DOI: http://dx.doi.org/10.23857/dc.v8i3

Ciencias Económicas y Empresariales
Artículo de Investigación

Procesos de protección en entornos de ejecución de contenedores Kubernetes para una entidad financiera: una revisión sistemática

Protection processes in Kubernetes container execution environments for a financial institution: a systematic review

Processos de proteção em ambientes de execução de containers Kubernetes para uma instituição financeira: uma revisão sistemática

Cristian Segundo Tello-Valladares [I]
cristian.tello.25@est.ucacue.edu.ec
https://orcid.org/0000-0002-4364-643X

Andrés Sebastián Quevedo-Sacoto [II]
asquevedos@ucacue.edu.ec
https://orcid.org/0000-0001-5585-0270

Correspondencia: cristian.tello.25@est.ucacue.edu.ec

*__Recibido:__ 29 de septiembre del 2022 *__Aceptado:__ 28 de octubre del 2022 __* Publicado:__ 28 de noviembre del 2022

I. Estudiante de Posgrado, Universidad Católica de Cuenca, Cuenca, Ecuador.
II. Docente de Posgrado, Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

Actualmente, la manera más eficiente para el desarrollo y puesta en producción de aplicaciones es la implementación de microservicios contenerizados, orquestados en Kubernetes, y ya no los procesos tradicionales a través de monolitos.

Kubernetes permite el desarrollo y puesta en producción de aplicaciones de manera más rápida y con propiedades de escalamientos y alta disponibilidad. Si bien, cada vez más son las empresas que implementan contenedores y kubernetes, sin embargo, su seguridad sigue siendo la mayor preocupación. En este estudio se busca identificar buenas prácticas de seguridad que garanticen la seguridad de estos ambientes contenerizados.

En primer lugar, se lleva a cabo una investigación realizando una revisión sistemática de la ciberseguridad en contenedores y kubernetes, que brinde soluciones tentativas oportunas ante la implementación de las Tecnologías de la Información (TI), para poder emitir procesos de protección para la ciberseguridad, que permita mitigar ciberdelitos y protegerse adecuadamente ante las diferentes amenazas.

Los resultados de la revisión ofrecen el estado actual de la ciberseguridad en contenedores y kubernetes que puede ser útil para la compresión de su concepto. Además, se destaca que la educación y la capacitación son las necesidades más pertinentes para este sector de la seguridad en de microservicios.

Palabras clave: Ciberseguridad; kubernetes; Contenedores; Microservicios; Aplicaciones.

Abstract

Currently, the most efficient way to develop and put into production applications is the implementation of containerized microservices, orchestrated in Kubernetes, and no longer the traditional processes through monoliths. Kubernetes allows the development and production of applications faster and with scaling and high availability properties. While more and more companies are implementing containers and kubernetes, however, their security remains the biggest concern. This study seeks to identify good security practices that guarantee the security of these containerized environments. In the first place, an investigation is carried out carrying out a systematic review of cybersecurity in containers and kubernetes, which provides timely tentative

solutions before the implementation of Information Technology (IT), in order to issue protection processes for cybersecurity, that allows mitigating cybercrimes and adequately protecting against different threats. The results of the review offer the current state of cybersecurity in containers and kubernetes that can be useful for understanding your concept. In addition, it is highlighted that education and training are the most relevant needs for this sector of security in microservices.
Keywords: Cybersecurity; kubernetes; containers; microservices; Applications.

Resumo

Atualmente, a forma mais eficiente de desenvolver e colocar aplicações em produção é a implementação de microsserviços conteinerizados, orquestrados em Kubernetes, e não mais os processos tradicionais através de monólitos. O Kubernetes permite o desenvolvimento e a produção de aplicações de forma mais rápida e com propriedades de escalabilidade e alta disponibilidade. Embora cada vez mais empresas estejam implementando contêineres e kubernetes, sua segurança continua sendo a maior preocupação. Este estudo busca identificar boas práticas de segurança que garantam a segurança desses ambientes conteinerizados. Em primeiro lugar, é realizada uma investigação realizando uma revisão sistemática da segurança cibernética em contêineres e kubernetes, que fornece soluções experimentais oportunas antes da implementação da Tecnologia da Informação (TI), a fim de emitir processos de proteção para a segurança cibernética, que permitem mitigar os crimes cibernéticos e protegendo adequadamente contra diferentes ameaças. Os resultados da revisão oferecem o estado atual da segurança cibernética em contêineres e kubernetes que podem ser úteis para entender seu conceito. Além disso, destaca-se que educação e treinamento são as necessidades mais relevantes para este setor de segurança em microsserviços.
Palavras-chave: Cibersegurança; kubernetes; recipientes; microsserviços; Formulários.

Introducción

Ciberseguridad, Ciberespacio y Ciberdelincuencia

“Entendemos la ciberseguridad como la protección de activos de información, mediante el tratamiento de las amenazas. Con el uso de las Tecnologías de la Información y la Comunicación, se facilita un desarrollo sin precedentes en el intercambio de información y comunicaciones, que

conlleva serios riesgos y amenazas en un mundo globalizado; y las amenazas en el espacio digital adquieren una dimensión global que va más allá de la tecnología. La sociedad de la información, la ausencia de fronteras y la inmaterialidad de la comunicación a través de las Tecnologías de la Comunicación y la Información, conducen en el ámbito del Derecho Penal, a la escasa relevancia de los límites temporales y espaciales que han constituido, tradicionalmente, su límite. La delincuencia informática y los delitos relacionados con ella, suponen un tipo de criminalidad característica y especial; y con la expresión delito informático, cibercrimen o ciberdelito se define a todo ilícito penal llevado a cabo a través de medios informáticos, incluido el blanqueo de capitales" (Fernández Bermejo, Daniel; Martínez Atienza, Gorgonio, 2016-06).

Contenedores

Los contenedores son un paquete de elementos que le permiten crear un entorno en el que las aplicaciones se ejecutan independientemente del sistema operativo. (Ponsico Martin, 2017)

La Contenerizacion, también conocida como virtualización basada en contenedores, es una modalidad de virtualización a nivel de Sistema Operativo, que nos permite desplegar y ejecutar aplicaciones sin necesidad de contar con una máquina virtual completa, con su S.O y asignación de recursos. En su lugar, se puede montar uno o varios sistemas aislados denominados contenedores. Estos sistemas pueden ser ejecutados sobre un único servidor huésped host y acceden al mismo núcleo (kernel), que el de su servidor alojador, por lo cual comparten el mismo S.O sin necesidad de montar uno para cada contenedor, a diferencia de las máquinas virtuales, que además requieren de un hipervisor para la gestión de los recursos del host, que

consume recursos del mismo y conforman una infraestructura más pesada que la de contenedores. (Alonso Batuecas Francisco, 2021)

Kubernetes

Con los contenedores tenemos resuelto el soporte de las aplicaciones, y ahora nos enfrentamos a otro problema, que es conseguir que nuestra aplicación esté disponible siempre, comprobar el estado de cada contenedor y administrarlos para que se vayan arrancando (rollout) o parando (rollback) según la demanda. Esas capacidades son las que ofrece Kubernetes, un framework para correr sistemas distribuidos de manera resiliente. Sus prestaciones principales son: Descubrimiento de servicios y balanceo de carga Cuando tienes varios contenedores en funcionamiento tienes que

asignarles una dirección IP y repartir la carga entre todos ellos. Kubernetes se encarga de esta labor, además no necesitas saber la IP ya que puedes asignarle un nombre a cada servicio y será resuelto internamente. Orquestación de almacenamiento Con Kubernetes puedes tener varios sistemas de almacenamiento tanto local como por red y compartirlo entre distintos servicios. Bin Packing automático El problema de Bin Packing consiste en optimizar el número de máquinas físicas (nodos) necesarias para albergar los contenedores con los recursos necesarios, sin dejar recursos libres sin poder ser utilizados de manera eficiente. Kubernetes se encarga de esto. Automatización de rollouts y rollbacks Cuando quieres aplicar cambios a los contenedores, por ejemplo, para hacer el despliegue de una nueva versión, Kubernetes se encarga de retirar los contenedores antiguos mientras despliega los nuevos de manera progresiva, y si falla algo, deshará los cambios, lo cual es bastante cómodo. Recuperación automática Kubernetes se encarga de restaurar o reemplazar los contenedores que están fallando o no responden comprobando periódicamente los health check definidos por el usuario. Gestión de secretos Una buena práctica a la hora de crear contenedores es hacer uso de variables de entorno y que la imagen no almacene esta información por razones de seguridad. Además, esto permite que podamos crear un contenedor con la misma imagen para distintos entornos. La gestión de estas variables de entorno puede hacerse desde Kubernetes, y cuando arranque los contenedores se encargará de asignar las variables de entorno. (López Rico, 2022)

Microservicios

Es un enfoque para el desarrollo de una aplicación única como un conjunto de pequeños servicios, cada uno ejecutándose en su propio proceso y mecanismos ligeros de comunicación, a menudo un recurso de una interfaz de programación de aplicaciones (API) sobre protocolo de transferencia de hipertexto (HTTP). Estos servicios están construidos alrededor de las capacidades del negocio y con independencia de despliegue e implementación totalmente automatizada. Existe un mínimo de gestión centralizada de estos servicios, los que pueden estar escritos en lenguajes de programación diferentes y utilizar diferentes tecnologías de almacenamiento de datos.

El término microservicios no es relativamente nuevo, este estilo arquitectura fue acuñado por Martin Fowler en un taller de arquitectos de software como una descripción del nuevo campo que los participantes estaban explorando. No existe una definición en concreto para microservicio, sin

embargo, una aproximación que la realiza lo define como: "Pequeños servicios autónomos que trabajan juntos. (López, 2017)

Bibliotecas digitales

Están diseñadas para admitir distintos tipos de búsquedas, dependiendo de las necesidades específicas del usuario, estás varían una de otra, de acuerdo con el alcance geográfico e histórico, y por el tipo de contenido que estas disponen como son: revistas, libros, actas de conferencia, entre otros. También las búsquedas pueden ser limitadas en base a los campos accesibles de los documentos; además las bibliotecas digitales, cuentan con varias herramientas para recuperar resultados de investigaciones relevantes, visualizar y analizar los resultados obtenidos (WIPO, 2012)

En la Tabla 1 se detallan los operadores que se usan en las cadenas de búsquedas de las bibliotecas digitales.

Figura 1: Operadores utilizados en consulta (WIPO, 2008).

Operador	Descripción	Tipo
AND	Los términos detallados han de ser incluidos.	Booleanos
OR	Alguno de los términos definidos, tienen que ser incluidos	Booleanos
NOT	La variable especificada debe ser excluido.	Booleanos
XOR	La búsqueda debe contener algún término especificado; pero no los dos a la vez.	Booleanos
+	La variable a continuación debe incluirse	Booleanos
-	El término siguiente debe excluirse	Booleanos

NEAR	Los términos introducidos deben estar cerca, sin importar su orden.	Proximidad
ADJ	Los términos introducidos deben estar juntos y en el orden definido.	Proximidad

En la revisión sistemática se ha determinado realizar la selección de estudios en dos bases de datos científicas presentadas a continuación:

Web of Science: "propiedad de la empresa Clarivate Analytics, es la colección de bases de datos de referencias bibliográficas y citas de publicaciones periódicas que recogen información desde 1900 a la actualidad. La WOS está compuesta por la colección básica Core Collection que abarca los índices de Ciencias, Ciencias Sociales y Artes y Humanidades, además de los Proceedings tanto de Ciencias como de Ciencias Sociales y Humanidades junto con las herramientas para análisis y evaluación, como son el Journal Citation Report y Essential Science Indicators. Adicionalmente, cuenta con las bases de datos que la complementan incluidas en la licencia para España: Medline, Scielo y Korean Citation Index". (Mangan, 2020)

Scopus: "es la base de datos más amplia de resúmenes y citas sobre literatura revisada por pares, cuenta con herramientas bibliométricas para rastrear, analizar y visualizar investigaciones. Contiene más de 21,900 títulos de más de 5,000 editoriales de todo el mundo, en el campo de la ciencia, tecnología, medicina, ciencias sociales y artes y humanidades. Scopus cuenta con 54 millones de registros que datan de 1823, 84% de estos hacen referencias desde 1996" (Codina, 2005).

Metodología

Esta revisión sistemática utilizó la metodología de Kitchenham, con las siguientes etapas: "planificación de la revisión, realización de la revisión y elaboración del informe de la revisión (Kitchenham, 2004). La figura 1 muestra el diagrama de flujo de las etapas de la metodología Revisión Sistemática.

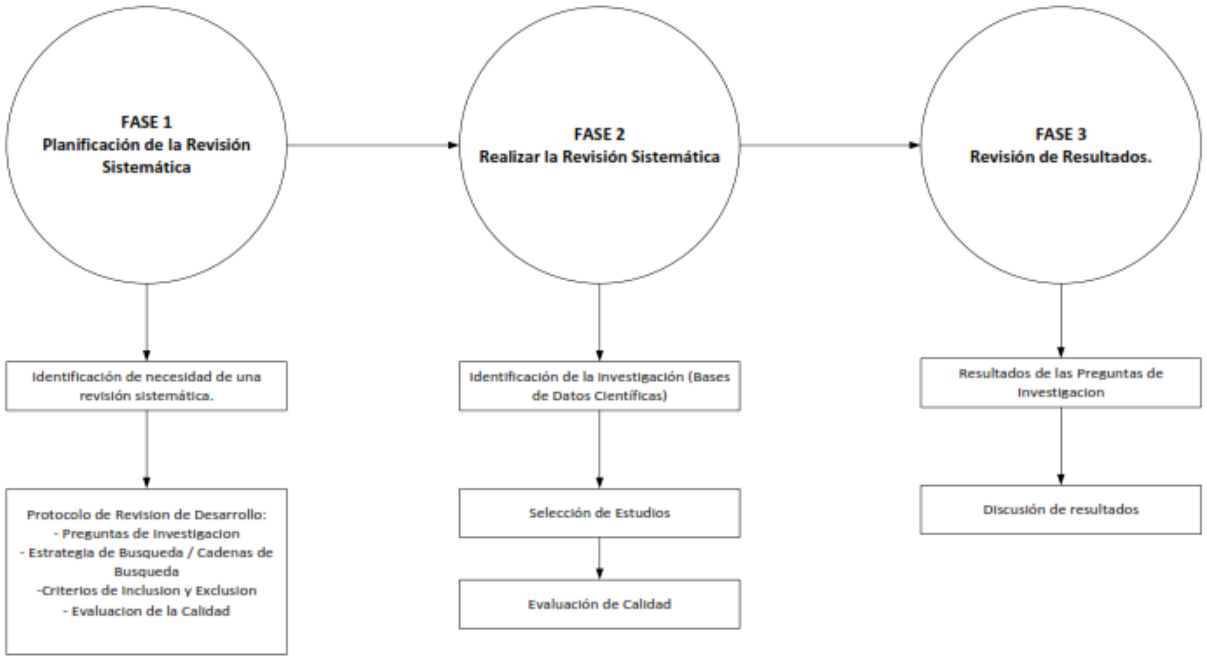

Figura 1: Diagrama de flujo de las etapas de la metodología Revisión Sistemática.

Planificación de la revisión sistemática de la literatura

En la planificación, en primer lugar, se identifica la necesidad de realizar una revisión sistemática, para lo cual se buscan Revisión Sistemática similares en bases de datos científicas bases de datos científicas. En segundo lugar, se elabora el protocolo de revisión.

Identificación de la necesidad de una revisión sistemática

La necesidad de una revisión sistemática se determinó buscando Revisiones Sistemáticas similares en las bases de datos científicas Scopus y Web of Science. Se crearon cadenas de búsqueda personalizadas para la consulta utilizando las palabras clave ciberseguridad, kubernetes y contenedores y Revisión Sistemática con algunos de sus sinónimos. Las cadenas de búsqueda utilizadas pueden verse a continuación:

Scopus: TITLE-ABS-KEY ("kubernetes*" AND "containers*" AND "security*") AND (“systematic literature review” OR “literature review” OR “systematic review”))

Web of Science: TOPIC = ("kubernetes*" or "containers*" AND "security*") AND (“systematic literature review” OR “literature review” OR “systematic review”))

La búsqueda en las bases de datos científicas Scopus y Web of Science no entrego ningún resultado. Por lo tanto, es necesario de una revisión sistemática sobre ciberseguridad en kubernetes y contenedores.

Elaboración de un protocolo de revisión

Esta investigación contempla los artículos publicados en las bases de datos científicas Scopus y Web of Science hasta agosto de 2022 sobre ciberseguridad o seguridad en kubernetes y contenedores. El protocolo de revisión determina las preguntas de investigación, las estrategias de búsqueda para la extracción de publicaciones, los criterios de inclusión y exclusión, y la evaluación de la calidad de los artículos seleccionados.

a) Preguntas de investigación

En esta revisión sistemática se definieron nueve preguntas de investigación. Las preguntas de investigación están relacionadas con la ciberseguridad en los sistemas y recursos tecnológicos agrícolas.

RQ1. ¿Cuántos estudios se han publicado a lo largo de los años sobre la seguridad en kubernetes y contenedores?

RQ2. ¿Qué países aportan más artículos sobre ciberseguridad en contenedores y kubernetes?

RQ3. ¿Qué prácticas sobre ciberseguridad en kubernetes informan los estudios?

RQ4. ¿Cuáles son las principales limitaciones de la ciberseguridad en contenedores y kubernetes?

RQ5. ¿Cuáles son los principales ciberataques en Kubernetes, contenedores y su impacto?

b) Estrategia de búsqueda

Aquí definimos las palabras clave y términos de sustitución en las cadenas de búsqueda de acuerdo con las preguntas de la investigación. Las palabras clave y sus sinónimos utilizados se presentan a continuación:

Kubernetes, containers Cybersecurity: ("kubernetes*" AND "containers*" AND "security*")

Las cadenas de búsqueda se personalizaron utilizando palabras clave, sinónimos, operadores booleanos (AND), comillas dobles ("") y el asterisco (*). Los operadores booleanos permiten unir y combinar palabras clave y sinónimos. Las comillas dobles permiten buscar frases específicas. El asterisco permite buscar el singular y el plural de las palabras clave o los sinónimos.

Las publicaciones se extrajeron de las bases de datos científicas Scopus y Web of Science. Para ello, se creó una cadena de búsqueda para cada base de datos científica. Las cadenas de búsqueda utilizadas se presentan a continuación:

Scopus: TITLE-ABS-KEY

Web of Science: TOPIC = ("kubernetes*" or "containers*" AND "security*")

c) Criterios de inclusión y exclusión

Los criterios de inclusión y exclusión tienen por objeto ayudar a seleccionar los artículos analizados en un RSL. Para ello, los artículos que no cumplen todos los criterios de inclusión se excluyen del RSL. Del mismo modo, los artículos que cumplen al menos un criterio de exclusión se excluyen del RSL. Los criterios de inclusión definidos para la selección de artículos en este RSL son los siguientes:

I1. Artículos publicados en una revista Y,

I2. Artículos en inglés Y,

I3. Artículos que contengan las palabras clave cibersecurity kubernetes o security containers en su título, resumen o palabras clave.

Los criterios de exclusión definidos en este RSL son los siguientes:

E1. Artículos que sean de investigación secundaria (por ejemplo, un RSL) O,

E2. Artículos duplicados O,

E3. Artículos que no tienen como objeto de estudio la ciberseguridad en contenedores o kubernetes

d) Evaluación de la calidad

La evaluación de la calidad (QA) permite la inclusión o exclusión de artículos mediante un conjunto de preguntas. Se han definido cuatro preguntas de evaluación para medir la calidad de cada artículo. Cada pregunta tiene un valor Cada pregunta tiene un valor de 1, lo que da un total de 4. La puntuación mínima que deben alcanzar los artículos es de 3. cumplir es de 3. Las preguntas de evaluación se presentan en la Tabla 2.

Figura 2: Lista de verificación de la evaluación de la calidad.

No.	Pregunta de evaluación de la calidad	Respuesta
1	¿Se especifican claramente los objetivos de la investigación en el artículo?	Sí->1 / No->0
2	¿Los resultados sobre la ciberseguridad en kubernetes y	Sí->1 / No->0

	contenedores están especificados en el artículo?	
3	¿Existe una relación entre los datos, la interpretación y las conclusiones del artículo?	Sí->1 / No->0
4	¿La revista en la que se publicó el artículo está indexada en el JCR o en el SJR?	Sí->1 / No->0

Etapa 2. Desarrollo de la revisión sistemática

Identificación de la investigación

Las bases de datos científicas utilizadas para seleccionar los artículos son Scopus y Web of Science. Debido a que estas bases de datos almacenan artículos de diferentes revistas indexadas de alto impacto revistas de alto impacto. Además, cumplen los siguientes requisitos:

Los revisores evalúan los artículos.

Las revistas están indexadas en SJR o JCR.

Permiten el uso de cadenas de búsqueda personalizadas.

Selección de estudios

Tras aplicar cadenas de búsqueda en las bases de datos científicas Scopus y Web of Science, se encontraron 29 artículos. A continuación, aplicando los criterios de inclusión y exclusión se seleccionaron 25 artículos para su análisis en este RSL. El proceso de selección de artículos se presenta en la Figura 2.

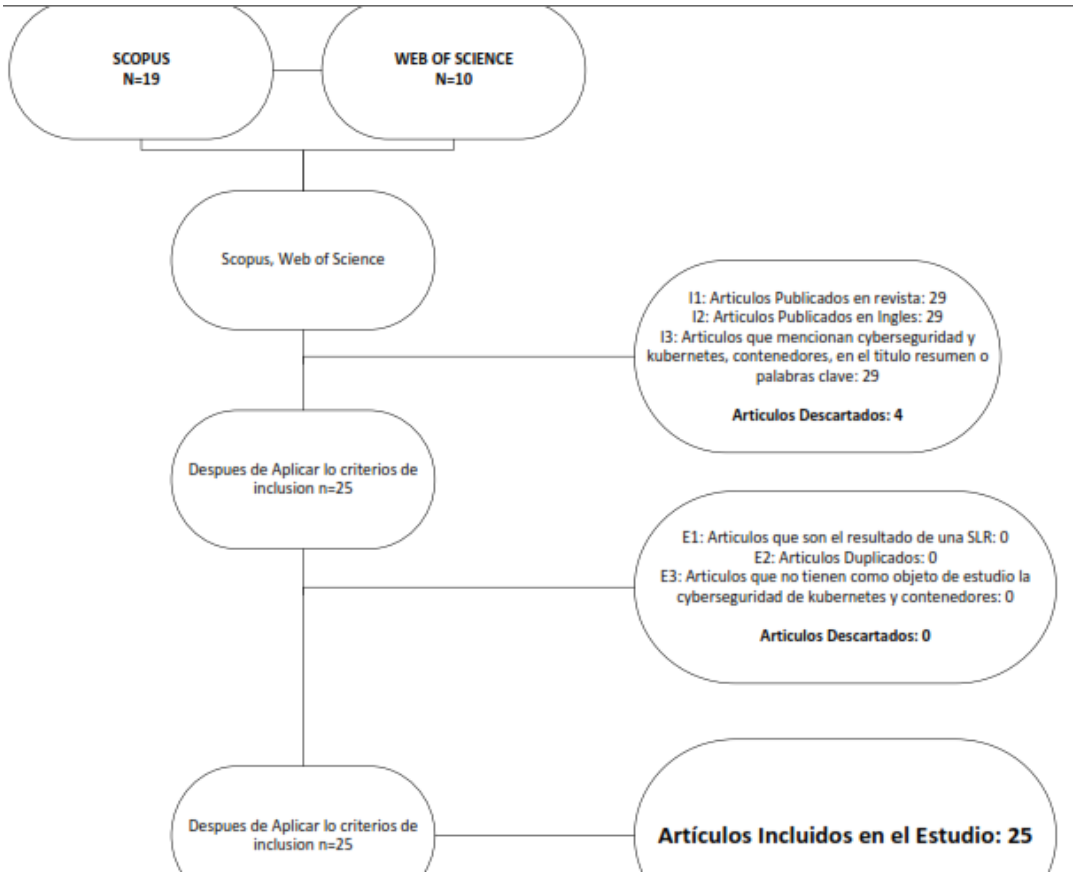

Figura 3: Diagrama de flujo del proceso de selección Revisión Sistemática.

Evaluación de la calidad del estudio

Los artículos extraídos teniendo en cuenta los criterios de inclusión y exclusión también se evaluaron con las preguntas de calidad. La Tabla 3 presenta los resultados de la evaluación de la calidad de los artículos seleccionados.

Figura 4: Datos extraídos para RQ3, RQ4, RQ5.

Artículo	**RQ3**	**RQ4**	**RQ5**	
	Practicas de seguridad	**Limitaciones**	Ataques cibernéticos	Impacto

(Bambhore Tukaram, Towards a Security Benchmark for the Architectural Design of Microservice Applications., 2022)	Configuracion de RBAC	Experiencia	Escalamiento de Privilegios	Secuestro de Recursos
(Md. Shazibul Islam Shamim, 2020)	Segmantacion de redes	Experiencia	Malware	Secuestro de Recursos
(Chen, 2022)	Gestion de la Configuracion	Experiencia	Malware	Pérdidas financieras
(Pecka, 2022)	Configuracion de RBAC	Conocimiento	Escalamiento de Privilegios	Indisponibilidad de Servicio
(Kermabon-Bobinnec, 2022)	Gestion del tiempo de Ejecucion del Contenedor	Conocimiento	Ransomwere	Pérdidas financieras
(Haque, 2022)	Proteccion del Kublet	Conocimiento	Denegación de servicio (DoS)	Indisponibilidad de Servicio

(Shamim S. I., 2021)	Proteccion del Servidor de la API	Conocimiento	Malware	Indisponibilidad del Servicio
(Cavalcanti, 2021)	Gestion del tiempo de Ejecucion del Contenedor	Conocimiento	Ransomwere	Pérdidas financieras
(Lambert, 2021)	Proteccion de la Infraestructura	Recursos (dinero, tiempo)	Malware	Pérdidas financieras
(Budigiri, 2021)	Proteccion de la Infraestructura	Soporte externo experto	Malware	Pérdidas financieras
(Bose, 2021)	Diseñó de Imágenes Seguras	Conocimiento	Malware	Pérdidas financieras
(Karn, 2020)	Segmentacion de redes	Experiencia	Malware	Desventaja comercial
(Viktorsson, 2020)	Diseno de Imágenes Seguras	Falta de Practicas de Diseno	Escalamiento de Privilegios	Indisponibilidad del Servicio

(Shringarputale, 2020)	Gestion del tiempo de Ejecucion del Contenedor	Conocimiento	Ransomwere	Pérdidas financieras
(Sun, 2020)	Diseno de Imágenes Seguras	Falta de Practicas de Diseno	Escalamiento de Privilegios	Indisponibilidad del Servicio
(Shamim M. S., 2020)	Gestion de la Configuracion	Conocimiento	malware	Pérdidas financieras
(Surantha, 2016)	Segmentacion de redes	Recursos (dinero, tiempo)	Escalamiento de privilegios	Pérdidas financieras
(Bila, 2017)	Análisis de las Imágenes a Instalar.	Conocimiento	Malware	Indisponibilidad de equipos
(Ying, 2022)	Gestion de Puntos Vulnerables	Recursos (dinero, tiempo)	Malware	Red inaccesible
(Tien, 2019)	Análisis de las Imágenes a Instalar.	Conocimiento	Malware	Indisponibilidad de equipos

(Alyas, 2022)	Diseno de Imágenes Seguras	Conocimiento	Malware	Pérdidas financieras
(Ju, 2022)	Uso de configuraciones predeterminadas	Falta de Conocimiento	Malware	Indisponibilidad del Servicio
(Doan, 2022)	Diseno de Imágenes Seguras	Falta de Practicas de Diseno	Escalamiento de Privilegios	Indisponibilidad del Servicio
(Kaur, 2021)	Diseno de Imágenes Seguras	Falta de Practicas de Diseno	Malware	Indisponibilidad del Servicio
(Kwon, 2020)	Configuracion de RBAC	Falta de Practicas de Diseno	Escalamiento de Privilegios	Acceso no autorizado

Resultados y discusión

Los resultados responden a las preguntas de la investigación mediante el análisis y la interpretación de los artículos seleccionados. Los resultados destacan los aspectos más importantes encontrados en los artículos.

RQ1. ¿Cuántos estudios se han publicado a lo largo de los años sobre la ciberseguridad en kubernetes y contenedores?

De los 25 artículos seleccionados, un artículo (Surantha, 2016)se publicó antes de 2017, lo que corresponde al 4 % del total, y los 24 artículos restantes se publicaron a partir de 2017, que es cuando comienza se populariza el uso de contenedores y kuberenetes y que corresponde al 96 %. La Figura 3 muestra el número de publicaciones por año.

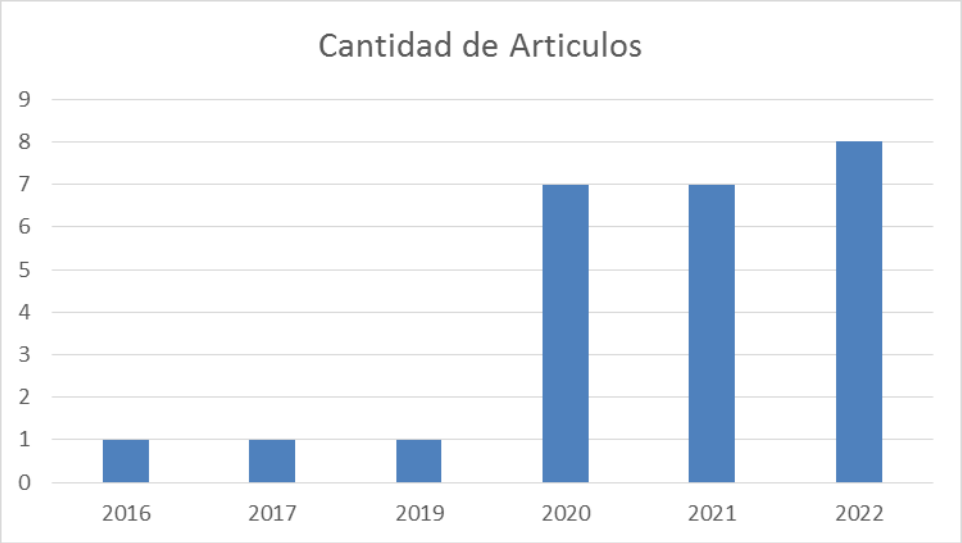

Figura 5: Tendencia en el tiempo de la publicación de artículos sobre ciberseguridad en kubernetes y Contenedores.

RQ2. ¿Qué países aportan más artículos sobre ciberseguridad en contenedores y kubernetes?

Los países de los estudios se vincularon a la afiliación del primer autor de cada artículo. Los resultados revelaron que los artículos procedían de 14 países. Además, se comprobó que Estados Unidos era el país con mayor número de artículos en este RSL. En la Figura 4, podemos ver el número de artículos por país.

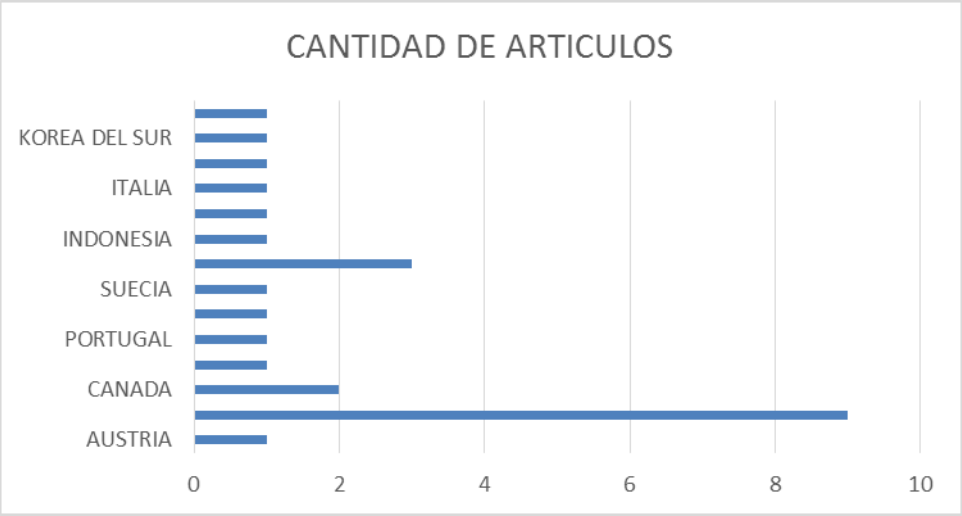

Figura 6: Países donde se ha aplicado la ciberseguridad en la agricultura.

RQ3. ¿Qué practicas sobre ciberseguridad en kubernetes informan los estudios?

Según los resultados, podemos ver que un 24% de los trabajos seleccionados hacen referencia al Diseñó de Imágenes Seguras, un 12% para configuración de accesos basados en roles , un 12% la Gestión de tiempo de Ejecución del Contenedor, 8% en Gestión de la Configuración, 8% en la protección de la Infraestructura, 8% en la Segmentación de redes, 8% en el Análisis de las Imágenes a Instalar y finalmente el 20% restante se divide en No usar configuración predeterminadas, usar name spaces para los despliegues, protección del servidor de la API, protección del Kublet y la segmentación de redes, cada uno de ellos con un 4%. En la Figura 5 podemos ver podemos ver las prácticas de seguridad recomendadas en los artículos analizados.

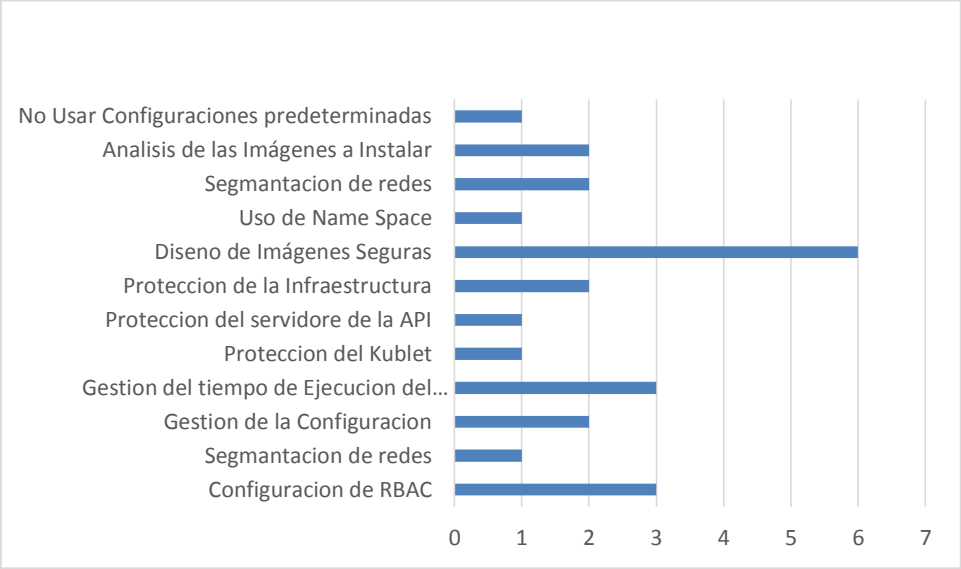

Figura 7: Buenas Prácticas utilizadas en ciberseguridad en contenedores.

RQ4. ¿Cuáles son las principales limitaciones de la ciberseguridad en contenedores y kubernetes?

En esta pregunta identifica las principales limitaciones encontradas en los artículos seleccionados sobre una adecuada seguridad en entornos de contenedores y kubermetes. Los resultados determinaron que las principales limitaciones son: Falta de Conocimiento, Falta de buenas prácticas de Diseño, Experiencia., Recursos y soporte externo experto. La Figura 6 muestra las limitaciones en el uso de buenas prácticas de acuerdo al número de artículos.

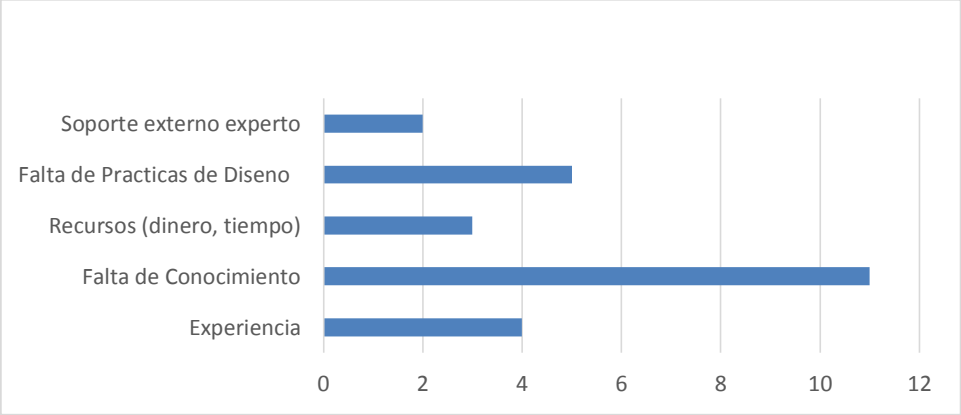

Figura 8: Limitaciones para el uso de buenas prácticas Ciberseguridad.

RQ5. ¿Cuáles son los principales ciberataques en Kubernetes, contenedores y su impacto?

Los resultados de los estudios seleccionados, indican con un 56% que el principal ciberataque en contenedores y kubernetes es el malware: un software malicioso que se infiltra en los Docker file de las aplicaciones contenerizadas; con el 32% el ciberataque hace refernacia a escalamiento de provilegios y un 8 % denegación de servicio (DoS) que causa la inaccesibilidad a los equipos o sistemas.

Como resultado de los estudios seleccionados en la Figura 3 se indican los principales ciberataques y en la Figura 7 los impactos que se les atribuye.

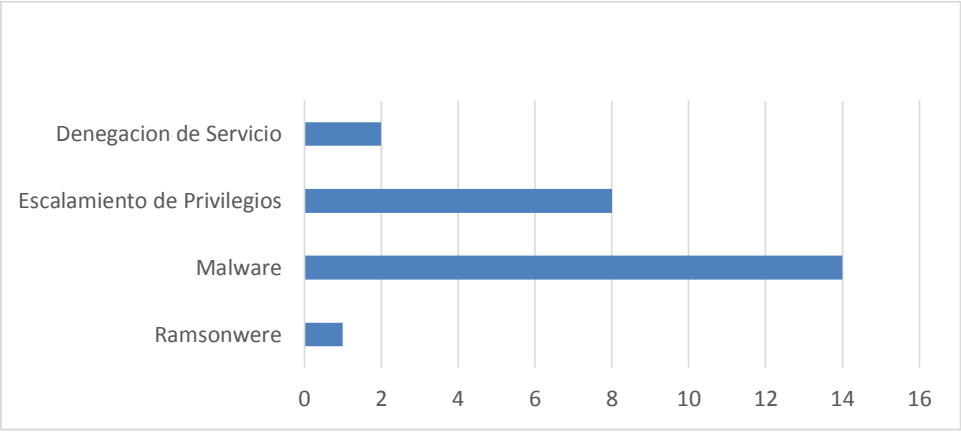

Figura 9: Principales Ciberataques en contenedores.

Discusión

La discusión se divide en dos partes. En la primera parte se realiza un análisis bibliométrico de los trabajos seleccionados. En la segunda parte, se discuten los resultados encontrados en los artículos analizados.

El análisis bibliométrico comienza por determinar la tendencia de publicaciones de los resultados de la investigación sobre la ciberseguridad en contenedores y kubernetes en los últimos años. Como dato importante, se ha observado un incremento en los últimos años, de 2017 a 2021, en la investigación de la ciberseguridad en contenedores y kubermtes. Esta tendencia se puede ver en la Figura 3.

El país con mayor número de publicaciones es Estados Unidos de acuerdo a la afiliación de los autores principales. Microservicios contenerizados es uno de los pilares fundamentales para el Desarrollo de aplicaciones. Proteger contenedores y kubernetes de los ataques cibernéticos es fundamental para garantizar la Confidencialidad, Integridad y Disponibilidad de las Aplicaciones.

Existen dos importantes limitaciones al momento de aplicar la ciberseguridad en contenedores y kubernetes, Falta de Conocimiento, Falta de buenas prácticas de Diseño, esto podrá evitar diversos ataques

Los principales ciberataques son: malware, escalamiento de privilegios y denegación de servicios (DoS. Al conocer los principales ciber ataques existe la capacidad de responder a las ciber amenazas tanto de forma preventiva (antes del ataque) como reactiva (después del ataque). Además, se han evaluado los impactos que generan estos ciberataques indicados en la Figura 12.

Finalmente las mejores prácticas recomendadas comentadas en los artículos son un adecuado Diseñó de Imágenes Seguras y controles de accesos basados en roles , Gestión de tiempo de Ejecución del Contenedor y Configuración de los runtime, la protección de la Infraestructura, Segmentación de redes, Análisis de las Imágenes a Instalar, No usar configuración predeterminadas, usar name spaces para los despliegues, protección del servidor de la API , conjunto de prácticas que mitigaran los eventos de seguridad y su impacto en los ambientes contenerizados y kubernetes.

Conclusiones

El objetivo de esta RSL fue examinar el estado actual de la ciberseguridad en Contendeores y Kuberntes en 25 artículos seleccionados. Los artículos analizados evalúan la investigación realizada por 87 autores distribuidos en 4 continentes y 14 países. En resumen, los resultados obtenidos son los siguientes:

- En el año 2022 refleja el mayor número de publicaciones de los estudios seleccionados en la RSL, con un porcentaje del 32%;
- El 76% de los estudios radican en autores que residen en América y Asia;

Un hallazgo importante es que las limitaciones pueden ser acaparadas con capacitaciones constantes sobre las bondades del uso de seguridad en contenedores. Además, se puede observar que los recursos que se usan para la protección tienden a ciertas tecnologías, pero sin el debido conocimiento del desarrollador sobre su importancia.

Se pueden identificar y contrarrestar los ciberdelitos ya que se conoce los principales ciberataques y el impacto que causan al materializarse en los ambientes contenerizados. Por ello, los ambientes debidamente configurados con las buenas prácticas de seguridad identificadas a través de los artículos brindan contramedidas de ciberseguridad vitales para la salvaguarda de la confidencialidad, integridad y disponibilidad (CIA) de la información.

Además, este trabajo ofrece una revisión del estado actual de la ciberseguridad en contenedores y kubernets que puede ser útil para la compresión de su concepto. Además, se destaca que la educación y la capacitación son las necesidades más pertinentes para este sector de microservicios.

Referencias

1. Alonso Batuecas Francisco, S. L. (2021). Implantación de Tecnologías de Contenedores en una Organización. Obtenido de http://calderon.cud.uvigo.es/handle/123456789/488
2. Alyas, T. A. (Agosto de 2022). Container Performance and Vulnerability Management for Container Security Using Docker Engine. Security and Communication Networks, Volumen 2022. doi:https://doi.org/10.1155/2022/6819002
3. Bambhore Tukaram, A. S. (Agosto de 2022). Towards a Security Benchmark for the Architectural Design of Microservice Applications. doi:https://doi-org.vpn.ucacue.edu.ec/10.1145/3538969.3543807

4. Bila, N. D. (Julio de 2017). Leveraging the serverless architecture for securing linux containers. In 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), (pp. 401-404). doi:https://doi.org/10.1109/ICDCSW.2017.66
5. Bose, D. B. (Junio de 2021). Under-reported'Security Defects in Kubernetes Manifests. In 2021 IEEE/ACM 2nd International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS), (pp. 9-12). doi:https://doi.org/10.1109/EnCyCriS52570.2021.00009
6. Budigiri, G. B. (Junio de 2021). Network policies in kubernetes: Performance evaluation and security analysis. In 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), (pp. 407-412). doi:https://doi.org/10.1109/EuCNC/6GSummit51104.2021.9482526
7. Cavalcanti, M. I. (Agosto de 2021). Performance Evaluation of Container-Level Anomaly-Based Intrusion Detection Systems for Multi-Tenant Applications Using Machine Learning Algorithms. In The 16th International Conference on Availability, Reliability and Security, (pp. 1-9). doi:https://doi-org.vpn.ucacue.edu.ec/10.1145/3465481.3470066
8. Chen, J. H. (2022). Informer: irregular traffic detection for containerized microservices rpc in the real world. In Proceedings of the 4th ACM/IEEE Symposium on Edge Computing (pp. 389-394). doi:https://doi-org.vpn.ucacue.edu.ec/10.1016/j.hcc.2022.100050
9. Codina, P. L. (2005). Scopus: el mayor navegador científico de la web. El Profesional de La Informacion. 14(1). doi:https://doi.org/10.3145/epi.2005.feb.07
10. contenedores, E. d. (2021). https://repositorio.pucesa.edu.ec/handle/123456789/3302. Obtenido de https://repositorio.pucesa.edu.ec/handle/123456789/3302
11. Dibyendu Brinto Bose, Akond Rahman, & Shazibul Islam. (21 de October de 2020). XI Commandments of Kubernetes Security: A Systematization of Knowledge Related to Kubernetes Security Practices. IEEE Secure Development (SecDev). doi:10.1109/SecDev45635.2020.00025
12. Doan, T. P. (2022). DAVS: Dockerfile Analysis for Container Image Vulnerability Scanning. CMC-COMPUTERS MATERIALS & CONTINUA,, 1699-1711. doi:https://doi.org/10.32604/cmc.2022.025096
13. D'Silva, D. &. (Abril de 2021). Building a zero trust architecture using Kubernetes. In 2021 6th international conference for convergence in technology (i2ct), (pp. 1-8). doi:https://doi.org/10.1109/I2CT51068.2021.9418203

14. Fernández Bermejo, Daniel; Martínez Atienza, Gorgonio. (2016-06). Ciberseguridad, Ciberespacio y Ciberdelincuencia. Obtenido de http://hdl.handle.net/20.500.12226/84
15. Francesco Minna, A. B. (octubre de 2021). Understanding the Security Implications of Kubernetes Networking. doi:https://doi.ieeecomputersociety.org/10.1109/MSEC.2021.3094726
16. Gerald Budigiri, C. B. (2021). Network Policies in Kubernetes: Performance Evaluation and Security Analysis. doi:https://doi.org/10.1109/EuCNC/6GSummit51104.2021.9482526
17. Gonzalez, J. G. (Junio 2020). Metodologia de Pentesting para plataforma de microservicios Kubernetes. Madrid. Obtenido de http://oa.upm.es/64106/1/TFG_JAIME_GUARDIOLA_GONZALEZ.pdf
18. Haque, M. U. (Marzo de 2022). KGSecConfig: A Knowledge Graph Based Approach for Secured Container Orchestrator Configuration. In 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), (pp. 420-431). Obtenido de https://doi.org/10.1109/SANER53432.2022.00057
19. IEEE. (21 December 2020). Security-Performance Trade-offs of Kubernetes Container Runtimes. doi:10.1109/MASCOTS50786.2020.9285946
20. Ju, H. W. (2022). Design Scheme of a Docker Container File Isolation against Computer Virus Spreading. Mathematical Problems in Engineering. doi:https://doi.org/10.1155/2022/5348370
21. Karn, R. R. (2020). Cryptomining detection in container clouds using system calls and explainable machine learning. IEEE Transactions on Parallel and Distributed Systems, 674-691. doi:https://doi.org/10.1109/TPDS.2020.3029088
22. Kaur, B. D. (Junio de 2021). An analysis of security vulnerabilities in container images for scientific data analysis. GigaScience, 10(6), giab025. doi:https://doi.org/10.1093/gigascience/giab025
23. Kermabon-Bobinnec, H. G. (Abril de 2022). ProSPEC: Proactive Security Policy Enforcement for Containers. In Proceedings of the Twelveth ACM Conference on Data and Application Security and Privacy, (pp. 155-166). doi:https://doi-org.vpn.ucacue.edu.ec/10.1145/3508398.3511515
24. Kitchenham, B. (2004). Procedures for Performing. Obtenido de http://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf

25. Kwon, S. &. (2020). Divds: Docker image vulnerability diagnostic system. IEEE Access, 8, 42666-42673. doi:https://doi.org/10.1109/ACCESS.2020.2976874
26. Lambert, M. K. (2021). Securing CHEESEHub: A Cloud-based, Containerized Cybersecurity Education Platform. In Practice and Experience in Advanced Research Computing, (pp. 1-4). doi:https://doi-org.vpn.ucacue.edu.ec/10.1145/3437359.3465584
27. Lim, S. Y. (Noviembre de 2022). Secure Namespaced Kernel Audit for Containers. In Proceedings of the ACM Symposium on Cloud Computing, (pp. 518-532). Obtenido de https://doi-org.vpn.ucacue.edu.ec/10.1145/3472883.3486976
28. Linetskyi Artem, 2Babenko Tetiana, 3Myrutenko Larysa, 4Vialkova Vira. (2019). ELIMINATING PRIVILAGE ESCALATION TO ROOT IN CONTAINERS. Obtenido de https://journal.scsa.ge/wp-content/uploads/2020/04/11-41-spcsj.pdf
29. López Rico, S. (2022). Arquitectura de microservicios en Kubernetes. Obtenido de http://hdl.handle.net/10017/52830
30. Mangan, R. (2020). WEB OF SCIENCE autora del manual de uso. Clarivate Analytics. Obtenido de https://bib.us.es/sites/bib3.us.es/files/spanish_manual_wos_01_03_2019.pdf
31. Md. Shazibul Islam Shamim, F. A. (2020). XI Commandments of Kubernetes Security: A Systematization of Knowledge Related to Kubernetes Security Practices. doi:10.1109/SecDev45635.2020.00025
32. Pecka, N. B. (Mayo de 2022). Privilege Escalation Attack Scenarios on the DevOps Pipeline Within a Kubernetes Environment. In Proceedings of the International Conference on Software and System Processes and International Conference on Global Software Engineering (pp. 45-49). Obtenido de https://doi-org.vpn.ucacue.edu.ec/10.1145/3529320.3529325
33. Ponsico Martin, P. (2017). Tecnologia de Contendedores Docker. Obtenido de http://hdl.handle.net/2117/113040
34. Red Hat. (2021). State of Kubernetes Security Report. Obtenido de https://security.stackrox.com/rs/219-UEH-533/images/cl-state-kubernetes-security-report-ebook-f29117-202106-en.pdf
35. Sellan Reyes, D. P. (2022). Estrategia de fortalecimiento para la utilización de kubernetes en el sector privado de la provincia de los ríos. Obtenido de http://dspace.utb.edu.ec/handle/49000/11672

36. Shamim, M. S. (Septiembre de 2020). Xi commandments of kubernetes security: A systematization of knowledge related to kubernetes security practices. In 2020 IEEE Secure Development (SecDev), (pp. 58-64). doi:https://doi.org/10.1109/SecDev45635.2020.00025
37. Shamim, S. I. (Agosto de 2021). Mitigating security attacks in kubernetes manifests for security best practices violation. In Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, (pp. 1689-1690). Obtenido de https://doi-org.vpn.ucacue.edu.ec/10.1145/3468264.3473495
38. Shringarputale, S. M. (Noviembre de 2020). Co-residency attacks on containers are real. In Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop, (pp. 53-66). doi:https://doi-org.vpn.ucacue.edu.ec/10.1145/3411495.3421357
39. Sun, J. W. (Noviembre de 2020). Blockchain-based automated container cloud security enhancement system. In 2020 IEEE International Conference on Smart Cloud (SmartCloud), (pp. 1-6). doi:https://doi.org/10.1109/SmartCloud49737.2020.00010
40. Surantha, N. &. (Julio de 2016). Secure kubernetes networking design based on zero trust model: A case study of financial service enterprise in indonesia. In International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing , (pp. 348-361). doi:https://doi-org.vpn.ucacue.edu.ec/10.1007/978-3-030-22263-5_34
41. Tien, C. W. (Diciembre de 2019). Kubanomaly: anomaly detection for the docker orchestration platform with neural network approaches. Engineering reports, e12080. doi:https://doi.org/10.1002/eng2.12080
42. Viktorsson, W. K. (Noviembre de 2020). Security-performance trade-offs of kubernetes container runtimes. In 2020 28th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), (pp. 1-4). doi:https://doi.org/10.1109/MASCOTS50786.2020.9285946
43. WIPO. (2012). Guia para Base de Datos Tecnologicas. Obtenido de http://www.wipo.int/edocs/pubdocs/es/patents/434/wipo_pub_l434_11.pdf
44. Ying, F. Z. (2022). Microservice Security Framework for IoT by Mimic Defense Mechanism. Sensors. doi:https://doi.org/10.3390/s22062418