***Recibido** 04/03/2021* ***ReCIBE, Año 9 No. 2, Noviembre 2020***

***Aceptado** 25/04/2021*

# Tecnología de contenedores y su aplicación en el aprendizaje de ciberseguridad: una revisión sistemática deliteratura

## Container technology and its application in cybersecurity learning: a systematic review ofliterature

Roger A. Chingo[1]
roger.a.chingo.e@pucesa.edu.ec

Omar S. Gómez [1, 2]
ogomez@espoch.edu.ec

[1] Pontificia Universidad Católica del Ecuador - Sede Ambato[2] GrIISoft Research Group, Escuela Superior Politécnica de Chimborazo

**Resumen:** El aprendizaje de Ciberseguridad por su naturaleza cambiante exige de procesos cognitivos tanto teóricos como prácticos, particularmente, los prácticos requieren de entornos hiperrealistas que no pongan en riesgo infraestructura real o acarreen situaciones de índole legal, estas plataformas que contienen dichos entornos, son conocidos como ciber-rangos, debido a su complejidad pueden ser costosos y difíciles de implementar por lo que gran parte de los esfuerzos para su aprendizaje y enseñanza han estado enfocados en la utilización de distintas tecnologías que mejoren estos aspectos, así se ha empezado a utilizar la virtualización por contenedores que presenta ligereza y flexibilidad en su aplicación. En este artículo se presentan los resultados de una Revisión Sistemática de la Literatura realizada para identificar y caracterizar estudios primarios vinculados con la tecnología de contenedores aplicados a la enseñanza de la ciberseguridad. Los resultados obtenidos muestran que existen diversos estudios primarios que investigan la utilización de la tecnología de contenedores en el aprendizaje de Ciberseguridad; siendo la gran mayoría propuestas de plataformas, ciber-rangos (Cyber Ranges), laboratorios virtuales y competiciones de Captura la Bandera (*Capture The Flag – CTFs*) debido a la escasez de software especializado para el aprendizaje de Ciberseguridad.

**Palabras Clave:** Ciberseguridad, Seguridad Informática, Aprendizaje, Educación, Contenedores, Virtualización Ligera, Software Educativo, Revisión Sistemática de Literatura.

**Abstract:** Due to constating changing, Cybersecurity learning requires a theoretical and practical cognitive processes, particularly, practical approach requires to use hyper-realistic environments that do not put real infrastructure at risk or lead to situations of a legal nature, these platforms that contains these environments are known as Cyber Ranges, because of their Complexity it can be expensive and difficult to implement, for this reason, a large part of the efforts for learning and teaching have been focused on the use of different technologies that improve these aspects, therefore container virtualization has begun to be used, which is a lightweight and flexible in its application. This article presents the results of a Systematic Literature Review carried out to identify and characterize primary studies on the use of containers for learning Cybersecurity. The results show that there are several primary studies that investigate the use of container technology in learning Cybersecurity; Being the great majority proposals of platforms, Cyber Ranges, virtual laboratories, and Capture the Flag competitions (CTFs) due to the shortage of specialized software for learning Cybersecurity.

**Keywords:** Cybersecurity, Information Security, Learning, Education, Containers, Lightweight Virtualization, Educational Software, Systematic Literature Review.

## 1. Introducción

El aprendizaje de ciberseguridad es un proceso complejo y de una continua demanda de profesionales calificados, por lo que se han realizado diferentes esfuerzos para definir el rol, alcance, extensión y posición de la ciberseguridad dentro de las disciplinas académicas en la educación superior (Raj et al., 2017); dichos esfuerzos han ido enfocados a estrategias de aprendizaje y a la utilización de diferentes tecnologías como la virtualización por contenedores que según Singh & Singh (2016) ayudan a mejorar el rendimiento de los laboratorios ya que un único sistema operativo se encarga de todos las llamadas al hardware.

La investigación reportada en el presente artículo tiene como propósito presentar los usos de la tecnología de contenedores en el aprendizaje de ciberseguridad, características tecnológicas, beneficios cognitivos o posibles limitaciones del uso de la tecnología de contenedores en el aprendizaje de ciberseguridad. Para Genero et al. (2014) un estudio secundario como el que se reporta utiliza como metodología la Revisión Sistemática de Literatura con la cual se tiene como propósito seleccionar y analizar estudios primarios que utilicen la tecnología de contenedores en el aprendizaje de Ciberseguridad.

El presente artículo se encuentra organizado de la siguiente manera: la segunda sección conceptualiza la tecnología de contenedores y la educación de la ciberseguridad. La tercera sección explica las tareas a realizar en una Revisión Sistemática de Literatura, ya que es útil contar con un marco de trabajo para la investigación de un fenómeno o área de interés. En la cuarta sección se detalla la planificación a seguir para la realización de la investigación. La sección cinco describe la ejecución del protocolo de la Revisión Sistemática de Literatura. La sexta sección presenta los principales hallazgos de esta revisión, resultado de las preguntas de investigación propuestas. Por último, pero no menos importante, la última sección presenta algunas conclusiones alcanzadas con la realización del estudio.

## 2. Marco Teórico

### Tecnología de Contenedores

La virtualización es una tecnología que permite segregar recursos que toma una aplicación, un intérprete de órdenes (en Inglés, *shell)* invitado o un almacenamiento en la nube mediante la representación de hardware o software real (Anand et al., 2021). Existen varios tipos de virtualización, siendo en la actualidad las tecnologías más utilizadas las siguientes: virtualización completa, paravirtualización y virtualización a nivel de sistema operativo.

La virtualización completa utiliza una máquina virtual que funciona con hardware físico real a través de un hipervisor y sistema operativo host (Ageyev et al., 2018). Mientras que la paravirtualización requiere un núcleo (en Inglés, *kernel*) modificado del sistema operativo para administrar instrucciones privilegiadas del sistema (Barham et al., 2003). Al ser la tecnología de virtualización a nivel de sistema operativo la equivalente a la contenerización y tener relevancia en el tema de investigación se conceptualizará de manera independiente en el siguiente párrafo.

La tecnología de contenedores se basa en virtualizar el sistema operativo compartiendo el núcleo del ordenador anfitrión (en Inglés, *host)* con los contenedores por lo que puede considerarse un ambiente virtual pequeño y aislado, que incluye un conjunto de dependencias específicas necesarias para ejecutar una aplicación específica (Morabito, 2017), al ser un ambiente virtual aislado una aplicación que se ejecuta en un contenedor tiene acceso no compartido a una copia del sistema operativo (Shirinbab et al., 2017), así que contiene todo lo que se necesita para ejecutar código, tiempo de ejecución, herramientas del sistema y librerías (Aroraa, 2017), a diferencia de los virtualización completa a través de hipervisores la virtualización por contenedores se considera un tipo de virtualización ligera.

Para Yadav et al. (2019) existen diferentes tipos de contenedores o podemos decir modelos de entrega de acuerdo con los diferentes sistemas operativos:

• Linux: OpenVZ, LXC Linux containers, Docker.

• Windows: Sandboxie.

La tecnología de contenerización se ha ido desarrollando sobre todo en distribuciones Linux siendo una de las primeras tecnologías OpenVZ, continuando a LXC Linux Containers, que en la actualidad Docker acogió y extendió en varias maneras -principalmente a través de imágenes portables y una interfaz amigable al usuario- para crear una solución completa para la creación y distribución de contenedores (Mouat, 2016).

**Educación de la Ciberseguridad**

La ciberseguridad es un área multidisciplinaria que involucra tecnología, personas, información y procesos para permitir operaciones seguras. Implica la creación, operación, análisis y prueba de sistemas informáticos seguros (Burley et al., 2013); lo que la convierte en un área de difícil aprendizaje ya que su aplicación requiere del desarrollo diferentes habilidades teóricas y prácticas a un nivel medio-alto, para la parte teórica se ocupan diferentes metodologías de aprendizaje de corte tradicional, mientras la parte práctica requiere de la utilización de entornos virtuales hiperrealistas denominados ciber-rangos (en Inglés, *Cyber Ranges*) (Priyadarshini, 2018), que simulan una gran variedad de situaciones a las que los estudiantes podrían enfrentarse en el futuro, por lo que no se puede esperar que un único programa de educación cubra todas las habilidades especializadas y el conocimiento específico del sector deseado por cada empleador (Crumpler & Lewis, 2019).

La virtualización se convierte en una buena alternativa para poder simular estos entornos, en especial la virtualización por contenedores ya que permite desarrollar e implementar los laboratorios virtuales las veces que el estudiante o el profesor lo requieran de forma fácil y rápida sin comprometer el hardware y software real, ya que estos laboratorios virtuales se pueden ocupar en cualquier equipo que cumpla las características de hardware o software necesarias para desplegar los entornos.

Varias plataformas permiten el aprendizaje de ciberseguridad a través de ciber-rangos mediante la modalidad de aprendizaje e-learning, que de acuerdo con Arcos et al. (2018) permite suministrar material educativo en línea (a través del Internet) a los usuarios. Entre las plataformas que ocupan virtualización ligera Vykopal et al. (2017) listan: KYPO, Avatao, Hacking-Lab y CTFs (*Capture The Flag*).

## 3. Metodología de Investigación

La Revisión Sistemática de Literatura (RSL) es una metodología a través de la cual se logra identificar, valorar e interpretar la información de investigaciones disponibles en la literatura que resulta de interés sobre una temática en específico. La metodología para realizar la revisión seguirá el formato propuesto por Kitchenham (2004) la cual esta divida en tres fases principales que son: planificación, ejecución, reporte de la RSL. A continuación, se describen las actividades a realizar en cada fase.

### 3.1. Planificación

En esta fase se realizan las siguientes actividades como son la Identificación de la necesidad de la revisión donde se intenta resumir la información existente sobre la temática de interés. Se formulan las preguntas de investigación donde se guía el proceso de la revisión sistemática de literatura para determinar la información de importancia en los estudios primarios, estas preguntas deben ser claras y concisas. También se define el protocolo de la revisión donde se especifica la necesidad de investigación, preguntas de investigación, bases de datos científicas, cadenas de búsqueda, estrategias de búsqueda, además de criterios de inclusión y exclusión para la selección de estudios primarios. Por último, se válida el protocolo de la revisión. El protocolo es parte crucial para la elaboración de la RSL, es necesaria su verificación por parte de expertos.

### 3.2. Ejecución

En esta fase se realizan las siguientes actividades como la identificación de la información relevante donde se determina si los estudios primarios contribuyen a las preguntas de investigación planteadas de acuerdo con la estrategia de búsqueda que se presenta en el protocolo. En esta fase se seleccionan los estudios primarios. En esta actividad se sitúan los estudios primarios que estén relacionados a la temática y respondan a las preguntas de investigación, de acuerdo con los criterios y proceso que se establece en el protocolo. También se evalúa la calidad de los estudios primarios. Una vez seleccionados los estudios primarios, se procede a corroborar la calidad de estos y de ser necesario excluir los que no cumplan con los criterios, se extraen los datos relevantes. Es el proceso de analizar la información de los estudios primarios y seleccionar los datos de interés. Finalmente se sintetiza los datos extraídos donde se procesan los datos seleccionados por medio de tablas, gráficos u otros elementos para responder a las preguntas de investigación planteadas.

### 3.3. Reporte de la RSL

En esta última fase se redacta el informe de la revisión donde se reporta y se pone a disposición de otros investigadores el resultado de la RSL.
Una vez descritas las fases que conforman la metodología de revisiones sistemáticas de literatura, en los siguientes apartados se describen las actividades realizadas en la presente RSL con respecto a las diferentes fases de esta metodología.

## 4. Planificación

Con el propósito de conocer el estado del arte de la aplicación de la tecnología de contenedores en el aprendizaje de ciberseguridad esta investigación tiene por objetivo principal realizar una síntesis de la literatura existente, para lo cual se han establecido varias preguntas de investigación como guía del estudio.

### 4.1. Preguntas de Investigación

Las preguntas de investigación planteadas y desarrolladas son las siguientes:

- PI1. ¿Cuál es la evolución en número y tipo de publicaciones relacionadas con el uso de la tecnología de contenedores en el aprendizaje de ciberseguridad desde 2010 hasta 2020?
- PI2. ¿Cuáles son los sistemas operativos predilectos para desarrollar contenedores aplicados en el aprendizaje de Ciberseguridad?
- PI3. ¿Qué tipos de contenedores se han aplicado en el aprendizaje de Ciberseguridad?
- PI4. ¿Qué características tecnológicas son las más citadas en la tecnología de contenedores?
- PI5. ¿Cuáles han sido los beneficios reportados en el uso de contenedores para el aprendizaje de la ciberseguridad?
- PI6. ¿Cuáles han sido las dificultades tecnológicas reportadas en el uso de contenedores para el aprendizaje de la ciberseguridad?
- PI7. ¿Cuáles son las estrategias educativas utilizadas para el aprendizaje de la Ciberseguridad?
- PI8. ¿Cuáles son las principales limitaciones pedagógicas vinculadas con el uso de contenedores en el aprendizaje de la Ciberseguridad?
- PI9. ¿Existe Software Educativo exprofeso para el aprendizaje de la Ciberseguridad?

### 4.2. Selección de las bases de datos

Una vez definida las preguntas de investigación se procedió a seleccionar las bases de datos como fuentes de búsqueda de estudios primarios: IEEE Xplore y ACM Digital Library son bases de datos que incluyen una amplia gama de literatura científica en el área de la computación; también se analizó la posibilidad de incluir otras fuentes como Elsevier y Springer, no obstante por las limitantes en tiempo recursos disponibles para el proyecto en el que se circunscribe la RSL, se optó por incluir la base de datos de resúmenes SCOPUS que es una de las bases de datos con el mayor número de resúmenes sobre literatura científica. El acceso a los documentos completos se llevó a cabo utilizando las credenciales de acceso a la biblioteca virtual de la Pontificia Universidad Católica del Ecuador sede Ambato.

### 4.3. Definición de la cadena de Búsqueda

La cadena de búsqueda fue defina de acuerdo con la temática a investigar. Utilizando palabras clave en inglés, operadores lógicos “AND” y “OR”, además de tesauros digitales para ampliar la representación de los conceptos.

(container* OR docker* OR LXC OR "light virtualization") AND (learn* OR “training” OR e-learn* OR study OR educat* OR teach* OR “evaluation” OR assess*) AND (cybersecurity OR "Cyber Ranges" OR "computer security" OR "IT Security" OR "Cyber Security" OR “Information technology security”)

### 4.4. Criterios de inclusión y exclusión

Después de definir la selección de las bases de datos y las cadenas de búsqueda, se ha delimitado la selección de estudios primarios en los siguientes criterios de inclusión (CI) y criterios de exclusión (CE).

La selección de artículos primarios se basó en el título, resumen y palabras clave para clasificarlos como relevantes, se seleccionaron los trabajos teniendo en cuenta el cumplimiento de los siguientes criterios de inclusión:

1) Estudios primarios reportados en idioma inglés.
2) Estudios primarios reportados entre 2010 y 2020.
3) Estudios primarios que reporten iniciativas de investigación en el ámbito del aprendizaje de ciberseguridad.
4) Artículos que incluyan en el titulo o en el resumen al menos una palabra clave relacionada con el aprendizaje de la ciberseguridad.
5) Artículos de revistas o conferencias.

El criterio de inclusión de estudios reportados en idioma ingles responde a la escasez de estudios primarios relacionados a la tecnología de contenedores y su aplicación en el aprendizaje de ciberseguridad en idioma español que se determinó en la investigación preliminar a la RSL.

De la misma forma, se ignoraron aquellos artículos que cumplan con alguno de los siguientes criterios de exclusión:

1) Artículos duplicados en las bibliotecas digitales dando prioridad a las bibliotecas IEEE Xplore y ACM Digital Library.
2) Artículos vinculados con tecnologías de virtualización, diferentes a contenedores.
3) Artículos relacionados al mismo proyecto, se eliminarán los artículos que reporten progreso parcial; se mantendrá el estudio más completo.
4) Artículos cuyo contenido sea imposible de obtener.

## 5. Ejecución

En esta fase, el protocolo establecido es ejecutado, con la cadena de búsqueda definida se realizó la exploración de estudios primarios en las fuentes seleccionadas, cabe recalcar que en todas las fuentes se aplicó el filtró por año de publicación desde 2010 hasta 2020, en el caso de IEEE Xplore y SCOPUS se filtró por tipo de documento limitando a artículos de revistas o conferencias, la cadena de búsqueda no necesito ninguna modificación estructural, salvo en el caso de SCOPUS donde tuvo que agregarse TITLE-ABS-KEY () quedando de la siguiente manera:

TITLE-ABS-KEY ((*container** OR *docker** OR *LXC* OR "*light virtualization*") AND (*learn** OR "*training*" OR *e-learn** OR *study* OR *educat** OR *teach** OR "*evaluation*" OR *assess**) AND (*cybersecurity* OR "*Cyber Ranges*" OR "*computer security*" OR "*IT Security*" OR "*Cyber Security*" OR "*Information technology security*"))

La Figura 1 ilustra la ejecución de las tres etapas definidas por la RSL, de dicho proceso se obtuvieron finalmente un conjunto de 20 estudios primarios; estos estudios fueron analizados para dar respuesta a las preguntas de investigación propuestas para el estudio. Cabe mencionar que las tres etapas del proceso de ejecución se realizaron en una misma semana, iniciando la etapa 1 el día cinco de diciembre de 2020.

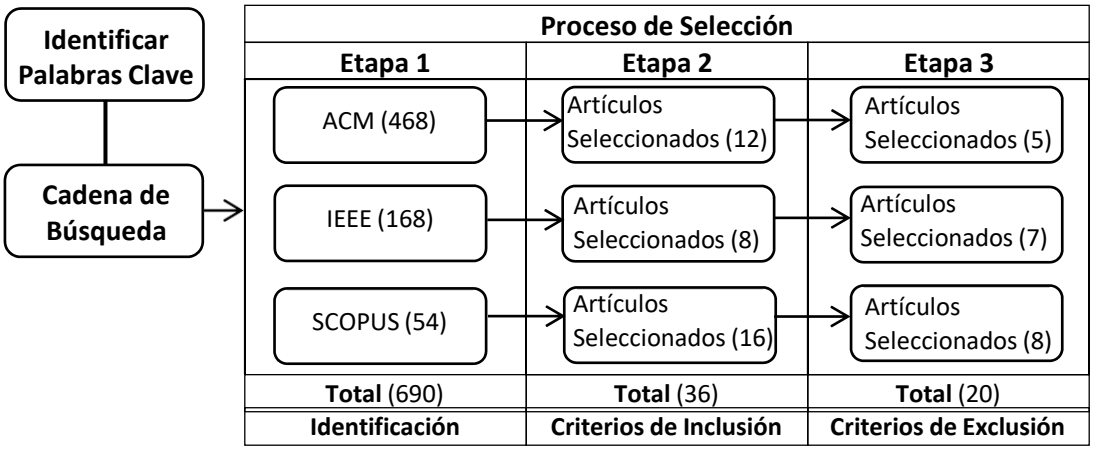


**Figura 1.** Proceso de selección de estudios primarios.

## 6. Resultados y discusiones

Los estudios primarios seleccionados de las tres bases de datos estuvieron integrados de la siguiente manera: cinco estudios fueron obtenidos de ACM Digital Library, siete de IEEE Xplore y ocho restantes de SCOPUS. En esta sección se presentan los resultados del análisis a los veinte estudios primarios seleccionados, con base en las preguntas de investigación. La Tabla 1 muestra los 20 estudios seleccionados junto al identificador usado en esta investigación.

**Tabla 1.** Estudios Seleccionados

| ID | Referencia | Título | Base de datos |
|---|---|---|---|
| E01 | (Robles-Gómez et al., 2019) | Analyzing the Students' Learning within a Container-based Virtual Laboratory for Cybersecurity | ACM Digital Library |
| E02 | (Čeleda et al., 2020) | KYPO4INDUSTRY: A Testbed for Teaching Cybersecurity of Industrial Control Systems | ACM Digital Library |
| E03 | (Oh et al., 2020) | Teaching Web-Attacks on a Raspberry Pi Cyber Range | ACM Digital Library |
| E04 | (Sianipar et al., 2017) | Team placement in crowd-Resourcing Virtual Laboratory for IT Security e-Learning | ACM Digital Library |
| E05 | (Kalyanam & Yang, 2017) | Try-CybSI: An Extensible Cybersecurity Learning and Demonstration Platform | ACM Digital Library |
| E06 | (Wang et al., 2015) | Benefit of construct information security environment based on lightweight virtualization technology | IEEE Xplore |
| E07 | (Shin & Seto, 2020) | Development of IoT Security Exercise Contents for Cyber Security Exercise System | IEEE Xplore |
| E08 | (Shin et al., 2019) | Development of Training System and Practice Contents for Cybersecurity Education | IEEE Xplore |
| E09 | (Perrone & Romano, 2017) | The Docker Security Playground: A hands-on approach to the study of network security | IEEE Xplore |
| E10 | (Liu et al., 2018) | A Web-Based Lightweight Testbed for Supporting Network Security Hands-on Labs | IEEE Xplore |
| E11 | (Kalyanam et al., 2020) | CHEESE: Cyber Human Ecosystem of Engaged Security Education | IEEE Xplore |
| E12 | (Caturano et al., 2020) | Capturing flags in a dynamically deployed microservices-based heterogeneous environment | IEEE Xplore |
| E13 | (Maki et al., 2020) | An effective cybersecurity exercises platform CyExec and its training contents | SCOPUS |
| E14 | (Tobarra et al., 2020) | Students' acceptance and tracking of a new container-based virtual laboratory | SCOPUS |
| E15 | (Caliskan & Vaarandi, 2020) | Career development in cyber security: Bootcamp training programs | SCOPUS |
| E16 | (Irvine et al., 2017) | Labtainers: A Docker-based framework for cybersecurity labs | SCOPUS |
| E17 | (AlSalamah et al., 2018) | Applying virtualization and containerization techniques in cybersecurity education | SCOPUS |
| E18 | (Irvine et al., 2017) | Labtainers: A Docker-based framework for cybersecurity labs | SCOPUS |
| E19 | (Buttyán et al., 2016) | Mentoring talent in IT security – A case study | SCOPUS |
| E20 | (A. S. Raj et al., 2016) | Scalable and lightweight CTF infrastructures using application containers | SCOPUS |

*PI1. ¿Cuál es la evolución en número y tipo de publicaciones relacionadas con el uso de la tecnología de contenedores en el aprendizaje de ciberseguridad desde 2010 hasta 2020?*

Con los estudios primarios seleccionados, se pudo observar que en el período de 2010 a 2014 no se encontraron publicaciones, todas se encuentran en la segunda mitad de la década, lo cual nos indica que es un tema novedoso; así mismo, se puede identificar que el 85% de los estudios fueron publicados en conferencias y solo el 15% en revistas, lo cual también nos indica que el área de investigación es poco maduro aún, incluso en la tercera parte del proceso de planificación, uno de los estudios reportados en ACM tuvo que ser descartado por corresponder a un trabajo en la modalidad de póster.

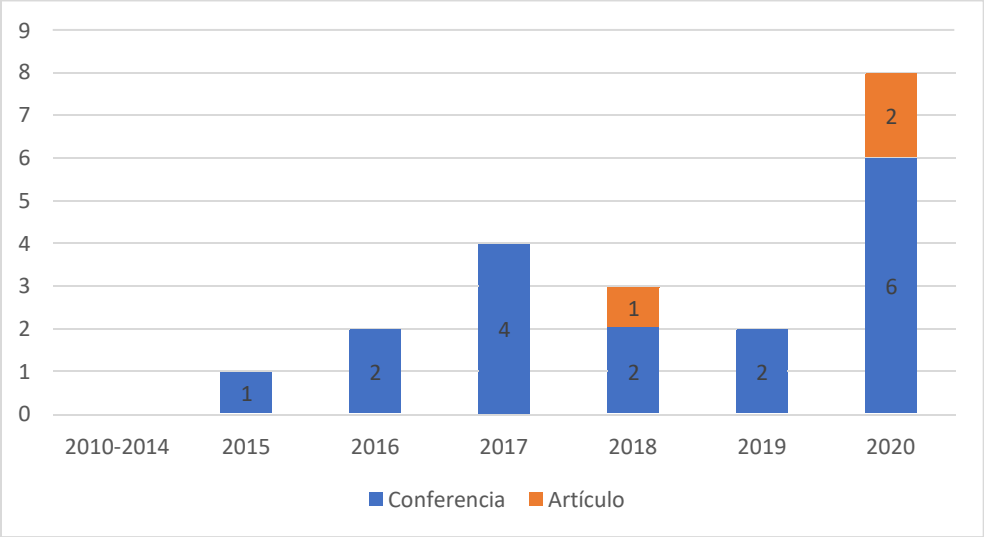


**Figura 1.** Estudios primarios en la última década.

*PI2. ¿Cuáles son los sistemas operativos predilectos para desarrollar contenedores aplicados en el aprendizaje de Ciberseguridad?*

Con base a los estudios primarios seleccionados, se pudo identificar que en el 15% de los mismos no se reporta el sistema operativo utilizado, mientras que en el 85% restante, el predilecto es el sistema operativo Linux.

*PI3. ¿Qué tipos de contenedores se han aplicado en el aprendizaje de Ciberseguridad?*

En relación con el tipo de contenedores utilizados para el aprendizaje de la Ciberseguridad, los estudios seleccionados reportan en un 90% el contenedor Docker, y el 5% el LXC; el 5% restante de los estudios no indica el tipo de contenedor utilizado.

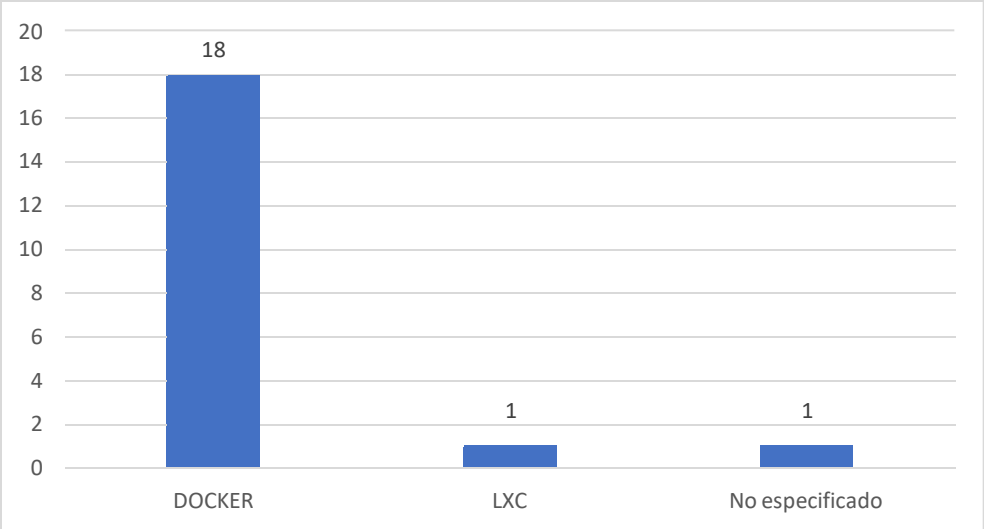


**Figura 2.** Tipos de contenedores utilizados en el aprendizaje de ciberseguridad.

*PI4. ¿Qué características tecnológicas son las más citadas en la tecnología de contenedores?*

De acuerdo con el análisis de los 20 estudios primarios seleccionados, resulta conveniente indicar que en todos se menciona al menos una característica tecnológica relacionada con la tecnología de contenedores, siendo la característica más citada, la optimización de recursos en un 65%, la Tabla 2 describe brevemente cada una de las características citadas en los estudios.

**Tabla 2.** Características de la tecnología de Contenedores

| Característica | Descripción | Estudio Primario |
|---|---|---|
| Optimización de Recursos | Al ser basados en virtualización a nivel de sistema operativo los contenedores permiten mejorar el rendimiento y obtener un beneficio máximo a través de una mejor utilización de recursos. | [E02], [E03], [E04], [E06], [E09], [E10], [E11], [E12], [E14], [E17], [E18], [E19], [E20] |
| Facilidad de Implementación | Debido a sus características el uso de contenedores logra el funcionamiento de manera sencilla de distintas tecnologías sin la necesidad de configuraciones complejas. | [E01], [E02], [E03], [E04], [E06], [E11], [E15]. [E16], [E17] |
| Escalabilidad | Los contenedores pueden expandirse al ritmo que requiera el usuario ya que la misma infraestructura puede admitir muchos contenedores. | [E05], [E06], [E08], [E11], [E12], [E13], [E14], [E17] |
| Flexibilidad | Los contenedores permiten instalar aplicaciones multiplataforma en diferentes infraestructuras sin la necesidad de adaptarlos a la configuración específica de los sistemas de hardware y software de cada sistema host. | [E05], [E07], [E09], [E11], [E12], [E17], [E18] |
| Aislamiento | Al ser componentes aislados, los procesos no pueden afectar a otros procesos de otros contenedores, tampoco influyen, ni afectan el funcionamiento del equipo o el sistema operativo sobre los que se despliegan. | [E03], [E05], [E06], [E14], [E17], [E19], [E20] |
| Portabilidad | Los contenedores proporcionan un formato estandarizado para empaquetar y mantener todos los componentes necesarios para ejecutar la aplicación deseada. | [E03], [E05], [E07], [E09], [E11], [E17] |
| Inicio rápido | La naturaleza ligera de los contenedores permite que puedan iniciarse y detenerse rápidamente. | [E05], [E06], [E17], [E19], [E20] |

*PI5. ¿Cuáles han sido los beneficios reportados en el uso de contenedores para el aprendizaje de la ciberseguridad?*

Con la RSL se pudo encontrar que son diversos los beneficios reportados con el uso de contenedores para el aprendizaje de la Ciberseguridad; en la Tabla 3 se presenta una descripción de cada uno de los beneficios identificados en los estudios primarios analizados.

**Tabla 3.** Beneficios con el uso de Contenedores

| Beneficio | Descripción | Estudio Primario |
|---|---|---|
| Desarrollo de habilidades prácticas | El aprendizaje de ciberseguridad requiere de la práctica de los conceptos que se estudian de manera teórica y esto se logra a través de la simulación de distintos escenarios. | [E01], [E02], [E03], [E04], [E05], [E07], [E08], [E09], [E10], [E11], [E12], [E13], [E14], [E15], [E16], [E17], [E19] |
| Variedad de laboratorios | La ciberseguridad abarca distintas áreas como redes, web, Internet de las cosas (del Inglés, Internet of Things – IoT) entre otras por lo que es necesario poder desplegar distintos tipos de laboratorios que son posibles gracias a la versatilidad de los contenedores. | [E03], [E05], [E06], [E07], [E08], [E09], [E11], [E13], [E15], [E16], [E17], [E18], [E19] |
| Simplificación del desarrollo de laboratorios | Muchos de los laboratorios que se requieren para el aprendizaje de ciberseguridad son complejos de simular, el uso de contenedores simplifica de manera considerable el tiempo de configuración. | [E02], [E05], [E06], [E08], [E09], [E11], [E14], [E16], [E17], [E18], [E19], [E20] |
| Fácil acceso a recursos de aprendizaje | La creación de imágenes de contenedores permite que esas sean compartidas en distintos repositorios ya sean públicos o privados. | [E03], [E05], [E07], [E10], [E11], [E14], [E16], [E17], [E19], [E20] |
| Desarrollo colaborativo | La estandarización en la creación de imágenes de contenedores permite la disponibilidad pública de la imagen y el desarrollo vía Internet. | [E03], [E05], [E07], [E08], [E09], [E11], [E12], [E13] |
| Laboratorios realistas | La mejor forma de adquirir habilidades en el área de ciberseguridad es a través de la practica en laboratorios que simulen un escenario real. | [E01], [E02], [E09], [E10], [E11], [E14], [E17], [E19] |
| Mejor planeación y diseño de los laboratorios | El uso de contendores reduce el tiempo de implementación de laboratorios lo que permite a los educadores tener más tiempo para su planeación y diseño. | [E01], [E06], [E11], [E12], [E14], [E18], [E19], [E20] |
| Facilidad de evaluación | Al ser imágenes independientes estas permiten al educador tener un mejor control de las actividades realizadas dentro del contenedor. | [E01], [E14], [E15], [E16], [E17], [E18], [E19] |
| Laboratorios de bajo costo | Al ser los contendores una tecnología de virtualización ligera se puede ejecutar en equipos con recursos limitados. | [E01], [E03], [E07], [E08], [E09], [E14], [E18] |

*PI6. ¿Cuáles han sido las dificultades tecnológicas reportadas en el uso de contenedores para el aprendizaje de la ciberseguridad?*

Del análisis de los estudios seleccionados, se pudo identificar que el 55% no reporta dificultad tecnológica alguna en cuanto al uso de contenedores para el proceso de aprendizaje de ciberseguridad, no obstante, el 45% restante de los estudios analizados, identifica un conjunto de aspectos que genera dificultades, según son descritas en la Tabla 4.

**Tabla 4.** Dificultades Tecnológicas en el uso de Contenedores

| Aspecto | Dificultad | Estudio Primario |
|---|---|---|
| Dependencia Jerárquica | Se puede traducir en preocupación por la seguridad del host al tener acceso directo al núcleo a través de los contenedores, esta compartición de núcleo a su vez evita que se puedan implementar ciertos tipos de laboratorios de ciberseguridad que requieran un núcleo o interfaces de red, esta dependencia hace que, si el equipo principal sufra un fallo afecte a todos los contenedores en este, además los logs también se comparten al host principal lo que dificulta la resolución de problemas. | [E05] [E06] [E11] [E12] [E17] [E18] |
| Incompatibilidad | Las imágenes de contenedores están principalmente diseñadas para arquitecturas basadas en x86 excluyendo la arquitectura ARM, así mismo, debido a la falta de madurez del tema de contenedores en el aprendizaje de ciberseguridad muchas de las herramientas tienen mejor soporte en distribuciones basadas en Linux dejando al margen otros sistemas operativos como Windows y macOS. | [E03] [E06] [E12] [E14] [E18] |
| Interfaz poco amigable | La falta de una interfaz amigable para el usuario requiere que la administración de contenedores sea realizada por líneas de comandos. | [E17] |
| Confiabilidad | Mantener repositorios públicos de imágenes de contenedores, especialmente en el caso de Docker, imposibilita el poder asegurar que la imagen se encuentre libre de virus o contenga alguna vulnerabilidad. | [E17] |
| Diversidad de servicios | Al momento de implementar más de un servicio asociado a la tecnología de contenedores, debido a que es un proceso muy técnico, se podría generar dificultades al momento de su implementación. | [E20] |

*PI7. ¿Cuáles son las estrategias educativas utilizadas para el aprendizaje de la Ciberseguridad?*

El análisis de los estudios primarios permitió identificar que las estrategias educativas reportadas se encuentran orientadas hacia la modalidad a distancia o en línea, es decir, actividades previamente diseñadas y centradas en el estudiante en las cuales el 40% hacen referencia el aprendizaje basado en la resolución de casos (situaciones particulares), 35% hacen referencia al uso de actividades de aprendizaje, pero sin especificar el tipo de actividad, 20% hacen referencia a dinámicas lúdicas (gamificación) y 20% hacen referencia a dinámicas basadas en la simulación (se incorporan roles), cabe resaltar que estos porcentajes se establecen sobre el 100% de estudios ya que muchas de estas estrategias se reportan en varios estudios como se observa en la Tabla 5.

**Tabla 5.** Estrategias educativas utilizadas para el aprendizaje de la Ciberseguridad

| Estrategia Educativa | Descripción | Estudio Primario |
|---|---|---|
| Resolución de casos | Escenarios específicos que representan situaciones particulares. | [E04], [E05], [E06], [E07], [E08], [E09], [E14], [E19] |
| Sin especificar | No se especifica ninguna estrategia educativa. | [E01], [E10], [E11], [E15], [E16], [E17], [E18] |
| Dinámicas lúdicas | Estrategias educativas como la gamificación. | [E02], [E12], [E19], [E20] |
| Simulación | Escenarios que simulan situaciones de la vida real. | [E03], [E08], [E09], [E13] |

*PI8. ¿Cuáles son las principales limitaciones pedagógicas vinculadas con el uso de contenedores en el aprendizaje de la Ciberseguridad?*

Aunado a que el 55% de los estudios no reporta dificultad tecnológica alguna en cuanto al uso de contenedores para el proceso del aprendizaje de la ciberseguridad, el 70% tampoco menciona limitaciones pedagógicas. Los únicos 6 estudios que mencionan algún problema en la implementación de la instrucción establecen situaciones vinculadas con las dificultades tecnológicas reportadas previamente en este estudio. La primera limitación analizada la reportan [E11], [E12] y es no poder desarrollar laboratorios no basados en el sistema operativo Linux, y en el caso de Linux, no poder desarrollar escenarios con vulnerabilidades asociadas al núcleo**.** Por otra parte [E03] menciona la falta de imágenes de contenedores Docker para la arquitectura ARM lo que conlleva la necesidad de que los instructores desarrollen sus propias imágenes para esta arquitectura. Por su parte [E17] reporta problemas de configuración de los laboratorios en los estudiantes con sistema operativo Windows debido al requerimiento extra de instalar "*Docker toolbox*", que se podrían explicar debido a lo novedoso de la tecnología de contenedores que en su estudio tuvo como reto explicar el funcionamiento de la contenerización y su interoperabilidad a los estudiantes. Por último, debido a la aplicación de esta tecnología en la estrategia de enseñanza con un enfoque práctico los estudios realizados por [E01] y [E19] resaltan que no es la forma más adecuada si se requiere comprender la seguridad física y electrónica, además de ciertos conocimientos teóricos.

*PI9. ¿Existe Software Educativo exprofeso para el aprendizaje de Ciberseguridad?*

En cuanto al uso de Software Educativo exprofeso para el aprendizaje de la Ciberseguridad, el análisis de los estudios primarios seleccionados permitió identificar el uso de WebGoat, mencionado por [E07], [E08] y [E13]. Un segundo sistema es mencionado DVWA (*Damn Vulnerable Web Application*), citado por [E03]. Metasploitable2 e IoTGoat también son mencionadas por [E07]. Finalmente, AppGoat es mencionado por [E08].

- WebGoat: Es una aplicación deliberadamente insegura que permite a los desarrolladores probar las vulnerabilidades que se encuentran comúnmente en aplicaciones basadas en Java que utilizan componentes comunes de código abierto y populares (*OWASP WebGoat - Learn the Hack - Stop the Attack*, 2020).
- Damn Vulnerable Web App (DVWA): Es una aplicación web PHP / MySQL que es muy vulnerable. Sus principales objetivos son ayudar a los profesionales de la seguridad a poner a prueba sus habilidades y herramientas en un entorno legal (*DVWA - Damn Vulnerable Web Application*, 2020).
- Metasploitable2: Es una máquina virtual Linux intencionalmente vulnerable. Esta máquina virtual se puede utilizar para realizar capacitación en seguridad, probar herramientas de seguridad y practicar técnicas de prueba de penetración comunes (*Metasploitable*, 2019).

- IoTGoat: Es un firmware deliberadamente inseguro basado en OpenWrt y mantenido por OWASP como una plataforma para educar a los desarrolladores de software y profesionales de la seguridad con las pruebas de vulnerabilidades comúnmente encontradas en dispositivos de IoT (*OWASP/IoTGoat*, 2020).
- AppGoat: Es una herramienta que permite aprender sistemáticamente conocimientos básicos sobre vulnerabilidades (*AppGoat*, 2020).

La poca existencia de software educativo exprofeso para el aprendizaje de la Ciberseguridad permite entender el que varios de los estudios reportados generan como resultado propuestas de plataformas educativas, laboratorios virtuales, cyber rangos y competiciones de captura la bandera.

En cuanto a las limitaciones, la presente RSL posee las limitaciones que se pueden presentar en este tipo de estudios secundarios. Por ejemplo, se incluye la posibilidad de sesgo de publicación la cual se intentó reducir realizando una búsqueda exhaustiva, escogiendo los estudios primarios que cumplieran con los criterios de inclusión y exclusión definidos en el protocolo. La búsqueda efectuada se hizo sobre las principales bases de datos que incorporan información sobre el tema de esta RSL. La selección de estudios primarios fue reproducible, así como la asignación de criterios de calidad metodológica. Otro factor de riesgo proviene del hecho de que sólo se examinaron documentos redactados en inglés y revisados por pares académicos por lo que se descartaron estudios publicados en otros idiomas.

## 7. Conclusiones

La Ciberseguridad es un área que ha cobrado especial importancia en la última década habiendo un gran déficit de profesionales especializados, ya que su estudio abarca diferentes áreas como redes, web, internet de las cosas, sistemas operativos e incluso factores sociales que necesitan de la simulación de diversos escenarios hiperrealistas que permitan desarrollar las habilidades necesarias, siendo estos laboratorios en muchas ocasiones complejos y costosos de desarrollar por lo que los interesados en aprender y enseñar ciberseguridad han recurrido a diferentes tecnologías para mejorar estos aspectos siendo una de estas la tecnología de contenedores.

El presente estudio tuvo como propósito, el caracterizar estudios primarios que han utilizado la tecnología de contenedores, con base en un conjunto de aspectos de interés para la educación de la Ciberseguridad. Del análisis de los estudios primarios seleccionados se puede concluir los siguiente:

- El uso de la tecnología de contenedores en el aprendizaje de ciberseguridad ha cobrado relevancia en los últimos cinco años.
- El sistema operativo predilecto para el desarrollo de contenedores en el aprendizaje de ciberseguridad es Linux.
- El tipo de contenedor más usado para el aprendizaje de Ciberseguridad resultó ser Docker.
- La característica tecnológica más recurrida en el uso de contenedores es la optimización de recursos.
- El principal beneficio del uso de contenedores en el aprendizaje de ciberseguridad es el desarrollo de habilidades prácticas.
- Muy pocos estudios reportan dificultades tecnológicas relacionadas al uso de contenedores en el aprendizaje de ciberseguridad siendo la más relevante la dependencia jerárquica.
- La principal estrategia educativa relacionada al uso de contenedores en el aprendizaje de ciberseguridad es el aprendizaje por resolución de casos.
- Muy pocos estudios presentan limitaciones pedagógicas vinculadas con el uso de contenedores en el aprendizaje de la ciberseguridad.
- Existe muy poco software educativo desarrollado específicamente para el aprendizaje de ciberseguridad.

Como se ha resaltado uno de los principales aspectos del aprendizaje en ciberseguridad es la parte práctica que requiere de escenarios especializados, los cuales dependiendo de su complejidad requieren de la utilización de numerosos recursos ya sean de hardware o software, los mismos que se han reducido gracias a las diversas tecnologías de virtualización, pero las mismas acarrean diferentes limitaciones como la complejidad de implementación, falta de portabilidad y un despliegue lento de software. Luego de analizar los diferentes estudios primarios se puede discernir las ventajas de la tecnología de contenedores para el aprendizaje de ciberseguridad sobre las demás tecnologías de virtualización como una mejor optimización de recursos, facilidad de implementación, portabilidad e inicio rápido; sin embargo, también se han encontrado ciertas limitaciones asociadas a la tecnología de contenedores, siendo las más relevantes la dependencia jerárquica que evitaría la implementación de ciertos escenarios que requieran de un núcleo o interfaces de red independientes, y la incompatibilidad con otras arquitecturas como ARM que requiere del desarrollo de sus propias imágenes de contenedores.

También se puede concluir, que debido a que la mayoría de los estudios primarios seleccionados proceden de conferencias especializadas, y no de artículos, demuestra lo reciente del uso de la tecnología de contenedores en el aprendizaje de ciberseguridad, además la gran mayoría de estudios son propuestas de plataformas, laboratorios virtuales, ciber-rangos y competiciones de captura la bandera por la falta de software especializado para esta área.

**Referencias**


Ageyev, D., Bondarenko, O., Radivilova, T., & Alfroukh, W. (2018). Classification of existing virtualization methods used in telecommunication networks. *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 83–86. https://doi.org/10.1109/DESSERT.2018.8409104

AlSalamah, A. K., Cámara, J. M. S., & Kelly, S. (2018). Applying virtualization and containerization techniques in cybersecurity education. *Proceedings of the 34th Information Systems Education Conference, ISECON 2018*, 1–14.

Anand, A., Chaudhary, A., & Arvindhan, M. (2021). The Need for Virtualization: When and Why Virtualization Took Over Physical Servers. *Advances in Communication and Computational Technology*, *668*, 1351–1359. https://doi.org/10.1007/978-981-15-5341-7_102

*AppGoat*. (2020). https://www.ipa.go.jp/security/vuln/appgoat/

Arcos, G., Aguirre, G. L., Hidalgo, B., Rosero, R. H., & Gómez, O. S. (2018). Current Trends of Teaching Computer Programming in Undergraduate CS Programs: A Survey from Ecuadorian Universities. *KnE Engineering*, *1*(2), 253. https://doi.org/10.18502/keg.v1i2.1499

Aroraa, G. (2017). *Building Microservices with .NET Core 2.0* (Second edi). Packt Publishing.

Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., Neugebauer, R., Pratt, I., & Warfield, A. (2003). Xen and the art of virtualization. *Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles (SOSP '03)*, *37*(5), 164–177. https://doi.org/10.1145/1165389.945462

Burley, D., Bishop, M., Kaza, S., Gibson, D. S., Hawthorne, E., & Buck, S. (2013). ACM Joint Task Force on Cybersecurity Education. In *Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science* (pp. 683–684). Association for Computing Machinery. https://doi.org/10.1145/12345.67890

Buttyán, L., Félegyházi, M., & Pék, G. (2016). Mentoring talent in IT security – A case study. *2016 USENIX Workshop on Advances in Security Education, ASE 2016, Co-Located with the 25th USENIX Security Symposium*, 1–8.

Caliskan, E., & Vaarandi, R. (2020). Career development in cyber security: Bootcamp training programs. *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020*, 503–511. https://doi.org/10.34190/ICCWS.20.080

Caturano, F., Perrone, G., & Romano, S. Pietro. (2020). Capturing flags in a dynamically deployed microservices-based heterogeneous environment. *2020 Principles, Systems and Applications of IP Telecommunications (IPTComm)*, 1–7. https://doi.org/10.1109/IPTComm50535.2020.9261519

Čeleda, P., Vykopal, J., Švábenský, V., & Slavíček, K. (2020). KYPO4INDUSTRY: A Testbed for Teaching Cybersecurity of Industrial Control Systems. *Proceedings of the 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20)*, 1026–1032. https://doi.org/10.1145/3328778.3366908

Crumpler, W., & Lewis, J. A. (2019). The Cybersecurity Workforce Gap. *Center for Strategic and International Studies (CSIS)*, *JANUARY*, 1–10.

*DVWA - Damn Vulnerable Web Application*. (2020). http://www.dvwa.co.uk/

Genero, M., Cruz-Lemus, J., & Piattini, M. (2014). *Métodos de investigación en ingeniería del software* (1st ed.). Ra-Ma.

Irvine, C. E., Michael, F., & Khosalim, J. (2017). Labtainers: A Docker-based framework for cybersecurity labs. *ASE 2017 - 2017 USENIX Workshop on Advances in Security*, 1–6.

Kalyanam, R., & Yang, B. (2017). Try-CybSI: An Extensible Cybersecurity Learning and Demonstration Platform. *Proceedings of the 18th Annual Conference on Information Technology Education (SIGITE '17)*, 41–46. https://doi.org/10.1145/3125659.3125683

Kalyanam, R., Yang, B., Willis, C., Lambert, M., & Kirkpatrick, C. (2020). CHEESE: Cyber Human Ecosystem of Engaged Security Education. *2020 IEEE Frontiers in Education Conference (FIE)*, 1–7. https://doi.org/10.1109/FIE44824.2020.9273931

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. *Keele University*, *33*, 1–16.

Liu, W., Niyaz, Q., Sun, W., & Javaid, A. Y. (2018). A Web-Based Lightweight Testbed for Supporting Network Security Hands-on Labs. *2018 IEEE International Conference on Electro/Information Technology (EIT)*, 0498–0503. https://doi.org/10.1109/EIT.2018.8500270

Maki, N., Nakata, R., Toyoda, S., Kasai, Y., Shin, S., & Seto, Y. (2020). An effective cybersecurity exercises platform CyExec and its training contents. *International Journal of Information and Education Technology*, *10*(3), 215–221. https://doi.org/10.18178/ijiet.2020.10.3.1366

*Metasploitable*. (2019). https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Morabito, R. (2017). Virtualization on internet of things edge devices with container technologies: A performance evaluation. *IEEE Access*, *5*, 8835–8850. https://doi.org/10.1109/ACCESS.2017.2704444

Mouat, A. (2016). Using Docker: Developing and Deploying Software with Containers. In B. Anderson (Ed.), *O'Reilly* (First Edit). O'Reilly Media.

Oh, S. K., Stickney, N., Hawthorne, D., & Matthews, S. J. (2020). Teaching Web-Attacks on a Raspberry Pi Cyber Range. *Proceedings of the 21st Annual Conference on Information Technology Education (SIGITE '20)*, 324–329. https://doi.org/10.1145/3368308.3415364

*OWASP/IoTGoat*. (2020). https://github.com/OWASP/IoTGoat

*OWASP WebGoat - Learn the hack - Stop the attack*. (2020). https://owasp.org/www-project-webgoat/

Perrone, G., & Romano, S. P. (2017). The Docker Security Playground: A hands-on approach to the study of network security. *2017 Principles, Systems and Applications of IP Telecommunications (IPTComm)*, 1–8. https://doi.org/10.1109/IPTCOMM.2017.8169747

Priyadarshini, I. (2018). FEATURES AND ARCHITECTURE OF THE MODERN CYBER RANGE: A QUALITATIVE ANALYSIS AND SURVEY [University of Delaware]. In *University of Delaware*. https://doi.org/1052564268

Raj, A. S., Alangot, B., Prabhu, S., & Achuthan, K. (2016). Scalable and lightweight CTF infrastructures using application containers. *2016 USENIX Workshop on Advances in Security Education, ASE 2016, Co-Located with the 25th USENIX Security Symposium*, 1–8.

Raj, R. K., Ekstrom, J. J., Impagliazzo, J., Lingafelt, S., Parrish, A., Reif, H., & Sobiesk, E. (2017). Perspectives on the future of cybersecurity education. *2017 IEEE Frontiers in Education Conference (FIE)*, 1–2. https://doi.org/10.1109/FIE.2017.8190498

Robles-Gómez, A., Tobarra, L., Pastor, R., Hernández, R., Duque, A., & Cano, J. (2019). Analyzing the Students' Learning within a Container-based Virtual Laboratory for Cybersecurity. *Proceedings of the Seventh International Conference on Technological Ecosystems for Enhancing Multiculturality*, 275–283. https://doi.org/10.1145/3362789.3362840

Shin, S., & Seto, Y. (2020). Development of IoT Security Exercise Contents for Cyber Security Exercise System. *2020 13th International Conference on Human System Interaction (HSI)*, 1–6. https://doi.org/10.1109/HSI49210.2020.9142678

Shin, S., Seto, Y., Kasai, Y., Ka, R., Kuroki, D., Toyoda, S., Hasegawa, K., & Midorikawa, K. (2019). Development of Training System and Practice Contents for Cybersecurity Education. *2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI)*, 172–177. https://doi.org/10.1109/IIAI-AAI.2019.00043

Shirinbab, S., Lundberg, L., & Casalicchio, E. (2017). Performance evaluation of container and virtual machine running cassandra workload. *2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech)*, 1–8. https://doi.org/10.1109/CloudTech.2017.8284700

Sianipar, J., Willems, C., & Meinel, C. (2017). Team placement in crowd-Resourcing Virtual Laboratory for IT Security e-Learning. *Proceedings of the 2017 International Conference on Cloud and Big Data Computing (ICCBDC 2017)*, 60–66. https://doi.org/10.1145/3141128.3141146

Singh, S., & Singh, N. (2016). Containers & Docker: Emerging roles & future of Cloud technology. *2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (ICATccT)*, 804–807. https://doi.org/10.1109/ICATCCT.2016.7912109

Tobarra, L., Robles-Gómez, A., Pastor, R., Hernández, R., Duque, A., & Cano, J. (2020). Students' acceptance and tracking of a new container-based virtual laboratory. *Applied Sciences (Switzerland)*, *10*(3). https://doi.org/10.3390/app10031091

Vykopal, J., Ošlejšek, R., Čeleda, P., Vizváry, M., & Tovarňák, D. (2017). KYPO cyber range:Design and use cases. *Proceedings of the 12th International Conference on Software Technologies*, *ICSOFT*, 310–321. https://doi.org/10.5220/0006428203100321

Wang, J.-C., Cheng, W.-F., Chen, H.-C., & Chien, H.-L. (2015). Benefit of construct information security environment based on lightweight virtualization technology. *2015 International Carnahan Conference on Security Technology (ICCST)*. https://doi.org/10.1109/CCST.2015.7389695

Yadav, A. K., Garg, M. L., & Ritika. (2019). Docker containers versus virtual machine-based virtualization. *Advances in Intelligent Systems and Computing*, *814*, 141–150. https://doi.org/10.1007/978-981-13-1501-5_12

Notas bibliografías de los Autores:

Nombre: Roger Andres Chingo Esquivel
Correo electrónico: roger.a.chingo.e@pucesa.edu.ec

"Ingeniero en Sistemas e Informática por la Universidad Regional Autónoma de los Andes de Ecuador. Estudiante de Posgrado de Maestría en Ciberseguridad por parte de la Pontificia Universidad Católica del Ecuador sede Ambato."

Nombre: Omar Salvador Gómez Gómez
Correo electrónico: ogomez@espoch.edu.ec

"Ingeniero en Computación por la Universidad de Guadalajara (México), Maestro en Ingeniería de Software por el Centro de Investigación en Matemáticas (México), y Doctor en Software y Sistemas por la Universidad Politécnica de Madrid (España). Cuenta con estudios de Post-Doctorado en la Universidad de Oulu (Finlandia). Se desempeñó como investigador Prometeo-Senescyt, proyecto del gobierno del Ecuador para fortalecer las capacidades de investigación científica en instituciones de educación superior. Actualmente se encuentra adscrito como docente en la Facultad de Informática y Electrónica de la Escuela Superior Politécnica de Chimborazo. Cuenta con diversas publicaciones técnicas en el ámbito de la informática. Sus áreas de investigación se centran en la ingeniería de software."

Esta obra está bajo una licencia de Creative Commons
Atribución-NoComercial-Compartirlgual 4.0 Internacional.