

Anexo 2 INNOVA
MEMORIA FINAL. COMPROMISOS Y RESULTADOS
PROYECTOS DE INNOVACIÓN Y MEJORA DOCENTE
2025/2026

Identificación del proyecto	
Código	sol-202500299689-tra
Título	Creación de laboratorios educativos sobre seguridad en sistemas informáticos y análisis de riesgos mediante <i>prompts</i> de inteligencia artificial
Responsable	Juan Boubeta Puig

1. Describa los resultados obtenidos a la luz de los objetivos y compromisos que adquirió en la solicitud de su proyecto. Incluya tantas tablas como objetivos contempló.

Objetivo nº 1	Diseñar, desarrollar, probar e implantar los laboratorios educativos sobre seguridad en sistemas informáticos
Actividades que había previsto en la solicitud del proyecto:	A1. Diseñar el contenido de los distintos laboratorios educativos sobre los diversos temas prácticos que se imparten en la asignatura Seguridad en los Sistemas Informáticos (SSI) del Grado en Ingeniería Informática de la Universidad de Cádiz (UCA): Gestión de contraseñas, Auditoría y análisis forense, Recolección de información en fuentes abiertas, Escaneo y enumeración de activos, Explotación de aplicaciones web y bases de datos, Explotación de redes, sistemas y contraseñas, Escalada de privilegios y Criptografía aplicada. A2. Desarrollar y probar estos laboratorios educativos mediante la creación de <i>prompts</i> interactivos. Estos <i>prompts</i> deberán guiar paso a paso al estudiantado, requiriendo que introduzca cierta información sobre la actividad en cuestión cuando sea necesario, antes de poder continuar con su ejecución. Las herramientas de Inteligencia Artificial (IA) como Google Gemini y ChatGPT (junto con sus versiones públicas como PentestGPT y Ethical Hacker GPT) actuarán como instructor del laboratorio. Cada <i>prompt</i> estará compuesto por las siguientes secciones: título, instrucciones iniciales donde se indicará a la herramienta de IA cómo debe comportarse y actuar, información que se requerirá al alumnado sobre la actividad, asignatura, grado y fecha en la que se realiza la actividad, introducción a la actividad del laboratorio presentando los objetivos a satisfacer, estructura del laboratorio compuesta por una serie de pasos a llevar a cabo, finalizando con la exportación en PDF de toda la información proporcionada por la IA durante la interacción del estudiantado con el laboratorio desarrollado. A3. Implantar los laboratorios educativos desarrollados en la asignatura SSI.

Actividades realizadas y resultados obtenidos:	Se han diseñado, desarrollado, probado e implantado cuatro laboratorios educativos en la asignatura SSI: P1 Auditoría de contraseñas (hashing SHA-256, ataques de diccionario con Hashcat, verificación Have I Been Pwned, políticas de contraseñas), P2 Reconocimiento OSINT (Google dorks, Shodan, Wayback Machine, análisis DNS/Whois, huella tecnológica y social), P3 Decisiones de criptografía aplicada y seguridad real (selección de algoritmos, configuraciones seguras, gestión de certificados) y P4 Reconocimiento y enumeración (recon pasivo vs. activo, escaneo de bajo impacto, interpretación de banners). Todos los laboratorios comparten una arquitectura común: recogida de metadatos anónimos por ID institucional, <i>prompt</i> en inglés con interacción en español, límites éticos explícitos, comportamiento adaptativo, progresión guiada con pistas y generación automática de un informe final en Markdown exportado a PDF y entregado en Moodle. El corpus de evidencia recogido en SSI (véase fichero <i>laboratorios-educativos-artefactos-evidencias.zip</i> disponible para su descarga en: https://drive.google.com/drive/folders/1w-yOpy9nMQy4WjIYpTAG8pIWfmym6sE?usp=sharing) asciende a 439 artefactos clasificados (153 en P1, 147 en P2, 83 en P3 y 56 en P4, entre informes de IA, comparativas multi-modelo y retroalimentación docente). Estos resultados se documentan en detalle en el artículo aceptado para su publicación y presentación en 19th annual International Conference of Education, Research and Innovation (ICERI2026), congreso internacional de innovación docente (véase artículo adjunto).
Objetivo nº 2	Diseñar, desarrollar, probar e implantar el laboratorio educativo sobre análisis de riesgos
Actividades que había previsto en la solicitud del proyecto:	A4. Diseñar el contenido del laboratorio educativo sobre análisis de riesgos utilizando la metodología MAGERIT del Ministerio de Hacienda y Administraciones Públicas. A5. Desarrollar y probar este laboratorio educativo mediante la creación de <i>prompts</i> interactivos, siguiendo las mismas pautas establecidas en la actividad A2. A6. Implantar el laboratorio educativo desarrollado en la asignatura AAR.
Actividades realizadas y resultados obtenidos:	Se ha diseñado, desarrollado, probado e implantado el laboratorio interactivo de análisis de riesgos basado en MAGERIT (identificación de activos, clasificación de amenazas, análisis cualitativo y cuantitativo, diseño de salvaguardas, riesgo residual y árboles de ataque) en la asignatura Auditoría y Análisis de Riesgos (AAR) del Máster en Seguridad Informática (Ciberseguridad) de la UCA, con 40 artefactos clasificados (10 por cada uno de ChatGPT, Gemini, asistente especializado y comparativa). Adicionalmente, y como extensión no prevista inicialmente, pero alineada con el objetivo de transferibilidad del proyecto,

	se trasladó el laboratorio de auditoría de contraseñas de la asignatura SSI a AAR con un enfoque orientado a la interpretación de riesgo y la elaboración de informes profesionales, generando 40 artefactos adicionales. En total, el corpus de AAR asciende a 80 artefactos clasificados (véase fichero <i>laboratorios-educativos-artefactos-evidencias.zip</i> en: https://drive.google.com/drive/folders/1w-yOpy9nMQy4WjIIYpTAG8pIWfmym6sE?usp=sharing). Ambos laboratorios demuestran que la misma arquitectura de <i>prompt</i> es transferible a un contexto de máster más analítico y orientado a la toma de decisiones.
Objetivo nº 3	Evaluar los laboratorios educativos desarrollados para analizar su impacto en las asignaturas implantadas
Actividades que había previsto en la solicitud del proyecto:	A7. Realizar un cuestionario anónimo en Moodle a los estudiantes de las asignaturas SSI y AAR para analizar los resultados obtenidos y extraer conclusiones sobre aspectos como son: el grado de motivación, funcionalidad y utilidad (refuerzo de conocimientos, entre otros) en el proceso de enseñanza-aprendizaje de los <i>prompts</i> interactivos utilizados para llevar a cabo los laboratorios educativos, el grado de satisfacción con las herramientas IA usadas como Google Gemini y ChatGPT (junto con sus versiones públicas como PentestGPT y Ethical Hacker GPT), posibles errores detectados durante la ejecución de los <i>prompts</i>, sugerencias de mejora sobre estos laboratorios desarrollados e impulsados por la IA y la necesidad de seguir implantándolos en cursos posteriores.
Actividades realizadas y resultados obtenidos:	Se ha realizado un doble análisis de impacto. Por un lado, un análisis cualitativo del corpus de 525 artefactos (véase fichero <i>laboratorios-educativos-artefactos-evidencias.zip</i> disponible para su descarga en: https://drive.google.com/drive/folders/1w-yOpy9nMQy4WjIIYpTAG8pIWfmym6sE?usp=sharing) generados durante el despliegue de los seis laboratorios (informes de IA, documentos comparativos entre modelos y retroalimentación docente), presentado y discutido en el artículo aceptado en ICERI2026 (adjunto a esta memoria). Por otro lado, un análisis cuantitativo mediante encuesta anónima en Moodle, respondida por 59 estudiantes de SSI (sobre 121 matriculados) y 15 de AAR (sobre 20 matriculados), cuyos resultados se detallan en el apartado “Análisis del impacto” y en la tabla de opinión del alumnado de esta memoria.
Objetivo nº 4	Fomentar la sostenibilidad y replicabilidad de los laboratorios en otras asignaturas y difundir los resultados
Actividades que había previsto en la solicitud del proyecto:	A8. Crear un catálogo de todos los laboratorios educativos creados en este proyecto con sus <i>prompts</i> y publicarlos en acceso abierto a través de plataformas como RODIN y Zenodo. A9. Elaborar un informe de buenas prácticas sobre cómo

	crear laboratorios educativos impulsados por IA para otras asignaturas de ciberseguridad y otras materias tanto de grado como de máster. A10. Difundir las contribuciones y los resultados de este proyecto a través de su publicación y presentación en un congreso de innovación docente, preferiblemente de carácter internacional, y la organización de un seminario en la Escuela Superior de Ingeniería.
Actividades realizadas y resultados obtenidos:	Se ha creado el catálogo de los seis laboratorios educativos con sus <i>prompts</i> interactivos y se ha publicado en acceso abierto en Zenodo junto con el artículo de ICERI2026 https://doi.org/10.5281/zenodo.22713445. Se ha elaborado el informe de buenas prácticas “Informe de buenas prácticas sobre cómo crear laboratorios educativos impulsados por IA”, que recoge principios de diseño, arquitectura recomendada de <i>prompt</i>, patrones de escenarios y casos, criterios de evaluación (rúbrica 0-10) y una <i>checklist</i> de calidad técnica y ética, aplicable a otras asignaturas de ciberseguridad y de grado/máster (documento adjunto a esta memoria). Como se ha indicado previamente, los resultados del proyecto han sido aceptados para su publicación y presentación en ICERI2026 (artículo adjunto). Asimismo, se ha organizado un seminario de difusión en la Escuela Superior de Ingeniería (véase el apartado de difusión de esta memoria).
Objetivo nº 5	Coordinar y realizar un seguimiento de las actividades previstas
Actividades que había previsto en la solicitud del proyecto:	A11. Realizar reuniones (preferentemente virtuales) mensuales de coordinación y seguimiento de las actividades planificadas en el cronograma, analizando el porcentaje de completitud de cada tarea realizada y los resultados obtenidos.
Actividades realizadas y resultados obtenidos:	El equipo del proyecto (Juan Boubeta Puig, Jesús Rosa Bilbao y Kevin Jesús Valle Gómez) ha mantenido reuniones periódicas de coordinación y seguimiento del cronograma, revisando el grado de completitud de cada actividad y los resultados obtenidos en cada laboratorio. Asimismo, ha realizado un seguimiento adicional específico del trabajo del becario Anderson Araújo Alves, contratado con cargo a este proyecto de innovación docente, en el soporte al desarrollo de los laboratorios y en la elaboración del informe de buenas prácticas.

2. Realice una breve valoración sobre la influencia del proyecto ejecutado en la evolución de las asignaturas implicadas.

<i>Análisis del impacto de la innovación en las asignaturas relacionadas con el proyecto</i>
En cuanto a la asignatura SSI:

- Las expectativas iniciales de dificultad estaban repartidas: un 38,98% anticipaba dificultad media y solo un 18,64% (bastante/mucha) esperaba una experiencia muy exigente.
- Al finalizar la asignatura, la percepción de dificultad mejoró claramente: un 71,18% de los estudiantes declaró ninguna o poca dificultad para comprender los contenidos.
- La satisfacción general fue muy alta: un 86,44% se mostró muy o completamente satisfecho con los conocimientos adquiridos.
- Hubo un apoyo mayoritario a que los laboratorios impulsados por IA sigan proponiéndose en esta y otras asignaturas: un 69,49% se mostró muy o completamente de acuerdo.

En cuanto a la asignatura AAR:

- Un 60% de los estudiantes anticipaba dificultad media, bastante o mucha antes de comenzar la asignatura.
- Al finalizar, un 80% declaró ninguna o poca dificultad, lo que evidencia una mejora notable respecto a las expectativas iniciales.
- La satisfacción con los conocimientos adquiridos fue muy elevada: un 93,33% se mostró muy o completamente satisfecho.
- El apoyo a la continuidad de los laboratorios con IA fue igualmente alto: un 80% se mostró muy o completamente de acuerdo.

En ambas asignaturas, SSI y AAR, los laboratorios educativos impulsados por IA han contribuido a reducir la brecha entre la dificultad percibida al inicio y la dificultad real experimentada al finalizar la asignatura, y han sido valorados de forma muy positiva por el alumnado como recurso de aprendizaje, en línea con lo reportado en el artículo aceptado en ICERI2026 adjunto a esta memoria.

Por tanto, este Proyecto de Innovación Docente (PID) ha mejorado los procesos de enseñanza-aprendizaje sobre ciberseguridad (línea prioritaria 1 de “metodologías activas y nuevas formas de proporcionar al alumnado recursos que mejoren su aprendizaje”) mediante la creación de laboratorios educativos potenciados por la IA (línea prioritaria 3 de “materiales y recursos educativos” y línea prioritaria 4 de “docencia multimodal, y uso y aplicación de recursos tecnológicos e IA”), haciendo uso de herramientas novedosas de IA como Google Gemini, ChatGPT, HackerAI y PentestGPT.

3. **Incluya en la siguiente tabla el número de alumnado matriculado y el de respuestas recibidas en cada opción y realice una valoración crítica sobre la influencia que el proyecto ha ejercido en la opinión del alumnado.**

Opinión del alumnado al inicio del proyecto				
Número de alumnado matriculado:		SSI: 121 matriculados / 59 respuestas (48,76%) AAR: 20 matriculados / 15 respuestas (75%)		
Valoración del grado de dificultad que cree que va a tener en la comprensión de los contenidos y/o en la adquisición de competencias asociadas a la asignatura en la que se enmarca el proyecto de innovación docente				
Ninguna dificultad	Poca dificultad	Dificultad media	Bastante dificultad	Mucha dificultad
SSI: 13,56% AAR: 6,67%	SSI: 28,81% AAR: 33,33%	SSI: 38,98% AAR: 33,33%	SSI: 15,25% AAR: 20%	SSI: 3,39% AAR: 6,67%
Opinión del alumnado en la etapa final del proyecto				
Valoración del grado de dificultad que ha tenido en la comprensión de los contenidos y/o en la adquisición de competencias asociadas a la asignatura en la que se enmarca el proyecto de innovación docente				
Ninguna dificultad	Poca dificultad	Dificultad media	Bastante dificultad	Mucha dificultad

SSI: 28,81% AAR: 33,33%	SSI: 42,37% AAR: 46,67%	SSI: 22,03% AAR: 6,67%	SSI: 3,39% AAR: 13,33%	SSI: 3,39% AAR: 0%
<i>Los elementos de innovación y mejora docente aplicados en esta asignatura han favorecido mi comprensión de los contenidos y/o la adquisición de competencias asociadas a la asignatura</i>				
Nada de acuerdo	Poco de acuerdo	Ni en acuerdo ni en desacuerdo	Muy de acuerdo	Completamente de acuerdo
SSI: 10,17% AAR: 0%	SSI: 5,08% AAR: 0%	SSI: 15,25% AAR: 20%	SSI: 45,76% AAR: 33,33%	SSI: 23,73% AAR: 46,67%
En el caso de la participación de profesorado invitado				
<i>La participación del profesorado invitado ha supuesto un gran beneficio en mi formación</i>				
Nada de acuerdo	Poco de acuerdo	Ni en acuerdo ni en desacuerdo	Muy de acuerdo	Completamente de acuerdo
Valoración crítica sobre la influencia que ha ejercido el proyecto en la opinión del alumnado				
Este PID ha impactado muy significativamente en el estudiantado, como demuestran los resultados recogidos en esta tabla, en el apartado de análisis del impacto de esta memoria y en el artículo adjunto y aceptado para su publicación en el congreso internacional ICERI2026. En las dos asignaturas (SSI y AAR), buena parte del estudiantado esperaba, antes de comenzar la asignatura, una dificultad media o alta para comprender sus contenidos. Tras finalizar las asignaturas, e influido por la puesta en marcha de este PID, ese nivel de dificultad percibida se redujo de forma notable a ninguna/poca dificultad en la mayoría de los casos. Además, la satisfacción con los conocimientos adquiridos fue muy alta en ambas asignaturas. Asimismo, los laboratorios educativos impulsados por IA desarrollados en este PID han favorecido significativamente la comprensión de los contenidos por parte del estudiantado: un 69,49% en SSI y un 80% en AAR se mostraron muy o completamente de acuerdo en que deberían seguir proponiéndose en esta y otras asignaturas. A continuación, se citan literalmente algunos de los comentarios realizados por los estudiantes sobre dichos laboratorios: - “Las tareas de los prompts son muy amenas y educativas.” - “Considero que en los ejercicios de prompt, el apartado de comparar los resultados puede resultar pesado, y en muchos casos lo hace una inteligencia artificial. Por el contrario, considero que se hace entretenido y amena la parte de usar el prompt.” - “Hay que darle una vuelta al tema de las entregas de los prompts, consumen más tiempo del deseado. Con hacerlos solo con un solo modelo y no con varios.” - “Los prompts son buena idea como actividad extra pero no debería sustituir a las prácticas de la asignatura o cualquier contenido teórico. Por mucho que esté controlado el contenido que enseña la LA con los prompts, sigo prefiriendo que dicho contenido esté supervisado al milímetro y enseñado por un profesor real.” Por tanto, en líneas generales, una gran mayoría de estudiantes está satisfecha con los laboratorios propuestos en este PID, aunque mencionan como línea de mejora la posibilidad de que conlleven una menor carga de trabajo en futuras ediciones reduciendo el número de modelos a emplear y comparar (de hecho, ya se aplicó esta medida en los últimos laboratorios implantados). Por otro lado, hay que destacar el deseo de uno de los estudiantes para que este tipo de laboratorios impulsados por IA nunca reemplace la labor del docente (precisamente el enfoque que se ha seguido en este PID ha sido siempre como actividad formativa complementaria, nunca sustitutiva de la labor docente).				

4. **Describa las medidas de difusión a las que se comprometió en la solicitud y las que ha llevado a cabo. Describe, analice y valore los desajustes respecto a lo previsto en el proyecto y las soluciones aplicadas.**

Descripción de las medidas comprometidas en la solicitud
Se llevará a cabo un seminario en la Escuela Superior de Ingeniería para presentar la experiencia y las conclusiones derivadas del análisis de los resultados obtenidos en este proyecto. Concretamente, el programa del seminario será el siguiente: 1. Introducción 2. Objetivos del proyecto 3. Actividades realizadas 4. Resultados del proyecto 5. Conclusiones El evento está programado para realizarse entre julio y septiembre de 2026, y se proporcionará una grabación del seminario a través de los canales de la UCA. Una vez que se hayan alcanzado los objetivos de este proyecto, se prevé presentar las contribuciones en un congreso de innovación docente, preferiblemente de carácter internacional, con el propósito de dar a conocer el proyecto y sus beneficios y resultados.
Descripción de las medidas que se han llevado a cabo
El 25 de septiembre de 2026, a las 11:00 h., en el aula FS16 de la Escuela Superior de Ingeniería de la UCA se ha impartido un seminario sobre los resultados de este PID. La grabación del seminario se encuentra disponible en: https://drive.google.com/drive/folders/1w-yOpy9nMQy4WjIIYpTAG8pIWfmym6sE?usp=sharing Además, se han publicado los resultados en el congreso de innovación docente internacional ICERI2026 (véase artículo adjunto): J. Boubeta-Puig, J. Rosa-Bilbao, A. Araújo-Alves, K.J. Valle-Gómez. “From Prompts to AI-Powered Cybersecurity Labs: A Design and Deployment Study in Security in Computer Systems and Audit and Risk Analysis Courses”, en 19th annual International Conference of Education, Research and Innovation (ICERI2026), Seville, Spain: IATED, Nov. 2026 (<i>aceptado para su publicación</i>). Asimismo, se ha creado y publicado en acceso abierto en Zenodo el catálogo de los seis laboratorios educativos con sus <i>prompts</i> (https://doi.org/10.5281/zenodo.22713445), y se ha elaborado el informe de buenas prácticas para la creación de laboratorios educativos impulsados por IA (documento adjunto a esta memoria).

5. **Conclusiones. Entre ellas, describa las aplicaciones futuras del proyecto, su sostenibilidad y posible continuidad y estrategias para ello.**

Conclusiones
Este PID ha permitido evolucionar de un enfoque centrado en <i>prompts</i> aislados a un modelo completo de laboratorios educativos potenciados por IA, desplegado con éxito en dos asignaturas de perfiles muy distintos: SSI (Grado en Ingeniería Informática) y AAR (Máster en Seguridad Informática). Los seis laboratorios desarrollados, el corpus de 525 artefactos analizado y las encuestas anónimas realizadas confirman que el modelo es viable, transferible entre grado y máster, y bien valorado por el estudiantado. De cara a la aplicación futura del proyecto, se prevé: (i) la reutilización directa de los seis laboratorios y del catálogo publicado en Zenodo en próximas ediciones de SSI y AAR; (ii) la extrapolación del patrón de diseño validado y del informe de buenas prácticas elaborado a otras asignaturas de ciberseguridad y a otras materias del Grado en Ingeniería Informática y del Máster en Seguridad Informática; y (iii) la

profundización de la evaluación de impacto mediante rúbricas explícitas y la analítica de aprendizaje con los resultados obtenidos en este curso.

La sostenibilidad del proyecto está reforzada por su bajo coste operativo (los laboratorios funcionan con herramientas de IA ya accesibles al estudiantado y con los mecanismos de entrega ya utilizados en Moodle), por la documentación generada (*prompts*, informe de buenas prácticas y artículo científico) y por la continuidad del equipo de trabajo, que ya ha liderado cinco PID consecutivos sobre estas asignaturas.

FROM PROMPTS TO AI-POWERED CYBERSECURITY LABS: A DESIGN AND DEPLOYMENT STUDY IN SECURITY IN COMPUTER SYSTEMS AND AUDIT AND RISK ANALYSIS COURSES

J. Boubeta-Puig, J. Rosa-Bilbao, A. Araújo-Alves, K.J. Valle-Gómez

University of Cadiz (SPAIN)

Abstract

The widespread adoption of Large Language Models (LLMs) is driving pedagogical innovation in higher education. This paper presents the outcomes of a teaching innovation project conducted at the University of Cadiz (Spain) during the academic year 2025–2026. Evolving from isolated prompt design to fully integrated, Artificial Intelligence (AI)-powered cybersecurity laboratories, the project was deployed across two courses: Security in Computer Systems (Bachelor's Degree in Computer Science and Engineering) and Audit and Risk Analysis (Master's Degree in Cybersecurity). Six laboratory experiences were implemented, covering password auditing, Open Source Intelligence (OSINT) reconnaissance, enumeration, applied cryptography, and MAGERIT-based risk analysis. Based on a qualitative, corpus-oriented analysis of 525 generated artifacts, including AI-produced reports, cross-model comparisons, and instructor feedback, the results indicate that the proposed laboratory model is feasible across the undergraduate and master's context studied, adaptable to diverse AI ecosystems, and applicable to both procedural and decision-oriented learning. Multi-model deployments comparing ChatGPT, Gemini, and domain-specific AI assistants such as HackerAI and PentestGPT provided the most extensive comparative evidence. Overall, this study suggests that structured prompts can serve as reusable, scalable laboratory blueprints when embedded with ethical guidelines, transparent output simulation, and systematic student reporting.

Keywords: Cybersecurity, artificial intelligence, prompt, large language model, ChatGPT, Gemini.

1 INTRODUCTION

The rapid adoption of Large Language Models (LLMs) in higher education is reshaping the design of practical learning activities, especially in technically demanding domains such as cybersecurity [1], [2]. In this context, prompt engineering is no longer a merely technical issue: it becomes a pedagogical design problem because the quality of the student-Artificial Intelligence (AI) interaction depends on how goals, constraints, scaffolding, and expected outputs are specified [3], [4], [5].

During the academic year 2024–2025, we developed a Teaching Innovation Project (TIP) focused on the analysis and creation of AI prompts for learning to attack and defend computer systems. The results, presented at the 18th annual International Conference of Education, Research and Innovation (ICERI 2025) [6], suggested that well-designed prompts can support the teaching-learning process in cybersecurity courses at the University of Cadiz (UCA), Spain. However, that previous experience focused primarily on the prompt as a standalone instructional artifact.

To address this limitation, during the academic year 2025–2026, we developed a new TIP whose outcomes are reported in this paper. This TIP took a further step: prompts were redesigned as complete AI-powered laboratories. Instead of simply eliciting answers from a chatbot, each prompt scripted a guided practical session with staged interaction, adaptive difficulty, ethics and privacy checks, evidence gathering, and final report generation. This evolution is consistent with our previous line of teaching innovation in cybersecurity, which has already explored gamification, digital self-assessment resources, and mobile-compatible learning materials [7], [8], [9], [10]. The TIP was deployed in two complementary courses: Security in Computer Systems (SCS), in the Bachelor's Degree in Computer Science and Engineering, with a strong hands-on orientation in pentesting, password security, Open Source Intelligence (OSINT) and system analysis; and Audit and Risk Analysis (ARA), in the Master's Degree in Cybersecurity, oriented towards audit, risk analysis and professional decision-making. Combining both settings allowed us to test whether the same AI-based laboratory philosophy could support students with different prior knowledge, curricular profiles, and expected learning outcomes.

The contribution of this paper is threefold: (i) it documents the instructional design principles used to transform prompts into reusable laboratories, (ii) it reports the actual deployment across SCS and ARA, and (iii) it analyses a corpus of 525 artifacts generated during the project to characterize recurrent instructional and deployment patterns.

The results show that the proposed laboratory model is feasible in both the undergraduate and master's contexts studied, can support both procedural and decision-oriented activities, and can be adapted to different AI ecosystems. The richest evidence comes from the multi-model deployments of several laboratories, where students compared ChatGPT, Gemini, and specialized cybersecurity assistants. Overall, the results indicate that carefully scripted prompts can act as reusable laboratory blueprints, provided that ethical boundaries, transparency about simulated outputs, and structured reporting are embedded from the start.

The remainder of this paper is structured as follows. Section 2 describes the project context, laboratory design, and research methodology. Section 3 presents and discusses the deployment results and corpus findings. Finally, Section 4 summarizes the main conclusions and outlines future work.

2 METHODOLOGY

This section describes the project context, the design architecture of the AI-powered laboratories, the instructional design process, the deployment workflow across the target courses, the generated artifact corpus, and the analysis strategy.

2.1 Project context and laboratory design

The TIP pursued four practical goals: to design AI-powered cybersecurity laboratories for SCS, to build specific laboratories for ARA, to assess their feasibility and instructional value through student work, and to prepare transferable materials for reuse in future editions. Table 1 summarizes the six laboratory experiences that were deployed.

Table 1. Laboratory experiences deployed in the project

Course	Lab	Title	Main learning focus
SCS	P1	Password Security Audit	SHA-256 hashing, dictionary attacks with Hashcat, Have I Been Pwned (HIBP) verification, strength estimation, password policy recommendations, structured report writing
	P2	OSINT Reconnaissance Interactive Lab	Google dorks, Shodan, Wayback Machine, Domain Name System (DNS) and Whois analysis, technology fingerprinting, social footprinting, ethical reflection
	P3	Crypto Decision & Real-World Security Lab	Applied cryptography choices, algorithm selection, secure configurations, certificate handling, identification of common cryptographic mistakes
	P4	Reconnaissance & Enumeration Decision Lab	Passive versus active recon, footprinting strategies, low-impact scanning decisions, enumeration interpretation, banner analysis
ARA	P1	MAGERIT Interactive Risk Analysis Lab	Asset identification, threat classification, qualitative and quantitative risk analysis, safeguard design, residual risk evaluation, attack-tree reasoning

	P2	Password Security Audit	Transfer of the password-auditing lab to a master's context focused on risk-oriented interpretation and reporting
--	----	-------------------------	---

Although the topics were different, the prompts shared a stable instructional architecture:

- collection of pseudonymized student identifiers using institutional IDs only;
- prompts authored in English, but student-facing interaction fully conducted in Spanish;
- explicit ethics and scope limitations, discouraging misuse and real-world abuse;
- adaptive behavior based on an initial diagnostic question;
- step-by-step progression with hints before complete answers;
- encouragement of synthetic or academic examples instead of real credentials or sensitive data;
- automatic generation of a final report in Markdown, intended to be exported as PDF and uploaded to Moodle.

This common pattern positions the AI system as a laboratory facilitator. The prompt does not merely request content: it organizes the practical activity, manages pacing, collects evidence, and produces a traceable deliverable. In addition, the first deployment rounds were intentionally designed for cross-model comparison, asking students to execute the same prompt with ChatGPT, Gemini, and specialized cybersecurity assistants such as HackerAI and PentestGPT.

The shift from prompt to laboratory was motivated by a recurring teaching problem: many cybersecurity practical activities are conceptually rich but operationally fragmented. Students may know that they must use a tool, inspect a result, or make a decision, but they are not always able to connect the sequence of actions with the underlying rationale. In conventional labs, instructors may need to intervene to restore that connection. The prompts were therefore designed to externalize part of that mentoring process.

From an instructional point of view, each laboratory was expected to satisfy five conditions. First, it had to preserve the authentic flavor of cybersecurity practice instead of replacing it with generic AI conversation. Second, it had to offer just enough scaffolding to keep novice learners moving without removing productive struggle. Third, it had to make reflection visible by asking students to justify choices and interpret outputs. Fourth, it had to be safe by design, explicitly limiting real-world misuse. Fifth, it had to produce an assessable artifact compatible with existing course workflows.

These conditions explain why the laboratories mixed operational steps and reflective tasks. For example, the password-auditing lab combined hashing, dictionary attacks, HIBP checks, and policy discussion; the OSINT lab combined public-source querying with ethical reflection; the cryptography lab emphasized scenario-based decision-making; and the Methodology for the Analysis and Management of Information System Risks (MAGERIT) lab moved from assets and threats to residual risk and recommendations. In all cases, AI was framed as a structured interlocutor that supported reasoning, not as a black-box answer engine.

2.2 Instructional design process

The first step was to identify practical activities that usually require repeated explanations, iterative feedback, and support in interpreting technical results. This led to the selection of password auditing, OSINT, applied cryptography, reconnaissance/enumeration, and risk analysis.

The second step was to author prompts as laboratory scripts rather than as isolated questions. Each script specified the AI role, language policy, ethical constraints, expected workflow, intermediate evidence, and final report template. The laboratories were therefore designed to be executable learning sequences. All lab exercises are openly published and accessible at [11].

The third step was deployment. In the initial laboratories, students were explicitly instructed to copy, paste, and execute each prompt with four AI systems: Gemini, ChatGPT, HackerAI and PentestGPT. Note that students used the premium version of Gemini provided by UCA to its community, while using the free versions of the other AI systems. For every run, students submitted the generated report and a short comparative document discussing differences, detected issues, and potential prompt

improvements. In later laboratories, the available corpus reflects a more focused implementation pattern, with stronger concentration on Gemini reports and instructor feedback documents.

2.3 Deployment workflow in the courses

In SCS, the laboratories were integrated into the practical dynamics of the course, where students usually work in small groups and submit evidence through Moodle. The AI-supported activities were therefore not external demonstrations, but part of the standard workflow through which students document their practical progress. In ARA, the same strategy was adapted to a smaller sample and to a more analytical profile, especially in the MAGERIT-based activity.

Students were instructed to avoid personal names and surnames in their interactions with AI systems and in the PDF deliverables. Instead, they identified themselves exclusively through their institutional student ID. This also aligned the activity with basic privacy and data-minimization principles. The prompts themselves reinforced that policy by insisting on synthetic examples and by forbidding the use of real passwords or sensitive operational data.

The delivery model was deliberately simple: each AI execution ended with a report exported as PDF, and the comparative tasks asked students to synthesize differences among models. This simplicity was intended to avoid fragile workflows dependent on external integrations. In this project, by contrast, the prompts were designed to work with the tools already accessible to students and through standard campus submission mechanisms.

2.4 Artifact corpus

The study is based on a corpus of 525 files generated during the deployment of the laboratories. Of these, 519 can be directly classified as AI-generated reports, student comparative reports, or instructor feedback documents; the remaining files correspond to ancillary materials such as working notes and text/markdown variants. Table 2 summarizes the classified evidence by course and laboratory.

Table 2. Classified evidence available in the analyzed corpus

Course	Lab	ChatGPT	Gemini	Specialized AI systems	Comparative	Feedback
SCS	P1 Password audit	38	39	38	38	0
	P2 OSINT	37	38	36	36	0
	P3 Crypto decisions	4	38	3	3	35
	P4 Recon & enumeration	0	30	0	0	26
ARA	P1 MAGERIT risk analysis	10	10	10	10	0
	P2 Password audit	10	10	10	10	0

The corpus shows two relevant features. First, the early laboratories produced a rich four-model comparison dataset in both SCS and ARA. Second, the later SCS laboratories shifted towards a more focused deployment pattern, with Gemini becoming dominant in the available evidence and instructor comments appearing as an additional feedback layer. This variation reflects the evolution of the project under real classroom conditions.

2.5 Analysis strategy

The analysis reported here is qualitative and corpus-oriented. We examined the laboratory prompts, the delivery instructions, the distribution of submissions, and the comparative documents produced by

students in the multi-model deployments. Our aim was not to estimate causal learning gains through experimental design, but to assess feasibility, transferability, and recurrent instructional patterns.

More specifically, the analysis focused on four dimensions. The first was *instructional structure*: whether the prompt created a clear sequence of phases, checkpoints, and expected products. The second was *pedagogical support*: whether the interaction included diagnostics, hints, or progressive disclosure. The third was *model behavior*: differences in continuity, technical depth, formatting quality, and transparency when a model could not execute or verify an external action. The fourth was *assessment readiness*: whether the final artifact was sufficiently structured to support teacher review and student self-reflection.

This analytical approach is coherent with the purpose of the paper. The objective is not to benchmark AI systems as commercial products, but to understand how different systems behave when embedded in authentic laboratory scripts and how those behaviors may shape the learning experience.

3 RESULTS

The results are presented at two complementary levels. First, we discuss what the deployment reveals about the laboratory model itself across SCS and ARA. Second, we analyze what the corpus suggests about the behavior of different AI-supported laboratory formats and their pedagogical implications.

3.1 A reusable laboratory pattern across two courses

The first result is design-related: prompts can be transformed into reusable laboratory blueprints. This was observed not only in SCS, where technical procedural guidance was central, but also in ARA, where the same philosophy was used to support a more analytical and decision-oriented activity based on MAGERIT.

The two-course deployment matters pedagogically. In SCS, the prompts guided students through practical steps such as hashing, search queries, or reconnaissance choices. In ARA, the same architecture supported asset analysis, threat classification, residual risk reasoning, and structured reporting. This suggests that the approach can be applied across different topics and the two academic levels studied.

A relevant nuance is that the same design pattern did not produce identical laboratories. Instead, it supported a family of laboratories with shared pedagogical grammar. The prompt always opened with context collection, framed the scope of the task, adapted the level of support, and closed with a report. What changed was the balance between procedural execution and professional judgment. This is precisely what makes the pattern reusable: it is stable enough to be recognizable, but flexible enough to fit different cybersecurity competencies.

3.2 What the corpus says about deployment patterns

The second result concerns variation across the deployments. The password and OSINT laboratories generated the most balanced multi-model evidence, while the applied cryptography and reconnaissance/enumeration laboratories show a more asymmetric distribution of submissions. In practical terms, this means that the project ended the year with two recurring deployment patterns:

- *Fully comparative laboratories*, where the same prompt was executed with several AI systems and students explicitly documented differences;
- *Focused laboratories*, where the prompt acted as a guided instructional script, but the archived evidence concentrated on one dominant AI platform together with instructor comments.

These patterns illustrate two complementary modes of pedagogical use. Comparative deployment can be useful when the learning objective includes critical evaluation of AI behavior. Focused deployment may be more suitable when the priority is sustained guidance in concept-heavy decision tasks.

It is also worth noting that the comparative mode has meta-learning value. When students compare several AI systems on the same prompt, they do not only learn the cybersecurity topic; they also learn to interrogate AI critically. They notice differences in verbosity, reliability, continuity, and confidence. In an era where students are already using LLMs informally, converting that informal use into an explicit object of analysis can provide educational value by fostering the development of AI literacy.

3.3 Detailed findings from the password-auditing laboratory

The richest qualitative evidence comes from the password-auditing laboratory, which was deployed in both SCS and ARA and served as the clearest four-model comparison exercise. Four findings stand out:

- *The laboratory format was feasible and understandable.* Students were generally able to follow the workflow, collect intermediate evidence, and submit a final report. The combination of progressive steps, adaptive hints, and a predefined reporting structure helped turn a technically fragmented exercise into a coherent laboratory sequence.
- *Gemini was often perceived as the most stable option for long workflows.* In the comparative documents, Gemini was repeatedly associated with orderly progression, visually clean outputs, and strong continuity across several steps of the same activity.
- *ChatGPT was valued for clarity and accessibility.* Students often described ChatGPT as concise and beginner-friendly, which is particularly useful in the early stages of a laboratory. However, some groups also reported continuity issues when long conversations were interrupted.
- *Specialized cybersecurity assistants tended to provide deeper technical detail, but sometimes with less consistency.* HackerAI and PentestGPT were often perceived as technically ambitious, which can be valuable for advanced students, although this occasionally came with overelaborated explanations or outputs that looked more simulated than directly grounded.

Across the comparative evidence, one issue appeared repeatedly: some systems simulated the results of external services such as Have I Been Pwned or password-strength estimators. From a teaching perspective, simulated outputs can keep the activity moving when browsing or tool execution is unavailable. Nevertheless, transparency is essential. Students and instructors need the prompt to clearly distinguish what is executed, what is estimated, and what is simulated.

This finding is particularly relevant to cybersecurity education, where evidence provenance matters. If a learner cannot distinguish between an observed result, a plausible estimate, and a fabricated but pedagogically convenient simulation, the activity may accidentally instill incorrect epistemic habits. One of the clearest design implications of the project is therefore the need to encode provenance cues directly into the prompt.

3.4 Findings from OSINT, cryptography, and risk-analysis laboratories

The broader corpus also helps characterize the remaining laboratories, even where evidence is less symmetrical than in the password case.

In the OSINT laboratory, the prompt helped structure open-ended exploration. OSINT activities can easily become unbounded because students have many possible tools, queries, and targets to choose from. The laboratory script reduced that dispersion by dividing the process into recognizable phases: Google dorks, Shodan, Wayback Machine, DNS analysis, technology fingerprinting, and social-footprint exploration. This phased design combined freedom of exploration with enough order to make the resulting report coherent.

In the applied cryptography laboratory, the value of AI support was less procedural and more dialogic. Students were not primarily executing commands; they were deciding whether to use symmetric or asymmetric cryptography, whether a certificate configuration was acceptable, or why a given design choice was unsafe. This suggests that AI-powered laboratories are not limited to command-driven practice. They can also support activities where the key competence is judgment under constraints.

In the reconnaissance and enumeration laboratory, the prompt emphasized strategic thinking before action. This is pedagogically relevant because novice learners often associate pentesting with immediate tool execution. By contrast, the lab asked them to reason about passive versus active reconnaissance, the cost of aggressive scanning, the interpretation of partial evidence, and the distinction between useful information and noise. Even with a more focused evidence pattern, the lab illustrates the potential of AI to scaffold professional thought habits.

Finally, the MAGERIT-based risk-analysis laboratory provided an example of transfer beyond strictly offensive or technical security tasks. Here, the AI-supported interaction revolved around assets, threats, qualitative and quantitative risk analysis, safeguards, residual risk, and attack trees. This reinforces the methodological contribution of the project: a well-scripted prompt can support different forms of cybersecurity reasoning, from hands-on technical practice to formal analytical reasoning.

3.5 Cross-lab instructional lessons

Beyond individual laboratories, the corpus yields five broader instructional lessons.

First, the final Markdown-to-PDF report is not a minor implementation detail. It serves as a pedagogical device by requiring the AI interaction to end in a structured, assessable artifact. This makes the laboratory compatible with standard virtual campus workflows and can reduce ambiguity in grading.

Second, ethical and privacy constraints need to be embedded directly in the prompt. The most robust scripts explicitly prohibited the use of real credentials, requested only academic or fictitious data, and reminded students not to disclose personal information in either the AI conversation or the PDF submission.

Third, AI laboratories can be particularly useful when they combine explanation with decision-making. The strongest prompts did not simply provide commands or definitions; they asked students to choose, justify, compare, interpret, and reflect. This is why the same design logic worked in both technical labs such as password auditing or OSINT and analytical labs such as MAGERIT-based risk analysis.

Fourth, language adaptation should not be underestimated. Writing the prompts in English while requiring all student-facing interaction in Spanish provided a practical implementation choice. It allowed prompt authors to work with a flexible drafting style while preserving accessibility for students. In multilingual educational settings, this separation between authoring language and interaction language may be especially useful.

Finally, the project suggests that prompt quality in education should be judged less by rhetorical brilliance and more by operational robustness. The more operationally robust prompts were not necessarily the most sophisticated in wording; rather, they were the ones that controlled scope, paced the interaction, reduced ambiguity, and yielded a final artifact that both students and teachers could use.

3.6 Limitations

This study has clear limitations. First, the artifact corpus is not uniform across all laboratories; some activities generated balanced four-model comparisons, whereas others relied primarily on one dominant model and instructor comments. Second, the analysis is based on authentic student deliverables rather than on controlled pre/post testing. Consequently, the findings support feasibility, transferability, and instructional design quality rather than causal learning gains.

Additionally, the volatility of AI platforms presents an ongoing contextual constraint. Model behaviors change over time due to system updates, usage caps, or interface modifications. This highlights the importance of designing prompts and workflows that remain pedagogically effective despite changing underlying technologies.

4 CONCLUSIONS AND FUTURE WORK

This paper has presented the full first-year deployment of an AI-powered laboratory model in two cybersecurity courses at the University of Cadiz. The project moved from prompt engineering as an isolated activity to prompt engineering as laboratory orchestration. Across six deployed experiences and 525 analyzed artifacts, the results support the feasibility, reusability, and adaptability of this model to both undergraduate and master's teaching.

The results suggest that educational value does not stem from using AI alone, but from scripting the interaction so that AI behaves as a structured lab facilitator. The laboratory design combined ethical framing, adaptive questioning, step-by-step support, evidence collection, and automatic report generation.

From a practical perspective, the project leaves three consolidated outcomes: six AI-supported cybersecurity laboratory experiences deployed under real teaching conditions, a large corpus of authentic artifacts suitable for pedagogical analysis, and a documented design pattern that can inform future course editions. Future work will focus on deepening evaluation through learning analytics, rubric-based grading, and expansion to other cybersecurity courses.

ACKNOWLEDGEMENTS

This TIP was supported by the University of Cadiz during the academic year 2025–2026 [grant number sol-202500299689-tra]. The rest of coauthors of this paper would like to thank the student Anderson Araújo-Alves for his contribution to the development of the base prompts, as well as all students who participated in the laboratory activities.

REFERENCES

- [1] S. Milano, J. A. McGrane, and S. Leonelli, 'Large language models challenge the future of higher education', *Nature Machine Intelligence*, vol. 5, no. 4, pp. 333–334, Apr. 2023, doi: 10.1038/s42256-023-00644-2.
- [2] L. R. Fernández, A. L. F. Mena, M. P. T. Magaña, M. A. R. Magaña, and M. A. R. Fernández, 'Inteligencia artificial en la educación: Modelo de lenguaje de gran tamaño (LLM) como recurso educativo', *IPSUMTEC*, vol. 7, no. 2, Art. no. 2, Nov. 2024, doi: 10.61117/ipsumtec.v7i2.321.
- [3] A. Muñoz, *Seguridad ofensiva en machine learning. +100 prompts injections en ChatGPT: Atacando y defendiendo organizaciones con prompt engineering*. Madrid: Independently published, 2023.
- [4] N. Mathews, C. Schwartz, and M. Wright, 'Teaching Generative AI for Cybersecurity: A Project-Based Learning Approach', *Journal of The Colloquium for Information Systems Security Education*, vol. 12, no. 1, pp. 10–10, Apr. 2025, doi: 10.53735/cisse.v12i1.211.
- [5] A. Reina, M. Bermúdez, E. García-Salcines, J. A. Lara, and C. Romero, 'Aplicación web de ayuda en la corrección automatizada de exámenes escritos de desarrollo utilizando IA generativa', *RIED-Revista Iberoamericana de Educación a Distancia*, vol. 29, no. 2, pp. 369–392, Apr. 2026, doi: 10.5944/ried.47116.
- [6] J. Boubeta-Puig, J. Rosa-Bilbao, and K. J. Valle-Gómez, 'Analysis and development of artificial intelligence prompts for learning to attack and defend computer systems', in *ICERI2025 Proceedings*, Seville, Spain: IATED, Nov. 2025, pp. 4619–4624. doi: 10.21125/iceri.2025.1328.
- [7] J. Boubeta-Puig, Á. Ruiz-Zafra, and K. J. Valle-Gómez, 'Improving the distance learning of the security in computer systems in time of crisis through serious games', in *EDULEARN21 Proceedings*, Online Conference: IATED, Jul. 2021, pp. 12322–12330. doi: 10.21125/edulearn.2021.2590.
- [8] J. Boubeta-Puig, K. J. Valle-Gómez, and A. Estero-Botaro, 'Developing gamified activities for improving online teaching-learning processes of the security in computer systems and risk analysis and management subjects', in *EDULEARN22 Proceedings*, Palma, Spain: IATED, Jul. 2022, pp. 9733–9741. doi: 10.21125/edulearn.2022.2346.
- [9] J. Boubeta-Puig, K. J. Valle-Gómez, J. Rosa-Bilbao, A. Muñoz, and G. Ortiz, 'Gamifying teaching-learning processes: A study on security in computer systems, security in distributed systems, and risk analysis and management courses', in *ICERI2023 Proceedings*, Seville, Spain: IATED, Nov. 2023, pp. 8975–8982. doi: 10.21125/iceri.2023.2292.
- [10] J. Boubeta-Puig, K. J. Valle-Gómez, and J. Rosa-Bilbao, 'Developing interactive self-assessment resources compatible with mobile devices for Bachelor's and Master's degree courses', in *ICERI2024 Proceedings*, Seville, Spain: IATED, Nov. 2024, pp. 4689–4697. doi: 10.21125/iceri.2024.1157.
- [11] J. Boubeta-Puig, J. Rosa-Bilbao, A. Araújo-Alves, and K. J. Valle-Gómez, 'Dataset for: From Prompts to AI-powered Cybersecurity Labs: A Design and Deployment Study in Security in Computer Systems and Audit and Risk Analysis Courses'. Zenodo, Sep. 2026. doi: 10.5281/zenodo.22713445.

Informe de buenas prácticas sobre cómo crear laboratorios educativos impulsados por IA

Aplicable a asignaturas de ciberseguridad y otras materias (Grado y Máster)

Proyecto de Innovación y Mejora Docente (curso 2025/2026): Creación de laboratorios educativos sobre seguridad en sistemas informáticos y análisis de riesgos mediante *prompts* de inteligencia artificial

Autores: Anderson Araújo Alves y Juan Boubeta Puig (Universidad de Cádiz)

Versión: v1.0

1) Contexto y propósito del informe

Este informe recoge un conjunto de **buenas prácticas, patrones de diseño y criterios de calidad** para crear **laboratorios educativos impulsados por IA** (LLM/chatbots) que actúan como **instructor interactivo** y guían al estudiantado paso a paso mediante **prompts estructurados**.

El objetivo es **facilitar la replicabilidad** de los laboratorios en distintas asignaturas y niveles (Grado/Máster), y asegurar que:

- la experiencia sea **pedagógicamente sólida**,
- el contenido sea **seguro y ético**,
- la interacción sea **evaluable**,
- y los laboratorios sean **sostenibles** (reusables y mantenibles en cursos posteriores).

2) Principios rectores (lo que NO debe romperse)

2.1. Enfoque didáctico: aprendizaje activo y guiado

- El laboratorio debe fomentar **aprendizaje activo**: el alumno decide, justifica, clasifica, reflexiona, corrige.
- La IA no “da la respuesta” de inmediato: **provoca razonamiento**, desafía supuestos y valida decisiones.

2.2. Ética y seguridad: laboratorio ≠ ataque real

- Debe existir un **Ethics Statement** explícito y visible.

- Prohibido fomentar acciones contra sistemas reales; todo debe ser **simulado/controlado/académico**.
- Evitar instrucciones accionables para daño (p. ej., “haz X en un objetivo real”). En su lugar:
 - *razonamiento, riesgo, impacto, mitigación, interpretación de evidencias,*
 - y ejecución solo cuando sea estrictamente sobre **herramientas académicas** o **entornos deliberadamente vulnerables** y autorizados (si aplica).

2.3. Reproducibilidad y trazabilidad

- El laboratorio debe producir un **informe final en Markdown** exportable a PDF.
- El informe final debe ser completo y servir como evidencia de aprendizaje y evaluación.
- Debe registrar “qué respondió el alumno” + “observaciones de la IA” + “nota/feedback”.

2.4. Multimodalidad y herramientas

- Diseñar para funcionar bien en **Google Gemini** y **ChatGPT** (y opcionalmente variantes).
- Controlar la salida: formato estable, instrucciones robustas, y no depender de funciones específicas de una IA.

3) Arquitectura recomendada del laboratorio (estructura estándar)

De acuerdo con la guía del proyecto, cada prompt debe contener secciones fijas: título, instrucciones de rol, información requerida del alumno, introducción, pasos del laboratorio, y exportación a PDF.

La estructura recomendada (ya validada en los prompts desarrollados) es:

1. **TITLE** (con versión y año)
2. **LANGUAGE RULE** (prompt en inglés, interacción en español)
3. **ROLE** (IA como instructor, NO ejecutor)
4. **ETHICS STATEMENT** (en español)
5. **EXERCISE HEADER** (datos del alumno: id, programa, curso, asignatura, fecha)
6. **INTRODUCTION** (objetivo pedagógico y reglas)
7. **PART 1 — Decision Lab** (pensamiento estratégico y justificación)
8. **PART 2 — Analysis Lab** (interpretación de evidencias simuladas / casos)
9. **FINAL REFLECTION** (metacognición)
10. **FINAL REPORT GENERATION** (Markdown + evaluación + nota 0–10 + instrucción de PDF)
11. **START THE LAB NOW** (inicio y espera de datos)

Regla clave: el prompt debe obligar a “**Wait for the student to respond**” antes de avanzar, para preservar el carácter interactivo.

4) Diseño pedagógico: cómo maximizar aprendizaje (sin convertirlo en un examen)

4.1. Definir resultados de aprendizaje observables (LOs)

Antes de escribir el prompt, definir 4–8 resultados observables, por ejemplo:

- “Identifica correctamente superficies de ataque y prioriza por riesgo.”
- “Distingue evidencia fuerte vs parcial vs falso positivo.”
- “Propone mitigaciones realistas alineadas con el fallo.”
- “Justifica decisiones con coherencia técnica.”

Recomendación: incluir los LOs implícitos en la estructura de SCENARIOS y CASES.

4.2. Niveles de dificultad adaptativos

Instruir a la IA:

- Si el alumno dice **YES** (experiencia) → menos pistas, mayor profundidad, más exigencia.
- Si el alumno dice **NO** → más didáctica, ejemplos, analogías, y pequeñas comprobaciones.

4.3. Evaluación formativa integrada (feedback continuo)

Cada SCENARIO y CASE debe incluir:

- validación + corrección,
- explicación de consecuencias,
- y recomendación de mejora.

Esto refuerza la línea de “metodologías activas” y “seguimiento del aprendizaje” (aunque la evaluación formal del impacto se recoja luego con cuestionarios).

4.4. Evitar el “modo tutorial”

Un laboratorio de IA no debe ser un manual.

Buenas prácticas:

- preguntas abiertas,
- comparación de alternativas,
- “¿qué harías si...?”
- “¿por qué tu decisión es mejor que otra?”
- “¿qué evidencia faltaría para confirmar?”

- “¿qué impacto/mitigación?”

5) Diseño de interacción: cómo escribir prompts robustos para Gemini y ChatGPT

5.1. Instrucciones “no negociables” al inicio

- “No ejecutes comandos”
- “No des pasos operativos de ataque en sistemas reales”
- “Espera la respuesta del alumno antes de continuar”
- “Interacciones siempre en es-ES”

5.2. Control del flujo conversacional (state machine simple)

Patrón recomendado:

- **Estado 0:** pedir datos del alumno
- **Estado 1:** introducción + pregunta de experiencia
- **Estado 2:** SCENARIO 1 → respuesta → feedback → pasar al siguiente
- ...
- **Estado final:** informe en Markdown + nota

El prompt debe explicitar:

- “Only after commenting... proceed to the next case.”

5.3. Antialucinación y rigor

Instruir a la IA a:

- marcar supuestos (“si no se especifica X, asumiré Y”),
- pedir evidencia adicional cuando sea necesario,
- evitar inventar outputs de herramientas (a menos que el prompt provea un output simulado).

5.4. Uso de evidencias simuladas (muy recomendable)

Para laboratorios de ciberseguridad, el “input” debe ser seguro:

- fragmentos de logs,
- respuestas HTTP simuladas,
- resúmenes de EVTX,
- listas de permisos,
- outputs recortados.

Esto evita que el alumno necesite atacar nada real y aun así practica análisis profesional.

6) Diseño de SCENARIOS y CASES: patrones reutilizables

6.1. SCENARIOS (Parte 1): decisiones estratégicas

Cada SCENARIO debe obligar a responder cinco ejes:

1. hipótesis de vulnerabilidad / vector,
2. información prioritaria,
3. herramientas adecuadas (solo a nivel conceptual),
4. riesgos y huella,
5. mitigación/corrección.

Plantilla recomendada por SCENARIO:

- *Contexto* (2–4 líneas)
- *Restricciones* (impacto mínimo, entorno crítico, etc.)
- *Preguntas* (4–6)
- *Criterios de corrección* (para la IA: qué es “bueno”, “parcial”, “malo”)

6.2. CASES (Parte 2): interpretación y clasificación

Cada CASE debe:

- incluir evidencia (texto simulado),
- exigir clasificación  /  /  ,
- pedir justificación,
- pedir “siguiente paso seguro” (sin daño),
- y cerrar con mitigación.

Plantilla recomendada por CASE:

- *Evidencia simulada*
- *Clasificación + justificación*
- *Hipótesis*
- *Siguiente paso seguro*
- *Mitigación*

7) Buenas prácticas específicas para evaluación (incluyendo nota 0–10)

El proyecto requiere laboratorios que guíen al alumno y terminen con exportación en PDF de la interacción.

Para maximizar valor docente, se recomienda que el informe final incluya:

7.1. Observaciones por SCENARIO y CASE

- Resumen de la respuesta del alumno.
- Comentarios de la IA sobre:
 - corrección técnica,
 - riesgos ignorados,
 - evidencia faltante,
 - claridad.

7.2. Rúbrica explícita para la calificación (recomendación fuerte)

Para consistencia entre alumnos y entre IA, definir criterios ponderables, por ejemplo:

- **Comprensión técnica (0–3):** conceptos correctos, términos bien usados.
- **Razonamiento y coherencia (0–3):** decisiones justificadas, orden lógico.
- **Evidencia y pensamiento crítico (0–2):** distingue señales vs ruido, pide pruebas.
- **Mitigación y enfoque defensivo (0–2):** propone controles realistas.

Total: **0–10**.

La IA debe explicar brevemente por qué asigna esa nota.

7.3. Evitar sesgo por “estilo”

Instruir a la IA:

- no penalizar por redacción imperfecta si el razonamiento es correcto,
- sí penalizar suposiciones peligrosas, incoherencias o afirmaciones sin evidencia.

8) Calidad técnica: cómo evitar fallos comunes (checklist de revisión)

Antes de publicar un laboratorio, validar:

8.1. Checklist de seguridad y ética

- Ethics statement claro
- No hay pasos de ataque a sistemas reales
- Evidencias son simuladas o de entornos autorizados
- Se enfatiza mitigación y aprendizaje

8.2. Checklist de interacción

- Pide datos del alumno y espera respuesta
- Pregunta experiencia y adapta nivel
- Cada SCENARIO y CASE obliga a respuesta antes de seguir
- Feedback específico, no genérico

8.3. Checklist de salida (informe)

- Informe en Markdown dentro de un único bloque
- Incluye observaciones por SCENARIO y CASE
- Incluye evaluación final y nota 0–10
- Incluye instrucción de exportación a PDF

8.4. Checklist de estabilidad multi-LLM (Gemini/ChatGPT)

- Evita dependencias de funciones específicas
- Instrucciones de formato y flujo muy explícitas
- No usa enlaces como requisito (solo como opcional)

9) Sostenibilidad y replicabilidad: cómo “productizar” los laboratorios

La documentación será clave para la sostenibilidad y aplicabilidad futura, y se publicará un catálogo en acceso abierto (RODIN/Zenodo) con los laboratorios educativos desarrollados.

Buenas prácticas de empaquetado:

9.1. Convención de nombres y versionado

- `SSI_LabXX_Tema_v1.0_2026.md`
- Changelog breve: qué cambió y por qué.

9.2. Estructura de repositorio recomendada

- `/labs/SSI/` (cada laboratorio)
- `/examples/` (respuestas ejemplo)
- `/reports/` (informes generados)
- `/screenshots/` (capturas de Gemini/ChatGPT)
- `/rubrics/` (rúbricas por laboratorio)
- `/README.md` (cómo usar y qué esperar)

9.3. Guía de ejecución para el profesorado

Para cada lab, incluir 1 página con:

- objetivo pedagógico,
- duración estimada,
- prerequisites,
- qué observar al corregir,
- riesgos típicos y cómo responder en clase.

9.4. Plantillas para adaptación a otras materias

Crear una “plantilla madre” con campos a rellenar:

- Tema, resultados de aprendizaje, escenarios, evidencias simuladas, rúbrica.

Esto permite extrapolar el método más allá de ciberseguridad (p. ej., redes, sistemas operativos, calidad del software, incluso materias no técnicas con análisis de casos).

10) Plan de mejora continua con feedback del alumnado

Se realizará un cuestionario anónimo en Moodle para evaluar motivación, utilidad, satisfacción, errores detectados y sugerencias de mejora.

Buenas prácticas para cerrar el ciclo:

1. **Recolectar feedback** con preguntas orientadas a:
 - claridad del prompt,
 - dificultad,
 - percepción de aprendizaje,
 - problemas de formato,
 - sugerencias de casos nuevos.
2. **Triaging de mejoras:**
 - bug (formato/flujo),
 - mejora pedagógica (mejor feedback),
 - ampliación técnica (nuevos casos),
 - ajuste de dificultad.
3. **Versionado:**
 - v1.1, v1.2... con registro de cambios.
4. **Evidencias de mejora:**
 - comparar resultados y satisfacción entre versiones.

11) Recomendaciones específicas por tipo de laboratorio (patrones por dominio)

11.1. Laboratorios de ofensiva (explotación / escalada)

- Evitar “recetas”.
- Priorizar análisis: cadena de ataque, impacto, detección, mitigación.
- Evidencias simuladas: banners, logs, permisos, rutas, tokens.

11.2. Laboratorios de auditoría/forense

- Enfatizar integridad, cadena de custodia y trazabilidad.

- Casos basados en logs y artefactos.

11.3. Laboratorios de gestión de riesgos (MAGERIT u otros)

- Escenarios de negocio + activos + amenazas + salvaguardas.
- Rúbricas que premien la coherencia y justificación del riesgo.

12) Conclusiones

Los laboratorios educativos impulsados por IA son especialmente adecuados para ciberseguridad porque permiten:

- aprendizaje basado en casos,
- diálogo guiado,
- práctica de toma de decisiones,
- y generación automática de evidencias (informes) para evaluación y mejora.

Para que el enfoque sea sostenible y replicable, es imprescindible:

- una **estructura estándar** de prompt,
- evidencias simuladas seguras,
- feedback formativo,
- informe final en PDF,
- y una rúbrica clara con calificación 0–10.

Esto alinea el laboratorio con las líneas prioritarias del proyecto (metodologías activas, recursos educativos, docencia multimodal con IA) y permite que los resultados se difundan y reutilicen en cursos posteriores y otras materias.

13) Anexo: Plantilla corta reutilizable (para crear nuevos labs)

(Recomendación) Plantilla “copiar/pegar” para nuevos laboratorios

- TITLE
- LANGUAGE RULE
- ROLE
- ETHICS STATEMENT
- EXERCISE HEADER
- INTRODUCTION + pregunta experiencia (YES/NO)
- PART 1: 3 SCENARIOS
- PART 2: 4–6 CASES con evidencias simuladas
- FINAL REFLECTION
- FINAL REPORT GENERATION (con observaciones + nota 0–10)
- START THE LAB NOW



23rd of September, 2026

ABSTRACT ACCEPTANCE LETTER

This is a confirmation that the abstract entitled:

**FROM PROMPTS TO AI-POWERED CYBERSECURITY LABS: A DESIGN AND
DEPLOYMENT STUDY IN SECURITY IN COMPUTER SYSTEMS AND AUDIT AND RISK
ANALYSIS COURSES**

Author(s): J. Boubeta-Puig, J. Rosa-Bilbao, A. Araújo-Alves, K.J. Valle-Gómez

has been accepted as a VIRTUAL presentation at ICERI2026.

Name of event: ICERI2026 (19th annual International Conference of Education, Research and Innovation)

Dates: 9-11 November 2026

Place: Seville (Spain)

Organising entity: IATED

ICERI2026 Organising Committee

