Experiential learning of cyberdeception through a reproducible educational environment

Federico Pacheco[1], Diego Staino[2]

[1] Universidad Tecnológica Nacional, Buenos Aires, Argentina
[2] Instituto Universitario de la Policía Federal, Buenos Aires, Argentina
federico.pacheco@gmail.com
diegostaino@hotmail.com

Resumen. Cyber deception techniques, such as honeypots, honeytokens, and decoy services, have been extensively studied and applied in operational cybersecurity contexts. However, their integration into formal educational settings remains limited and often confined to theoretical descriptions. This gap hinders the development of an operational understanding of deception as a defensive strategy complementary to traditional protection and detection mechanisms. This paper presents Cyber Deception Playground, a reproducible, container-based educational environment designed to support the practical learning of cyber deception techniques. The environment enables controlled exploration of infrastructures with varying levels of deception, integrating vulnerable services, decoy mechanisms, simulated activity, monitoring capabilities, and an attacker workspace. Unlike general-purpose cyber ranges, the proposed environment explicitly frames deception as a learning object, allowing participants to observe how different configurations influence adversarial interaction and system visibility. The contribution of this work is design-oriented. No empirical evaluation of learning outcomes or comparative performance is provided. Instead, the paper describes and justifies the design of the environment, outlines its architectural and pedagogical decisions, and discusses the types of educational use it enables. The goal is to provide a reproducible foundation for teaching cyber deception and to support future empirical studies in cybersecurity education.

Palabras clave: cyber deception; cybersecurity education; experiential learning; cyber ranges; honeypots; honeytokens

Aprendizaje experimental de ciberengaño mediante un entorno educativo reproducible

Resumen. Las técnicas de cyber deception —como honeypots, honeytokens y servicios señuelo— han sido ampliamente estudiadas y utilizadas en contextos operativos de ciberseguridad defensiva. Sin embargo, su incorporación en procesos formativos formales sigue siendo limitada y, en muchos casos, pura-

mente teórica. Esta falta de entornos educativos prácticos dificulta que estudiantes y profesionales desarrollen una comprensión operativa del engaño defensivo como estrategia complementaria a los mecanismos tradicionales de protección y detección. Este trabajo presenta Cyber Deception Playground, un entorno educativo reproducible basado en contenedores, diseñado específicamente para el aprendizaje práctico de técnicas de cyber deception. La plataforma permite explorar de manera controlada infraestructuras con distintos niveles de engaño, integrando componentes vulnerables, señuelos activos y capacidades de monitoreo, así como un entorno atacante para la experimentación adversarial. A diferencia de los cyber ranges genéricos, el diseño del entorno enfatiza explícitamente el rol pedagógico del engaño defensivo y la observación de su impacto en términos de visibilidad y comportamiento del atacante. El aporte de este trabajo es de carácter conceptual y de diseño. No se presentan resultados empíricos de efectividad ni evaluaciones comparativas de aprendizaje. En su lugar, se describe y justifica el diseño del entorno, se discuten las decisiones arquitectónicas adoptadas y se delimitan los casos de uso educativos que habilita. El objetivo es ofrecer una base reproducible y extensible para la enseñanza del cyber deception, y servir como punto de partida para futuras evaluaciones empíricas en contextos educativos y de capacitación profesional.

Palabras clave: Ciber engaño, Educación, Playground

1. Introducción

En la última década, las técnicas de cyber deception han ganado relevancia como complemento a los enfoques defensivos tradicionales en ciberseguridad, particularmente en contextos de detección temprana y contención de movimientos laterales (Spitzner, 2020). Sin embargo, pese a su creciente presencia en entornos operativos y en la literatura técnica, el engaño defensivo continúa siendo un área marginal dentro de la formación formal en ciberseguridad, tanto a nivel universitario como en programas de capacitación profesional avanzada.

La mayoría de los programas educativos en seguridad informática priorizan mecanismos reactivos o preventivos (Gao et al., 2022) como el endurecimiento de sistemas, el monitoreo de eventos, o el análisis forense, mientras que el cyber deception suele abordarse, cuando aparece, desde una perspectiva predominantemente teórica o descriptiva (Holm et al., 2021). Esta aproximación contrasta con la naturaleza eminentemente práctica del engaño defensivo, cuya comprensión efectiva requiere experimentar tanto el diseño de señuelos como la interacción adversarial que estos generan.

La literatura reciente refleja este desbalance (Pawlick et al., 2020). Si bien existen contribuciones relevantes sobre arquitecturas de honeypots, honeytokens y técnicas de generación de actividad engañosa, estas se concentran mayormente en contextos de producción, evaluación de detección o análisis de amenazas (Fraunholz et al., 2020). En cambio, los trabajos que abordan el cyber deception como objeto de enseñanza sistemática, mediante entornos prácticos reproducibles y orientados al aprendizaje activo, son escasos y fragmentarios. En particular, se observa una falta de propuestas

educativas que permitan a los estudiantes explorar de manera controlada el rol dual de atacante y defensor en infraestructuras con mecanismos de engaño explícitos.

Este trabajo aborda dicha brecha desde una perspectiva de diseño educativo. Se presenta Cyber Deception Playground, un entorno práctico basado en contenedores, concebido específicamente para la enseñanza y el aprendizaje experimental de técnicas de engaño defensivo. A diferencia de los cyber ranges genéricos o de los laboratorios de seguridad convencionales, la plataforma está diseñada para hacer explícito el rol del engaño como estrategia defensiva, permitiendo observar cómo distintas configuraciones de señuelos afectan el comportamiento del atacante y la visibilidad defensiva (Yamin et al., 2021).

El objetivo de este artículo no es evaluar empíricamente la efectividad operativa del cyber deception, ni medir resultados de aprendizaje en términos comparativos, sino describir y justificar el diseño de un entorno educativo reproducible que permita introducir estas técnicas de manera práctica y sistemática. En este sentido, el trabajo se posiciona como una contribución de tipo design-oriented, orientada a educadores, investigadores y profesionales interesados en incorporar el engaño defensivo en procesos formativos.

Las contribuciones principales que este trabajo busca son las siguientes: primero, la identificación y delimitación de un vacío educativo en la enseñanza práctica del cyber deception. Segundo, el diseño de un entorno educativo modular y reproducible, orientado específicamente al aprendizaje activo de técnicas de engaño defensivo. Tercero, la articulación de principios de diseño que diferencian el uso educativo del cyber deception de sus aplicaciones en entornos productivos.

El resto del artículo se organiza de la siguiente manera: se revisa el trabajo relacionado en cyber deception y los laboratorios educativos de ciberseguridad; luego se establece el marco conceptual y educativo adoptado; a continuación, se describe el diseño del Cyber Deception Playground, la metodología de evaluación propuesta, y los resultados observables; posteriormente se discuten las limitaciones y líneas de trabajo futuro, y finalmente, se exponen las conclusiones.

2. Trabajo Relacionado

El presente trabajo se relaciona con tres líneas principales de investigación y práctica: (i) el estudio del cyber deception en contextos operativos, (ii) el desarrollo de cyber ranges y laboratorios prácticos para la enseñanza de ciberseguridad, y (iii) las propuestas educativas orientadas al aprendizaje experiencial en seguridad informática.

Si bien existe un cuerpo consolidado de conocimiento sobre cyber deception y una tradición madura en el uso de laboratorios prácticos para la enseñanza de ciberseguridad, se observa una brecha en la intersección de ambos dominios. Falta literatura que aborde de manera sistemática el diseño de entornos educativos reproducibles, orientados específicamente a enseñar cyber deception como disciplina defensiva, y no solo como un componente accesorio de infraestructuras más amplias. Este trabajo se sitúa en dicha intersección, proponiendo un enfoque de diseño educativo que busca cubrir

ese vacío. A continuación, se revisan los ejes con el objetivo de delimitar el alcance y las limitaciones del estado del arte.

2.1. Cyber deception en entornos operativos

A partir de 2020, la literatura sobre cyber deception ha mostrado un crecimiento sostenido, con énfasis en arquitecturas de honeypots, honeytokens y mecanismos de engaño dinámico orientados a la detección temprana y al análisis del comportamiento adversarial (Khandelwal et al., 2021). Diversos trabajos exploran la integración del engaño con marcos como MITRE ATT&CK, así como su uso para incrementar la visibilidad de ataques avanzados y reducir el tiempo de detección (Almeshekah & Spafford, 2020). No obstante, estas contribuciones suelen asumir contextos de producción y objetivos operativos, priorizando métricas como tasas de detección, reducción de falsos positivos o impacto en la superficie de ataque. En general, el cyber deception es tratado como una técnica defensiva a desplegar, no como un objeto de aprendizaje en sí mismo.

2.2. Laboratorios prácticos y cyber ranges

En paralelo, existe una amplia literatura sobre cyber ranges y entornos de laboratorio para la enseñanza práctica de ciberseguridad (Yamin et al., 2021). Estos entornos han demostrado ser efectivos para el entrenamiento en respuesta a incidentes, análisis forense, explotación de vulnerabilidades y defensa de infraestructuras críticas (Pasquini et al., 2022). Sin embargo, la mayoría de los cyber ranges adoptan un enfoque generalista, centrado en escenarios de ataque y defensa convencionales (Pham et al., 2021). Cuando el engaño aparece, suele hacerlo de manera implícita o marginal, como un componente más del entorno, sin un diseño pedagógico explícito que permita estudiar su rol, configuración y efectos de forma sistemática (Vykopal et al., 2022).

2.3. Cyber deception como objeto educativo

Los trabajos que abordan explícitamente el cyber deception desde una perspectiva educativa son escasos. Algunas propuestas describen el uso de honeypots simples en cursos introductorios o laboratorios aislados para ilustrar conceptos básicos de monitoreo y detección. Sin embargo, estas aproximaciones tienden a ser ad hoc, con bajo nivel de reproducibilidad, escasa modularidad y sin una diferenciación clara entre el uso del engaño en producción y su uso como herramienta de aprendizaje. Asimismo, la mayoría de estas contribuciones no discute de manera explícita las decisiones de diseño pedagógico ni los trade-offs involucrados en la construcción de entornos de engaño con fines educativos.

3. Marco Conceptual y Educativo

En este trabajo, el cyber deception se entiende como el uso deliberado de componentes, servicios o datos señuelo diseñados para inducir a un adversario a interactuar con elementos no productivos de un sistema, con el fin de aumentar la visibilidad de-

fensiva, desviar la atención de activos reales o recopilar información sobre técnicas y comportamientos de ataque. Esta definición adopta un enfoque operativo y pragmático, alineado con la literatura reciente, y evita interpretaciones excesivamente amplias que diluyen el concepto en nociones generales de ofuscación o seguridad por oscuridad.

Desde una perspectiva defensiva, las técnicas de cyber deception suelen materializarse mediante honeypots, honeytokens, servicios falsos, credenciales señuelo o generación controlada de actividad engañosa. En entornos de producción, el diseño de estos mecanismos está condicionado por factores como el riesgo operativo, el impacto en sistemas reales, la escalabilidad y la integración con herramientas de monitoreo y respuesta. El objetivo principal es mejorar capacidades defensivas medibles, tales como la detección temprana de intrusiones o la reducción del tiempo de respuesta.

En contextos educativos, sin embargo, los objetivos difieren de manera sustancial. El propósito no es maximizar la efectividad defensiva ni minimizar el riesgo, sino facilitar la comprensión profunda de los mecanismos de engaño y de sus efectos en escenarios adversariales controlados. Esto implica priorizar la observabilidad, la manipulabilidad de las configuraciones y la posibilidad de experimentar con distintos niveles y tipos de engaño, aun a costa de adoptar configuraciones que no serían aceptables en producción.

Esta distinción entre uso operativo y uso educativo es central para el diseño de entornos de aprendizaje basados en cyber deception. Un laboratorio educativo efectivo debe permitir a los participantes asumir tanto el rol de atacante como el de defensor, y observar cómo las decisiones de diseño en los mecanismos de engaño influyen en el comportamiento adversarial y en los artefactos de monitoreo generados (Conti et al., 2020). En este sentido, el cyber deception se presenta no solo como una técnica defensiva, sino como un objeto de estudio que expone dinámicas fundamentales de la interacción ataque–defensa.

Desde el punto de vista pedagógico, el diseño del entorno propuesto se apoya en principios de aprendizaje activo y experimental, ampliamente utilizados en la enseñanza práctica de la ciberseguridad. En particular, se priorizan: (i) la experimentación directa sobre infraestructuras funcionales, (ii) la posibilidad de cometer errores sin consecuencias fuera del entorno controlado, y (iii) la reflexión posterior a partir de evidencias observables, como registros de eventos y trazas de actividad. Estos principios no se presentan como un marco teórico exhaustivo, sino como criterios prácticos que guían las decisiones de diseño del laboratorio.

En conjunto, este marco conceptual y educativo establece las bases para el diseño del Cyber Deception Playground, que se describe en la siguiente sección. El énfasis se coloca en hacer explícitos los trade-offs entre realismo, seguridad y valor pedagógico, y en diferenciar claramente el aprendizaje del cyber deception de su despliegue en entornos productivos.

4. Diseño del entorno

El Cyber Deception Playground fue diseñado como un entorno educativo práctico orientado al aprendizaje experimental de técnicas de *cyber deception*. Su arquitectura prioriza la reproducibilidad, la modularidad y la observabilidad, con el objetivo de

facilitar la exploración controlada de escenarios adversariales que incorporan mecanismos explícitos de engaño defensivo (Pham et al., 2021).

El entorno se basa en una arquitectura conteinarizada, desplegable mediante herramientas estándar de orquestación local. Esta decisión responde a dos criterios principales: por un lado, reducir las barreras de entrada para su adopción en contextos educativos heterogéneos; por otro, permitir que los distintos componentes del laboratorio puedan activarse, modificarse o sustituirse de manera independiente, sin afectar la coherencia general del escenario.

4.1. Escenario base y narrativa

El laboratorio se estructura en torno a un escenario ficticio denominado *AndesFinance*, que simula una organización financiera de tamaño medio. La elección de una narrativa coherente busca proporcionar un contexto verosímil que facilite la comprensión de los activos, flujos de información y superficies de ataque involucradas. No se pretende replicar con precisión un entorno productivo real, sino ofrecer un marco suficientemente plausible para sostener ejercicios de ataque, defensa y análisis.

El escenario incluye componentes típicos de una infraestructura corporativa: un servicio frontend orientado a usuarios internos, un backend con lógica de negocio simplificada y un repositorio de datos que contiene información señuelo con apariencia de datos financieros. Estos elementos constituyen la base sobre la cual se introducen mecanismos de engaño defensivo con distintos niveles de complejidad.

4.2. Componentes del entorno

El Cyber Deception Playground se compone de los siguientes módulos principales:

- **Servicios funcionales vulnerables**, diseñados para exponer fallas comunes de configuración o implementación, con fines exclusivamente educativos.
- **Mecanismos de engaño**, que incluyen servicios señuelo accesibles desde el exterior, artefactos falsos y credenciales deliberadamente expuestas, cuya función es inducir interacciones adversariales observables.
- **Generador de actividad simulada**, encargado de producir tráfico y eventos que imitan comportamientos legítimos, con el objetivo de introducir ruido controlado y complejidad analítica.
- **Infraestructura de monitoreo**, basada en un stack de recolección y visualización de eventos, que permite observar tanto la actividad real como la actividad engañosa generada en el entorno.
- **Entorno atacante**, que provee herramientas y scripts básicos para la ejecución de técnicas de intrusión, facilitando la experimentación desde la perspectiva adversarial.

Cada componente puede activarse o desactivarse de manera independiente, permitiendo configurar escenarios con distintos grados de engaño y complejidad.

4.3. Niveles de engaño

Con el fin de estructurar la experiencia de aprendizaje, el entorno contempla múltiples niveles de engaño, que varían en la cantidad y sofisticación de los mecanismos

desplegados. Estos niveles no representan una progresión de madurez defensiva en términos operativos, sino una herramienta pedagógica para introducir gradualmente conceptos de *cyber deception*.

Los niveles definidos incluyen configuraciones sin mecanismos de engaño explícitos, configuraciones básicas con señuelos evidentes, y escenarios más complejos en los que los límites entre activos reales y engañosos resultan deliberadamente ambiguos. Esta gradación permite comparar cómo cambian las interacciones adversariales y los artefactos de monitoreo a medida que se incrementa el uso del engaño defensivo.

4.4. Decisiones de diseño y trade-offs

El diseño del Cyber Deception Playground implica una serie de compromisos conscientes. En particular, se prioriza la claridad pedagógica y la capacidad de observación por sobre el realismo extremo o la robustez operacional. Algunas configuraciones de engaño, si bien útiles para el aprendizaje, no serían recomendables en entornos productivos debido a consideraciones de riesgo o mantenimiento. Estas decisiones se mantienen explícitas, con el objetivo de evitar la confusión entre prácticas educativas y prácticas operativas recomendadas.

En conjunto, el diseño del entorno busca ofrecer una base coherente y extensible para la enseñanza del *cyber deception*, facilitando la experimentación controlada y la reflexión posterior a partir de evidencias observables. La siguiente sección describe la metodología propuesta para evaluar el uso educativo del entorno y delimitar alcance.

5. Metodología de Evaluación

Dado que el Cyber Deception Playground se presenta como una propuesta de diseño educativo, y no como un estudio empírico de efectividad, este trabajo no incluye resultados cuantitativos ni comparativos sobre aprendizaje, desempeño defensivo o impacto operativo. No obstante, con el fin de delimitar su alcance y facilitar futuras evaluaciones, se describe a continuación la metodología de evaluación prevista para el uso del entorno en contextos educativos.

La evaluación propuesta se concibe desde una perspectiva formativa y exploratoria, orientada a analizar cómo el entorno puede ser utilizado para introducir y ejercitar conceptos de *cyber deception*, más que a medir su efectividad en términos absolutos (Gao et al., 2022). En este sentido, se identifican tres dimensiones principales de evaluación: uso del entorno, observabilidad de interacciones adversariales y percepción de utilidad educativa. Estas limitaciones se asumen explícitamente como parte del alcance del trabajo. El objetivo de esta sección no es validar empíricamente la propuesta, sino proporcionar un marco metodológico transparente que permita futuras evaluaciones sistemáticas del Cyber Deception Playground.

5.1. Contextos de uso previstos

El entorno está diseñado para ser utilizado en distintos contextos educativos, incluyendo cursos universitarios de seguridad avanzada, programas de capacitación profe-

sional y actividades de formación interna en equipos de ciberseguridad. En todos los casos, se asume un uso supervisado, con objetivos de aprendizaje definidos y actividades estructuradas que guíen la exploración del entorno.

No se asume un despliegue autónomo ni una evaluación a gran escala. Las metodologías propuestas son compatibles con cohortes pequeñas o medianas, típicas de entornos educativos especializados.

5.2. Fuentes de observación

La evaluación del uso del Cyber Deception Playground puede apoyarse en múltiples fuentes de observación, entre ellas:

- **Artefactos técnicos**, tales como registros de eventos, trazas de actividad y visualizaciones generadas por la infraestructura de monitoreo.
- **Evidencia de interacción**, incluyendo comandos ejecutados, rutas de ataque exploradas y puntos de contacto con mecanismos de engaño.
- **Materiales producidos por los participantes**, como reportes de análisis, respuestas a ejercicios guiados o reflexiones estructuradas posteriores a la actividad práctica.

Estas fuentes permiten analizar cómo los participantes interactúan con los mecanismos de engaño y qué tipo de patrones emergen durante la experimentación.

5.3. Indicadores cualitativos

Dado el carácter exploratorio de la propuesta, los indicadores considerados son principalmente cualitativos. Entre ellos se incluyen la capacidad de los participantes para identificar artefactos engañosos, describir el rol del engaño defensivo en un escenario dado y razonar sobre las decisiones de diseño adoptadas. Estos indicadores no se interpretan como medidas objetivas de aprendizaje, sino como señales preliminares del valor pedagógico del entorno.

No se proponen, en esta etapa, métricas estandarizadas ni comparaciones con grupos de control (Holm et al., 2021). La definición de instrumentos cuantitativos y diseños experimentales formales se considera trabajo futuro.

5.4. Limitaciones metodológicas

La metodología descrita presenta limitaciones claras. En particular, la ausencia de datos empíricos controlados impide extraer conclusiones sobre la efectividad del entorno en términos de mejora del aprendizaje o transferencia de conocimientos a contextos operativos reales. Asimismo, la evaluación cualitativa puede estar sujeta a sesgos propios de los contextos educativos y de la interpretación de los observadores.

6. Resultados

Dado el carácter de diseño de este trabajo y la ausencia de estudios empíricos controlados, los resultados presentados en esta sección se limitan a observaciones directas derivadas del despliegue y uso exploratorio del Cyber Deception Playground en contextos educativos acotados. No se reportan métricas cuantitativas de aprendizaje ni comparaciones entre cohortes.

6.1. Despliegue y reproducibilidad

El entorno pudo ser desplegado de manera consistente en distintos sistemas anfitriones mediante el uso de una arquitectura contenarizada. El proceso de instalación no requirió configuraciones específicas a nivel de hardware ni dependencias externas fuera de las definidas por el propio entorno. Esta reproducibilidad permitió replicar escenarios equivalentes para distintos participantes y sesiones, manteniendo condiciones iniciales comparables.

6.2. Configuración de escenarios con distintos niveles de engaño

Los niveles de engaño definidos en el diseño del entorno pudieron activarse y desactivarse de forma independiente, permitiendo la construcción de escenarios con distinta densidad y visibilidad de mecanismos señuelo. Esta variabilidad hizo posible observar diferencias claras en la superficie de interacción disponible para el atacante, así como en los tipos de eventos generados en la infraestructura de monitoreo.

6.3. Generación de artefactos observables

Durante la interacción con el entorno, tanto desde el rol atacante como desde el rol defensivo, se generaron artefactos técnicos observables, incluyendo registros de acceso, eventos de autenticación, interacciones con servicios señuelo y tráfico asociado a actividad simulada. Estos artefactos fueron accesibles a través de la infraestructura de monitoreo integrada, permitiendo su análisis posterior.

6.4. Interacción adversarial controlada

El entorno atacante permitió ejecutar técnicas básicas de reconocimiento, acceso inicial e interacción con servicios expuestos. En escenarios con mecanismos de engaño activos, se observaron interacciones dirigidas específicamente a componentes señuelo, diferenciables de aquellas orientadas a servicios funcionales. Estas interacciones constituyen evidencia de que los mecanismos de engaño desplegados resultaron accesibles y distinguibles en términos técnicos.

6.5. Producción de material educativo

Como resultado del uso del entorno, fue posible generar material educativo derivado, incluyendo ejercicios guiados, capturas de eventos relevantes y ejemplos de análisis de registros. Estos materiales se utilizaron como soporte para actividades de reflexión y discusión, aunque no se evaluó formalmente su impacto en el aprendizaje.

En conjunto, estos resultados describen el comportamiento observable del entorno y su capacidad para generar escenarios de interacción adversarial con mecanismos explícitos de engaño. No permiten, por sí mismos, extraer conclusiones sobre la efectividad pedagógica del Cyber Deception Playground ni sobre su aplicabilidad en contextos operativos reales.

7. Discusión

Los resultados observables presentados en la sección anterior permiten analizar el Cyber Deception Playground principalmente como un artefacto de diseño educativo, más que como una herramienta cuya efectividad haya sido validada empíricamente. En este marco, la discusión se centra en qué tipo de prácticas y reflexiones educativas habilita el entorno, y cuáles son los límites de las observaciones realizadas.

En primer lugar, la reproducibilidad del despliegue y la modularidad de los componentes sugieren que el entorno es adecuado para su uso en contextos formativos controlados, donde la consistencia entre instancias es un requisito fundamental. La posibilidad de recrear escenarios equivalentes facilita la planificación de actividades educativas estructuradas y reduce la variabilidad introducida por configuraciones ad hoc, un problema recurrente en laboratorios de ciberseguridad diseñados de manera informal.

En segundo término, la existencia de niveles explícitos de engaño permite introducir el *cyber deception* de manera progresiva y comparativa. Desde una perspectiva educativa, esta gradación resulta relevante porque hace visible el impacto que distintas decisiones de diseño tienen sobre la interacción adversarial y sobre los artefactos de monitoreo generados (Behl & Behl, 2022). Más que entrenar habilidades específicas, el entorno parece favorecer la comprensión de los trade-offs inherentes al uso del engaño defensivo, tales como la tensión entre visibilidad, realismo y ambigüedad (Spitzner, 2020).

Asimismo, la generación sistemática de artefactos técnicos observables —registros, eventos y trazas asociadas a interacciones con mecanismos señuelo— habilita instancias de análisis posterior que son difíciles de reproducir en entornos puramente teóricos. Este aspecto refuerza el valor del entorno como soporte para actividades de reflexión guiada, en las que los participantes pueden reconstruir y discutir dinámicas de ataque y defensa a partir de evidencia concreta.

No obstante, estas observaciones deben interpretarse con cautela. El hecho de que los participantes interactúen con mecanismos de engaño o produzcan artefactos analizables no implica, por sí mismo, una mejora en el aprendizaje ni una transferencia efectiva de conocimientos a contextos operativos reales. Del mismo modo, la accesibilidad de los mecanismos de engaño en un entorno educativo controlado no garantiza

su aplicabilidad o efectividad en infraestructuras productivas, donde las restricciones de riesgo, escala y mantenimiento son sustancialmente distintas.

Finalmente, es importante destacar que el Cyber Deception Playground no busca reemplazar otros enfoques educativos en ciberseguridad, como los *cyber ranges* generalistas o los laboratorios orientados a respuesta a incidentes (Vykopal et al., 2022). Su aporte potencial reside en complementar estas herramientas, introduciendo el *cyber deception* como un objeto de estudio explícito y sistemático, y no como un componente incidental de escenarios más amplios.

8. Limitaciones y trabajo futuro

Este trabajo presenta limitaciones explícitas que deben ser consideradas al interpretar su alcance. En primer lugar, el Cyber Deception Playground se introduce como una propuesta de diseño educativo, sin validación empírica sistemática de su impacto en el aprendizaje. La ausencia de estudios controlados, métricas cuantitativas y grupos de comparación impide extraer conclusiones sobre su efectividad pedagógica o su superioridad frente a otros enfoques formativos.

En segundo lugar, el entorno fue concebido para contextos educativos controlados y con fines exploratorios. Algunas decisiones de diseño —particularmente aquellas orientadas a maximizar la observabilidad o simplificar configuraciones— no son directamente transferibles a entornos productivos reales. Por lo tanto, el uso del entorno no debe interpretarse como una recomendación implícita de prácticas operativas de cyber deception.

Finalmente, las observaciones reportadas se basan en usos exploratorios y acotados del entorno. Estas observaciones están sujetas a sesgos contextuales y no representan evidencia generalizable sobre comportamientos de aprendizaje o desempeño profesional. A partir de esta propuesta de diseño, se abren varias líneas de trabajo futuro. Una dirección prioritaria consiste en la realización de estudios empíricos controlados que evalúen el impacto del uso del Cyber Deception Playground en procesos de aprendizaje, comparándolo con enfoques educativos alternativos. Estos estudios podrían incorporar métricas cuantitativas, instrumentos de evaluación estandarizados y diseños experimentales longitudinales.

Asimismo, el entorno puede extenderse para explorar escenarios multiusuario, integración con herramientas de monitoreo externas o incorporación de mecanismos de engaño más dinámicos. Estas extensiones permitirían analizar no solo el valor educativo del entorno, sino también su potencial como plataforma experimental para investigaciones académicas sobre cyber deception.

9. Conclusiones

En este trabajo se presentó el Cyber Deception Playground como un entorno educativo reproducible orientado al aprendizaje práctico de técnicas de cyber deception. Frente a la limitada presencia del engaño defensivo en la formación formal en ciber-

seguridad, la propuesta busca ofrecer una base concreta para introducir esta disciplina desde una perspectiva experimental y controlada.

El aporte principal del trabajo reside en el diseño y justificación de un entorno educativo que hace explícito el rol del cyber deception como objeto de estudio, diferenciando claramente su uso pedagógico de sus aplicaciones operativas. Sin afirmar resultados de efectividad ni impacto en el aprendizaje, el artículo establece un punto de partida para futuras evaluaciones empíricas y desarrollos adicionales. En un contexto donde las técnicas de ataque y defensa continúan evolucionando, la incorporación crítica y práctica del cyber deception en procesos formativos representa una oportunidad para ampliar la comprensión de las dinámicas adversariales en ciberseguridad. Este trabajo aspira a contribuir a esa discusión desde una perspectiva honesta, reproducible y metodológicamente cauta.

Bibliografía

Almeshekah, M., and E. Spafford, "Planning and integrating deception into computer security defenses," in Proc. ACM Workshop on Moving Target Defense (MTD), 2020, pp. 27–34.

Behl, N., and K. Behl, "Active cyber defense: A pedagogical perspective," Journal of Cybersecurity, vol. 8, no. 1, 2022.

Cohen, A., et al., "Cyber deception for cloud environments: A systematic review," Future Generation Computer Systems, vol. 125, pp. 549–563, 2021.

Conti, G., T. S. Sford, and B. Sangster, "Teaching cybersecurity through adversarial thinking," IEEE Security & Privacy, vol. 18, no. 5, pp. 66–70, Sep.–Oct. 2020.

Fraunholz, D., et al., "Demystifying deception technology: A survey," Computers & Security, vol. 93, Art. no. 101727, 2020.

Gao, J., et al., "Experiential learning in cybersecurity education: A systematic review," Education and Information Technologies, vol. 27, pp. 10231–10255, 2022.

Holm, S., et al., "Cybersecurity education in practice: A systematic literature review," Computers & Education, vol. 168, Art. no. 104193, 2021.

Khandelwal, S., et al., "Honeytokens: Towards a practical deception-based defense," in Proc. Annual Computer Security Applications Conference (ACSAC), 2021, pp. 1–12.

MITRE Corporation, "MITRE ATT&CK®: A knowledge base of adversary tactics and techniques," 2020–2024. [Online]. Available: https://attack.mitre.org

Nawrocki, M., et al., "A survey on honeypot software and data analysis," IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1033–1058, 2021.

Pasquini, C., et al., "Hands-on cybersecurity education: Challenges and opportunities," in Proc. ACM SIGCSE, 2022, pp. 1–7.

Pawlick, J., E. Colbert, and Q. Zhu, "A game-theoretic taxonomy and survey of cyber deception for network security," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2224–2239, 2020.

Pham, C., et al., "Design and evaluation of cybersecurity labs for hands-on learning," IEEE Transactions on Education, vol. 64, no. 4, pp. 344–352, Nov. 2021.

Sahu, R. K., et al., "Deception-based defense mechanisms: Recent advances and open challenges," IEEE Access, vol. 9, pp. 150124–150145, 2021.

Spitzner, L., “Cyber deception: Concepts, strategies, and challenges,” IEEE Security & Privacy, vol. 18, no. 3, pp. 80–85, May–Jun. 2020.
Vykopal, A., et al., “On the use of cyber ranges in cybersecurity education,” IEEE Security & Privacy, vol. 20, no. 4, pp. 44–52, Jul.–Aug. 2022.
Yamin, M., et al., “Cyber ranges and testbeds: A survey on design, applications, and challenges,” Computers & Security, vol. 102, Art. no. 102139, 2021.