Diseño de un Grado en Ciberseguridad e Inteligencia Artificial

Rodrigo Román*, Isaac Agudo†, Rubén Ríos‡ y Javier López§
NICS Lab, Universidad de Málaga
Email: *rroman@uma.es, †isaac@lcc.uma.es, ‡ruben.rdp@uma.es, §javierlopez@uma.es

***Resumen*—La ciberseguridad y la inteligencia artificial son disciplinas estrechamente relacionadas con una importancia cada vez mayor, y a su vez con una demanda laboral creciente a nivel mundial. Este artículo se centra en uno de los esfuerzos para combatir dicha demanda: el proceso de creación del Grado en Ciberseguridad e Inteligencia Artificial de la Universidad de Málaga, pionero en España, el cual comenzó a impartirse en el curso académico 2023/24. Para ello, se describe la relación entre ambas disciplinas a nivel estratégico, regulatorio y tecnológico, la definición de los planes de estudio del grado incluyendo las fuentes de información consultadas, y un resumen de los contenidos del grado detallando aspectos específicos de su diseño. Con ello esperamos poner de relieve la importancia de proporcionar ofertas formativas específicas a nivel de grado para solventar la brecha laboral en estas disciplinas.**

***Index Terms*—Grado, Ciberseguridad, Inteligencia Artificial, IA, Docencia**

Tipo de contribución: *Formación e innovación educativa*

I. Introducción

La ciberseguridad es, a día de hoy, uno de los pilares esenciales para que nuestro ecosistema digitalizado e hiperconectado se mantenga sólido. Esta importancia se ve reflejada en las múltiples regulaciones, estrategias de I+D+i, inversiones, y programas de formación existentes tanto a nivel nacional como internacional. Por ejemplo, sólo en Europa en los últimos años se han definido diversos reglamentos (como el "Cyber Resilience Act", "Cybersecurity Act", y el "Cyber Solidarity Act") dentro del marco de la estrategia de ciberseguridad Europea [2] para responder y reaccionar ante las amenazas presentes y futuras que puedan afectar a nuestro entorno. No obstante, la necesidad de profesionales en ciberseguridad no para de aumentar: en Europa el déficit de profesionales de la ciberseguridad se acerca al millón de personas, mientras que a nivel mundial ya ha superado la cifra de los cuatro millones de personas [1]. Esto hace necesaria la creación de nuevas iniciativas formativas, a todos los niveles, que permitan afrontar esta demanda laboral.

Existe otra disciplina, además de la ciberseguridad, cuya importancia no para de crecer a todos los niveles – tanto empresarial como académico, tecnológico, y político. Nos referimos a la inteligencia artificial (IA), cuya capacidad para analizar grandes volúmenes de datos y predecir tendencias, entre otros aspectos, la ha convertido en un componente fundamental para la innovación y el desarrollo en múltiples sectores (p.ej. fiabilidad de sistemas críticos, salud, finanzas y educación). La inteligencia artificial se ha convertido en un elemento de importancia estratégica en las relaciones y políticas internacionales, generando la necesidad de marcos regulatorios como el "EU Artificial Intelligence Act" a nivel Europeo [4]. Sin embargo, al igual que con la ciberseguridad, la creciente importancia de esta disciplina ha generado una brecha laboral a nivel mundial – la cual afecta especialmente a Europa [3].

Para solventar dicha brecha laboral, ambas disciplinas, ciberseguridad e inteligencia artificial, están contando con un número cada vez más creciente de ofertas formativas a todos los niveles. Sin embargo, aún cuando ambas disciplinas están íntimamente relacionadas, la disponibilidad de una formación que aunase ambas disciplinas a nivel de grado era extremadamente limitada a nivel mundial. Por esta razón la Universidad de Málaga, dentro de la actualización de sus planes de estudio, diseñó el Grado en Ciberseguridad e Inteligencia Artificial, pionero en España, entre el año 2021 y 2022, el cual empezó a impartirse en el curso académico 2023/24 (septiembre de 2023).

El objetivo de este artículo es describir el proceso de creación de dicho grado y sus contenidos finales, de cara a mostrar tanto la necesidad de integrar ambas disciplinas en el ámbito educativo como la importancia de disponer de estas ofertas formativas. Para ello, dentro de la sección II se mostrará la relación entre ambas disciplinas, analizando además las titulaciones de grado y máster existentes a nivel Español y mundial. Posteriormente, la sección III describirá el proceso de diseño del grado, indicando tanto las fuentes de información como el proceso completo de definición de los planes de estudio y la propuesta de título. La sección IV ofrecerá un resumen de los contenidos del grado, incidiendo en aspectos específicos de su diseño e implantación. Finalmente, la sección V mostrará las conclusiones de nuestra exposición.

II. Ciberseguridad e Inteligencia Artificial

II-A. Relación entre ambas disciplinas

La naturaleza transversal tanto de la ciberseguridad como de la inteligencia artificial hacen que ambas disciplinas tengan una relación muy cercana entre ellas, relación cuya importancia no hace más que crecer. Esta relación puede encontrarse en diversos ámbitos, tanto estratégico como regulatorio y tecnológico. Un ejemplo de esta relación a nivel estratégico la podemos encontrar dentro del ámbito de las estrategias de Investigación y Desarrollo en Tecnologías de la Información y las Comunicaciones (TIC) desarrolladas en España, Europa y el resto del mundo. Por ejemplo, en Europa, la Comisión Europea desarrolló su "Plan Coordinado sobre Inteligencia Artificial", en 2018, que fue revisado en 2021 [5]. En este plan, la ciberseguridad se considera como una de las áreas estratégicas donde se debe integrar la inteligencia artificial. Dicha importancia se ratifica en la "Estrategia de Ciberseguridad" de la UE, desarrollada en diciembre de 2020 [6]. En cuanto a España, la "Estrategia Nacional de Inteligencia

Artificial" (ENIA) [7], derivada del plan coordinado de la CE, es uno de los ejes de la "Agenda España Digital 2026" [8] y uno de los componentes centrales del "Plan de Recuperación, Transformación y Resiliencia" de la economía española. En dichas estrategias se menciona explícitamente que "la I+D+i en IA aplicada a la ciberseguridad (...) es esencial para nuestra sociedad".

Más allá del ámbito estratégico, a nivel regulatorio podemos observar la importancia de la protección del ciclo de vida de la inteligencia artificial, y los peligros relacionados con los usos maliciosos de la misma. Por ejemplo, dentro de la Ley de Inteligencia Artificial de la Unión Europea [4], se menciona explícitamente como "la ciberseguridad desempeña un papel crucial a la hora de garantizar que los sistemas de inteligencia artificial sean resistentes a los intentos de manipular su comportamiento, (...) siendo necesario adoptar medidas adecuadas de protección (...) en sistemas del alto riesgo". Adicionalmente, dentro de la misma ley se describen condiciones de transparencia en el uso de tecnologías generativas de contenidos de imagen, audio y/o vídeo que puedan utilizarse para falsificar la realidad y engañar a las personas ("deep fakes"). Esta regulación también viene respaldada por el trabajo realizado por la ENISA en el ámbito de la ciberseguridad de la inteligencia artificial [9], la cual ha elaborado diversos documentos relacionados con la estandarización de la ciberseguridad aplicada a la IA, la definición de amenazas, y la protección tanto de la IA en general como de verticales específicos, documentos que sirven como base para las medidas de protección definidas dentro de la propia Ley de Inteligencia Artificial.

A nivel tecnológico, la unión entre la ciberseguridad y la inteligencia artificial siempre ha estado presente: inicialmente centrada en la creación de sistemas de detección de anomalías (incluyendo el correo basura o "spam") [10], esta unión ha evolucionado hacia otras áreas tales como el análisis de malware, la automatización de procesos de prevención (p.ej. gestión de alertas, evaluación de riesgos), el desarrollo de agentes inteligentes para la ciberdefensa y el ciberataque (p.ej. descubrimiento de vulnerabilidades), la integración con entornos de aprendizaje ("cyber-ranges"), y muchos otros [11]. Otro ámbito de evolución se encuentra en las inteligencias artificiales generativas, donde más allá de su potencial aplicación maliciosa (y mecanismos de defensa asociados como la identificación de "deep fakes" [12]), encontramos otras aplicaciones relacionadas con la ciberseguridad – en la forma del análisis del comportamiento de código fuente [13] y la definición de señuelos ("honeypots") adaptables a escenarios particulares como la Internet de las Cosas [14]. Finalmente, también cabe mencionar que aún existen varios desafíos a nivel I+D+i, incluyendo la optimización de su funcionamiento, la protección de la privacidad de los datos, y la existencia de herramientas y entornos estandarizados para verificar el funcionamiento de los mecanismos de forma continua [15].

II-B. Ámbito académico existente

Durante el periodo de definición del Grado en Ciberseguridad e Inteligencia Artificial, a nivel Español no existían títulos de grado que abarcasen ambas disciplinas, sin embargo, sí existían diversos títulos de grado que se centraban en alguna de estas disciplinas. Un resumen de dichos títulos puede verse en la Tabla I. Puede comprobarse que la mayoría de los títulos (12) se dedican al ámbito de la inteligencia artificial, mientras que el resto (5) se centran en la ciberseguridad. Adicionalmente, sólo uno de los títulos relacionados con la ciberseguridad es impartido por una universidad pública (Universidad Rey Juan Carlos), siendo el resto impartidos por universidades privadas.

Tabla I
GRADOS SOBRE CIBERSEGURIDAD O IA A SEPTIEMBRE DE 2022.

Área	Universidad	Código RUCT
Ciencia de datos e IA	Univ. Deusto	2504021
Ciencia de datos e IA	Univ. Politécnica Madrid	2503943
Ciencia de datos e IA	Univ. León	2504435
Ing. Datos e IA	Univ. Complutense Madrid	2504344
Computación e IA	IE Universidad	2503928
Computación e IA	Univ. Alfonso X El Sabio	2504450
Ing. Matemática e IA	Univ. Pontificia Comillas	2504382
IA	Univ. País Vasco	2504060
IA	Univ. Pol. Catalunya	2504183
IA	Univ. Rey Juan Carlos	2504258
IA	Univ. San Jorge	2504553
IA	Univ. a Coruña Univ. Santiago Compostela Univ. Vigo	2504532
Gestión Ciberseguridad	Univ. Francisco de Vitoria	2503932
Ing. Ciberseguridad	Univ. Rey Juan Carlos	2503932
Ing. Ciberseguridad	Univ. Europea Madrid	2504457
Ing. Ciberseguridad	Univ. San Jorge	2504551
Ciberseguridad	Univ. Int. la Rioja	2504425

Todos estos títulos de grado se encuentran adscritos a Escuelas o Facultades de Informática. Precisamente, el ACM Computer Curricula 2020 [17], referente de la guía de títulos de Informática a nivel mundial, y una de las bases en la preparación de este grado, describe las especialidades de la Ciberseguridad, Ciencia de datos, y la futura especialidad de Inteligencia Artificial como parte del ámbito de la Informática. Asimismo, la Estrategia Nacional de Inteligencia Artificial Española 2021-2023 [7] refleja como las competencias de la IA "(...) están incluidas en todos los Grados de Informática y Computación y en los Máster de Tecnologías Informáticas".

Respecto al ámbito internacional, también podemos encontrar múltiples títulos de grado relacionados con la IA o la ciberseguridad – pero no títulos explícitamente enfocados a la formación en ambas disciplinas. Esta formación dual si podemos encontrarla en títulos de máster de diversas universidades europeas y norteamericanas (p.ej. University of Klagenfurt, University of Udine, University of Sheffield, Radboud University, ESIEE Paris, Purdue University Northwest), así como de diversas universidades españolas (p.ej. Universidad Rovira i Virgili).

Cabe mencionar que, desde Septiembre de 2022 hasta la fecha de publicación de este artículo, se han empezado a impartir nuevos títulos de grado relacionados con la IA y la ciberseguridad. En particular, 4 títulos relacionados con la inteligencia artificial y 1 título relacionado con la ciberseguridad (impartido por una universidad privada). Adicionalmente, se están definiendo otros títulos que aúnan las disciplinas de la ciberseguridad y la IA, como el grado interuniversitario de Inteligencia Artificial y Ciberseguridad impartido conjuntamente por la Universidad de Almería y la Universidad de Jaén.

III. Diseño del grado

III-A. Enfoque del grado

Durante la fase del diseño del grado, se valoró inicialmente seguir el libro blanco del grado de ingeniería informática, creando una especialidad en ciberseguridad e IA. Esta opción hubiera sido mucho más directa, y habría permitido a los egresados retener la calificación de graduados en informática. No obstante, el coste a pagar era disponer de un número reducido de créditos específicos, los cuales serían relegados a los cursos superiores, quedando así un primer y segundo curso muy similar al del resto de titulaciones del centro. Adicionalmente, dicho número de créditos no sería suficiente para cubrir las competencias y resultados de aprendizaje esperados de una formación específica e interconectada de ambas disciplinas.

Por ello, la apuesta del centro fue proporcionar una formación específica amplia y desde el primero curso, renunciando a la calificación de graduado en informática. Esta apuesta obligaba a adaptar contenidos que actualmente se ofertaban en otros grados en cursos superiores a los primeros cursos del grado, para que sirvieran de base para los contenidos específicos avanzados. Además, se prestó especial atención dentro del diseño del grado en cubrir las necesidades de formación básica en informática, esenciales para la formación del alumnado en su profesión.

III-B. Fuentes de información

Más allá del uso del "ACM Computer Curricula 2020" (CC2020, [17]) y la normativa existente (Libro Blanco del Título de Grado en Ingeniería Informática [19], Reales Decretos 1393/2007 y 822/2021, etc), para la definición de las competencias y los objetivos de aprendizaje relacionados con la informática dentro del nuevo grado, la integración de los itinerarios de la ciberseguridad y la inteligencia artificial obligó al análisis de fuentes de información adicionales, las cuales se detallan a continuación.

III-B1. Planes de estudio e Informes: Dentro de los planes de estudio relacionados con la *ciberseguridad*, las principales fuentes de información fueron no sólo el "ACM Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity" (CSEC2017 [17]), sino también el "ACM Cybersecurity Curricular Guidance for Associate-Degree Programs 2020" (Cyber2yr2020 [18]). Se decidió por este enfoque dada la naturaleza dual del grado, puesto que Cyber2yr2020 persigue proporcionar un plan de estudios para programas de ciberseguridad de dos años. Adicionalmente, se consideró el curriculum de referencia en ciberseguridad definido por ECSO dentro de su grupo de trabajo 5, incluido dentro del documento "European Cybersecurity Education and Professional Training: Minimum Reference Curriculum" [20].

Respecto a los planes de estudio relacionados con la *inteligencia artificial*, aunque a la fecha de la definición del grado no existía ninguna guía de planes de estudio específica para este itinerario, sí que se consideraron aquellos aspectos relacionados ya definidos dentro del "ACM Computing Competencies for Undergraduate Data Science Curricula" (CCDS2021 [17]). Adicionalmente, también se tuvieron en cuenta aquellos aspectos definidos dentro de los diversos planes estratégicos nacionales y europeos, incluyendo la "Estrategia Nacional de Inteligencia Artificial" y el "Plan Coordinado sobre Inteligencia Artificial".

Finalmente, para la definición de aquellos aspectos comunes a la *ciberseguridad y la inteligencia artificial*, se utilizaron diversas fuentes disponibles en varios ámbitos. Por ejemplo, el currículum de referencia en ciberseguridad definido por ECSO define el contenido y los resultados de aprendizaje de diversas asignaturas comunes a la ciberseguridad y la inteligencia artificial – en particular "Cybersecurity for Artificial Intelligence" (10 ECTS) y "Machine Learning Security" (5 ECTS). Adicionalmente, existen diversos informes creados por entidades afines a la Comisión Europea, como el "Artificial Intelligence and Cybersecurity: Technology, Governance and Policy Challenges" desarrollado por el "Centre for European Policy Studies (CEPS)" [21], o las diversas guías desarrolladas por la ENISA dentro de su grupo de trabajo de inteligencia artificial [9].

III-B2. Certificaciones: Debido a la importancia de las certificaciones profesionales dentro del ámbito empresarial a nivel internacional, para el diseño de los contenidos del grado también se tuvieron en cuenta las principales certificaciones existentes en la actualidad, principalmente aquellas relacionadas con el campo de la ciberseguridad. Aunque el diseño del grado no perseguía que los graduados/as obtengan dichas certificaciones de forma inmediata tras finalizar sus estudios, si consideraba la necesidad de facilitar a dichos egresados/as la obtención de dichas certificaciones en su futura carrera profesional, mediante la inclusión de aquellas competencias y resultados de aprendizaje considerados como básicos.

En particular, durante el diseño del grado se consultaron y revisaron las siguientes certificaciones:

a. **COMPTIA** – Computing Technology Industry Association [22]
   - *Security+*: Cybersecurity
   - *CASP+*: Advanced Security Practitioner
   - *PenTest+*: Penetration Testing
   - *CySA+*: Cybersecurity Analyst

b. **ISC2** – International Information System Security Certification Consortium [23]
   - *SSCP*: Systems Security Certified Practitioner
   - *CCSP*: Certified Cloud Security Professional
   - *CSSLP*: Certified Secure Software Lifecycle Professional
   - *ISSEP*: Information Systems Security Engineering Professional
   - *ISSMP*: Information Systems Security Management Professional

III-B3. I+D+i: Dentro del diseño de los planes de estudio del nuevo grado también se consideraron los principales avances de I+D+i en el campo de la ciberseguridad y la inteligencia artificial. Para ello se realizó un análisis del estado del arte en este campo, cuyos resultados se encuentran resumidos en la sección II-A. Dicho análisis del estado del arte permitió identificar no sólo los principales campos de aplicación de la inteligencia artificial hacia la ciberseguridad, sino también sus principales problemas de ciberseguridad, así como las soluciones existentes. Esta información se utilizó para determinar con exactitud qué temáticas (p.ej. Gestión de Anomalías y Ciberincidentes) se beneficiarían de la in-

Tabla II
ESTRUCTURA DE LAS ENSEÑANZAS DEL GRADO POR MÓDULOS Y MATERIAS

Módulo Formación Básica (60 créditos)	
Matemática	Matemática I, Matemática II, Probabilidad y Estadística, Representación del Conocimiento y Razonamiento
Fundamentos de Informática	Programación I, Programación II, Fundamentos de Redes Telemáticas, Arquitectura de Computadores, Identidad Digital y Privacidad, Fundamentos de Ciberseguridad
Módulo Formación Común (60 créditos)	
Ing. SW y Procesamiento Información	Bases de Datos, Minería de Datos, Programación Segura, Ingeniería del SW Seguro, Seguridad en Aplicaciones Web
Inteligencia Computacional	Fundamentos de Inteligencia Artificial, Algoritmos de Búsqueda y Optimización Computacional
Tecn. Informáticas y de Sistemas	Arquitectura de Sistemas Virtualizados, Sistemas Operativos
Informática y Sociedad	Aspectos Sociales, Éticos y Legales de la Ciberseguridad e IA
Módulo Formación Específica en Ciberseguridad (24 créditos)	
Ciberseguridad	Seguridad en Servicios y Protocolos de Internet, Pentesting y Hacking Ético, Informática Forense y Ciberdelincuencia, Seguridad en Entornos Móviles
Módulo Formación Específica en Inteligencia Artificial (24 créditos)	
Inteligencia Artificial	Aprendizaje Computacional I, Aprendizaje Computacional II, Aprendizaje profundo, Robótica Inteligente
Módulo Formación Específica en Sistemas CiberSeguros e Inteligentes (30 créditos)	
Integración de Ciberseguridad e IA	Inteligencia Malware, Seguridad en Sistemas de Inteligencia Artificial, Gestión Inteligente de Anomalías y Ciberincidentes, Sistemas de Inteligencia Artificial Ciberseguros, Sistemas Biométricos
Módulo Trabajo Fin de Grado (12 créditos)	
Módulo Formación Complementaria en Prácticas Externas (18 créditos)	
Módulo Materias Optativas (30 créditos)	

tegración de la inteligencia artificial durante las actividades formativas.

III-C. Definición de los Planes de Estudio

III-C1. Creación de Grupos de Trabajo: Para la definición de los planes de estudio del grado, se involucraron a diversos grupos de trabajo internos y externos a la Universidad de Málaga. Los *grupos de trabajo internos* vinieron definidos, según la normativa de la UMA, para el establecimiento de nuevos títulos de grado. Así, por un lado, se creó una Comisión de Expertos, con amplia experiencia en la docencia de los grados de informática y las necesidades del alumnado a nivel de conocimientos básicos en esta disciplina, la cual fue encargada de la creación de un 'Libro blanco' que incluyera las asignaturas más adecuadas para el nuevo grado (tanto básicas como específicas) junto con sus descriptores (datos generales de la asignatura (nombre, curso, cuatrimestre), objetivo general, resultados de aprendizaje, contenidos, competencias específicas, actividades formativas, sistemas de evaluación, otros comentarios). Por otro lado, se creó una Comisión de Grado de Centro encargada de definir las guías de cada asignatura según las directrices del 'Libro blanco'.

Respecto al *grupo de trabajo externo*, la semilla de dicho grupo surgió de una reunión con empresas bajo el paraguas de las jornadas Transfiere 2021, celebradas en Abril de 2021 en Málaga. Allí, se debatieron los perfiles profesionales más demandados, así como las competencias más importantes en ciberseguridad e inteligencia artificial. Posteriormente, se creó el grupo de trabajo "GT Talento", compuesto por representantes del tejido empresarial de Málaga y el Vicerrectorado de Empresa, Territorio y Transformación Digital de la UMA. Este grupo fue el encargado de proporcionar comentarios durante el proceso de definición de los planes de estudio a través de diversas consultas.

III-C2. Definición del 'Libro blanco': Para la definición de las asignaturas relacionadas con la ciberseguridad e inteligencia artificial en el 'Libro blanco' del nuevo grado, la Comisión de Expertos analizó las áreas de conocimiento definidas en los documentos indicados en la sección III-B1, agrupando las diversas competencias (tanto esenciales como optativas) y objetivos de aprendizaje en diversas temáticas. Posteriormente, se agruparon estas temáticas en potenciales asignaturas del grado. Tanto para esta agrupación como para la concreción de los descriptores específicos, incluyendo los contenidos necesarios para alcanzar las competencias y objetivos de aprendizaje necesarios, también se tuvieron en cuenta las certificaciones y estudios del estado del arte mencionados en las secciones III-B2 y III-B3, respectivamente. Un ejemplo de una ficha de asignatura del grado (Fundamentos de Ciberseguridad) tal y como fue descrita dentro del 'Libro Blanco' puede verse en el Anexo I[1].

Durante este proceso, la experiencia del personal docente e investigador de la UMA que formaba parte de la Comisión de Expertos posibilitó un análisis del dimensionamiento de cada una de estas asignaturas, lo cual permitió una mejor definición de los objetivos – posibilitando, por ejemplo, la inclusión de objetivos adicionales (p.ej. objetivos incluidos dentro del CSEC2017 más allá de los ya considerados por el Cyber2yr2020). Adicionalmente, la visión general de los directores de la comisión permitió una definición temprana de un gráfico de dependencias entre temáticas y posteriormente asignaturas, lo cual permitió una mejor coordinación tanto horizontal como vertical entre las diversas asignaturas y sus elementos.

Como paso final a la creación del 'Libro blanco', la dirección y las áreas de conocimiento se pusieron de acuerdo sobre la adscripción de las asignaturas a las diversas áreas. Este proceso se desarrollo persiguiendo que las asignaturas coincidieran con las áreas adecuadas y con la experiencia docente y/o investigadora del profesorado de dichas áreas. Asimismo, durante este proceso, se procuró limitar el impacto de los cambios indicados dentro del 'Libro blanco' sobre el trabajo del profesorado.

III-C3. Elaboración de las guías de las asignaturas: Una vez elaborado el 'Libro blanco', la Comisión de Grado de

[1]Se proporciona esta ficha para que pueda visualizarse la granularidad con la que se desarrolló el 'Libro blanco', así como para compararla con el plan docente final disponible en la web de la UMA.

Centro se encargó de la elaboración de las diversas guías docentes. Para ello, se definió un representante de área para cada una de las 11 áreas involucradas en el desarrollo del título de grado, y cada uno de dichos representantes se encargó de seleccionar y coordinar a los diversos equipos docentes – de forma que éstos pudieran refinar y completar las fichas de cada asignatura. Este proceso se realizó de forma iterativa, involucrando tanto a la Comisión de Grado de Centro, para cohesionar propuestas y mantener la consistencia con los contenidos del 'Libro blanco', como al grupo de trabajo externo "GT Talento", para enriquecer las propuestas considerando las necesidades empresariales.

También, durante la elaboración de las guías de las asignaturas, se completó la definición de competencias y resultados de aprendizaje, indicando cuáles eran para cada asignatura las competencias, conocimientos o contenidos, habilidades o destrezas, y competencias transversales a considerar. La Comisión de Grado de Centro también se encargó de revisar las competencias y resultados de aprendizaje del grado en su conjunto, comprobando la consistencia con los planes de estudio definidos en la sección III-B1 y las leyes vigentes.

III-C4. Finalización de la propuesta y aprobación: Una vez fueron finalizadas todas las guías, se realizó una reunión para finalizar el título completo, revisando que el plan de estudios fuera coherente y siguiera las sugerencias de los expertos mencionadas en el 'Libro blanco', y ultimando los detalles relacionados con las asignaturas optativas. Adicionalmente, se realizó una presentación al grupo de trabajo externo "GT Talento", recabando sus comentarios finales – aunque éstos fueron muy positivos y no implicaron cambios en la propuesta. Finalmente, dentro de la Junta de Centro de Julio de 2022 se aprobó la propuesta de título de grado. El Grado en Ciberseguridad e Inteligencia Artificial fue verificado en Mayo de 2023, y recibió la autorización del Consejo de Ministros en Octubre de 2023. Su plan de estudios fue publicado en el BOE del 30/12/2023, y su impartición dio comienzo en el curso 2023/24.

IV. Grado Ciberseguridad e IA

La definición del Grado en Ciberseguridad e Inteligencia Artificial de la Universidad de Málaga, así como una descripción detallada de sus competencias y resultados de aprendizaje, se encuentra disponible en su página web [16], la cual incluye tanto los planes de estudios finales como la memoria de verificación del título. No obstante, en esta sección ofrecemos tanto un resumen como una explicación del diseño de dichos contenidos.

IV-A. Características del grado

El Grado en Ciberseguridad e Inteligencia Artificial de la UMA es un grado de la rama Ingeniería y Arquitectura, bajo el código ISCED Ciencias de la Computación. Ofrece un tipo de enseñanza presencial, impartido en castellano, y está compuesto de 240 créditos, de los cuales 60 créditos son de formación básica, 138 créditos son obligatorios, 30 créditos son optativos, y 12 créditos pertenecen al trabajo de fin de grado. Cabe mencionarse que 18 de los 30 créditos optativos pueden realizarse mediante prácticas externas.

Los créditos de formación básica y obligatoria se reparten entre los departamentos que se listan a continuación:

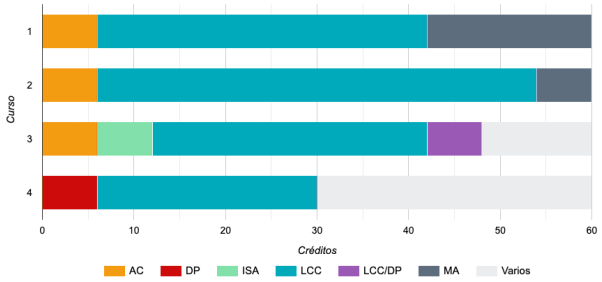

Figura 1. Distribución de créditos por departamento

- Arquitectura de Computadores (AC)
- Derecho Público (DP)
- Ingeniería de Sistemas y Automática (ISA)
- Lenguajes y Ciencias de la Computación (LCC)
- Matemática Aplicada (MA)

Como puede apreciarse en la Figura 1, aunque intervienen hasta cinco departamentos en las tareas docentes del grado, la mayor parte de los créditos recae sobre el departamento de Lenguajes y Ciencias de la Computación, principalmente por tratarse de un grado del ámbito de la ingeniería informática.

Por lo general, los créditos de cada asignatura pertenecen a un único departamento, aunque existe un caso excepcional (la asignatura 'Informática Forense y Ciberdelincuencia'), en el que los créditos se reparten entre dos departamentos debido a su carácter claramente multidisciplinar. Adicionalmente, cabe destacar que en los últimos cursos hay una carga importante de créditos optativos y de trabajo fin de grado, que no están pre-asignados a un departamento concreto. Por ese motivo, se incluye el item 'Varios' en la leyenda.

A nivel de áreas de conocimiento, el reparto de docencia se hace entre un total de 8 áreas de los cinco departamentos citados anteriormente:

- Arquitectura y Tecnología de Computadores (ATC)
- Ciencias de la Computación e Inteligencia Artificial (CCIA)
- Derecho Administrativo (DA)
- Derecho Penal (DP)
- Ingeniería de Sistemas y Automática (ISA)
- Ingeniería Telemática (ITEL)
- Lenguajes y Sistemas Informáticos (LSI)
- Matemática Aplicada (MA)

En la Figura 2 se muestra la distribución de créditos a nivel de área de conocimiento. En ésta puede observarse que las áreas de CCIA, ITEL y LSI, pertenecientes al departamento de Lenguajes y Ciencias de la Computación (LCC), son las que tienen una mayor carga docente. El resto de áreas tiene un mapeo uno a uno con sus respectivos departamentos, salvo en el caso de las áreas DA y DP, las cuales pertenecen al departamento de Derecho Público.

IV-B. Contenidos del grado

Un resumen de la estructura de las enseñanzas por módulos y materias se presenta en la Tabla II. A su vez, esta estructura se encuentra dividida en cuatro aspectos troncales, de los cuales nos centraremos en las especializaciones del grado:

(1) Formación en informática.

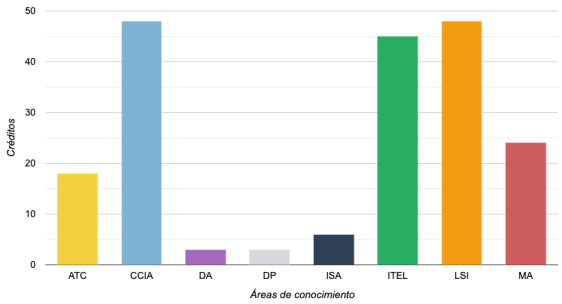

Figura 2. Distribución de créditos por áreas de conocimiento

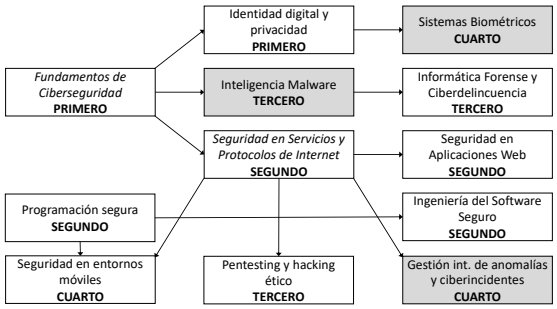

Figura 3. Tabla de dependencias ciberseguridad

(II) Formación en ciberseguridad.
(III) Formación en inteligencia artificial.
(IV) Formación interdisciplinar de IA y ciberseguridad.

IV-B1. Formación en ciberseguridad: El objetivo de esta formación dentro del grado se centra principalmente en dos ámbitos: la integración de capacidades de seguridad y privacidad en el diseño, desarrollo, configuración y evaluación de aplicaciones y sistemas de información interconectados, y la reacción – tanto reactiva como proactiva – ante los ciberincidentes, conociendo sus implicaciones, programas maliciosos, herramientas, soluciones, y otros.

La Figura 3 muestra una visión de la tabla de dependencias de las asignaturas relacionadas con ciberseguridad, desarrollada durante la elaboración del 'Libro blanco' (cf. sección III-C2). Esta figura contiene adicionalmente ciertas asignaturas de formación interdisciplinar, marcadas en gris y presentes en el diseño inicial de la tabla. Podemos observar que existen dos asignaturas, 'Fundamentos de Ciberseguridad', y 'Seguridad en Servicios y Protocolos de Internet', que ejercen gran influencia sobre el resto de asignaturas debido a su carácter fundacional. Ambas se encargan de proporcionar conceptos y capacidades esenciales, incluyendo la protección ante las amenazas más comunes a través de la aplicación de protocolos y servicios de seguridad básicos.

Respecto al resto de asignaturas, podemos observar que existen diversos itinerarios orientados a proporcionar al alumnado conocimientos, habilidades y competencias en diversas ramas de la ciberseguridad, consistentes con los objetivos de la formación en esta disciplina. Éstas incluyen, entre otras, la integración de mecanismos de identidad digital, el desarrollo seguro de aplicaciones y sistemas en varios contextos (p.ej. aplicaciones web, entornos móviles), los procedimientos y herramientas de seguridad ofensiva (p.ej. pentesting, malware), y la gestión de las amenazas – sea antes, durante, o después de un ciberataque.

IV-B2. Formación en inteligencia artificial: El objetivo de esta formación dentro del grado persigue el desarrollo de soluciones basadas en inteligencia artificial siguiendo todas las etapas necesarias en esta disciplina: desde la adquisición y procesamiento de datos hasta la evaluación, aplicación, y mantenimiento de los modelos resultantes, siempre teniendo en cuenta las implicaciones éticas asociadas.

La tabla de dependencias de las asignaturas relacionadas con la inteligencia artificial – y aquellas de formación básica en matemáticas que forman la base de los mecanismos de la IA – no se incluyen en este artículo, puesto que dicha relación de dependencias es más sencilla al seguir un itinerario más lineal. Inicialmente, en los primeros cursos, se proporcionan tanto las bases matemáticas de los mecanismos de inteligencia artificial (p.ej. 'Representación del Conocimiento y Razonamiento', 'Probabilidad y Estadística') como los conceptos fundacionales de esta disciplina (p.ej. 'Fundamentos de Inteligencia Artificial', 'Algoritmos de Búsqueda y Optimización Computacional').

Posteriormente, se introducen los diversos algoritmos que han conformado y conforman la inteligencia artificial hoy en día: desde los algoritmos de aprendizaje no profundo supervisado (p.ej. máquinas de vector soporte (SVM), árboles de decisión, bosques aleatorios), no supervisado (p.ej. Análisis de Componentes Principales (PCA), agrupamiento, modelos probabilísticos) y por refuerzo (p.ej. basados en modelos, libre de modelos), hasta los algoritmos de aprendizaje profundo (p.ej. Autocodificadores, Redes generativas de adversarios (GAN), transformadores). Adicionalmente, se ofrece una asignatura aplicada en el entorno de la robótica – gracias a la experiencia investigadora y docente de una de las áreas de conocimiento de la Escuela de Informática.

IV-B3. Formación interdisciplinar de IA y ciberseguridad: Como hemos mencionado a lo largo del artículo, ambas disciplinas se encuentran altamente interrelacionadas: la inteligencia artificial necesita ser protegida – tanto ante ataques externos como de sí misma (p.ej. "deep fakes") – para evitar manipulaciones en la toma de decisiones, y la ciberseguridad puede enriquecerse a todos los niveles gracias a la aplicación de la inteligencia artificial.

Precisamente, las asignaturas relacionadas con esta formación interdisciplinar siguen estas dos vertientes. Por una parte, existen asignaturas ('Ciberseguridad en Sistemas de Inteligencia Artificial' y 'Sistemas de Inteligencia Artificial Ciberseguros') que se centran en los desafíos asociados a las amenazas y vulnerabilidades de la inteligencia artificial (p.ej. por actividad maliciosa, por infraestructuras subyacentes inseguras, por causas externas) y en la robustez de ésta ante, p.ej., explotación de los modelos y datos sesgados, entre otros.

Por otra parte, existen asignaturas que proporcionan una formación específica en aspectos de ciberseguridad ('Inteligencia Malware', 'Gestión Inteligente de Anomalías y Ciberincidentes', 'Sistemas Biométricos'), donde la inteligencia artificial forma parte integral de los contenidos – en cuanto a que la mayoría de las actividades formativas consideran de una forma u otra la aplicación de la inteligencia artificial. No obstante, cabe mencionar que esta clase de integración no está

limitada a estas asignaturas, puesto que se anima al profesorado del grado a incorporar dentro de sus actividades formativas soluciones de inteligencia artificial que sean consistentes con el nivel del alumnado en ese momento.

IV-B4. Formación optativa: La oferta de asignaturas optativas cae en el ámbito de todos los aspectos troncales anteriormente mencionados. Esto es así porque, de las 37 asignaturas ofertadas, existen un total de 21 asignaturas que se han diseñado de manera específica para el grado, tratando aspectos específicos de ciberseguridad y/o inteligencia artificial. Ejemplos de ello son las asignaturas 'Aceleradores para Seguridad e Inteligencia Artificial', 'Aprendizaje Federado', 'Blockchain' o 'Seguridad en Entornos Industriales y Robotizados'.

De esta forma, la formación del estudiantado se complementa con un total de 30 créditos optativos con 5 asignaturas de libre elección, programadas para el tercer y cuarto curso del grado. También cabe la posibilidad de completar 18 de estos créditos optativos mediante prácticas externas.

IV-C. Implantación del grado

El Grado en Ciberseguridad e Inteligencia Artificial de la UMA empezó su primera edición en el curso lectivo 2023/24. Este grado se ha implantado a "coste cero"; es decir, su implantación no ha supuesto ningún coste para esta universidad al sustituir al Grado de Ingeniería de Computadores, aprovechando los recursos tanto materiales como humanos ya existentes – incluyendo profesorado y grupos de investigación con gran experiencia académica e investigadora en las disciplinas específicas del grado.

A la fecha de realización de este artículo ha concluido el 1er semestre del grado, el cual ha ofertado 65 plazas de nuevo ingreso para el curso 2023/24 – cubriéndose todas estas plazas con una nota de corte de 12,46 en la primera adjudicación del proceso de preinscripción, convirtiéndose en la sexta carrera más demandada de la UMA en este curso académico.

De cara a dar cobertura a los docentes implicados en la implantación de este nuevo grado, se han marcado diversas lineas de acción encaminadas a una mejor coordinación. Por ejemplo, se solicitó un proyecto de innovación docente donde unp de los objetivos principales era ayudar a la creación del contenido de las asignaturas de ciberseguridad del grado. Este proyecto ha permitido una mayor cohesión a la hora de definir contendidos concretos y actividades de evaluación, sirviendo como un foro de debate donde intercambiar ideas. También se han definido por parte del centro mecanismos de coordinación transversal, y se ha hecho un seguimiento de la implantación centrado en las metodologías docentes y de evaluación.

Con respecto a los resultados de los estudiantes aún es pronto para sacar conclusiones significativas, pero si observamos la distribución de las notas del primer semestre, representadas en la Figura 4, podemos obtener varias conclusiones. Primero, el ratio de aprobados supera el 80 % en todas las asignaturas. Esto supera tanto a la tasa de rendimiento media para el primer curso de la todas las titulaciones de la universidad de Málaga (78 %) como a la tasa de rendimiento del Grado de Ingeniería de Computadores (44 %), al que reemplaza este nuevo grado.

Segundo, la decisión de colocar asignaturas específicas de ciberseguridad desde el primer curso, como 'Fundamentos de Ciberseguridad' (FdC), no ha supuesto una dificultad para el estudiantado, sino una motivación extra. Aún cuando se

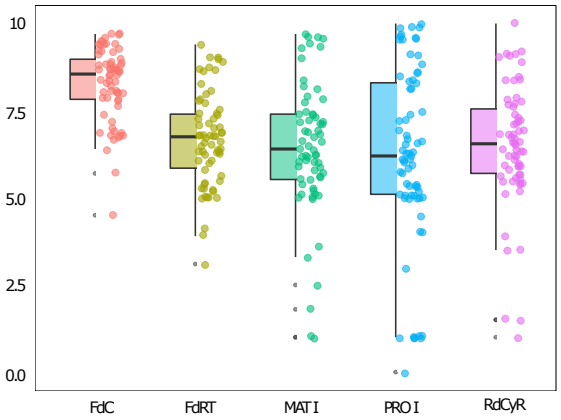

Figura 4. Distribución de notas del primer semestre

han tenido que adaptar contenidos que en otras titulaciones se imparten en tercer curso, esta asignatura ha tenido la mejor tasa de rendimiento del primer cuatrimestre – llegando al 98 % de aprobados en primera convocatoria y al 100 % de aprobados en segunda convocatoria.

V. Conclusiones

Este artículo ha perseguido mostrar no sólo los contenidos del nuevo Grado en Ciberseguridad e Inteligencia Artificial de la Universidad de Málaga, sino también su proceso de creación – desde su concepción inicial a su implantación. Esperamos que este artículo muestre la importancia de la creación de itinerarios formativos a nivel de grado que involucren ambas disciplinas, y sirva de inspiración para nuevas ofertas formativas en un futuro cercano.

Agradecimientos

Este artículo ha sido desarrollado en el ámbito del Grupo permamente de Innovación Educativa en Ciberseguridad (PIE22-040) del programa INNOVA22 de la Universidad de Málaga. El primer autor también ha recibido el soporte del Ministerio de Universidades de España a través de las "Ayudas para la recualificación del sistema universitario español", modalidad recualificación del profesorado universitario funcionario o contratado, financiado por la Unión Europea, NextGenerationEU (Resolución de 19 de julio de 2023).

Referencias

[1] Galina Misheva: "Mind the Cyber Skills Gap: a deep-dive", EU Digital Skills & Jobs Platform. https://digital-skills-jobs.europa.eu/en/latest/briefs/mind-cyber-skills-gap-deep-dive, 2023.

[2] Europe Digital Strategy: "Cybersecurity Policies". https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies, 2024.

[3] ARISA consortium: " AI Skills Strategy for Europe". https://aiskills.eu/news/arisa-launches-the-ai-skills-strategy-for-europe, 2024.

[4] European Commission: "Ley de Inteligencia Artificial", https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52021PC0206, 2024.

[5] Europe Digital Strategy: "Coordinated Plan on Artificial Intelligence", https://digital-strategy.ec.europa.eu/en/policies/plan-ai, 2021.

[6] European Commission: "The EU's Cybersecurity Strategy for the Digital Decade", https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0, 2020.

[7] Gobierno de España: "Estrategia Nacional de Inteligencia Artificial", https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIA2B.pdf, 2020.

[8] Gobierno de España: "España Digital 2026", https://espanadigital.gob.es/documentos, 2022.

[9] ENISA: "Topic - Artificial Intelligence (AI)", https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/artificial_intelligence, 2024.
[10] K. Shaukat, S. Luo, V. Varadharajan, I.A. Hameed, y M. Xu: "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade". en *IEEE Access*, vol. 8, pp. 222310–222354, 2020.
[11] Z. Zhang, H. Ning, F. Shi, et al.: "Artificial Intelligence in Cyber Security: Research Advances, Challenges, and Opportunities". en *Artificial Intelligence Review*, vol. 55, pp. 1029–1053, 2022.
[12] S. Jia et al.: "Can ChatGPT Detect DeepFakes? A Study of Using Multimodal Large Language Models for Media Forensics", arXiv:2403.14077, https://doi.org/10.48550/arXiv.2403.14077, 2024.
[13] Bernardo Quintero: "Crowdsourced AI += NICS Lab", VirusTotal blog, https://blog.virustotal.com/2023/08/crowdsourced-ai-nics-lab.html, 2023.
[14] J. Ragsdale, y B.V. Boppana: "On Designing Low-Risk Honeypots Using Generative Pre-Trained Transformer Models With Curated Inputs". en *IEEE Access*, vol. 11, pp. 117528-117545, 2023.
[15] ENISA: "Report: Artificial Intelligence and Cybersecurity Research", https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research, 2023.
[16] ETSI Informática UMA: "Grado en Ciberseguridad e Inteligencia Artificial", https://www.uma.es/grado-en-ciberseguridad-e-inteligencia-artificial, 2024.
[17] ACM: "Curricula Recommendations", https://www.acm.org/education/curricula-recommendations, 2024.
[18] ACM: "Cybersecurity Curricular Guidance for Associate-Degree Programs", http://ccecc.acm.org/guidance/cybersecurity, 2020.
[19] ANECA: "Libro Blanco: Título de Grado en Ingeniería Informática", https://www.aneca.es/documents/20123/63950/libroblanco_jun05_informatica.pdf, 2005.
[20] European Cybersecurity Organisation (ECSO): "WG5 Paper: European Cybersecurity Education and Professional Training: Minimum Reference Curriculum", https://ecs-org.eu/, 2022.
[21] Centre for European Policy Studies (CEPS): "Artificial Intelligence and Cybersecurity: Technology, Governance and Policy Challenges", https://www.ceps.eu/ceps-publications/artificial-intelligence-and-cybersecurity-2/, 2021.
[22] CompTIA: "Computing Technology Industry Association", https://www.comptia.org/, 2024.
[23] ISC2: "International Information System Security Certification Consortium", https://www.isc2.org/, 2024.

Anexo I: Ficha de "Fundamentos de Ciberseguridad"

Datos de la asignatura

- **Asignatura**: Fundamentos de Ciberseguridad
- **Grado**: Grado en Ciberseguridad e Inteligencia Artificial
- **Curso**: 1
- **Cuatrimestre**: 1

Resultados de Aprendizaje

- **RA1**: Evaluar las principales amenazas de seguridad y su impacto en redes y sistemas de información
- **RA2**: Distinguir los diferentes protocolos y servicios de seguridad aplicables a la protección frente a las amenazas más comunes

Contenidos

Bloque I: Introducción a la Ciberseguridad

1.1 Conceptos y principios básicos de seguridad
1.2 Amenazas y riesgos de seguridad
1.3 Servicios de seguridad
1.4 Organizaciones, normativas y estándares de seguridad
1.5 Roles y caminos de especialización en ciberseguridad

Bloque II: Algoritmos y Protocolos criptográficos

2.1 Criptografía clásica
2.2 Criptografía simétrica
2.3 Criptografía asimétrica
2.4 Protocolos de autenticación e Intercambio de claves
2.5 Protocolos avanzados

Bloque III: Fundamentos de seguridad en redes

3.1 Protocolos de seguridad en TCP/IP
3.2 Mecanismos de seguridad en internet

Competencias específicas

Diseñar y desplegar mecanismos que aborden la gestión de identidad, autenticación, autorización y auditoría (IAAA), además de saber configurarlos y gestionarlos adecuadamente.

Actividades formativas

Lecciones magistrales, Debates, Prácticas de laboratorio, Resolución de problemas.

Sistemas de evaluación

Examen escrito, Observación del desempeño, Examen tipo test, Resolución de problemas.