Technological-Educational Journal DOCENTES 2.0
LA2017000128 | ISSN: 2665-0266 | ISNI: 0000 0005 0409 1664 | Ringgold ID 608948 | ROR: 037jqrk16
RTED
Vol. 19 (2), 2026
June – November 2026
347-357

ESSAY

Classification of Digital Environments for Cybersecurity Education

Clasificación de Entornos Digitales para la Educación en Ciberseguridad

Enrique Ayala-Franco[1]

[1]Universidad Autónoma de Yucatán, Mérida, Mexico, email: enrique.ayala@correo.uady.mx

Received: April 25, 2026 | **Accepted:** September 23, 2026 | **Published:** November 29, 2026 | **DOI:** 10.37843/rted.v19i2.856

ABSTRACT

Cybersecurity training requires digital environments that go beyond traditional instruction and enable the development of practical and operational competencies aligned with the demands of the contemporary professional field. This essay aimed to construct a critical-technical classification of the primary digital environments used in cybersecurity education, considering their functional characteristics, pedagogical advantages, limitations, and potential for curricular integration. The study was framed within the humanistic-interpretive paradigm, employing an inductive-hermeneutic method and a qualitative, interpretive-documentary approach with a narrative-topical design. Methods included document analysis and a thematic-hermeneutic review of scientific literature published between 2020 and 2026, as well as specialized documents and technical frameworks related to cybersecurity training. The analysis identified eight types of environments: isolated physical laboratories, virtual laboratories, Capture the Flag (CTF) platforms, cyber ranges, threat simulators, specialized learning management systems, gamified environments, and isolated cloud environments. The interpretive synthesis indicated that no single environment, in isolation, fully covered the competencies identified in the analyzed literature, due to tensions between operational fidelity, accessibility, cost, scalability, and transferability to the workplace. As a conceptual contribution, a three-phase training progression (introductory, technical, and integrative) was proposed to align these environments with specific pedagogical objectives. The study concluded that cybersecurity education requires an instructional design that integrates multiple environments to strengthen technical, operational, and non-technical competencies.

KEYWORDS: Cybersecurity education, experiential learning, computer simulation, virtual learning environments, competency-based education.

RESUMEN

La formación en ciberseguridad requiere entornos digitales que superen la enseñanza tradicional y permitan desarrollar competencias prácticas y operativas acordes con las exigencias del campo profesional contemporáneo. El presente ensayo tuvo como objetivo construir una clasificación crítico-técnica de los principales entornos digitales utilizados en la educación en ciberseguridad, considerando sus características funcionales, ventajas pedagógicas, limitaciones y posibilidades de integración curricular. El estudio se enmarcó en el paradigma humanista-interpretativo, bajo el método inductivo-hermenéutico, con enfoque cualitativo, de tipo interpretativo-documental y con diseño narrativo de tópico. Se emplearon el análisis documental y el temático-hermenéutico de la literatura científica publicada entre 2020 y 2026, así como documentos especializados y marcos técnicos vinculados a la formación en ciberseguridad. El desarrollo argumentativo permitió identificar ocho tipos de entornos: laboratorios físicos aislados, laboratorios virtuales, plataformas de captura de bandera, rangos cibernéticos, simuladores de amenazas, sistemas de gestión del aprendizaje especializados, entornos gamificados y entornos aislados en la nube. La síntesis interpretativa indicó que ningún entorno, considerado de manera aislada, cubrió integralmente las competencias identificadas en la literatura analizada, debido a tensiones entre fidelidad operacional, accesibilidad, costo, escalabilidad y transferencia al contexto laboral. Como aporte conceptual, se propuso una progresión formativa en tres fases: introductoria, técnica e integradora, orientada a articular los entornos según objetivos pedagógicos específicos. Se concluyó que la educación en ciberseguridad requiere un diseño instruccional que integre múltiples entornos para fortalecer las competencias técnicas, operacionales y no técnicas.

PALABRAS CLAVE: Educación en ciberseguridad, aprendizaje práctico, simulación computacional, entornos virtuales de aprendizaje, formación basada en competencias.

How to Cite

Ayala-Franco, E. (2026). Classification of Digital Environments for Cybersecurity Education. *Docentes 2.0 Technological-Educational Journal, 19*(2), 347-357. https://doi.org/10.37843/rted.v19i2.856

OPEN ACCESS CC BY NC ND

RTED
Vol. 19 (2), 2026
June – November 2026
347-357

Introduction

Cybersecurity education requires digital environments that go beyond traditional instruction and enable the development of practical and operational competencies consistent with the demands of contemporary professional practice. This essay aims to develop a critical and technical classification of the principal digital environments used in cybersecurity education by examining their functional characteristics, pedagogical advantages, limitations, and possibilities for curricular integration. Accordingly, the guiding question is: What critical and technical classification of digital environments for cybersecurity education can inform curricular decisions aimed at developing professional competencies?

Effective cybersecurity education requires the integration of theoretical content with practical experiences through laboratories and interactive platforms (Blažič & Blažič, 2024). From the perspectives of experiential learning and authentic learning, the literature also associates the operational fidelity of environments with the transfer of competencies to professional practice (Glas et al., 2023; Karagiannis et al., 2024). Educational models incorporating practical technologies likewise offer possibilities for adaptation to different cybersecurity training needs (Mukherjee et al., 2024). Nevertheless, the literature reviewed points to the need to integrate technical and pedagogical criteria when selecting environments according to their instructional purpose, implementation conditions, and stage in the educational pathway (Modesti et al., 2024).

The analysis encompasses eight types of digital environments for cybersecurity education: isolated physical laboratories, virtual laboratories, Capture the Flag (CTF) platforms, cyber ranges, threat simulators, specialized learning management systems (LMS), gamified environments, and isolated cloud environments (sandboxes). Its scope focuses on their technical and pedagogical characteristics, advantages and limitations, and potential for curricular articulation. Proprietary platforms not represented in the specialized academic literature are excluded from the comparative analysis; thus, the proposed classification is restricted to environments documented in the sources examined.

The essay is situated within the humanistic-interpretive paradigm, applying an inductive-hermeneutic method, a qualitative approach, an interpretive-documentary type, and a narrative-topical design. The documentary corpus comprised scientific literature published between 2020 and 2026, located through Scopus, Web of Science, and Google Scholar, together with specialized documents and technical frameworks related to cybersecurity education. Searches used Spanish and English terms relating to cybersecurity education, practice environments, experiential learning, and competency-based education; selection considered thematic relevance, methodological rigor, and recency. Document and thematic-hermeneutic analysis involved critical reading, categorization, and interpretive synthesis of the sources. Information was organized by technical characteristics, functionality, pedagogical advantages, limitations, and use cases, and compared according to operational fidelity, scalability, cost, accessibility, and competency profiles.

Discussion

Analyzing resources used in cybersecurity education requires an operational definition and explicit criteria for comparing them from technical and pedagogical perspectives. In this essay, a digital learning environment is understood as a technological platform, system, or infrastructure designed or adapted to promote the development of knowledge, skills, or attitudes related to information security through interaction with tools, applications, or technical scenarios (Karagiannis et al., 2024; Mukherjee et al., 2024). This definition includes infrastructure developed for academic purposes, commercial training solutions, and professional tools repurposed for education. Their origin does not in itself determine their pedagogical value, although it can influence cost, accessibility, and implementation possibilities.

For the purposes of this essay, four modes of educational interaction are distinguished to interpret the differences among the environments examined. The first involves practice under controlled conditions, intended to develop skills without real operational consequences. The second is simulation,

How to Cite
Ayala-Franco, E. (2026). Classification of Digital Environments for Cybersecurity Education. *Docentes 2.0 Technological-Educational Journal, 19*(2), 347-357. https://doi.org/10.37843/rted.v19i2.856

OPEN ACCESS
CC BY NC ND

RTED
Vol. 19 (2), 2026
June – November 2026
347-357

which reproduces situations using logical or computational models. The third is emulation, which replicates the operation of real systems using hardware or software. The fourth involves training under controlled real-world conditions, characterized by interaction with infrastructures similar to those used in production settings. These modes are not mutually exclusive, because the same environment may combine more than one depending on its architecture and instructional purpose.

Differences among these modes are associated with varying degrees of operational fidelity and the possibility of transferring learning to professional settings (Glas et al., 2023). On the basis of this distinction and the previously defined methodological procedure, the analysis is organized around five dimensions: technical description, functional characteristics, pedagogical advantages, limitations, and representative use cases. The cross-cutting comparison additionally considers five criteria: operational fidelity, scalability, cost, accessibility, and the profile of competencies developed. This analytical framework allows the environments to be compared using shared criteria and provides the foundation for the subsequent comparative synthesis.

Physical Laboratories in Isolated Environments

The isolated physical laboratory represents a high-operational-fidelity benchmark among the environments analyzed. These infrastructures integrate real hardware, including switches, routers, firewalls, servers, and workstations, interconnected through segregated networks that allow practical exercises without affecting other systems. Karagiannis et al. (2024) note that this type of environment promotes authentic learning by bringing students closer to conditions resembling professional practice. Its principal strength, therefore, lies in the opportunity to interact directly with real technologies and configurations under controlled conditions.

From a pedagogical perspective, the high operational fidelity of these environments may facilitate the transfer of certain competencies to professional settings, particularly when activities require direct interaction with real infrastructure. Nevertheless, this advantage does not mean that physical laboratories alone constitute a complete solution for cybersecurity education. Their value depends on the competency being developed, the design of activities, and institutional implementation conditions. Accordingly, fidelity must be assessed alongside other criteria, including accessibility, cost, and scalability.

This relationship is particularly relevant to institutional feasibility. Vykopal et al. (2021) indicate that dedicated physical infrastructures have limitations associated with establishment and maintenance costs and their capacity to expand as the number of participants grows. Scalability is therefore a decisive criterion in assessing the sustainability of these environments in educational contexts. The same authors caution that no available solution comprehensively satisfies all requirements for cybersecurity learning environments. This evidence allows the tension between operational fidelity and scalability to be understood as a central problem in selecting instructional resources, thereby justifying an examination of the possibilities offered by virtual laboratories.

Virtual Laboratories

Virtual laboratories use virtualization and emulation technologies to provide practical scenarios without relying exclusively on dedicated physical infrastructure. Compared with physical laboratories, they can reduce hardware requirements per student, facilitate remote access, and increase capacity to accommodate multiple users, although operational fidelity depends on the architecture and tools employed. These characteristics favor their inclusion in technical training activities, particularly when exercises need to be repeated, configurations modified, or learning scenarios restored under controlled conditions.

The technologies used in these laboratories have different levels of abstraction and infrastructure requirements, which can influence the complexity and fidelity of educational scenarios. Type 1 hypervisors, such as VMware ESXi or Xen, operate directly on hardware and enable multiple virtual machines to be managed in centralized infrastructures. Other solutions operate on host operating systems and provide more accessible implementation conditions in certain educational

How to Cite
Ayala-Franco, E. (2026). Classification of Digital Environments for Cybersecurity Education. *Docentes 2.0 Technological-Educational Journal, 19*(2), 347-357. https://doi.org/10.37843/rted.v19i2.856

OPEN ACCESS
CC BY NC ND

RTED
Vol. 19 (2), 2026
June – November 2026
347-357

contexts. These technical differences do not in themselves determine learning quality, but they do affect resource availability, scalability, and the complexity of scenarios that can be implemented.

It is also important to distinguish simulation from emulation in virtual laboratories. Harahus et al. (2023) analyzed EVE-NG as a network emulation platform and highlighted its capacity to develop complex scenarios, while also identifying limitations in compatibility, reliability, and performance. In contrast, simulation tools such as Cisco Packet Tracer reproduce network behavior through computational models and are widely used in network education. Asadi et al. (2024) identified Packet Tracer as one of the most frequently represented tools in the literature on simulation-based learning. The choice between simulation and emulation should therefore consider instructional objectives, the complexity required, and available resources.

Recent evidence also suggests that the effectiveness of these environments depends on the interaction between technological infrastructure and pedagogical design. Savu-Jivanov et al. (2026) evaluated an integrated virtual laboratory based on ESXi, GNS3, and EVE-NG and reported technical stability with 50 concurrent users, along with improvements in scores obtained after training activities. However, the study used a single-group pretest-posttest design; the authors themselves cautioned that the observed changes did not permit causal attribution exclusively to the virtual laboratory. These findings support the educational potential of this infrastructure while underscoring the need to interpret its effects in light of both instructional design and assessment conditions.

From this perspective, the principal strength of virtual laboratories is not merely their ability to replace physical infrastructure but their capacity to create reproducible, scalable, and adaptable practical experiences at different educational levels. Their pedagogical utility increases when technical scenarios are aligned with learning objectives, progressive activities, and coherent assessment mechanisms. This relationship among infrastructure, authenticity, and instructional design introduces the analysis of cyber ranges, where complex scenario simulation extends to collaborative dynamics and incident response.

Cyber Ranges

Cyber ranges are controlled environments that reproduce or emulate systems, networks, and applications for cybersecurity education, training, assessment, and experimentation. Their configuration allows participants to interact with attack-and-defense scenarios without compromising production infrastructure. Katsantonis et al. (2023) distinguish four principal purposes for cyber ranges: education, training, certification, and testing. These environments may also incorporate individual or collaborative work through differentiated functions, particularly offensive and defensive teams, expanding their potential to develop technical and coordination competencies.

The educational value of these environments depends on the alignment of technological architecture, learning objectives, and scenario design. Karagiannis et al. (2024) show that the NICE Framework can be used to structure the objectives, professional roles, tasks, knowledge, and skills guiding cyber range design. From another perspective, Glas et al. (2023) emphasize that assessment of these exercises must consider learning outcomes as well as authenticity, educational experience, collaboration, and scenario characteristics. Lal et al. (2026) identify opportunities in federated cyber ranges to expand resources, interoperability, and scalability, while warning of challenges related to technological heterogeneity, security, governance, and interplatform coordination.

One of the principal tensions identified in the literature concerns learning assessment. Damianou et al. (2026) note that traditional assessment mechanisms in cyber ranges frequently focus on general indicators, such as task completion, response accuracy, or achievement of objectives, which do not fully capture the perceptual and cognitive processes involved in threat response. To extend assessment, the authors propose a situational-awareness framework incorporating dimensions of perception, comprehension, and projection, together with indicators such as execution time, number of hints, sequence of steps, and effectiveness of the tools used.

The contrast between cyber ranges' capacity to reproduce complex scenarios and the limitations of

RTED
Vol. 19 (2), 2026
June – November 2026
347-357

their assessment mechanisms is relevant to curricular integration. Additional considerations include infrastructure, design and administration requirements, and the ongoing updating of scenarios in response to evolving threats. Their educational adoption therefore requires joint consideration of operational fidelity, instructional objectives, institutional resources, and assessment mechanisms. Within this continuum of practical experiences, Capture the Flag platforms represent a mode more closely focused on structured technical problem-solving.

Threat Simulation Environments

Threat simulation environments rely on a knowledge base of documented attacks and an execution platform that automates attack behaviors under controlled conditions. The principal reference framework is MITRE ATT&CK (MITRE Corporation, 2024b), a knowledge base of tactics, techniques, and procedures based on real-world attacks. Complementarily, MITRE CALDERA (MITRE Corporation, 2024a) enables the emulation of those behaviors using agents deployed on target systems to validate detection mechanisms.

What distinguishes these environments from those discussed above is the explicit traceability between simulated attacker behavior and defensive system responses. Yoo et al. (2020) propose an attack-and-defense agent emulation framework to demonstrate that automating adversarial behavior is effective for routine threat assessment training. Emulators allow the same attack to be repeated as often as necessary to verify whether security tools generate the expected alerts. This repeatability is also their main pedagogical strength compared with CTFs and cyber ranges, where each exercise is often a one-off event that is difficult to compare over time.

The review by Al-Sada et al. (2025) documents attacker behavior and the assessment of defensive gaps as the main analytical categories. However, updating the catalog of emerging tactics depends on observing and documenting real-world incidents. One limitation of the framework is that it does not distinguish between legitimate and malicious uses of a technique, for example, when a command is used to administer a system or to carry out an attack. Thus, a simulation environment based exclusively on ATT&CK may train analysts to recognize behavioral patterns without necessarily teaching them to judge the context in which those behaviors occur.

For a beginning student, distinguishing pattern from context is a difficult competency to acquire. Threat simulation environments focus on the technical validation of alerts. They are therefore useful for professionals with prior experience, who can interpret an alert within an already developed framework of judgment, rather than for students still in training. In contrast to this specialization in particular technical roles, the cybersecurity-specific learning management systems discussed next allow this knowledge to be organized and delivered progressively.

Learning Management Systems Specialized in Cybersecurity

Learning management systems specialized in cybersecurity organize content, activities, assessments, and practical resources within a single educational experience. Their value lies not only in distributing information but also in integrating digital resources with activities intended to progressively develop knowledge and skills. In their review of online university cybersecurity teaching, Ahmed et al. (2024) identified substantial use of virtual laboratories, gamification, and simulations as resources that support practical experiences, motivation, and active learning. This integration suggests that a platform acquires greater pedagogical value when it supports practical activities rather than simply serving as a content repository.

Another characteristic of these systems is their capacity to record user interactions and employ those data to support educational monitoring and intervention. Pan et al. (2024) indicate that records generated by students and teachers in LMSs enable learning analytics-based interventions that support teaching and learning practices. Nevertheless, the usefulness of such data depends on their relationship to course objectives and activities, because activity indicators alone do not directly establish which knowledge or competencies a student has developed. This limitation is particularly relevant in cybersecurity environments when learning assessment requires observing technical

How to Cite
Ayala-Franco, E. (2026). Classification of Digital Environments for Cybersecurity Education. *Docentes 2.0 Technological-Educational Journal, 19*(2), 347-357. https://doi.org/10.37843/rted.v19i2.856

OPEN ACCESS
CC BY NC ND

RTED
Vol. 19 (2), 2026
June – November 2026
347-357

performance rather than merely patterns of platform interaction.

The literature on cybersecurity education also emphasizes the need to combine online learning structures with practical experiences. Mukherjee et al. (2024) analyze different educational models and stress the importance of incorporating remote laboratories, virtual classrooms, and other applied technologies to meet the need to develop competencies linked to professional practice. Similarly, Ahmed et al. (2024) show that online courses employ strategies such as active learning, case studies, simulations, and hands-on activities to complement content presentation. Consequently, the LMS should be understood as part of an educational ecosystem in which content, activities, technology, and assessment are aligned with educational objectives.

From this perspective, learning management systems primarily contribute organization, monitoring, and structured access to educational resources; they do not, by themselves, guarantee competency acquisition or transfer to professional contexts. Their utility increases when integrated with laboratories, simulations, practical activities, and performance-related assessment mechanisms. This relationship among educational structure, interaction, and participation leads to the analysis of gamified environments, whose experience design incorporates specific mechanisms intended to foster engagement and continuity of learning.

Gamified Environments

Gamified environments constitute a strategy for increasing participation and engagement in cybersecurity education, although their effects depend on pedagogical design and user characteristics. Gamification incorporates game elements, such as points, levels, badges, challenges, or leaderboards, into activities that are not games in the strict sense; serious games, by contrast, are designed as complete experiences with educational or training objectives. In a systematic review of cybersecurity games, Ng and Hasan (2024) found that a substantial proportion of the proposals analyzed targeted users with prior knowledge and that technical content predominated. These findings indicate that incorporating game dynamics does not in itself guarantee accessibility for all learner profiles.

Available evidence suggests favorable results mainly over short assessment periods. In a systematic review focused on cybersecurity awareness among professionals who do not specialize in information technology, Gwenhure and Rahayu (2024) found that elements such as narrative, leaderboards, and interactive scenarios were associated with improvements in knowledge, participation, and certain behaviors linked to learning objectives. However, the authors identified an important limitation: evidence of sustained long-term effects is insufficient. They also highlighted the need to examine habituation effects and determine whether motivation associated with these elements persists once the novelty of the experience diminishes.

Serious games may also broaden training possibilities through contextualized scenarios and adaptive experiences. In developing and evaluating CyberHero, Hodhod et al. (2023) reported that most participants stated that they had acquired new knowledge and rated the narrative and interaction experience positively. These findings support the potential of serious games to foster engagement and awareness, although user responses alone should not be interpreted as evidence of lasting learning transfer. Likewise, Batzos et al. (2023) caution that certain traditional awareness strategies based primarily on memorization may be insufficient when they do not promote reflection on security concepts and decisions.

Overall, the reviewed literature suggests that the main contribution of gamified environments is their capacity to combine engagement, contextualized practice, and feedback through experiences designed around specific learning objectives. Nevertheless, observable engagement during an activity does not necessarily equate to deep learning or guarantee sustained behavioral change. Their usefulness depends on the correspondence among game mechanics, content, participants' prior knowledge, and intended learning outcomes. Gamified environments should therefore be understood as complementary resources within a broader educational strategy. The need to combine accessibility with technical practice leads to the analysis of isolated cloud environments.

How to Cite
Ayala-Franco, E. (2026). Classification of Digital Environments for Cybersecurity Education. *Docentes 2.0 Technological-Educational Journal, 19*(2), 347-357. https://doi.org/10.37843/rted.v19i2.856

OPEN ACCESS
CC BY NC ND

RTED
Vol. 19 (2), 2026
June – November 2026
347-357

Isolated Cloud Environments

Isolated cloud environments provide virtualized computing resources on remote, controlled infrastructures, enabling practical activities without relying exclusively on hardware available at the educational institution. These configurations may include on-demand virtual laboratories and isolated environments for experimentation or specialized analysis. AWS Academy Learner Lab is an example of educational infrastructure that allows students to use cloud services in controlled environments. For malware analysis, tools such as Cuckoo Sandbox represent a more specialized approach designed to execute potentially dangerous files in isolated environments and record aspects of their behavior, including network connections, system interface calls, and modifications made during execution.

A major advantage of these environments is their ability to reduce reliance on local computing resources and provide remote access to configurable infrastructures. Comparing laboratories based on AWS EC2 and VirtualBox, Khan & Mohamed (2025) found differences in execution time and resource utilization. In a traffic analysis exercise, the activity was completed in approximately 5.5 minutes with AWS EC2, compared with 11 minutes with VirtualBox. These results indicate performance and operational-capacity advantages in the evaluated scenario, but they do not in themselves establish that a cloud environment produces better learning outcomes. Otoum et al. (2025) likewise note that remote laboratories can extend access to practical experiences and reduce some institutional infrastructure requirements, provided that technical, pedagogical, and security considerations are jointly addressed in their design.

These advantages are accompanied by challenges in resource management, security, scalability, and costs. On-demand infrastructure models require controls over provisioning and resource use to avoid unnecessary consumption, while connectivity quality can influence remote access experiences. Otoum et al. (2025) further stress the need to manage virtualization, orchestration, user access, security, and monitoring appropriately to ensure the reliability of remote laboratories. At the institutional level, Afolalu and Tsoeu (2025) also identify risks associated with the growing adoption of cloud-based systems in higher education within a wider context of governance, data protection, and digital infrastructure security.

Consequently, isolated cloud environments offer advantages in remote access, flexibility, and scalability, but their suitability depends on available infrastructure, operating costs, security requirements, and pedagogical objectives. Their adoption does not eliminate institutional technological challenges; instead, it transforms them into challenges involving resource management, connectivity, configuration, and reliance on external providers. Their curricular inclusion must therefore be assessed using the same criteria applied in this essay to the other environments: operational fidelity, scalability, cost, accessibility, and the profile of competencies developed.

Critical Comparative Analysis

Comparing the eight environments makes it possible to integrate the previously examined technical, pedagogical, and operational characteristics using common criteria. Tables 1 and 2 synthesize this interpretation from two complementary perspectives: implementation conditions related to institutional feasibility, and the competencies or instructional uses predominantly associated with each environment. The categories used are not derived from standardized scales or empirical measurements; rather, they constitute a qualitative synthesis based on the thematic-hermeneutic analysis of the reviewed literature. Where the sources provided direct evidence, the classification reflected those findings; where evidence was primarily descriptive or conceptual, assessments were established through interpretive comparison. Accordingly, the matrices should be understood as guiding comparative tools rather than validated scoring instruments.

How to Cite
Ayala-Franco, E. (2026). Classification of Digital Environments for Cybersecurity Education. *Docentes 2.0 Technological-Educational Journal, 19*(2), 347-357. https://doi.org/10.37843/rted.v19i2.856

OPEN ACCESS
CC BY NC ND

RTED
Vol. 19 (2), 2026
June – November 2026
347-357

Table 1

Multidimensional Comparative Matrix of Digital Environments for Cybersecurity Education.

Environment	Operational fidelity	Scalability	Implementation cost	Learner accessibility
1. Isolated physical lab	Very high	None	High–Very high	Low (in person)
2. Virtual lab	Medium	High	Low–Medium	High
3. Cyber range	Very high	Medium	High–Very high	Medium
4. CTF	Medium–Low	Very high	Low	Very high
5. Threat simulation	High (detection)	High	Medium–High	Medium
6. Specialized LMS	Low–Medium	Very high	Low–Medium	Very high
7. Gamified environments	Low	Very high	Low	Very high
8. Cloud sandbox	Medium	High	Low (variable)	High

Note. The classification criteria are explained in the text. Author's own work (2026).

Table 1 identifies a recurrent tension among operational fidelity, scalability, cost, and accessibility. In the reviewed literature, isolated physical laboratories and cyber ranges offer greater opportunities to approximate complex operational conditions, although they also require more infrastructure, administrative, and maintenance resources. By contrast, CTFs, specialized LMSs, and certain gamified environments offer favorable accessibility and scalability but develop different competency profiles and do not necessarily reproduce the complexity of professional scenarios. Virtual laboratories and cloud environments occupy intermediate positions, with their assessment dependent on configuration and design. These differences reinforce the advisability of selecting environments according to instructional objectives and institutional conditions rather than establishing a universal hierarchy among them.

Table 2

Detailed Competency Profile by Cybersecurity Learning Environment.

Environment	Predominant cognitive level	Role / Perspective	Principal technical domain
1. Isolated physical lab	Analysis and direct operation	Advanced technical / on-site	Forensic analysis, OT/ICS maintenance, tactical response
2. Virtual lab	Procedural application	Individual technical operator	Service configuration, network segmentation, system hardening
3. Cyber range	Synthesis and collaborative decision-making	Blue team / coordinated defense	Incident response, crisis management, communication under pressure
4. CTF	Assessment under pressure and time constraints	Red team / offensive	Exploitation, reverse engineering, cryptanalysis, OSINT
5. Threat simulation	Control assessment and validation	Analytical / detection	Threat hunting, event correlation, SIEM tuning
6. Specialized LMS	Conceptual understanding	Cross-cutting / regulatory	Standards (ISO, NIST), governance, theoretical foundations
7. Gamified environments	Recognition and behavioral change	End user / awareness	Phishing recognition, secure decision-making, security culture
8. Cloud sandbox	Experimentation and controlled analysis	Individual analytical / remote access	Malware analysis, tool testing, tactical threat intelligence

Note. The classification criteria are explained in the text. The comparison indicates that no single environment simultaneously encompasses the technical, operational, and nontechnical competencies required for cybersecurity education. Author's own work (2026).

Table 2 shows that the environments analyzed offer differentiated and partially complementary educational profiles. Physical and virtual laboratories are principally associated with technical and procedural competencies; cyber ranges incorporate complex scenarios that may integrate coordination and decision-making; CTFs focus on structured technical problem-solving; and threat simulation environments facilitate observation, detection, and validation of adversarial behaviors. Specialized LMSs contribute content organization and progression, while gamified environments may

RTED
Vol. 19 (2), 2026
June – November 2026
347-357

strengthen engagement, awareness, and contextualized decision-making. Cloud environments, in turn, broaden opportunities for remote access, experimentation, and scenario replication. This relative specialization indicates that no environment should be considered sufficient on its own to cover every dimension of cybersecurity education.

Based on the complementarities and limitations identified, this essay proposes a learning progression structured into three phases. During an introductory phase, specialized LMSs, gamified environments, and virtual laboratories may be combined through guided activities focusing on foundations, awareness, and initial practice. During a technical-development phase, more complex virtual laboratories, CTFs, and isolated cloud environments may be introduced to broaden autonomy, experimentation, and problem-solving. During an operational-integration phase, cyber ranges, threat simulators, advanced laboratories, and collaborative activities may bring students closer to complex professional scenarios. This progression is a conceptual proposal derived from the interpretive synthesis, not an empirically validated sequence; accordingly, its application must be adapted to the curricular objectives, prior knowledge, institutional resources, and professional profiles that each program intends to develop.

Conclusion

On the basis of the preceding discussion, the main findings and their scope for cybersecurity education can be synthesized. The analysis sought to establish which critical and technical classification of digital environments for cybersecurity education can inform curricular decisions aimed at developing professional competencies. The answer is inductive: the literature lacks an integrative framework to guide these decisions and instead documents tensions among operational fidelity, accessibility, cost, scalability, and learning transfer, whose synthesis constitutes the central contribution of this study. Analysis of the documentary corpus identified eight types of environments with distinct characteristics, advantages, and limitations, from which criteria can be applied to their selection and curricular integration.

The contribution is a multidimensional comparative framework, contrasted with NICE Framework profiles, that has thus far been absent from the literature reviewed. This framework gives rise to a three-phase learning progression that reframes the central issue: cybersecurity education should not be understood as selecting an appropriate platform, but as progressively designing technical-pedagogical experiences that combine multiple environments according to instructional objectives and learners' levels.

Three conclusions support this argument. First, no single environment simultaneously covers the technical, operational, and nontechnical competencies required in the field, making complementary integration of environments a structural condition of any program. Second, instructional design shapes the educational value of an environment as much as its technical capabilities: Glas et al. (2023) and Savu-Jivanov et al. (2026) indicate that the same infrastructure can produce different pedagogical outcomes depending on how the experience is structured around it. Third, the tension between fidelity and accessibility requires institutions to make explicit pedagogical decisions about what to prioritize at each point in the learning pathway.

The proposed framework provides teachers with pedagogical criteria for evidence-informed technology selection that help avoid purely intuitive decision-making. For curriculum designers, the three-phase progression makes it possible to coordinate environments along a coherent pathway. For educational institutions, the information presented can guide investment decisions based on actual infrastructure, budget, and delivery conditions.

The study has limitations that must be considered when interpreting its findings. The narrative review did not follow a systematic protocol, which introduces potential documentary selection bias. The proposed classifications are substantiated interpretations rather than empirical measurements, and they have not been validated by experts or tested against actual implementation data.

Future research could address the empirical validation of the proposed learning progression, the exploration of hybrid models, and the development of standardized instruments for assessing complex

How to Cite
Ayala-Franco, E. (2026). Classification of Digital Environments for Cybersecurity Education. *Docentes 2.0 Technological-Educational Journal, 19*(2), 347-357. https://doi.org/10.37843/rted.v19i2.856

OPEN ACCESS
CC BY NC ND

RTED
Vol. 19 (2), 2026
June – November 2026
347-357

competencies acquired in these environments. In a field where the proliferation of platforms exceeds institutions' capacity to assess them with pedagogical rigor, frameworks such as the one proposed are necessary for cybersecurity education to meet the actual demands of professional practice.

Declaration of Conflicts of Interest

The author declares that there are no conflicts of interest related to conducting this study or interpreting its findings. He further states that he has no personal, academic, or financial relationships that could influence the development or findings of the research.

Funding Statement

The author declares that this research received no funding from public, private, or commercial institutions and was conducted using his own resources, thereby ensuring the independence of the research process.

Ethics Statement

This essay did not require ethics committee approval because it was based exclusively on interpretive analysis of scientific literature, without involving human participants or using personally identifiable information. Academic integrity, appropriate citation, and responsible use of the information consulted were ensured.

References

Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity in higher education institutions: A systematic review of emerging trends, challenges and solutions. *Future Internet, 17*(12), 575. https://doi.org/10.3390/fi17120575

Ahmed, A., Watterson, C., Alhashmi, S., & Gaber, T. (2024). How universities teach cybersecurity courses online: a systematic literature review. *Frontiers in Computer Science, 6*, 1499490. https://doi.org/10.3389/fcomp.2024.1499490

Al-Sada, B., Sadighian, A., & Oligeri, G. (2025). MITRE ATT&CK: State of the art and way forward. *ACM Computing Surveys, 57*(1), Article 12. https://doi.org/10.1145/3687300

Asadi, S., Allison, J., Khurana, M., & Nilashi, M. (2024). Simulation-based learning for computer and networking teaching: A systematic literature review and bibliometric analysis. *Education and Information Technologies*. https://doi.org/10.1007/s10639-024-12476-7

Batzos, Z., Saoulidis, T., Margounakis, D., Fountoukidis, E., Grigoriou, E., Moukoulis, A., Liatifis, A., Karypidis, P. A., Bibi, S., Filippidis, A., Kazanidis, I., Nifakos, S., Kasig, T., & Heydari, M. (2023). Gamification and serious games for cybersecurity awareness and first responders training: An overview. *TechRxiv*. https://doi.org/10.36227/techrxiv.22650952.v1

Blažič, A., & Blažič, B. (2024). Toward effective learning of cybersecurity. *Journal of Cybersecurity, 10*(1), tyae018. https://doi.org/10.1093/cybsec/tyae018

Damianou, A., Mazi, M. S., Rizos, G., Bezas, K., Lazaridis, G., Voulgaridis, A., Votis, K., & Tzovaras, D. (2026). Measuring the unseen: a situational awareness scoring framework for cyber range training. *International Journal of Information Security, 25*(2), 73. https://doi.org/10.1007/s10207-026-01219-z

Glas, M., Messmann, G., & Pernul, G. (2023). Train as you fight: Evaluating authentic cybersecurity training in cyber ranges. In Proceedings of *the 2023 CHI Conference on Human Factors in Computing Systems* (CHI '23). ACM. https://doi.org/10.1145/3544548.3581046

Gwenhure, A. K., & Rahayu, F. S. (2024). Gamification of cybersecurity awareness for non-IT professionals: A systematic literature review. *International Journal of Serious Games, 11*(1), 83–99. https://doi.org/10.17083/ijsg.v11i1.719

Khan, A., & Mohamed, A. (2025). Optimizing cybersecurity education: A comparative study of on-premises and cloud-based lab environments using AWS EC2. *Computers, 14*(8), 297. https://doi.org/10.3390/computers14080297

Harahus, M., Cavojský, M., & Bugár, G. (2023). Interactive network learning: An assessment of EVE-NG platform. *Acta Electrotechnica et Informatica, 23*(3), 3–9. https://doi.org/10.2478/aei-2023-0011

Hodhod, R., Hardage, H., Abbas, S., & Aldakheel, E. A. (2023). CyberHero: An adaptive serious game to promote cybersecurity awareness. *Electronics, 12*(17), 3544. https://doi.org/10.3390/electronics12173544

Karagiannis, S., Magkos, E., Ntantogian, C., & Ribeiro, B. (2024). Towards NICE-by-design cybersecurity learning environments. *Journal of Network and Systems Management, 32*, 42. https://doi.org/10.1007/s10922-024-09816-w

Katsantonis, M. N., Fouliras, P., & Mavridis, I. (2023). Cyber range design framework for cyber security education and training. *International Journal of Information Security, 22*, 1005–1027. https://doi.org/10.1007/s10207-023-00680-4

Lal, C., Yamin, M. M., & Spathoulas, G. (2026). Navigating cyber range federations: An exploration of current landscape, obstacles, and prospects. *International Journal of Information Security, 25*, 53. https://doi.org/10.1007/s10207-026-01226-0

MITRE Corporation. (2024a). *MITRE ATT&CK: Design and philosophy*. https://attack.mitre.org/

RTED
Vol. 19 (2), 2026
June – November 2026
347-357

MITRE Corporation. (2024b). *CALDERA: Adversary emulation platform*. https://caldera.mitre.org/

Modesti, P., Golightly, L., Salah, M., Fernandez-Vargas, J., & Sarr, M. (2024). Bridging the gap: A survey and classification of research-informed ethical hacking tools. *Journal of Cybersecurity and Privacy*, *4*(3), 410–448. https://doi.org/10.3390/jcp4030021

Mukherjee, M., Le, N. T., Chow, Y. W., & Susilo, W. (2024). Strategic approaches to cybersecurity learning: A study of educational models and outcomes. *Information*, *15*(2), 117. https://doi.org/10.3390/info15020117

Ng, C. Y., & Hasan, M. K. B. (2024). Cybersecurity serious games development: A systematic review. *Computers & Security*, *150*, 104307. https://doi.org/10.1016/j.cose.2024.104307

Otoum, N., Al Maqousi, A., Alauthman, M., & Almomani, A. (2025). Remote labs in cybersecurity education: Analyzing software requirements and challenges. *International Journal of Cloud Applications and Computing*, *15*(1), 1–27. https://doi.org/10.4018/IJCAC.383300

Pan, Z., Biegley, L., Taylor, A., & Zheng, H. (2024). A systematic review of learning analytics: Incorporated instructional interventions on learning management systems. *Journal of Learning Analytics*, *11*(2), 52–72. https://doi.org/10.18608/jla.2023.8093

Savu-Jivanov, A., Stolojescu-Crisan, C., Gal, J., & Ancuti, C. (2026). Integrated virtual laboratory for networking, cybersecurity, and automation education with enhanced scalability. *Frontiers in Education*, *11*, 1708228. https://doi.org/10.3389/feduc.2026.1708228

Vykopal, J., Čeleda, P., Seda, P., Švábenský, V., & Tovarňák, D. (2021). Scalable learning environments for teaching cybersecurity hands-on. In Proceedings of *the 51st IEEE Frontiers in Education Conference* (FIE '21). IEEE. https://doi.org/10.1109/FIE49875.2021.9637180

Yoo, J. D., Park, E., Lee, G., Ahn, M. K., Kim, D., Seo, S., & Kim, H. K. (2020). Cyber attack and defense emulation agents. *Applied Sciences*, *10*(6), 2140. https://doi.org/10.3390/app10062140