Perspectiva de la Ciberseguridad en el Grado de Ingeniería Informática de la ESI en la UCLM

Antonio Santos-Olmo[1], David G. Rosado[1], Luis E. Sánchez[1], Carlos Blanco[2], Manuel A. Serrano[1], Eduardo Fernández-Medina[1]
[1] Dpto. de Tecnologías y Sistemas de Información, Universidad de Castilla-La Mancha
[2] Dpto. de Ingeniería Informática y Electrónica. Universidad de Cantabria
Antonio.SantosOlmo@uclm.es, David.GRosado@uclm.es, LuisE.Sanchez@uclm.es, Carlos.Blanco@unican.es, Manuel.Serrano@uclm.es, Eduardo.FdezMedina@uclm.es

Resumen

En este artículo se presenta el Marco de Competencias para Programas Superiores de Formación Especializada en Ciberseguridad y se analiza el nivel de cobertura actual de estas competencias por parte del actual Grado en Ingeniería Informática de la Escuela Superior de Informática (ESI) de Ciudad Real (Universidad de Castilla-La Mancha) y se hace una propuesta de adaptación de este grado para alcanzar un mejor cumplimiento de las competencias de dicho marco, y sin proponer por el momento la creación de una intensificación específica de Ciberseguridad, que sería la mejor opción, pero requiere un diseño más profundo.

Abstract

This article presents the Competence Framework for Higher Specialised Training Programmes in Cybersecurity and analyses the current coverage of these competences by the current Bachelor's Degree in Computer Engineering of the Computer Science School of Ciudad Real (University of Castilla-La Mancha), and suggests a proposal to adapt this degree to achieve better compliance with the competences of this framework, without proposing the creation of a concrete specialisation in Cybersecurity for the time being, which would be the best option, but it requires a more complex design.

Palabras clave

Ciberseguridad, plan de estudios, marco de competencias, cumplimiento de competencias.

1. Introducción

La ciberseguridad es una disciplina altamente demandada por la industria nacional e internacional de la informática, requiriendo profesionales con una formación específica y ofreciendo condiciones laborales muy favorables. Sin embargo, en España todavía no existe una estructura de formación adecuada que alimente esta alta demanda de profesionales, salvo por la existencia de diversos másteres y algún grado en ciberseguridad, valiosos, pero construidos sin una adecuación a un marco de competencias en ciberseguridad de referencia y con reconocimiento en España. Es cierto que a nivel internacional han aparecido en los últimos años diversos cuerpos de conocimiento y marcos de referencia en ciberseguridad que definen las bases de la disciplina. Quizás los tres hitos más relevantes en este sentido sean los siguientes: i) La incorporación de un nuevo currículum de Ciberseguridad en el *Computing Curricula* de ACM e IEEE [1], que complementa la clásica estructura de cinco currículums, ii) La creación de uno de los marcos de referencia en ciberseguridad más utilizados, creado por el NIST, con la colaboración del sector privado americano y organizaciones académicas, el *National Initiative for Cibersecurity Education* (conocido como NICE) [4], que define un conjunto de puestos de trabajo específicos en ciberseguridad, indicando tareas, conocimientos, habilidades y capacidades para cada uno de ellos, y iii) la aparición, también desde Estados Unidos de CyBOK, el Cuerpo de Conocimiento en Ciberseguridad [2], elaborado por el *National Cyber Security Centre* y que presenta de manera muy detallada una organización de categorías de conocimiento subdivididas en áreas de conocimiento, y éstas a su vez en temas.

Pero a nivel nacional, lo realmente significativo es que el Foro Nacional de Ciberseguridad, como órgano de asistencia al Consejo de Seguridad Nacional, ha elaborado el Marco de Competencias para Programas Superiores de Formación Especializada en Ciberseguridad [3], un marco de competencias en ciberseguridad completo, profundo, detallado y consensuado con la industria. Este marco de competencias está planteado como marco de referencia para la definición de planes de estudio de programas

superiores de formación (grado y máster) en ciberseguridad en España, y toma como referencia esos marcos y cuerpos de conocimiento que mencionábamos antes, entre otros. Este marco está especialmente diseñado para poder crear nuevos planes de estudio, tanto de grado como de máster, que estén especializados en ciberseguridad. Sin embargo, como es de esperar, los actuales títulos de grado en Ingeniería Informática, diseñados hace más de una década, y habiendo tenido que acoplar múltiples y variadas competencias, no cumplen muy bien estas competencias, siendo necesario, como mínimo unos reajustes en dichos planes de estudio, a falta de apuestas que no tardarán, como la creación de intensificaciones específicas de ciberseguridad en los grados de ingeniería informática, o incluso grados y másteres completos de ciberseguridad.

En este artículo se realiza un análisis del cumplimiento de competencias del marco indicado anteriormente, por parte del grado en Ingeniería Informática de la Escuela Superior de Informática (ESI) de Ciudad Real (UCLM), extrayéndose interesantes conclusiones sobre las actuales asignaturas con contenidos en ciberseguridad y sobre el cumplimiento de las competencias del marco, haciendo finalmente una propuesta sobre cómo se podrían realizar ajustes (no rediseños completos) del grado, que permitirían mejorar mucho el cumplimiento de estas competencias.

El resto del artículo está organizado como se indica a continuación: La sección 2 presenta la información de contexto sobre el grado en cuestión y sobre las asignaturas que actualmente se imparten con contenidos en ciberseguridad. En la sección 3 se presentan y resumen las principales características del Marco de Competencias para Programas Superiores de Formación Especializada en Ciberseguridad elaborado por el Foro Nacional de Ciberseguridad, indicando la organización de competencias planteada. En la sección 4 se realiza el análisis de cumplimiento de competencias en el grado en cuestión y en la 5 la propuesta de ajuste sobre el grado. Por último, en la sección 6 se presentan las principales conclusiones del trabajo.

2. Contexto del análisis

2.1. El grado en cuestión

El contexto sobre el que llevamos a cabo este análisis es el Grado en Ingeniería Informática de la ESI de la UCLM. Este grado está implantado en tres centros distintos (además de Ciudad Real, también en Talavera de la Reina y Albacete), pero con diferentes optativas e intensificaciones implantadas, motivo por el cual nos centraremos solamente en uno de los tres centros, en lugar de hacer el estudio general a nivel del grado completo en los tres centros.

En concreto, el grado cuenta con 240 ECTS, de los que 60 son créditos de asignaturas de formación básica, 96 son de asignaturas obligatorias, 72 son ECTS optativos y 12 son créditos destinados a realizar el trabajo fin de grado. Los 72 ECTS optativos se organizan en la elección por parte del estudiante de una de entre cuatro menciones disponibles (Ingeniería del Software, Ingeniería de Computadores, Computación y Tecnologías de la Información), cada una organizada en 8 asignaturas de 6 créditos, dando un total de 48 créditos en cada mención, y los 24 restantes se consiguen mediante asignaturas optativas (actualmente se ofertan 10, todas ellas de 6 ECTS) y mediante prácticas en empresa optativas por un total de 12 ECTS.

La configuración actual del grado hace que los estudiantes cursen las 10 asignaturas (60 ECTS) de formación básica, las 12 asignaturas (72 ECTS) de formación obligatoria, que elijan y cursen de manera excluyente las 8 asignaturas (48 ECTS) de una mención, que completen 24 ECTS optativos bien a través de elegir 4 asignaturas optativas, o bien eligiendo solo 2 optativas y realizando las prácticas en empresa, y, por último, que realicen el trabajo fin de grado.

2.2. Asignaturas sobre ciberseguridad

En el grado en cuestión, existe un total de 5 asignaturas con contenidos claramente de ciberseguridad, aunque hay otras asignaturas que pueden contener también algunos aspectos relacionados.

En concreto, las asignaturas sobre ciberseguridad son las siguientes:

- Seguridad de Sistemas Software, en la mención de Ingeniería del Software.
- Seguridad en Redes, en la mención de Ingeniería de Computadores.
- Seguridad en Sistemas Informáticos, en la mención de Tecnologías de la Información.
- Auditoría de Sistemas de Información, optativa.
- Análisis Forense Informático, optativa.

Sin embargo, aunque hay 5 asignaturas sobre ciberseguridad, ninguna de ellas se ubica en los bloques de asignaturas obligatorias, por lo que los estudiantes pueden obtener el grado en ingeniería informática sin haber cursado un solo ECTS sobre ciberseguridad (en el caso de cursar la mención de Computación). De hecho, 2 de las 5 asignaturas son optativas, y las otras 3 están repartidas en 3 de las 4 menciones que, de manera exclusiva pueden elegir los estudiantes.

Por lo tanto, desde el punto de vista de la formación en ciberseguridad en este grado, el peor de los casos viene dado cuando un estudiante elije la mención de Computación, que no tiene ninguna asignatura de ciberseguridad y no elije ninguna optativa de ciberseguridad, y el mejor de los casos se da cuando

el estudiante cursa alguna de las tres menciones que cuentan con una asignatura de ciberseguridad, y se cursan además, las dos optativas disponibles, alcanzando un total de 18 créditos sobre materias de ciberseguridad. El caso más frecuente es que los estudiantes acaben cursando una de las tres menciones, y además cero o una optativa de ciberseguridad, cursando por tanto entre 6 y 12 créditos de ciberseguridad.

3. El marco de competencias

3.1. El Foro Nacional de Ciberseguridad

Se comenzará indicando que el marco de competencias considerado ha sido elaborado por el Foro Nacional de Ciberseguridad, que se constituyó en 2020 con el objetivo de fomentar la cultura de ciberseguridad, ofrecer apoyo a la Industria e I+D+i y promover la formación y el talento, a través de un entorno de colaboración público-privada y siendo un órgano de asistencia al Consejo Nacional de Ciberseguridad, en su condición de órgano de apoyo del Consejo de Seguridad Nacional. El foro está compuesto por representantes de la sociedad civil, expertos independientes, sector privado, la academia, asociaciones (como por ejemplo la Red de Excelencia Nacional de Investigación en Ciberseguridad), y organismos sin ánimo de lucro, entre otros.

El Foro Nacional de Ciberseguridad se vertebra a través de 5 grupos de trabajo, i) de cultura de ciberseguridad, ii) de impulso a la industria y a la I+D+i, iii) de formación, capacitación y talento, iv) de análisis e impulso a la industria de ciberdefensa, y v) de regulación, siendo el grupo de trabajo de formación, capacitación y talento el que se ocupó de realizar un exhaustivo análisis previo de marcos y cuerpos de conocimiento internacionales sobre ciberseguridad y finalmente de la construcción del Marco de Competencias para Programas Superiores de Formación Especializada en Ciberseguridad.

3.2. El proceso de creación del marco

Previo a la definición del marco de competencias, se puede ver en [3], un resumen de los marcos internacionales más relevantes (también incluidas algunas propuestas fruto de proyectos europeos relevantes), y un análisis muy pormenorizado del marco curricular de ACM e IEEE en ciberseguridad, analizando la composición de las distintas áreas de conocimiento, y profundizando en cómo son cubiertas estas áreas de conocimiento y sus contenidos por parte de la oferta actual de grados y másteres con contenidos en ciberseguridad en España. Este análisis es considerado como el punto de partida para la construcción del marco de competencias, junto a una identificación de áreas en base al modelo NICE. Pero además de basarse en los marcos internacionales más relevantes, se pretendía unir al máximo el lenguaje académico con el profesional, y sobre todo, tener una visión realista del presente y futuro de la ciberseguridad con la mirada de los potenciales empleadores. Para ello, se preparó un formulario para la recogida de información de personas con perfiles especializados de una muestra completa de las organizaciones y sectores más relevantes en ciberseguridad en España. Esta muestra incluyó 95 entidades tanto del sector privado (consultoras de gran tamaño, consultoras especializadas, ingenierías, fábricas de software y empresas de desarrollo fabricantes y proveedores del sector de la ciberseguridad, banca, seguros, operadores de telecomunicaciones, etc.) como del sector público (administración central, autonómica, local, justicia, sanidad, educación, fuerzas armadas, fuerzas y cuerpos de seguridad del Estado, etc.).

El objetivo fundamental era recoger información sobre las actividades y tareas que necesitarán realizar los profesionales de la ciberseguridad en el medio o largo plazo, investigando sobre las competencias más adecuadas para los futuros planes de estudio especializados en función de los perfiles que los empleadores van a necesitar.

Así, en el formulario se mostraron las 10 funciones o áreas de ciberseguridad consideradas, y un conjunto de tareas o actividades elaboradas en base a la propuesta NICE, de modo que cada organización indicaba en qué medida esas tareas serían necesarias en su sector u organización, independientemente de la denominación que pueda tener el puesto o rol de la persona que se tenga que ocupar. También se pedía en el formulario, que priorizaran las 10 áreas de ciberseguridad según la importancia para la organización (indicando una puntuación variable). El detalle sobre el formulario de recogida de información se encuentra en el anexo I del propio marco de competencias [3].

En paralelo al proceso anterior, los integrantes del grupo de trabajo de formación, capacitación y talento trabajaron en la identificación de un conjunto de competencias específicas asociadas a las tareas y actividades listadas en cada función de ciberseguridad.

Con ello, se obtuvieron las competencias base para que un profesional pueda llevar a cabo cada una de esas tareas o actividades, y una vez recibidas las respuestas de los formularios, se pudieron priorizar unas competencias frente a otras, descartando algunas, identificando otras nuevas, compactando, dividiendo, etc. Finalmente se racionalizó el número de competencias de cada área (buscando un número objetivo de entre 10 y 20 competencias por área), siendo éstas las necesarias para realizar las tareas y actividades más importantes para los sectores y organizaciones de la muestra, que en realidad representan a la globalidad.

3.3. Contenido del marco

El marco de competencias está formado por 83 competencias específicas en total, repartidas entre las 10 áreas o funciones de ciberseguridad que se muestran en la Figura 1, donde, además, se presentan estas áreas con la indicación del número de puntos resultado de sumar la prioridad o importancia expresada por cada uno de los integrantes de la muestra de organizaciones que contestó el formulario. Así, las entidades consultadas, han considerado, por ejemplo, que el área relativa a responsabilidad y dirección de ciberseguridad es el doble de prioritaria o importante que el área de investigación. Para más detalle sobre el contenido del marco de competencias, recomendamos al lector dirigirse a la fuente original [3].

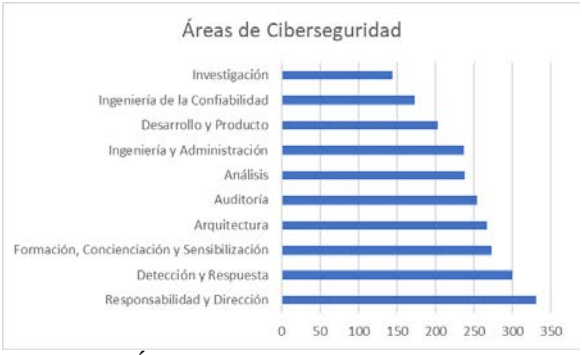

Figura 1. Áreas de ciberseguridad.

De entre todas las competencias, las hay exclusivas de una única área (por ejemplo, la competencia CE21 "Utilizar los principios y métodos de seguridad y confiabilidad en procesos de ingeniería del software para producir software seguro desde el diseño", que está vinculada con el área de "Desarrollo y Producto"), o bien otras competencias que están relacionada con varias áreas (por ejemplo, la competencia CE16 "Interpretar y aplicar las leyes, las regulaciones, las políticas y principios éticos en relación con la ciberseguridad y la confiabilidad", que se vincula con 6 de las áreas consideradas).

Además de estas 83 competencias, el marco también define un conjunto de 64 prerrequisitos o conocimientos previos necesarios que los estudiantes deben cumplir para cursar estas materias, y un conjunto de 25 competencias básicas, aunque también esenciales, relativas a *soft skills* o competencias blandas, necesarias en la mayoría de los puestos del ámbito de la ciberseguridad.

3.4. Objetivo del marco de competencias

Lo que pretende este marco de competencias es ayudar a las instituciones académicas a crear sus planes de estudio de grado o máster en ciberseguridad, para lo que se proporciona el siguiente conjunto de fases, con la recomendación de material a utilizar:

1. Decidir el perfil de los egresados de la titulación: Se puede utilizar los resultados de la consulta de los potenciales empleadores, entre otras muchas fuentes para tomar esta decisión.
2. Identificar las competencias básicas y generales: Se puede utilizar el listado de competencias básicas.
3. Identificar las competencias específicas: Se puede utilizar el listado de competencias específicas.
4. Agrupar competencias en materias: Se puede utilizar el marco curricular de ACM e IEEE y el análisis de la sección 4 del marco de competencias.
5. Definir asignaturas en materias: Se puede utilizar el marco curricular de ACM e IEEE y el análisis de la sección 4 del marco de competencias.
6. Desarrollar contenidos de las asignaturas: Se puede utilizar el marco curricular de ACM e IEEE y el análisis de la sección 4 del marco de competencias.
7. Establecer prerrequisitos de asignaturas. Se puede utilizar el listado de prerrequisitos definidos en el marco de competencias.

Incluso se proporcionan algunos ejemplos ilustrativos sobre cómo utilizar el documento en el proceso de diseño de planes de estudio.

4. Cumplimiento de competencias

Las asignaturas en cuestión están definidas en términos de un conjunto de competencias (se pueden ver en la memoria del grado y en las fichas de las asignaturas, ambas en https://esi.uclm.es/, y, además, están extraídas de las *Fichas* de Ingeniería Informática[1]), objetivos o resultados de aprendizaje, y un temario con los contenidos. Dado que las competencias del grado no tienen mucho contenido de ciberseguridad, y están mezcladas de muchos tipos (básicas, personales, de la universidad, etc.), mostraremos aquí los resultados de aprendizaje de las asignaturas, aunque para el análisis que hemos realizado, nos hemos basado en la unión de, competencias, resultados de aprendizaje y de los contenidos de los temarios:

- Seguridad de Sistemas Software (SSS): i) Identificar, modelar e integrar los requisitos de seguridad del software en el proceso de su desarrollo. ii) Conocer las normas, estándares y legislación más relevante sobre seguridad del software. iii) Conocer las principales técnicas y servicios de seguridad del software.

[1] Resolución 8 de junio de 2009, de la Secretaría General de Universidades, con recomendaciones para memorias de títulos oficiales en los ámbitos de la Ingeniería Informática, Ingeniería Técnica Informática e Ingeniería Química.

- Seguridad en Redes (SR): i) Explicar y aplicar los principios de seguridad necesarios para proteger a una red y a los dispositivos en ella incluidos. ii) Diseñar, implantar y configurar el acceso remoto seguro.
- Seguridad en Sistemas Informáticos (SSI): i) Gestionar la seguridad en sistemas informáticos. ii) Identificar vulnerabilidades del sistema informático, analizar y clasificar ataques. iii) Diseñar planes de seguridad y contingencia en Centros de Procesos de Datos. iv) Utilizar técnicas de codificación y criptografía para proteger la información. v) Conocer las últimas técnicas en seguridad en las transacciones, así como la legislación vigente en cuanto a protección de datos. vi) Configurar redes seguras empleando firewalls y redes privadas virtuales.
- Auditoría de Sistemas de Información (ASI): i) Conocer y saber aplicar las principales técnicas y metodologías de control interno y auditoría de sistemas de información. ii) Conocer el entorno jurídico de la auditoría de sistemas de información, así como las principales áreas de auditoría de sistemas de información, y tener destrezas en el uso de herramientas para la auditoría.
- Análisis Forense Informático (AFI): i) Conocer e identificar amenazas de seguridad, analizar las consecuencias, y diseñar sistemas de prevención equilibrando la relación coste/beneficio para una aplicación dada.

El Cuadro 1 muestra un extracto del análisis realizado sobre el cumplimiento de competencias por parte de las 5 asignaturas consideradas, solo con las 10 primeras competencias (por motivos de espacio no se muestra el cuadro completo). Se debe aclarar que, se ha considerado el cumplimiento de competencias en términos muy relativos, entendiendo que una competencia del marco está cubierta por alguna asignatura cuando es abordada al menos de manera parcial. Así, no debemos considerar que nos estamos refiriendo al cumplimiento *completo* de las competencias del marco, algo que sería solo alcanzable en el despliegue de títulos de grado o máster creados exprofeso en base a estas competencias.

Así, se puede observar que cada competencia está vinculada a una o varias áreas de ciberseguridad. Por ejemplo, la competencia CE1 (“Recolectar y definir las capacidades y requisitos de seguridad de los sistemas”) forma parte de la dimensión de “Arquitectura” y también de “Desarrollo y Producto”. También se puede observar que cada asignatura cubre diversas competencias, a menudo de manera repetida. Por ejemplo, las asignaturas SSS, SR y SSI, cumplen (parcialmente) la competencia CE3 (“Aplicar y analizar la aplicación de los principios básicos de la ciberseguridad y la privacidad durante el desarrollo, despliegue, instalación, integración, mantenimiento y optimización de sistemas”), lo que resulta algo curioso, y que puede hacer pensar que existe cierta redundancia en los contenidos de las asignaturas.

Un resumen del nivel de cumplimiento de competencias (organizadas por áreas de ciberseguridad) del marco del Foro Nacional de Ciberseguridad, por parte de las asignaturas consideradas se puede observar en el Cuadro 2. Es importante mencionar que, por cuestiones de espacio, sólo se muestra el resumen y las conclusiones, sin indicar detalle sobre las competencias específicas. Así, podemos observar en las filas, tanto el número de competencias del marco que son (parcialmente) abordadas por cada asignatura, respecto al número total de competencias de cada área de ciberseguridad consideradas por el marco, indicando también el porcentaje alcanzado.

Por ejemplo, si observamos la fila de la asignatura SSS (una visión gráfica se puede ver en la Figura 2), podemos comprobar que esta asignatura, como es esperable, hace cumplir un buen número de competencias del área de “Desarrollo y Producto”, alcanzando el 68.75% de las competencias de esa área. También se observa que se cubren otras competencias de otras áreas, lo que puede deberse, bien a que tiene contenidos alejados de lo que podría considerarse el *core* de la asignatura, como por ejemplo contenidos de introducción, de criptografía, etc., o bien porque se refiera a competencias que aplican a varias áreas de la ciberseguridad.

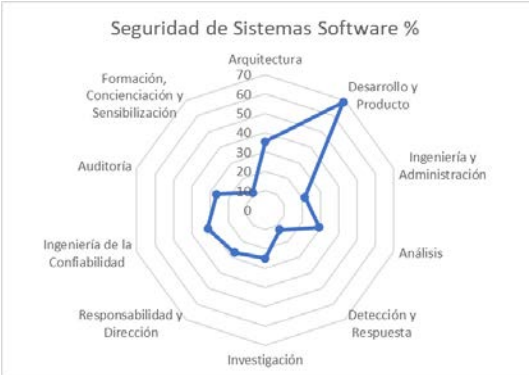

Figura 2. Cobertura de competencias de SSS.

Si bien la asignatura de SSS se empareja con intensidad con el área de “Desarrollo y Producto”, en el caso del resto de asignaturas eso no sucede con la misma intensidad. Por ejemplo, la asignatura de SR no alcanza el 50% de cumplimiento de ningún área, pero eso sí, alcanza un nivel de cobertura relevante para 5 de las áreas (ver Figura 3), cumpliendo además otro conjunto de competencias dispersas en el resto de áreas. En el caso de la asignatura de SSI (ver Figura 4), se acentúa el área de “Arquitectura”, y alcanza porcentajes de entre el 20 y el 30% de cobertura en casi todas las demás áreas.

Asignaturas relacionas con Ciberseguridad del Grado en Ingeniería Informática					Competencias	Áreas o Funciones de Ciberseguridad definidas en el Marco de Competencias									
Seguridad de Sistemas Software	Seguridad en Redes	Seguridad de los Sistemas Informáticos	Auditoría de Sistemas de Información	Análisis Forense Informático		Arquitectura	Desarrollo y Producto	Ingeniería y Administración	Análisis	Detección y Respuesta	Investigación	Responsabilidad y Dirección	Ingeniería de la Confiabilidad	Auditoría	Formación, Concienciación y Sensibilización
P	P	P			**CE1**	X	X								
P		P			**CE2**	X	X	X	X						
P	P	P			**CE3**	X	X		X		X				
P	P				**CE4**	X	X	X	X	X				X	
					CE5	X									
	P				**CE6**	X									
					CE7	X	X						X	X	
					CE8	X									X
P	P	P			**CE9**	X							X		
	P				**CE10**	X									

Cuadro 1. Muestra de cumplimiento de las 10 primeras competencias.

		Arquitectura	Desarrollo y Producto	Ingeniería y Administración	Análisis	Detección y Respuesta	Investigación	Responsabilidad y Dirección	Ingeniería de la Confiabilidad	Auditoría	Formación, Concienciación y Sensibilización
Nº competencias		17	16	14	17	16	8	11	16	15	9
SSS	n	6	11	3	5	2	2	3	5	4	1
	%	35.29	68.75	21.42	29.41	12.5	25	27.27	31.25	26.66	11.11
SR	n	8	7	6	6	6	2	1	4	5	0
	%	47.05	43.75	42.85	35.29	37.5	25	9.09	25	33.33	0
SSI	n	6	5	3	4	3	2	3	4	3	0
	%	35.29	31.25	21.42	23.52	18.75	25	27.27	25	20	0
ASI	n	1	1	0	0	2	2	2	2	4	0
	%	5.88	6.25	0	0	12.5	25	18.18	12.5	26.66	0
AFI	n	1	1	0	2	4	1	0	2	1	0
	%	5.88	6.25	0	11.76	25	12.5	0	12.5	6.66	0
Todos	n	11	15	7	12	10	3	5	7	8	1
	%	65.70	93.75	50	70.58	62.50	37.5	45.45	43.75	53.33	11.11
Redundantes		11	15	7	12	10	3	5	7	8	1

Cuadro 2. Resumen de cumplimiento de competencias.

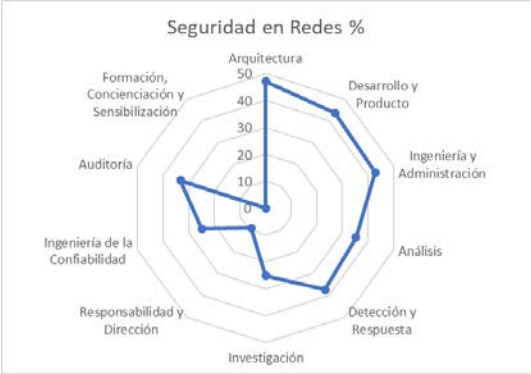

Figura 3. Cobertura de competencias de SR.

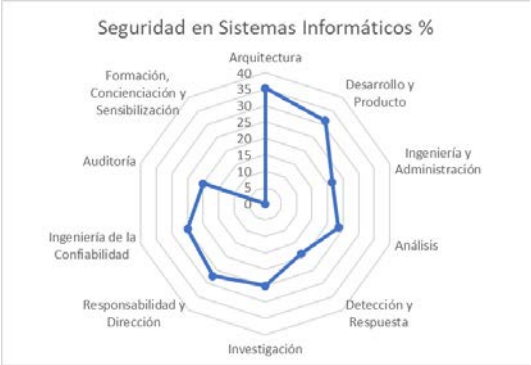

Figura 4. Cobertura de competencias de SSI.

Sin embargo, en el caso de las otras dos asignaturas (son las dos optativas), ASI (ver Figura 5) y AFI (Figura 6), se puede observar una menor dispersión de competencias, estando, en general, más concentradas en el área de "Auditoría", y en el de "Detección y Respuesta", respectivamente, y alcanzando pocas competencias del resto de áreas.

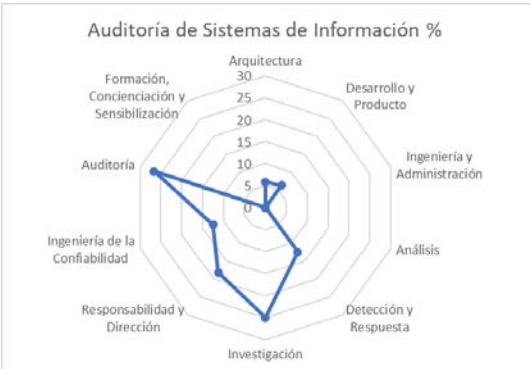

Figura 5. Cobertura de competencias de ASI.

Sin embargo, si consideramos de manera acumulativa el alcance de competencias entre todas las asignaturas observamos un dato curioso, y es que hay un buen número de competencias redundantes entre las cinco asignaturas, especialmente entre las tres primeras (que son las asignaturas de mención, siendo las otras dos, optativas). Los datos exactos sobre competencias redundantes se pueden observar en la última fila del Cuadro 2. Por ejemplo, de las 17 competencias del área de "Arquitectura", vemos que se aborda un total de 11 competencias en total entre todas las asignaturas, pero si lo vemos por asignaturas individuales, las competencias alcanzadas son 6, 8, 6, 1 y 1, respectivamente (sería un total de 22 competencias), lo que indica que hay una redundancia o repetición innecesaria de 11 competencias entre las asignaturas (a no ser que se refieran a facetas o dimensiones diferentes de las competencias). Esta misma situación se produce en el resto de las áreas de la ciberseguridad del marco de competencias.

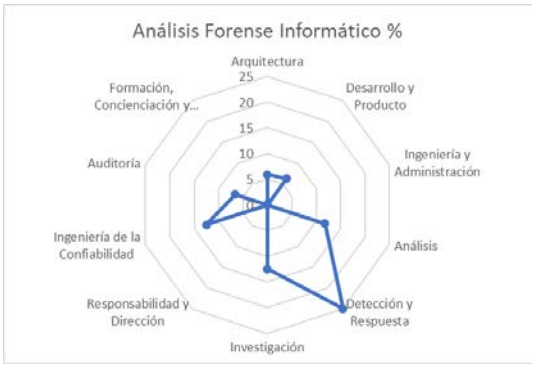

Figura 6. Cobertura de competencias de AFI.

No obstante, a pesar de tratarse de un número reducido de asignaturas (solamente 5) y de contar con un elevado número de competencias redundantes, se puede observar en la Figura 7 que entre estas asignaturas se tratan, al menos parcialmente, un buen número de competencias del marco considerado en casi todas las áreas, alcanzando su máximo en el caso del área de "Desarrollo y Producto" con un 93.75% de las competencias, estando el resto de áreas prácticamente por encima del 40%, a excepción de "Concienciación y Sensibilización", que tan solo cuenta con un 11.11%, lo que se ve reforzado con la organización de un concurso del tipo *Atrapa la Bandera* organizado por la Escuela.

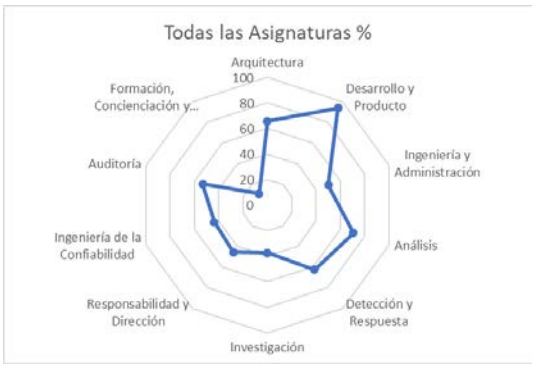

Figura 7. Cobertura del total de asignaturas.

5. Propuesta de ajuste del plan de estudios

Una vez analizados los datos de la sección 4, podemos observar dos hechos importantes. El primero es la existencia de mucha redundancia en las competencias abordadas por las asignaturas, especialmente por las tres primeras. El segundo es que, incluso con tal redundancia, considerando todas las asignaturas, se alcanza un buen número de competencias del marco considerado. Pero claro, el problema es que actualmente las asignaturas de mención son exclusivas de la mención elegida por el estudiante, lo que significa que, en la práctica, ningún estudiante cursa todas las asignaturas, sino que, en el mejor de los casos, cursará una asignatura de mención y dos optativas, teniendo entonces una importante reducción de competencias, respecto al máximo considerado.

Otro hecho observado en el caso de las tres asignaturas de mención es que, al ser la primera asignatura sobre ciberseguridad que cursan los estudiantes (según la mención elegida), todas incluyen una inevitable parte de conceptos básicos redundantes, y que reduce el tiempo para profundizar en aspectos realmente importantes de la asignatura. Así, asumiendo que lo mejor sería un rediseño completo del grado, para definir unos estudios que cumplan bien las competencias del marco, una opción parcial pero razonable podría pasar por los siguientes aspectos:

- Tener una asignatura obligatoria, o al menos una formación base que todos los estudiantes del grado cursen sobre fundamentos de ciberseguridad. Eso permite liberar a las asignaturas de mención de repetir fundamentos, concentrando el tiempo en lo realmente importante para los descriptores de esas asignaturas.
- Ampliar la optatividad del grado, para que los estudiantes interesados, puedan cursar como optativas, las asignaturas de las otras menciones, y de este modo, poder cursar las 5 asignaturas, pudiendo así formarse, de manera razonable en competencias de la mayoría de áreas definidas por el marco de competencias considerado.

6. Conclusiones

La Ciberseguridad en una disciplina estrechamente vinculada con la Ingeniería Informática, aunque también se aproxime a otras titulaciones, y que todavía no está siendo bien cubierta por el sistema de educación nacional en término de titulaciones de grado y máster. Sin embargo, ya se están sentando las bases para poder hacerlo, y el primer paso relevante ha sido la elaboración de un marco de competencias en ciberseguridad por parte del Foro Nacional de Seguridad, con la idea de establecer un necesario vínculo entre la industria o los empleadores, y la academia.

Por el momento no será fácil y rápido crear nuevos títulos de Grado en Ciberseguridad, y quizás una opción aceptable pueda ser incorporar menciones en los grados de Ingeniería Informática, o incluso reagrupar y orientar asignaturas que actualmente ya se están impartiendo, con el objetivo de tener un mejor cumplimiento de las competencias de este marco competencial en ciberseguridad. En este artículo se ha analizado en detalle la situación actual en la ESI, tanto desde el punto de vista estructural (asignaturas en menciones y optatividad) como de sus resultados de aprendizaje, competencias y temario, llegando a la conclusión de que es posible hacer cambios, relativamente menores, que permitan evitar redundancia en la actual impartición de contenidos, y conseguir un mejor alineamiento con las competencias del marco de competencias.

Agradecimientos

Queremos agradecer a los profesores de las asignaturas implicadas (Carlos Villarrubia, David G. Rosado, Cleto Martín, Nacho García y Sebastián Reyes), por su ayuda en el análisis de las competencias.

El trabajo ha sido desarrollado con financiación de los proyectos AETHER-UCLM (PID2020-112540RB-C42) financiado por MCIN/AEI/10.13039/501100011033, ALBA-UCLM (TED2021-130355B-C31, id.4809130355-130355-28-521), financiado por "Ministerio de Ciencia e Innovación" y por MESIAS (2022-GRIN-34202) financiado por FEDER.

Referencias

[1] ACM/IEEE, Computing Curricula 2020, CC2020, Paradigms for Global Computing Education, 31 de diciembre de 2020. URL: https://www.acm.org/education/curricula-recommendations

[2] CyBOK, The Cyber Security Body of Knowledge. https://www.cybok.org/

[3] Foro Nacional de Ciberseguridad. Marco de Competencias para Programas Superiores de Formación Especializada en Ciberseguridad, Noviembre 2021. https://foronacionalciberseguridad.es/index.php/documentacion/publico/114-marco-de-competencias-en-ciberseguridad

[4] NIST Special Publication 800-181. Workforce Framework for Cybersecurity (NICE Framework). November 2020. https://doi.org/10.6028/NIST.SP.800-181r1