

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

Identificación del proyecto	
Código	sol-202500299536-tra
Título	Infraestructuras Críticas Simuladas: Laboratorio activo de ciberseguridad con Raspberry Pi
Responsable	Jesús Rosa Bilbao

- Se recomienda:
 - Atender a los criterios de valoración de las memorias indicados en las bases de la convocatoria.
 - Incluir referencias bibliográficas y datos comparativos con proyectos previos, según casos, para reforzar la evaluación del impacto.
 - Incluir evidencias sobre las medidas de difusión desarrolladas.
- Otros aspectos que considerar:
 - La claridad, la coherencia y la justificación de los datos presentados serán clave en la valoración final.
 - La difusión de resultados debe priorizar la transparencia y accesibilidad a la comunidad universitaria.
 - Serán valoras como evidencias: registro de actividades, listados de participantes, programas de eventos, fotografías, documentos que acreditan la aceptación de una comunicación/ponencia o similar, informes, actas o resúmenes de las acciones realizadas, índices de impacto que respalden la cantidad de personas alcanzadas o el impacto de la difusión, etc.

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	<i>Sustituya este texto por el título del objetivo</i>
Actividades que había previsto en la solicitud del proyecto:	<i>A1. Selección de los componentes y roles de los dispositivos (PLC, HMI, sensores, firewall, etc.).</i> <i>A2. Instalación y configuración de sistemas operativos y software OT/ICS en Raspberry Pi.</i> <i>A3. Montaje físico y conexión de los equipos con elementos reales (relés, LEDs, sensores).</i> <i>A4. Pruebas de estabilidad, documentación técnica y validación del entorno.</i>
Actividades realizadas y resultados obtenidos:	<i>Se seleccionaron y configuraron los dispositivos Raspberry Pi que emulan los roles de controladores, HMIs, sensores y elementos de filtrado/protección. Se instalaron y configuraron los sistemas operativos y servicios OT/ICS necesarios, se realizó el montaje físico del laboratorio y se validó su estabilidad mediante pruebas técnicas. Resultado: un laboratorio modular y operativo, documentado técnicamente, que sirvió de base para los dos escenarios prácticos descritos en el Objetivo 2.</i>

Objetivo nº 2	<i>Diseñar actividades prácticas para la asignatura basadas en ataques y defensas simuladas.</i>
Actividades que había previsto en la solicitud del proyecto:	<i>A5. Desarrollo de retos prácticos tipo Red Team / Blue Team. A6. Preparación de rúbricas de evaluación y fichas de cada práctica. A7. Planificación del uso rotativo del laboratorio entre equipos. A8. Validación de las actividades mediante simulacros.</i>
Actividades realizadas y resultados obtenidos:	<i>Se diseñaron dos escenarios guiados Red Team / Blue Team: el Escenario 1, centrado en el compromiso de un servicio web vulnerable conectado a una base de datos interna, y el Escenario 2, centrado en la exploración y protección de una red de estilo industrial segmentada. Para cada escenario se definieron tareas diferenciadas de Red Team y Blue Team, rúbricas de evaluación y un calendario de uso rotativo del laboratorio entre equipos. Ambos escenarios se validaron mediante un simulacro previo a su aplicación con el alumnado. Resultado: dos prácticas guiadas, completas y evaluables, listas para su aplicación docente.</i>

Objetivo nº 3	Aplicar el entorno desarrollado en la docencia real de la asignatura.
Actividades que había previsto en la solicitud del proyecto:	A9. Puesta en marcha del laboratorio en el aula (marzo-mayo). A10. Realización de las prácticas programadas con el alumnado. A11. Recogida de evidencias y retroalimentación de estudiantes. A12. Evaluación de los resultados obtenidos.
Actividades realizadas y resultados obtenidos:	El laboratorio se puso en marcha en el aula durante el segundo semestre del curso 2025/2026, dentro de la asignatura Seguridad en Sistemas e Infraestructuras Críticas del Máster en Seguridad Informática (Ciberseguridad). El alumnado realizó los dos escenarios prácticos y se recogió evidencia de la experiencia mediante dos cuestionarios anónimos Likert (1-5): uno previo al laboratorio (n=22) y otro posterior (n=15). Resultado: baja exposición previa del alumnado a este tipo de práctica (media 2,09/5, solo 9,1% en valores 4-5), confirmando que el laboratorio cubría una carencia formativa real; asistencia muy alta (media 4,87/5, 93,3% en 4-5); satisfacción con el conocimiento adquirido de 4,33/5; adecuación del tiempo y los recursos de 4,47/5; mejora percibida en la comprensión de ataques y defensas de 4,27/5 (80% en 4-5); y apoyo prácticamente unánime a la continuidad de la actividad (media 4,67/5, 100% en 4-5).

Objetivo nº 4	Difundir los resultados y materiales del proyecto para su reutilización.
Actividades que había	A13. Elaboración de guías técnicas, vídeos y materiales explicativos.

previsto en la solicitud del proyecto:	A14. Publicación en repositorio abierto (GitHub, RODIN). A15. Propuesta de comunicación en jornadas, congresos o revistas docentes.
Actividades realizadas y resultados obtenidos:	Se elaboraron las guías técnicas y fichas de cada práctica utilizadas en el laboratorio. Se redactó y envió una comunicación científica sobre la experiencia, titulada “Simulated Critical Infrastructures: An Active Cybersecurity Laboratory with Raspberry Pi for Red Team / Blue Team Learning” (J. Rosa-Bilbao, J. Boubeta-Puig), que ha sido ACEPTADA para su presentación en ICERI2026 (18th International Conference of Education, Research and Innovation), cumpliendo así el compromiso de difusión en un congreso internacional de innovación docente recogido en la solicitud. Asimismo, se ha celebrado el seminario de difusión en la Escuela Superior de Ingeniería (viernes 25 de septiembre de 2026, 10:30h, aula FS16), con el programa previsto (introducción, objetivos, actividades realizadas, resultados y conclusiones del proyecto), cuya grabación está disponible en: https://drive.google.com/file/d/1PmCNat21fSaqcNQRs2A0KNro5-Ze2jbU/view?usp=sharing . Se han publicado los materiales del proyecto (guía técnica, cuestionarios y resultados, artículo y diapositivas del seminario) en el repositorio abierto de GitHub: https://github.com/JesusRosaB/PID_2526_SSIC .

Objetivo nº 5	Fomentar la sostenibilidad y replicabilidad del laboratorio en otras asignaturas o contextos.
Actividades que había previsto en la solicitud del proyecto:	A16. Creación de un modelo modular del laboratorio replicable por otros docentes. A17. Redacción de buenas prácticas y checklist de implementación. A18. Estudio de ampliación del uso del laboratorio a otras asignaturas del máster o grados.
Actividades realizadas y resultados obtenidos:	El diseño modular del laboratorio, basado en dispositivos Raspberry Pi independientes y roles reconfigurables, facilita su réplica por otro profesorado con un coste reducido. La documentación técnica generada durante el proyecto sienta la base de una futura guía de buenas prácticas. Como trabajo futuro, identificado también en el artículo aceptado en ICERI2026, se contempla ampliar el laboratorio con escenarios adicionales, tareas de respuesta a incidentes más detalladas y mecanismos de evaluación más completos, así como su extensión a otras asignaturas del máster o de los grados relacionados con ciberseguridad industrial.

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>
La incorporación de este laboratorio activo ha supuesto un cambio significativo en la asignatura Seguridad en Sistemas e Infraestructuras Críticas, que hasta ahora carecía de un componente práctico realista sobre infraestructuras críticas. Los resultados del cuestionario post-laboratorio muestran una valoración muy positiva de la experiencia (satisfacción con el conocimiento adquirido: 4,33/5; mejora percibida en la comprensión de ataques y defensas: 4,27/5) y un respaldo prácticamente unánime a su continuidad (4,67/5, 100% de respuestas en 4-5). La baja exposición previa del alumnado a laboratorios de ataque y defensa (2,09/5) confirma que el proyecto ha cubierto una carencia formativa relevante en la asignatura, reforzando su orientación práctica y su conexión con escenarios profesionales reales.

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:		24 alumnos/as		
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
1	3	4	5	2
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
2	4	3	4	2
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				
Nada de acuerdo	Poco de acuerdo	Ni en acuerdo ni en desacuerdo	Muy de acuerdo	Completamente de acuerdo
0	0	3	5	7
En el caso de la participación de profesorado invitado				
La participación del profesorado invitado ha supuesto un gran beneficio en mi formación				
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				
La comparación entre el cuestionario previo y el posterior muestra un efecto positivo del laboratorio: la dificultad esperada antes de la experiencia (media 3,27/5, sobre n=15) fue superior				

a la dificultad realmente percibida en las actividades (media 3,00/5), y el alumnado valoró muy positivamente que el laboratorio hubiera mejorado su comprensión de los ataques y defensas en ciberseguridad (media 4,27/5, 80% de respuestas en 4-5, con ninguna respuesta en desacuerdo). Además, el cuestionario previo (n=22) evidenció una exposición previa muy baja a este tipo de práctica (media 2,09/5), lo que refuerza la conclusión de que el proyecto ha tenido una influencia clara y positiva en la percepción del alumnado sobre la asignatura. El proyecto no ha contado con profesorado invitado, por lo que ese bloque no aplica.

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
Seminario en la Escuela Superior de Ingeniería para presentar la experiencia y las conclusiones del proyecto (programa: introducción, objetivos, actividades realizadas, resultados y conclusiones), previsto entre junio y septiembre de 2026, con grabación difundida a través de los canales de la UCA. Presentación posterior de las contribuciones en un congreso de innovación docente de carácter preferiblemente internacional.
Descripción de las medidas que se han llevado a cabo
Se ha redactado y enviado la comunicación científica derivada del proyecto, que ha sido ACEPTADA en ICERI2026 (18th International Conference of Education, Research and Innovation), cumpliendo el compromiso de presentar los resultados en un congreso internacional de innovación docente. Se han elaborado las guías técnicas y fichas de las dos prácticas del laboratorio. El seminario de difusión en la Escuela Superior de Ingeniería se ha celebrado el viernes 25 de septiembre de 2026, a las 10:30h, en el aula FS16, siguiendo el programa comprometido en la solicitud (introducción, objetivos del proyecto, actividades realizadas, resultados del proyecto y conclusiones). La grabación del seminario está disponible en: https://drive.google.com/file/d/1PmCNat21fSaqcNQrs2A0KNro5-Ze2jbU/view?usp=sharing . Todo el material del proyecto (guía técnica del laboratorio, cuestionarios y resultados, artículo enviado a ICERI2026 y diapositivas del seminario) se ha publicado en el repositorio abierto de GitHub: https://github.com/JesusRosaB/PID_2526_SSIC . No se han detectado desajustes relevantes respecto a lo comprometido en la solicitud.

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

Conclusiones
Los resultados obtenidos confirman la viabilidad de un laboratorio activo de ciberseguridad basado en Raspberry Pi para la docencia práctica sobre infraestructuras críticas, sin necesidad de entornos industriales reales. La baja exposición previa del alumnado a este tipo de prácticas, junto con la alta satisfacción y el respaldo casi unánime a su continuidad, avalan tanto la pertinencia como la sostenibilidad de la propuesta. Como aplicaciones futuras, se contempla ampliar el laboratorio con nuevos escenarios y tareas de respuesta a incidentes, incorporar medidas pre/post emparejadas para reforzar la evaluación del aprendizaje, y extender su uso a otras asignaturas del máster y de los grados relacionados con ciberseguridad industrial. La difusión de la experiencia, ya materializada en la aceptación de una comunicación en ICERI2026, y el diseño modular y de bajo coste del laboratorio refuerzan su continuidad y replicabilidad en próximas ediciones.

SIMULATED CRITICAL INFRASTRUCTURES: AN ACTIVE CYBERSECURITY LABORATORY WITH RASPBERRY PI FOR RED/BLUE TEAM LEARNING

J. Rosa-Bilbao, J. Boubeta-Puig

University of Cadiz (SPAIN)

Abstract

Critical infrastructures such as energy, water, transport, and industrial production systems increasingly depend on interconnected digital technologies. As a result, cybersecurity education must prepare students not only to understand threats conceptually, but also to analyze how attacks and defenses unfold in environments that combine networking, services, monitoring, and operational constraints. This requirement is especially relevant in master's courses devoted to critical infrastructure security, where students are expected to reason about both offensive and defensive perspectives. However, bringing realistic industrial cybersecurity practice into the classroom is not straightforward. Real industrial environments are costly, difficult to reconfigure, and often inappropriate for repeated experimentation by students. For this reason, active and experiential learning strategies are especially valuable in this domain, as they allow students to engage with concrete scenarios, make decisions, and learn from guided practice and feedback. Likewise, cyber ranges and simulated environments have become a relevant approach for cybersecurity education because they provide controlled spaces for hands-on exercises, role-based training, and scenario-driven learning. Cybersecurity education on critical infrastructures requires hands-on practice that is rarely feasible with real industrial environments, which are costly, hard to reconfigure, and unsuitable for classroom use. This paper presents a Teaching Innovation Project (TIP) that designed and deployed a modular active laboratory based on Raspberry Pi devices to simulate small-scale critical infrastructure components, enabling master's students to engage in Red Team / Blue Team exercises through two guided scenarios. The experience was evaluated through pre-laboratory ($n=22$) and post-laboratory ($n=15$) questionnaires, revealing low prior exposure to this kind of practice and high student satisfaction, perceived learning, and support for future editions.

Keywords: Cybersecurity education, critical infrastructures, Raspberry Pi, active learning, Red Team, Blue Team.

1 INTRODUCTION

Critical infrastructures such as energy, water, transport, and industrial production systems increasingly depend on interconnected digital technologies. As a result, cybersecurity education must prepare students not only to understand threats conceptually, but also to analyze how attacks and defenses unfold in environments that combine networking, services, monitoring, and operational constraints. This requirement is especially relevant in master's courses devoted to critical infrastructure security, where students are expected to reason about both offensive and defensive perspectives.

However, bringing realistic industrial cybersecurity practice into the classroom is not straightforward. Real industrial environments are costly, difficult to reconfigure, and often inappropriate for repeated experimentation by students. For this reason, active and experiential learning strategies are especially valuable in this domain, as they allow students to engage with concrete scenarios, make decisions, and learn from guided practice and feedback [1, 2]. Likewise, cyber ranges and simulated environments have become a relevant approach for cybersecurity education because they provide controlled spaces for hands-on exercises, role-based training, and scenario-driven learning [3, 4].

Within this context, this paper presents the teaching innovation project "Simulated Critical Infrastructures: Active Cybersecurity Laboratory with Raspberry Pi", developed for the course Security in Systems and Critical Infrastructures in the Master's Degree in Cybersecurity at the University of Cadiz. The project aimed to create a low-cost, modular, and replicable laboratory that emulates devices playing roles similar to controllers, human-machine interfaces (HMI), sensors, and filtering or

protection elements, letting students work with realistic Red Team / Blue Team dynamics over small-scale simulated infrastructures. The contribution of this paper is threefold. First, it describes the pedagogical and technical design of the laboratory. Second, it explains the two guided scenarios used during the teaching experience. Third, it analyzes the evidence collected through pre-laboratory ($n=22$) and post-laboratory ($n=15$) questionnaires to assess students' background, perceived learning, and satisfaction.

The remainder of this paper is structured as follows. Section 2 describes the methodology and the laboratory design. Section 3 presents and discusses the results obtained from the questionnaires. Finally, Section 4 summarizes the main conclusions and future work.

2 METHODOLOGY

The teaching experience was designed as an active laboratory for a master's level cybersecurity course focused on systems and critical infrastructures. The project sought to move beyond lecture-only explanations by giving students direct exposure to adversarial and defensive tasks in controlled environments that approximate real-world situations while remaining safe, affordable, and reusable.

2.1 Laboratory Design

The laboratory was conceived as a modular environment based on Raspberry Pi devices that emulate the role of different infrastructure components. According to the project plan, these components include services and devices that can play functions similar to controllers, HMIs, sensors, and filtering or protection elements. This design choice was motivated by four practical goals:

- to provide a realistic but contained environment for cybersecurity experimentation,
- to support attack-and-defense activities without affecting production systems,
- to keep deployment costs low and the architecture easy to replicate, and
- to produce technical and teaching materials that can later be reused in related courses.

The laboratory experience was organized around Red Team / Blue Team dynamics. Students alternated between the perspective of an attacker trying to understand and compromise a target environment and the perspective of a defender responsible for monitoring, detecting, and responding to suspicious activity. This role-based organization is aligned with the educational value of scenario-based cyber exercises [3, 5], since it encourages students to connect offensive techniques with defensive reasoning instead of treating them as isolated topics.

2.2 Practice Scenarios

Two guided scenarios were prepared for the course. Table 1 summarizes their educational focus.

Table 1. Summary of the practical scenarios used in the laboratory.

Scenario	Role	Main tasks
1	Red Team	
1	Blue Team	Traffic monitoring, log and alert analysis, identification of suspicious actions, and application of protective measures for the target service and data.
2	Red Team	Exploration of an industrial-style network from a separate segment, device identification, interaction with control-oriented services, and evaluation of the potential impact on system operation.
2	Blue Team	

Scenario 1 was oriented to the compromise of a service that exposed a web application connected to an internal database. From the offensive perspective, students had to enumerate available services, inspect the target application, search for exploitable weaknesses, and reason about the consequences

of a successful compromise. From the defensive perspective, students had to watch system and network activity, interpret evidence generated by monitoring tools, and respond to attacker actions.

Scenario 2 extended the experience to an industrial-style setting. In this case, the exercise emphasized the exposure of systems across network segments and the interaction with devices playing operational roles. The scenario helped students understand that security in critical infrastructures is not limited to classic IT assets but also involves communications, process visibility, and the protection of devices that influence physical or operational behavior.

2.3 Data Collection and Analysis

The experience was evaluated through two anonymous questionnaires based on a 5-point Likert scale (1 = strongly disagree, 5 = strongly agree). The pre-laboratory questionnaire collected 22 responses and explored previous experience, tool familiarity, and self-perceived capability before the practical sessions. The post-laboratory questionnaire collected 15 responses and focused on attendance, perceived difficulty, satisfaction, adequacy of time and resources, perceived learning improvement, and willingness to continue this type of activity.

The pre- and post-laboratory instruments were designed for different purposes, so they are not directly paired nor do they measure exactly the same constructs. Consequently, the analysis reported in this paper is descriptive rather than causal. This limitation should be considered when interpreting the results. Even so, the two questionnaires together provide useful evidence about the initial profile of the students and their perception of the teaching experience after completing the laboratory.

3 RESULTS

This section presents the evidence collected through the pre-laboratory and post-laboratory questionnaires. First, we describe the students' initial profile in terms of previous experience, familiarity with relevant tools, and self-perceived capability before the practical sessions. Next, we summarize their perception of the laboratory after completing the activities, focusing on satisfaction, difficulty, adequacy of resources, and perceived learning value.

3.1 Pre-Laboratory Questionnaire

Table 2 summarizes the pre-laboratory results. The data suggest that students entered the experience with uneven prior preparation. Previous participation in attack-and-defense laboratories was low (mean 2.09), with only 9.1% of respondents selecting values 4 or 5. This is relevant because it indicates that the experience addressed a real training gap rather than simply reinforcing a familiar practice.

Table 2. Pre-laboratory questionnaire results (n=22).

Q#	Statement (abridged)	Mean	% 4–5
Q1	Previous participation in attack-and-defense cybersecurity labs.	2.09	9.1
Q2	Use of scanning, web auditing, or traffic monitoring tools.	3.73	68.2
Q3	Use or configuration of virtual environments for security testing.	2.95	31.8
Q4	Understanding of Red Team and Blue Team roles.	4.00	68.2
Q5	Familiarity with common cyberattacks and how they work.	3.59	54.5
Q6	Capability to identify suspicious activity during a practical exercise.	3.09	27.3
Q7	Capability to investigate and respond to a cyberattack in a lab environment.	3.05	27.3

At the same time, students reported some partial prior knowledge. Familiarity with network scanning, web auditing, or traffic monitoring tools reached a mean of 3.73, and understanding of Red Team and Blue Team roles reached a mean of 4.00. In contrast, confidence in actually identifying suspicious activity (mean 3.09) or investigating and responding to a cyberattack in a laboratory environment (mean 3.05) was noticeably lower. Taken together, these results depict a cohort with theoretical awareness and some tool exposure, but without strong previous hands-on confidence in adversarial laboratory work.

3.2 Post-Laboratory Questionnaire

Table 3 presents the post-laboratory results. Student attendance was very high, with a mean of 4.87 and 93.3% of respondents selecting 4 or 5. Satisfaction with the knowledge acquired was also strong (mean 4.33), suggesting that the laboratory was perceived as a meaningful complement to the course.

The conditions under which the laboratory was delivered were positively valued. Students considered the time available for the activities adequate (mean 4.47), and they also rated access to tools and virtual environments very positively (mean 4.47). Moreover, the statement “This laboratory has improved my understanding of cybersecurity attacks and defenses” obtained a mean of 4.27, with 80.0% of responses in the 4–5 range.

Some results deserve a more nuanced interpretation. The difficulty of the activities obtained an intermediate mean of 3.00, indicating that students did not perceive the exercises as either trivial or overwhelmingly difficult. This is pedagogically reasonable for a master's level course, where challenge is expected as long as it remains manageable. Likewise, the statement regarding group work masking the insufficient contribution of some classmates obtained a relatively low mean of 2.40, which suggests that teamwork issues were present but were not dominant in the experience.

Finally, one of the clearest results concerns future continuity. All respondents supported the continuation of this type of activity, with a mean of 4.67 and 100% of answers in the 4–5 range. This strong endorsement reinforces the value of maintaining and refining the laboratory in subsequent course editions.

Table 3. Post-laboratory questionnaire results (n=15).

Q#	Statement (abridged)	Mean	% 4–5
Q1	Regular attendance.	4.87	93.3
Q2	Before the course, I expected strong difficulty understanding the contents.	3.27	46.7
Q3	After the course, I have not had difficulty understanding the contents.	3.80	73.3
Q4	Satisfaction with the knowledge acquired.	4.33	86.7
Q5	Adequacy of the time available for the activities.	4.47	80.0
Q6	The activities were very difficult.	3.00	40.0
Q7	Adequacy of access to laboratory tools and virtual environments.	4.47	86.7
Q8	The laboratory improved my understanding of attacks and defenses.	4.27	80.0
Q9	Group work masked classmates who did not really contribute or learn enough.	2.40	13.3
Q10	This type of Red Team / Blue Team laboratory activity should continue in this and other courses.	4.67	100.0

3.3 Discussion

The questionnaires allow three main observations. First, the laboratory responded to a real educational need. Although many students had some familiarity with tools and concepts before the sessions, very few had previously participated in attack-and-defense laboratories of this kind. Second, the combination of realistic scenarios, role-based work, and accessible infrastructure appears to have generated a positive learning experience, as reflected in the ratings on satisfaction, resource adequacy, and improved understanding. Third, the results support the feasibility of using Raspberry Pi-based infrastructures to implement hands-on cybersecurity training for critical infrastructure topics without relying on complex industrial facilities.

The results should nevertheless be interpreted with caution. The sample size is modest, the post-laboratory response rate is lower than the pre-laboratory one, and the two questionnaires are not paired. Therefore, the evidence does not justify strong claims about measured learning gains. Even so, the descriptive results are sufficiently consistent to support the educational usefulness of the laboratory and to justify its continuation and refinement.

4 CONCLUSIONS

This paper has presented a teaching innovation project based on a Raspberry Pi laboratory designed to support active learning in cybersecurity for critical infrastructures. The proposal enabled master's students to work on realistic Red Team / Blue Team exercises through two guided scenarios, one focused on the compromise of a vulnerable service and another on the analysis and protection of an industrial-style network.

The evidence collected through the questionnaires suggests that the laboratory filled a relevant practical training gap, since previous exposure to similar activities was limited, while post-laboratory perceptions were clearly positive in terms of satisfaction, resource adequacy, and perceived improvement in understanding attacks and defenses. In addition, students strongly supported the continuation of this type of activity in future courses.

As future work, the laboratory can be expanded with additional scenarios, more detailed incident-response tasks, and richer monitoring and assessment mechanisms. A natural next step is also to improve the evaluation design by incorporating matched pre/post measures and performance-based evidence, which would allow a more robust analysis of learning outcomes.

ACKNOWLEDGEMENTS

This teaching innovation project was supported by the University of Cadiz during the 2025-2026 academic year [grant number sol-202500299536-tra]. The authors would like to thank student Marta Jones Gonzalez for her contribution to the development of the laboratory, as well as all students who participated in the sessions and contributed feedback through the questionnaires.

REFERENCES

- [1] M. Prince, "Does Active Learning Work? A Review of the Research," *Journal of Engineering Education*, vol. 93, no. 3, pp. 223–231, 2004.
- [2] D. A. Kolb, *Experiential Learning: Experience as the Source of Learning and Development*. Englewood Cliffs, NJ: Prentice-Hall, 1984.
- [3] M. N. Katsantonis, A. Manikas, I. Mavridis, and D. Gritzalis, "Cyber range design framework for cyber security education and training," *International Journal of Information Security*, vol. 22, pp. 1005–1027, 2023.
- [4] R. Candell, T. Zimmerman, and K. Stouffer, *An Industrial Control System Cybersecurity Performance Testbed*. Gaithersburg, MD: National Institute of Standards and Technology, 2015.
- [5] D. Kim, S. Jeon, K. Kim, J. Kang, S. Lee, and J. T. Seo, "Guide to developing case-based attack scenarios and establishing defense strategies for cybersecurity exercise in ICS environment," *The Journal of Supercomputing*, vol. 80, pp. 21642–21675, 2024.