



# **Diseño e implementación de un entorno de ciberseguridad para la formación y defensa ante amenazas cibernéticas: Un enfoque basado en MITRE ATT&CK**



## **Design and implementation of a cybersecurity environment for training and defense against cyber threats: A MITRE ATT&CK approach**

David Felipe Galindo-Gutiérrez<sup>1</sup>, Sebastián Cerquera-Carvajal<sup>2</sup>

Galindo-Gutiérrez, D.F; Cerquera-Carvajal, S. Diseño e implementación de un entorno de ciberseguridad para la formación y defensa ante amenazas cibernéticas. *Seguridad y privacidad en redes. VIII Congreso Internacional en Inteligencia Ambiental, Ingeniería de Software, Salud Electrónica y Móvil (AmITIC)*.

---

1 Universidad Surcolombiana.  
 [u20201189121@usco.edu.co](mailto:u20201189121@usco.edu.co)  
 [www.linkedin.com/in/davidfgut](https://www.linkedin.com/in/davidfgut)

2 Universidad Surcolombiana  
 [u20211195928@usco.edu.co](mailto:u20211195928@usco.edu.co)  
 <https://www.linkedin.com/in/sebastian-cerquera-carvajal-6845aa249/>

## Resumen

El aumento en la frecuencia y automatización de los ciberataques ha evidenciado limitaciones en la preparación técnica del talento humano. Según el *Cost of a Data Breach Report 2024* de IBM, el costo promedio global de una brecha de seguridad alcanzó los 4,45 millones de dólares [1]. Por su parte, el *ENISA Threat Landscape Report* señala que el 82 % de los incidentes involucran el factor humano [2]. Diversas investigaciones destacan que los entornos de simulación mejoran la capacidad operativa ante amenazas reales.

En este contexto, la presente investigación propone el diseño e implementación de un entorno de ciberseguridad en un campus universitario, orientado a la formación y defensa ante ciberamenazas. El entorno integrará infraestructura híbrida, herramientas de detección y respuesta, y escenarios basados en TTPs reales, estructurados con base en el framework MITRE ATT&CK.

La metodología seguirá un enfoque mixto, articulado a través del ciclo de vida del software. Se evaluarán competencias técnicas mediante simulaciones, documentación sistemática y análisis de desempeño, generando un modelo replicable para entornos académicos. Esta iniciativa pretende fomentar el aprendizaje práctico, fortalecer competencias técnicas y promover la innovación desde un enfoque investigativo dentro de un entorno real de telecomunicaciones.

## Palabras clave

*Ciberataques, ciberamenazas, entorno de ciberseguridad, tácticas, técnicas y procedimientos (TTPs), MITRE ATT&CK framework.*

## Abstract

The increase in the frequency and automation of cyberattacks has revealed limitations in the technical readiness of human talent. According to IBM's *Cost of a Data Breach Report 2024*, the global average cost of a security breach has reached \$4.45 million [1]. In this regard, the *ENISA Threat Landscape Report* indicates that 82% of incidents involve the human factor [2]. Various studies highlight that simulation environments enhance operational capabilities against real threats.

In this context, the present research proposes the design and implementation of a cybersecurity environment within a university campus, aimed at training and defending against cyber threats. The environment will integrate hybrid infrastructure, detection and response tools, and scenarios based on real-world TTPs, structured according to the MITRE ATT&CK framework.

The methodology will follow a mixed-methods approach, articulated through the software development life cycle. Technical competencies will be assessed through simulations, systematic documentation, and performance analysis, generating a replicable model for academic environments. This initiative seeks to promote hands-on learning, strengthen technical skills, and foster innovation through a research-oriented approach within a real telecommunications setting.

## Keywords

*Cyberattacks, cyber threats, cybersecurity environment, tactics, techniques and procedures (TTPs), MITRE ATT&CK framework.*

## Introducción

En el panorama actual, la acelerada transformación digital ha expandido de manera considerable la superficie de exposición de organizaciones frente a amenazas cibernéticas cada vez más sofisticadas. Estas combinan técnicas de intrusión, evasión y explotación de vulnerabilidades que superan con facilidad las defensas tradicionales. Según el *Global Threat Landscape Report* de Fortinet [3], la actividad de escaneo automatizado aumentó un 16,7 %, con más de 36 000 escaneos por segundo, mientras que los ataques dirigidos al robo de credenciales crecieron un 42 %, con más de 1,7 mil millones de registros comprometidos circulando en foros clandestinos.

El escenario anterior pone en evidencia una brecha significativa entre las exigencias tácticas de la industria en materia de ciberseguridad y la formación que aún predomina en el ámbito académico, caracterizada por enfoques teóricos y ejercicios poco contextualizados. Estudios recientes advierten que sólo una fracción limitada de las instituciones educativas implementa laboratorios con simulaciones prácticas estructuradas. Como destacan Shin et al. [4], la ausencia de un enfoque formativo basado en escenarios ha generado dificultades significativas para la ejecución efectiva de actividades cibernéticas, lo que restringe el desarrollo de competencias esenciales como la detección de amenazas, la respuesta a incidentes y el análisis forense.

A nivel operativo, las herramientas tecnológicas empleadas para la detección y monitoreo de amenazas, como los sistemas SIEM, también presentan limitaciones significativas frente a las tácticas empleadas por actores maliciosos. Aunque el framework MITRE ATT&CK ha sido adoptado por más del 80 % de las organizaciones como estándar para describir comportamientos adversarios [5], su integración efectiva en los entornos productivos sigue siendo limitada. Según un análisis realizado por Cardinal Ops, los sistemas SIEM solo logran detectar el 24 % de las 196 técnicas incluidas en la versión 13 del framework, lo que representa una cobertura operacional claramente insuficiente [6].

En respuesta a esta brecha, el presente proyecto plantea el diseño e implementación futura de un entorno de ciberseguridad orientado a la formación y defensa ante ciberamenazas, alineado con la estructura táctica del framework MITRE ATT&CK. Este entorno tendrá una infraestructura híbrida que integra dispositivos físicos y software, así como la configuración de escenarios simulados de ataque y defensa. Su propósito es replicar condiciones controladas que permitan desarrollar competencias operativas en detección, análisis y contención de incidentes. Estudios destacan que este tipo de entornos, al recrear escenarios realistas, constituyen herramientas altamente efectivas para fortalecer las capacidades del personal de seguridad de la información [7].

Paralelamente, el framework MITRE ATT&CK aporta una base metodológica sólida para estructurar el entorno propuesto y contextualizar sus escenarios de entrenamiento. Su capacidad para representar de manera sistemática las tácticas, técnicas y procedimientos

(TTPs) adversarios ha consolidado su adopción tanto en la industria como en el ámbito académico. Un estudio reciente titulado “*MITRE ATT&CK Applications in Cybersecurity and The Way Forward*”, basado en el análisis sistemático de 417 publicaciones académicas, evidencia que el uso del framework se ha consolidado como una práctica transversal en áreas como inteligencia de amenazas, respuesta a incidentes, modelado de ataques y priorización de vulnerabilidades [8].

El diseño de un entorno de ciberseguridad que integre escenarios tácticos basados en el framework de alto nivel constituye una respuesta estructurada a las brechas formativas actuales. Esta iniciativa propone un modelo replicable que fortalece competencias operativas mediante simulaciones realistas y aporta valor estratégico en la formación técnica. Como ha señalado el CEO de Microsoft, “*Cybersecurity is the central challenge of the digital age*” [9], lo cual destaca la necesidad de enfoques formativos avanzados que consoliden capacidades especializadas frente a amenazas emergentes.

## **Marco teórico**

### **Cyber ranges**

Un *cyber range* es un entorno controlado diseñado para simular infraestructuras reales y ataques cibernéticos con fines de formación, pruebas o investigación. IBM los define como espacios que permiten entrenar bajo condiciones realistas sin comprometer sistemas productivos [10]. De acuerdo con investigadores del sector, estos entornos fortalecen la conciencia situacional y la respuesta táctica ante amenazas, y su implementación puede adoptar diversas modalidades, como la simulación virtual, emulación de hardware/software, integración sobre redes reales (*overlay*) o modelos híbridos [11].

### **Cybersecurity homelab**

Investigaciones definen un *homelab* como un entorno local autogestionado, normalmente desplegado en una residencia, que permite probar, desarrollar o entrenar aplicaciones y sistemas virtualizados en condiciones controladas, con el fin de consolidar conocimientos teóricos a través de la práctica en entornos virtuales de pequeña escala [12].

### **MITRE ATT&CK como eje metodológico**

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) es una base de conocimiento empírica que documenta tácticas, técnicas y procedimientos (TTPs) utilizados por adversarios reales. Su estructura permite mapear amenazas en diversos entornos operativos, y ha sido adoptada ampliamente en prácticas de inteligencia, simulación y validación de defensas [13]. Autores afirman que su integración en procesos formativos permite alinear escenarios de entrenamiento con amenazas actuales, mejorando la capacidad táctica del personal de ciberseguridad [14].

### **Defense in depth**

De acuerdo con el documento *NIST Special Publication 800-53 Rev. 5*, la defensa en profundidad es una estrategia de seguridad que integra personas, tecnología y procesos operativos para establecer múltiples barreras a lo largo de toda la organización [15]. Su valor

estratégico radica en la implementación de múltiples mecanismos de protección distribuidos en capas que aseguran una defensa robusta mediante controles independientes, así como en su flexibilidad para adaptarse a los requerimientos particulares de cada organización frente a un entorno digital complejo y en constante amenaza [16].

## **Materiales y métodos**

El proyecto adopta una metodología de enfoque mixto para evaluar integralmente el impacto técnico y formativo del entorno de ciberseguridad propuesto. Se analizará el desempeño operativo en escenarios tácticos y la evolución de las competencias adquiridas, guiado por dos variables: la estrategia de formación basada en MITRE ATT&CK y el nivel de competencia técnica alcanzado. La ejecución se estructurará según el ciclo de vida del software, mediante actividades progresivas en las fases de análisis, diseño, desarrollo, pruebas, implementación y despliegue.

Durante la fase de análisis se definirá el alcance técnico y funcional del entorno, se identificarán los recursos de hardware y software necesarios, se caracterizarán los departamentos involucrados y se establecerán las competencias e indicadores de desempeño técnico a desarrollar.

En la fase de diseño, se proyectará la arquitectura lógica y física del entorno. Esta incluirá la elaboración de diagramas de topología de red, así como la distribución de dispositivos clave como cortafuegos, servidores, y estaciones de trabajo. Se definirán también las tablas de direccionamiento IP, y se establecerán los esquemas de protocolos a implementar. Además, se diseñarán diagramas de control de acceso que aborden aspectos técnicos, lógicos y administrativos bajo la estrategia de *defense in depth*.

Durante la fase de desarrollo, se llevará a cabo la instalación y configuración detallada de cada uno de los componentes que conforman la infraestructura tecnológica. Esta etapa resulta clave para la materialización de la arquitectura lógica y operativa del entorno, sobre la cual se evaluará tanto la estrategia técnica implementada como el nivel de competencia alcanzado por los participantes.

En la fase de pruebas se validará la efectividad técnica y formativa del entorno mediante auditorías de seguridad (caja blanca, negra y gris) y simulaciones de amenazas avanzadas. Los resultados se evaluarán con métricas de desempeño y herramientas cualitativas como entrevistas y encuestas a involucrados.

Durante la fase de implementación, el entorno validado será desplegado en un contexto simulado con condiciones operativas reales. Se llevarán a cabo sesiones prácticas centradas en escenarios estructurados según el modelo MITRE ATT&CK, con énfasis en la adquisición de competencias operativas.

Finalmente, en la fase de despliegue y documentación se sistematizará la experiencia técnica y pedagógica adquirida mediante la elaboración de manuales, diagramas, lineamientos y documentación de simulaciones, consolidando todo en un repositorio digital

institucional.

## Resultados esperados

Se proyecta que el entorno de ciberseguridad propuesto permitirá mejorar significativamente las competencias técnicas de los participantes en áreas clave como la seguridad ofensiva y defensiva. Al estructurar los escenarios prácticos con base en el framework MITRE ATT&CK, se espera lograr una mayor contextualización táctica en la formación.

Desde una perspectiva académica, se anticipa el fortalecimiento del enfoque pedagógico mediante la incorporación de metodologías activas, que integren simulación, documentación sistemática y evaluación por desempeño. Este proceso permitirá establecer indicadores claros de progreso, tanto individuales como grupales.

Asimismo, se espera que el proyecto genere un modelo técnico y formativo replicable, documentado en guías, manuales y esquemas de implementación que puedan ser adoptados por otras instituciones educativas.

Finalmente, se prevé que la iniciativa contribuya a reducir la brecha entre el entrenamiento académico y los requerimientos reales del sector, posicionando a la universidad como referente en la formación de profesionales altamente capacitados para enfrentar desafíos de ciberseguridad en entornos reales.

## Conclusiones

- El proyecto propuesto responde a una necesidad crítica identificada en el actual panorama de ciberseguridad: la limitada preparación técnica del talento humano frente a amenazas cada vez más sofisticadas. La integración del framework MITRE ATT&CK en entornos simulados representa una estrategia formativa robusta que permite contextualizar escenarios reales de ataque y defensa, fortaleciendo competencias operativas de manera práctica.
- La implementación de un entorno de ciberseguridad en el campus universitario no solo busca cerrar la brecha entre la formación académica y los desafíos del sector, sino también ofrecer un modelo replicable y escalable para otras instituciones educativas.
- Se espera que esta iniciativa contribuya significativamente a la generación de conocimiento aplicado, la consolidación de capacidades técnicas especializadas y el impulso a la innovación en el ámbito académico.

## Referencias

- [1] IBM Security. (2024). *Cost of a data breach report 2024*. Ponemon Institute. <https://www.ibm.com/reports/data-breach>
- [2] European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape 2023*. <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf>
- [3] Fortinet. (2025). *Global threat landscape report 2025*. FortiGuard Labs. <https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report-2025.pdf>

- [4] Shin, Y., Kwon, H., Jeong, J., & Shin, D. (2024). A study on designing cyber training and cyber range to effectively respond to cyber threats. *Electronics*, 13(19), 3867. <https://doi.org/10.3390/electronics13193867>
- [5] Basra, K. S., & Kaushik, T. (2020). MITRE ATT&CK as a framework for cloud threat investigation. *McAfee & Center for Long-Term Cybersecurity (CLTC), University of California, Berkeley*. [https://cltc.berkeley.edu/wp-content/uploads/2020/10/MITRE\\_ATTCK\\_Framework\\_Report.pdf](https://cltc.berkeley.edu/wp-content/uploads/2020/10/MITRE_ATTCK_Framework_Report.pdf)
- [6] Goldman, J. (2023). Enterprise SIEMs miss 76% of MITRE ATT&CK techniques. *eSecurity Planet*. <https://www.esecurityplanet.com/threats/mitre-attck-detection-gap/>
- [7] Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G., & Ferrag, M. A. (2021). *Cyber Ranges and TestBeds for Education, Training, and Research*. *Applied Sciences*, 11(4), 1809. <https://doi.org/10.3390/app11041809>
- [8] Jiang, Y., Meng, Q., Shang, F., Oo, N., Minh, L. T. H., Lim, H. W., & Sikdar, B. (2025). *MITRE ATT&CK applications in cybersecurity and the way forward: A systematic review* (arXiv preprint). <https://arxiv.org/abs/2502.10825>
- [9] Nadella, S. (2018, September 24). *Microsoft fortifies security and brings AI to the masses at Ignite 2018*. Microsoft News. <https://news.microsoft.com/2018/09/24/microsoft-fortifies-security-and-brings-ai-to-the-masses-at-ignite-2018/>
- [10] Finio, M., & Downie, A. (2024, May 16). *What is a cyber range?* IBM Consulting. <https://www.ibm.com/think/topics/cyber-range-ibm.com>
- [11] Ukwandu, E., van Niekerk, B., & Loock, M. (2020). *A review of cyber ranges and testbeds: Current and future trends*. arXiv. <https://doi.org/10.48550/arXiv.2010.06850>
- [12] Dadiyala, C. (2023, July). *Designing and implementing an effective cybersecurity home lab for detection and monitoring*. In *Proceedings of the 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE. <https://doi.org/10.1109/ICCCNT56998.2023.10306937>
- [13] MITRE. (2024). *MITRE ATT&CK Framework*. <https://attack.mitre.org/>
- [14] Roy, S., Panaousis, E., Noakes, C., et al. (2023). *SoK: The MITRE ATT&CK Framework in Research and Practice*. arXiv. <https://arxiv.org/abs/2304.07411>
- [15] NIST. (2020). *Security and Privacy Controls for Information Systems and Organizations (Special Publication 800-53 Revision 5)*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-53r5>
- [16] Babanov, V. (December 2024). *Internals of Defense-In-Depth Strategy in Cybersecurity*. *Security and Defense*(2), 37-42. <https://doi.org/10.70265/PNEZ3158>