesionales (técnicos superiores) procedentes de la Formación Profesional (FP) son un referente más.

Estas nuevas necesidades de especialización que aparecen en el mercado laboral y han dado lugar a la publicación de nuevas titulaciones [7]. El objetivo de estas titulaciones es cubrir las deficiencias del mercado dotando de profesionales técnicos especialistas con alta especialización, concretamente en materia de Ciberseguridad. Por tanto, es de vital importancia considerar la actualización formativa de los docentes y la concienciación de la importancia de las competencias digitales [9] de quienes imparten docencia en estas titulaciones.

En el contexto de las 6 titulaciones de la familia "Informática y Comunicaciones", tan sólo existen un par de módulos profesionales dedicados a la seguridad informática: (a) **Seguridad Informática** en el Título de Técnico en Sistemas Microinformáticos y Redes; y el otro es (2) **Seguridad y Alta Disponibilidad** en el Título de Técnico Superior en Administración de Sistemas Informáticos en Red. Si bien es cierto que los contenidos necesitan una revisión para adaptarse a la realidad del mercado laboral, cabe destacar que el resto de titulaciones carecen de la formación necesaria en materia de Ciberseguridad, aspecto que hace más que necesaria la aparición de la nueva titulación [7] como forma de especialización en esta materia y que se accede desde cualquiera de los títulos de grado superior de la misma familia profesional.

Para abordar estos nuevos retos en la Formación Profesional, desde el Ministerio de Educación y Formación Profesional se ha publicado el *I Plan Estratégico de Formación Profesional del Sistema Educativo 2019-2022* [9] donde en el *Eje 7* se hace referencia a la mejora de la actualización y formación permanente del profesorado. Resaltamos los Objetivos 12 y 13:

- **Objetivo 12**. Promover la formación especializada del profesorado.
- **Objetivo 14.** Impulsar la implantación de metodologías didácticas novedosas que supongan innovación educativa.

Estos antecedentes unidos a la existencia de un título denominado **Curso de Especialización en Ciberseguridad en entornos de las tecnologías de la información** [7] y que

pretende dar respuesta rápida a las innovaciones producidas en el sector productivo y a la necesidad de formar a los futuros profesionales de la Ciberseguridad, profundizando en los conocimientos o bien ampliando las competencias propias de cada título de referencia. Por todo ello, en primer lugar, debemos indagar el nivel inicial y la necesidad de formar al profesorado en esta disciplina, Ciberseguridad. Para realizar este estudio, haremos una evaluación inicial de conocimientos en materia de Ciberseguridad a través de un cuestionario de autovaloración sobre las diferentes unidades de conocimiento integradas en el modelo ACM/IEEE/AIS SIGSEC/IFIP CYBERSECURITY CURRICULA 2017 (CSEC 2017) [10] y que consideramos que están relacionadas con este nuevo título. El objetivo final de dicho estudio será plantear un itinerario formativo para la formación de los docentes con el nuevo título en Ciberseguridad de manera que de respuesta a las necesidades reales y que permita adecuar los conocimientos y habilidades técnicas del profesorado a los retos planteados en la disciplina de la Ciberseguridad.

El articulo se ha estructurado en los siguientes apartados: en la Sección II daremos un vistazo al modelo de curriculum expuesto en CSEC 2017; a continuación, en la Sección III presentaremos el nuevo título en ciberseguridad; en la Sección IV describimos la metodología empleada para llevar a cabo el estudio; ya en la Sección V describiremos y analizaremos los datos obtenidos en el estudio; como consecuencia de los resultados obtenidos proponemos un itinerario formativo en la Sección VI, exponiendo a continuación una discusión en la Sección VII y finalmente en la Sección VIII presentaremos las conclusiones derivadas de este trabajo.

II. El modelo *CSEC 2017*

El Joint Task Force on Cybersecurity Education, conocido como CSEC 2017 JTF, surge de la necesidad de aunar fuerzas entre profesionales del entorno productivo y la sociedad científica en materia de computación para llevar a cabo el desarrollo exhaustivo de una guía curricular para la formación en materia de ciberseguridad. Esta iniciativa es el resultado de la colaboración entre las mayores sociedades internacionales de ciencias de la computación: Association for Computing Machinery (ACM), IEEE Computer Society (IEEECS), Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC), y la International Federation for Information Processing Technical Committee on Information Security Education.

Entre los destinatarios del modelo curricular propuesto se encuentran por una parte el profesorado de disciplinas basadas en la informática interesados en desarrollar o incorporar programas de Ciberseguridad, y por otra parte, la administración educativa con competencias para el desarrollo y revisión de programas formativos y cursos.

El marco curricular de ciberseguridad propuesto por CSEC 2017 JTF supone una guía para el desarrollo que incluye recomendaciones en la formación en Ciberseguridad y un esfuerzo por cualificar profesionales en ciberseguridad. Este modelo trata de alinear los programas académicos con las necesidades del mercado.

Este modelo incorpora dos tipos de habilidades a desarrollar:

- Por una parte tenemos las habilidades técnicas (hard-skills). En el modelo curricular propone tres dimensiones:
  1. Áreas de conocimiento y desglosadas en unidades de conocimiento que desprenden un total de 142 resultados de aprendizaje.
  2. Conceptos transversales que suponen los principios de la ciberseguridad: confidencialidad, integridad, disponibilidad, riesgo, pensamiento adversario y pensamiento sistémico.
  3. El desarrollo de las actuales disciplinas de computación: ciencias de la computación, ingeniería de computadores, sistemas de información, tecnología de la información e ingeniería del software.
- Por otra parte, tenemos las habilidades no-técnicas (soft-skills). Se trata de habilidades necesarias para el éxito de los profesionales de la ciberseguridad. Estaríamos hablando del trabajo en equipo, asignación adecuada de recursos, conciencia de la situación, trabajar con culturas heterogéneas. Podríamos añadir la capacidad de contabilizar, atención a los detalles, resiliencia, gestión de conflictos razonadamente, comunicación.

Este modelo trata de analizar la relación entre las demandas específicas en materia de ciberseguridad y la relación entre curriculum y el marco de referencia para el personal de ciberseguridad. La visión de este proyecto es aportar un recurso de contenido curricular en Ciberseguridad de forma integral para las instituciones académicas que pretendan ofrecer formación en ciberseguridad a nivel post-secundaria. De esta forma, CSEC 2017 JTF avanza la ciberseguridad como una nueva disciplina de computación, que se añade a las otras cinco ya existentes: Ingeniería Informática, Ciencias de la Computación, Sistemas de Información, Tecnologías de la Información, Ingeniería del Software.

III. Curso de Especialización: Ciberseguridad en entornos de las tecnologías de la información.

Este Real Decreto [7] está fundamentado en la necesidad de incluir en la FP del sistema educativo una profundización en el campo del conocimiento de los títulos de referencia o que suponen una ampliación de las competencias que se incluyen en los mismos. Estos nuevos títulos de especialización [7] pretenden *"dar una respuesta de forma rápida a las innovaciones que se produzcan en el sistema productivo así como a los ámbitos emergentes que complementen la formación incluida en los títulos de referencia"*.

En este caso en concreto, estamos ante un curso de especialización denominado *"Ciberseguridad en entornos de las tecnologías de la información"*, considerado en el nivel de FP de Grado Superior y con un total de 720 horas (43 ECTS). Pertenece a la familia profesional de Informática y Comunicaciones y se encuadra en la rama de conocimiento de Ingeniería y Arquitectura. Se accede desde los títulos de referencia de grado superior:

- Técnico Superior en Administración de Sistemas Informáticos en Red.
- Técnico Superior en Desarrollo de Aplicaciones Multiplataforma.
- Técnico Superior en Desarrollo de Aplicaciones Web.

- Técnico Superior en Sistemas de Telecomunicaciones e Informáticos.
- Técnico Superior en Mantenimiento Electrónico.

El objetivo general del título, recogido en [7]: *"consiste en definir e implementar estrategias de seguridad en los sistemas de información realizando diagnósticos de ciberseguridad, identificando vulnerabilidades e implementando las medidas necesarias para mitigarlas aplicando la normativa vigente y estándares del sector, siguiendo los protocolos de calidad, de prevención de riesgos laborales y respeto ambiental."*

Para el desarrollo de los contenidos, el curso se estructura en 6 módulos profesionales, cada uno con atribución para profesorado de los dos cuerpos docentes, tanto Profesores Técnicos de Formación Profesional (PTFP), correspondiente a la especialidad Sistemas y Aplicaciones Informáticas, como el cuerpo de Profesores de Enseñanza Secundaria (PES), de la especialidad de Informática. Las atribuciones del profesorado puede consultarse en la Tabla I.

Tabla I
ATRIBUCIÓN DE CUERPOS DOCENTES A MÓDULOS PROFESIONALES.

Cuerpo	Módulos profesionales
P.T.F.P.	Bastionado de redes y sistemas
	Puesta en producción segura
	Análisis forense informático
P.E.S.	Incidentes de ciberseguridad
	Hacking ético
	Normativa de ciberseguridad

IV. METODOLOGÍA

La metodología usada para recabar información relativa a las necesidades del profesorado está fundamentada en la realización de encuestas de opinión (Personal Opinion Surveys) [11][12]. El objetivo principal de encuesta es arrojar información de la situación actual respecto al nivel de conocimientos en materia de Ciberseguridad que presenta el profesorado de FP involucrado en los ciclos formativos correspondientes a la familia profesional de Informática y Comnunicaciones.

Definimos los pasos propuestos para llevar a cabo el estudio:

1. Seleccionar los objetivos.
2. Diseño del cuestionario.
3. Confección del cuestionario con la herramienta seleccionada.
4. Evaluar el instrumento empleado para el cuestionario.
5. Obtención de datos válidos.
6. Análisis de datos.

Selección del objetivo.

El estudio de situación respecto a las necesidades de formación que el profesorado que impartía docencia en los ciclos formativos de formación profesional de la familia profesional de Informática y Comunicaciones, profesorado objetivo de nuestro estudio.

Diseño del cuestionario.

Se diseñó un cuestionario basado en las unidades de conocimiento de CSEC 2017 JTF [10] que tenían relación con la nueva titulación en Ciberseguridad [7]. Este cuestionario está formado por 31 preguntas, cada una correspondía a una unidad de conocimiento con 5 posibles respuestas. Las respuestas están valoradas usando una escala de Likert, desde 1 (muy bajo) a 5 (muy alto). En el cuestionario se incluyó también el cuerpo docente al que pertenece el participante y la provincia en la que trabaja.

Confección del cuestionario con la herramienta seleccionada.

El instrumento seleccionado para llevar a cabo la recogida de datos fue un formulario electrónico (Google Forms).

Evaluación del cuestionario confeccionado mediante la herramienta seleccionada.

Previamente a lanzar dicho cuestionario, se llevaron a cabo varias pruebas por parte de un grupo cerrado de participantes para comprobar y verificar que la recepción de datos a través del cuestionario confeccionado era correcta.

Obtención de datos válidos.

Se envió el cuestionario mediante un enlace a través del correo electrónico, al profesorado objeto de este estudio en las 8 provincias de Andalucía. Se dejó un mes de plazo para cumplimentar el cuestionario.

Análisis de datos.

Sobre los resultados obtenidos y volcados a una hoja de cálculo, se realizó una valoración global de cada unidad de conocimiento para posteriormente centrar el análisis de resultados en la distribución de las 5 posibles respuestas (autovaloración de los niveles de conocimiento) relativas a cada cuestión planteada en el cuestionario.

En una primera fase de análisis, se determinaron aquellas unidades de conocimiento que suponían que más del 50 % de la muestra había reportado entre "1-muy bajo" y "2-bajo".

En la segunda fase, de valores totales de cada unidad de conocimiento se seleccionó por orden de menor a mayor puntuación las 10 unidades de conocimiento sobre las que el profesorado había reportado mayor desconocimiento.

V. ANÁLISIS DE RESULTADOS

Una vez obtenidos los resultados, recogidos en una hoja de cálculo, se procesan un total de 273 respuestas a cuestionarios (n=273) (ver Tabla III) procedentes de las ocho provincias de Andalucía. En el curso 2019/2020 hay un total de 1174 docentes del cuerpo de Profesores de Enseñanza Secundaria y 560 pertenecientes al cuerpo de Profesores Técnicos de Formación Profesional, lo que supone una población objetivo de 1734 [8]. Las respuestas obtenidas suponen un 15,75 %, teniendo en cuenta que no todos los docentes imparten clase en formación profesional, la tasa podría ser algo superior. Durante el presente curso 2020-2021, en los 11 centros educativos de Andalucía en los que se imparte la nueva titulación hay 56 docentes dedicados a estas enseñanzas, lo que indica que están dedicados al nuevo título un 3,23 %. Con estos datos se puede considerar la muestra como representativa y proporcionar validez a la muestra final.

La participación en el estudio ha sido heterogénea, ya que aparecen diferencias significativas en el número de cuestionarios respondidos en cada una de las diferentes provincias de Andalucía:

Referente a la distribución de la participación por cuerpos y especialidad (figura 1), los datos obtenidos son compatibles

Tabla II
PARTICIPACIÓN POR PROVINCIAS.

Provincia	% respuestas
Almería	15,9 %
Granada	4,8 %
Jaén	10,3 %
Málaga	19,6 %
Córdoba	3 %
Cádiz	4,1 %
Sevilla	38, 4 %
Huelva	4,1 %

con la dotación de personal por ciclo formativo, en la que los Profesores de Educación Secundaria es mayor a la de Profesores Técnicos de Formación Profesional. En los ciclos de grado superior la proporción es de 1PTFP/3PES mientras que en ciclos de grado medio es de 2PTFP/2PTFP.

Esta distinción del profesorado por cuerpos docentes no ha sido de mucha utilidad al no apreciar diferencias significativas entre los resultados obtenidos.

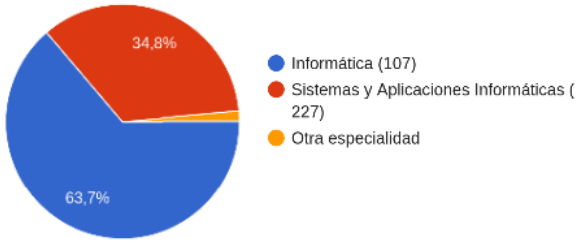

Figura 1. Participación del profesorado por cuerpo docente.

En un primer análisis de sobre cada una de las áreas de conocimiento, y con el objetivo de identificar aquellas unidades de conocimiento sobre las que existe un mayor desconocimiento, ponemos el foco de atención sobre aquellas en las que más del 50 % de la muestra había respondido con "muy bajo" o "bajo". Este dato supone que más de la mitad del profesorado reporta un nivel de muy bajo o bajo para esa unidad de conocimiento en cuestión. Esta primera identificación ya presenta la necesidad de incidir en la mejora a través de la actualización del profesorado en estos aspectos.

En la segunda fase de análisis de los resultados, se pretende determinar cuales son las 10 unidades de conocimiento, detalladas en la tabla IV, de entre las seleccionadas en la primera fase del análisis (tabla III) que obtienen menor puntuación absoluta lo que nos dará una priorización sobre las unidades de conocimiento reportadas como de mayor desconocimiento por parte de los docentes. Esta información obtenida nos servirá de ayuda para organizar las distintas necesidades formativas y el posterior diseño de un itinerario formativo en materia de ciberseguridad, de manera que se aumente el nivel de competencia del profesorado.

VI. PROPUESTA DE ITINERARIO FORMATIVO

Una vez obtenidos resultados cuantitativos sobre el problema planteado inicialmente en referencia a la necesidad de actualización del profesorado de Formación Profesional en materia de ciberseguridad, queremos proponer un itinerario formativo con estructura modular con la finalidad de dotar al profesorado de los conocimientos y habilidades necesarias para impartir docencia en esta materia. Los contenidos estarán estrechamente relacionados con los descritos en el nuevo Título [7].

Entendemos como itinerario formativo en ciberseguridad una serie de cursos o módulos formativos sobre unos temas concretos encaminados a mejorar la competencia necesaria en materia de ciberseguridad, haciendo especial hincapié en aquellos aspectos en los que se ha detectado, durante la realización de este estudio, una mayor necesidad de conocer, ya que el nivel de conocimiento reportado por los participantes en la investigación a través de sus valoraciones así lo refleja. Nuestra propuesta consta de un total de cuatro cursos y aunque recomendamos la realización secuencial y distinguiendo por cuerpos docentes (ver Figura 2). En el caso de los cursos de Hacking ético e Informática forense, en realidad no habría mayor problema en participar en todos ellos. El hecho de haber hecho distinción en estos dos cursos es por la atribución docente que se hace en cada módulo profesional a los cuerpos y especialidades recogidos en el título [7]. En este caso los PTFP de la especialidad de Sistemas y Aplicaciones Informáticas se le atribuye la docencia del módulo profesional de Informática forense, y a los PES de la especialidad de Informática el de Hacking ético. Los otros dos cursos siguientes, serían comunes a ambos cuerpos y especialidades.

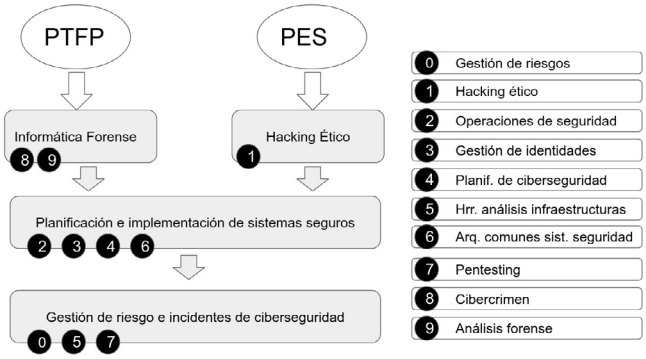

Figura 2. Itinerario formativo relacionado con unidades de conocimiento.

VI-A. Hacking ético

Objetivo: Aprender a utilizar herramientas de análisis y monitorización para detectar vulnerabilidades de sistemas aplicando técnicas de hacking ético.
Duración: 20 horas.
Contenidos:

- Fundamentos del hacking ético.
- Monitorización de sistemas informáticos.
- Ataques a sistemas informáticos y redes de comunicaciones. Escaneo y enumeración.
- Análisis de vulnerabilidades.
- Consolidación y uso de sistemas comprometidos.
- Auditoría de sistemas informáticos y redes.
- Ataques a sitos y aplicaciones web.

Recursos: Máquinas virtuales, software de monitorización de sistemas, sistemas operativos específicos, herramientas de detección y análisis de vulnerabilidades, conexión a Internet.

Tabla III
AUTOINFORME DEL PROFESORADO SOBRE ÁREAS Y UNIDADES DE CONOCIMIENTO.

Área de conoc.	Unidad de conocimiento	Muy bajo 1	Bajo 2	Inter 3	Alto 4	Muy alto 5
Seguridad de la información						
	Criptografía	0,17	0,30	0,26	0,22	0,06
	Informática forense	**0,41**	**0,32**	**0,17**	**0,07**	**0,03**
	Integridad de datos y Autenticación	0,19	0,30	0,32	0,16	0,04
	Control de acceso	0,20	0,31	0,29	0,16	0,04
	Protocolos de comunicación segura	0,16	0,29	0,31	0,16	0,07
	Privacidad de la información	0,14	0,25	0,34	0,22	0,06
	Seguridad en el almacenamiento de la información	0,14	0,27	0,28	0,25	0,07
Seguridad del software						
	Seguridad en el desarrollo del software	0,26	0,30	0,25	0,15	0,03
	Documentación y manuales	0,15	0,22	0,33	0,21	0,08
Seguridad de conexión						
	Arquitectura de sistemas distribuidos	0,30	0,31	0,24	0,11	0,04
	Arquitectura de red	0,12	0,23	0,32	0,21	0,12
	Servicios de red	0,11	0,19	0,29	0,27	0,13
	Defensa de red	0,25	0,31	0,26	0,13	0,04
Seguridad del sistema						
	Pensamiento sistémico	0,21	0,32	0,29	0,12	0,05
	Testeo de sistemas	0,25	0,33	0,26	0,13	0,03
	Arquitecturas comunes en sist. de seguridad	**0,35**	**0,35**	**0,19**	**0,08**	**0,02**
	Pentesting - Test de intrusión	**0,43**	**0,29**	**0,16**	**0,06**	**0,05**
Seguridad personal						
	Gestión de identidades	**0,32**	**0,33**	**0,21**	**0,11**	**0,02**
	Ingeniería social	0,28	0,30	0,27	0,11	0,03
	Implementación de medidas, reglas y políticas de seguridad en la organización	0,27	0,32	0,23	0,14	0,03
	Privacidad y seguridad de los datos personales	0,16	0,27	0,34	0,17	0,05
Seguridad organizacional						
	Gestión de riesgos	**0,28**	**0,33**	**0,24**	**0,12**	**0,03**
	Herramientas de análisis de infraestructuras	**0,36**	**0,33**	**0,19**	**0,09**	**0,03**
	Administración de sistemas	0,14	0,22	0,26	0,27	0,09
	Planificación de la ciberseguridad	**0,38**	**0,27**	**0,21**	**0,11**	**0,03**
	Continuidad de negocio, desastres y recuperación en la gestión de incidentes	0,28	0,33	0,22	0,14	0,03
	Operaciones de seguridad	**0,29**	**0,33**	**0,26**	**0,09**	**0,02**
Seguridad de la sociedad						
	Cibercrimen	**0,38**	**0,32**	**0,20**	**0,08**	**0,01**
	Legislación normativa sobre seguridad informática	0,27	0,33	0,27	0,09	0,03
	Privacidad de la información	0,19	0,32	0,30	0,14	0,04
	Hacking ético	**0,36**	**0,29**	**0,19**	**0,11**	**0,04**

Tabla IV
UNIDADES DE CONOCIMIENTO QUE OBTIENEN MENOR VALORACIÓN ABSOLUTA

Unidad de conocimiento	Valoración
Informática forense	544
Cibercrimen	546
Pentesting - Test de intrusión	548
Arquitecturas comunes en sistemas de seguridad	562
Herramientas de análisis de infraestructuras	570
Planificación de ciberseguridad	576
Gestión de identidades	586
Operaciones de seguridad	592
Hacking ético	596
Gestión de riesgos	617

VI-B. Informática forense

Objetivos: Aplicar metodologías de análisis forense distinguiendo las fases que intervienen en el proceso y elaboración de documentación de reporte.
Duración: 20 horas.
Contenidos:

- Fundamentos legales.
- Cibercrimen.
- Estándares.
- Fases del análisis forense. Metodología.
- Proceso de investigación. Adquisición, conservación y custodia de evidencias.
- Análisis de evidencias en sistemas Windows y Linux.
- Análisis forense de Navegadores de Internet.
- Análisis forense de correo electrónico.
- Análisis forense de dispositivos móviles.
- Análisis forense en cloud.
- Análisis forense en entornos IoT.
- Elaboración de informes periciales.

Recursos: Máquinas virtuales, software específico de investigación y análisis forense (Kits de análisis forense y herramientas de fines específicos), conexión a Internet.

VI-C. Planificación e implementación de sistemas seguros

Objetivos: Planificar y diseñar la securización de sistemas informáticos considerando los dispositivos y entornos disponibles.
Duración: 30 horas.
Contenidos:

- Diseño de plan de seguridad.
- Sistemas de acceso y credenciales.
- Diseño de redes seguras.
- Configuración de dispositivos y sistemas.

- Análisis de infraestructuras.
- Implementación de hardening en aplicaciones web.

Recursos: Máquinas virtuales, software específico de análisis y monitorización de sistemas y redes, conexión a Internet.

VI-D. Gestión de riesgos e incidentes de ciberseguridad

Objetivos: Desarrollar planes de prevención y concienciación en ciberseguridad estableciendo normas y medidas de protección.
Duración: 30 horas.
Contenidos:

- Planes de prevención y concienciación.
- Auditoría de seguridad.
- Investigación de incidentes.
- Monitorización. Detección de incidentes.
- Implementación de medidas.
- Documentación e informes.
- Gestión de conformidad (compliance).

Recursos: Máquinas virtuales, software de auditoría de seguridad informática y de investigación de evidencias así como monitorización de sistemas, documentación específica sobre compliance y conexión a Internet.

VII. Discusión

Aunque se esperaba una formación específica para el profesorado de Andalucía con atribución docente en esta nueva titulación sobre ciberseguridad por parte de la administración educativa, finalmente no fue posible llevarla a cabo antes de que iniciara el curso académico con unos resultados adecuados. Se organizó una actividad formativa de 40 horas de duración entre los meses de octubre y noviembre, la cual no consiguió dar respuesta a las necesidades formativas de los docentes debido a la poca profundidad en el tratamiento de los contenidos y la falta de especialización en cada uno de los contenidos propuestos y relacionados con la nueva titulación. Posteriormente se pusieron en marcha dos cursos, a pesar de que el profesorado manifestaba preferencia por realizar un curso por módulo profesional, paralelos en el tiempo y de 48 horas de duración cada uno, agrupando los contenidos de los seis módulos profesionales que componen la nueva titulación en ciberseguridad. Por una parte - CIBERSEGURIDAD: PUESTA EN PRODUCCIÓN SEGURA. INCIDENTES.BASTIONADO - y por otra - CIBERSEGURIDAD: FORENSE. HACKING ÉTICO. NORMATIVA - ambos cursos en modalidad online y comprendidos entre los meses de noviembre de 2020 y marzo de 2021. Pero la abundancia y complejidad de los contenidos en todo su conjunto, junto con la dificultad de encontrar empresas con dilatada experiencia en el sector de la ciberseguridad, que a su vez estuvieran dispuestas a realizar la formación del profesorado en estos plazos, dio lugar al retraso en el desarrollo del mismo. El hecho de no conseguir dar solución eficaz a las necesidades formativas del profesorado a nivel regional en toda Andalucía, ha llevado a planificar más acciones formativas para tratar de dar una respuesta adicional y conseguir dotar al profesorado de los recursos necesarios en materia de ciberseguridad, esta iniciativa destinada al profesorado de la provincia de Cádiz, ha llevado a organizar dos actividades formativas sobre ciberseguridad, una de ellas de HACKING ÉTICO, de 20 horas de duración, y una segunda actividad sobre BASTIONADO DE REDES Y SISTEMAS, de 25 horas. Una alternativa posible, pero no contemplada hasta la fecha, habría sido acudir a las universidades donde se imparten algunos de los cursos de máster en ciberseguridad, proporcionando una formación validada. Todo el profesorado implicado en la docencia de esta nueva titulación está haciendo un gran esfuerzo por conseguir la formación que consideran que necesitan (mediante sus propios medios y recursos en muchos casos) para estar a la altura de las circunstancias y del nivel que el mercado laboral espera de los futuros profesionales. Cabe realizar algunas preguntas que nos ayuden a la reflexión. ¿Cuál es el coste que está dispuesto a asumir una organización educativa por no dotar de la formación adecuada a sus profesionales docentes? ¿Repercute de algún modo en el aula los éxitos y fracasos en la formación del profesorado? ¿Es eficaz y eficiente la Red de Formación del Profesorado en Andalucía ante los retos que supone implantar una nueva titulación de Formación Profesional? ¿Existe la colaboración necesaria dentro de la propia Administración para materializar estos proyectos?

VIII. Conclusiones

A través de este estudio se ha indagado en el nivel de conocimientos sobre Ciberseguridad entre el profesorado de FP de de la familia profesional de Informática y Comunicaciones en Andalucía, relacionando la propuesta de diseño curricular en ciberseguridad CSEC 2017 JTF, con la necesidad de actualización y formación del profesorado susceptible de estar implicado en la nueva titulación en ciberseguridad: Curso de Especialización en Ciberseguridad en entornos de las tecnologías de la información.

Se ha obtenido la relación de unidades de conocimiento, según el modelo CSEC2017 JTF sobre las que se recomienda implementar un itinerario formativo de forma prioritaria, a ser posible antes de la implantación del nuevo título formativo. Esto implica que el profesorado relacionado con estas nuevas titulaciones debe llevar a cabo un esfuerzo adicional para la actualización de sus competencias profesionales específicas, con el objeto de desarrollar planes de formación relacionados con la ciberseguridad.

Se propone un itinerario formativo para ambos cuerpos docentes, Profesores Técnicos de Formación Profesional (PTFP) de la especialidad de Sistemas y Aplicaciones Informáticas así como de Profesores de Enseñanza Secundaria (PES) de la especialidad de Informática, acorde con las módulos profesionales, incluidos en la nueva titulación, sobre la que tienen competencia docente.

De los resultados desprendidos en este estudio, estaríamos en disposición de planificar la formación necesaria de los profesionales docentes, de forma que garantice una enseñanza de calidad para los futuros profesionales en el campo de la ciberseguridad que el sector productivo está demandando y que, a fecha de hoy, no consigue dar solución a todas sus necesidades de personal especializado.

Agradecimientos

A todos los profesionales docentes dedicados a la Formación Profesional y que han contribuido a la realización de este trabajo. Este trabajo ha sido parcialmente financiado por el Ministerio de Ciencia y Tecnología de España a

través del project ECLIPSE (RTI2018-094283-B-C33), y la Junta de Andalucia mediante el projecto the METAMORFOSIS, los fondos European Regional Development Fund (ERDF/FEDER).

Referencias

[1] Yadav, T., Rao, A.M.: Technical aspects of cyber kill chain. In: J.H. Abawajy,1086S. Mukherjea, S.M. Thampi, A. Ruiz-Martínez (eds.) Security in Computing1087and Communications, pp. 438–452. Springer International Publishing, Cham1088 (2015).

[2] B. Ramos, "Se necesitan urgentemente expertos en ciberseguridad: ¿Qué estudiar para ser uno de ellos?", en *EL PAÍS, 2020*. [Online]. Available: https://elpais.com/economia/2019/01/14/actualidad/1547486152_048652.html. [Accedido: 03-Mar-2020].

[3] Diario Siglo XXI, "España necesita profesionales de la ciberseguridad", 2020. [Online]. Available: http://www.diariosigloxxi.com/texto-diario/mostrar/1629553/espana-necesita-profesionales-ciberseguridad. [Accedido: 03-Mar-2020].

[4] Wyser Spain. (2018, September 28). Demanda de expertos en ciberseguridad. Wyser Spain. Retrieved from https://bit.ly/2JQSTr0

[5] Ramírez, V. (2019, January 4). Alemania: El "Bundestag"sufre el mayor hackeo de su historia. CyberSecurity News. Retrieved from https://bit.ly/3aZr1g9

[6] Basallo, A. (2018, July 18). Existen más puestos de trabajo en el sector de Ciberseguridad que profesionales formados. *UNIR Revista*. Retrieved from https://bit.ly/3eaRB8f

[7] Ministerio Educación y Formación Profesional (Ed.)(2020). Real Decreto Curso de Especialización: Ciberseguridad en entornos de tecnologías de la información. TodoFP. Retrieved from https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-4963

[8] Junta de Andalucía - Recursos humanos del sistema educativo en Andalucía. (2021). [Online]. Available: https://www.juntadeandalucia.es/organismos/educacionydeporte/servicios/estadistica-cartografia/actividad/detalle/175115/175501.html

[9] Ministerio de Educación y Formación Profesional (Ed)(2019). I Plan Estratégico de Formación Profesional del Sistema Educativo 2019-2020. Ministerio de Educación y Formación Profesional. [Online] Available: https://www.todofp.es/dam/jcr:163978c0-a214-471e-868d-82862b5a3aa3/plan-estrategico--enero-2020.pdf

[10] CSEC2017-JTF. (Ed.)(2017). Cybersecurity Curricula 2017. *A Report in the Computing Curricula Series Joint Task Force on Cybersecurity Education*. https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf

[11] Shull, F., Singer, J. and Sjoberg, D. (2008). *Guide to advanced empirical software engineering*. London: Springer London. https://doi.org/10.1007/978-1-84800-044-5

[12] Wohlin, C., Runeson, P., Höst, M., Ohlsson, M., Regnell, B. and Wesslén, A. (2012). *Experimentation in software engineering*. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-29044-2

[13] Bailetti, T., & Craigen, D. (2020). Examining the relationship between cybersecurity and scaling value for new companies. *Technology Innovation Management Review*, 10(2), 62-70. https://doi:10.22215/timreview/1329

[14] Soblechero, M. V. L., Gaya, C. G., & Ramírez, J. J. H. (2014). A comparative study of classroom and online distance modes of official vocational education and training. *PLoS ONE*, 9(5). https://doi:10.1371/journal.pone.0096052

[15] González-Manzano, L., & de Fuentes, J. M. (2019). Design recommendations for online cybersecurity courses. Computers & Security, 80, 238–256. https://doi.org/10.1016/j.cose.2018.09.009

[16] Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 35(6), 105336. https://doi.org/10.1016/j.clsr.2019.06.007

[17] Muller, J. (2015). The future of knowledge and skills in science and technology higher education. Higher Education, 70(3), 409–416. https://doi.org/10.1007/s10734-014-9842-x

[18] Gallego-Arrufat, M., Torres-Hernández, N., & Pessoa, T. (2019). Competence of future teachers in the digital security area. [Competencia de futuros docentes en el área de seguridad digital]. *Comunicar*, 61, 57-67. https://doi.org/10.3916/C61-2019-05

[19] Engen, B.K. (2019). Understanding social and cultural aspects of teachers' digital competencies. [Comprendiendo los aspectos culturales y sociales de las competencias digitales docentes]. *Comunicar*, 61, 9-19. https://doi.org/10.3916/C61-2019-01

[20] Fang, B., Ren, K., Jia, Y. (2018). The New Frontiers of Cybersecurity. *Engineering*, 4(1), 1-2. https://doi:10.1016/j.eng.2018.02.007

[21] Ávila, J.A. & Tello, J. (2004). Reflections on curricular integration of new communication technologies. [Reflexiones sobre la integración curricular de las tecnologías de la comunicación]. *Comunicar*, 22, 177-182. https://doi.org/10.3916/C22-2004-27

[22] Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. Computers & Security, 75, 24–35. https://doi.org/10.1016/j.cose.2018.01.015

[23] Colás-Bravo, P., Conde-Jiménez, J., & Reyes-de-Cózar, S. (2019). The development of the digital teaching competence from a sociocultural approach. [El desarrollo de la competencia digital docente desde un enfoque sociocultural]. *Comunicar*, 61, 21-32. https://doi.org/10.3916/C61-2019-02

[24] Hodhod, R., Khan, S., & Wang, S. (2019). CyberMaster: An expert system to guide the development of cybersecurity curricula. *International Journal of Online and Biomedical Engineering*, 15(3), 70-81. https://doi:10.3991/ijoe.v15i03.9890

[25] Buckley, I. A., & Zalewski, J. (2019). Course development in the cybersecurity curriculum. Paper presented at *the Proceedings of the LACCEI International Multi-Conference for Engineering, Education and Technology*. https://doi:10.18687/LACCEI2019.1.1.238

[26] Duffany, J. L. (2019). Developing cybersecurity skills in intermediate programming courses. Paper presented at the *Proceedings of the LACCEI International Multi-Conference for Engineering, Education and Technology*. https://doi:10.18687/LACCEI2019.1.1.414

[27] Imbernón, F., Silva, P., & Guzmán, C. (2011). Teaching skills in virtual and blended learning environments. [Competencias en los procesos de enseñanza-aprendizaje virtual y semipresencial]. *Comunicar*, 36, 107-114. https://doi.org/10.3916/C36-2011-03-01

[28] Gordillo, A., López-Pernas, S., & Barra, E. (2019). Effectiveness of MOOCs for teachers in safe ICT use training. [Efectividad de los MOOC para docentes en el uso seguro de las TIC]. *Comunicar*, 61, 103-112. https://doi.org/10.3916/C61-2019-09

[29] Velandia-Mesa, C., Serrano-Pastor, F., & Martínez-Segura, M. (2017). Formative research in ubiquitous and virtual environments in Higher Education. [La investigación formativa en ambientes ubicuos y virtuales en educación superior]. *Comunicar*, 51, 09-18. https://doi.org/10.3916/C51-2017-01

[30] Rego-Agraso, L. (2018). Vocational training schools and its relationship with the community: Perspective of trainers and trainees. [Los centros de formación profesional y su vinculación con el entorno: La perspectiva de alumnado y profesorado] .*Revista Complutense De Educación*, 29(3), 683-697. https://doi:10.5209/RCED.53622

[31] Dameff, C. J., Selzer, J. A., Fisher, J., Killeen, J. P., & Tully, J. L. (2019). Clinical Cybersecurity Training Through Novel High-Fidelity Simulations. The Journal of Emergency Medicine, 56(2), 233–238. https://doi.org/10.1016/j.jemermed.2018.10.029

[32] Tynjälä, P., Välimaa, J., & Sarja, A. (2003). Pedagogical perspectives on the relationships between higher education and working life. Higher Education, 46(2), 147–166. https://doi.org/10.1023/A:1024761820500