ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Utmach
Calidad, Pertinencia y Calidez

PROGRAMA DE MAESTRÍA EN SOFTWARE. PROYECTO DE TITULACIÓN II

SEMANA II: EL MÉTODO CIENTÍFICO

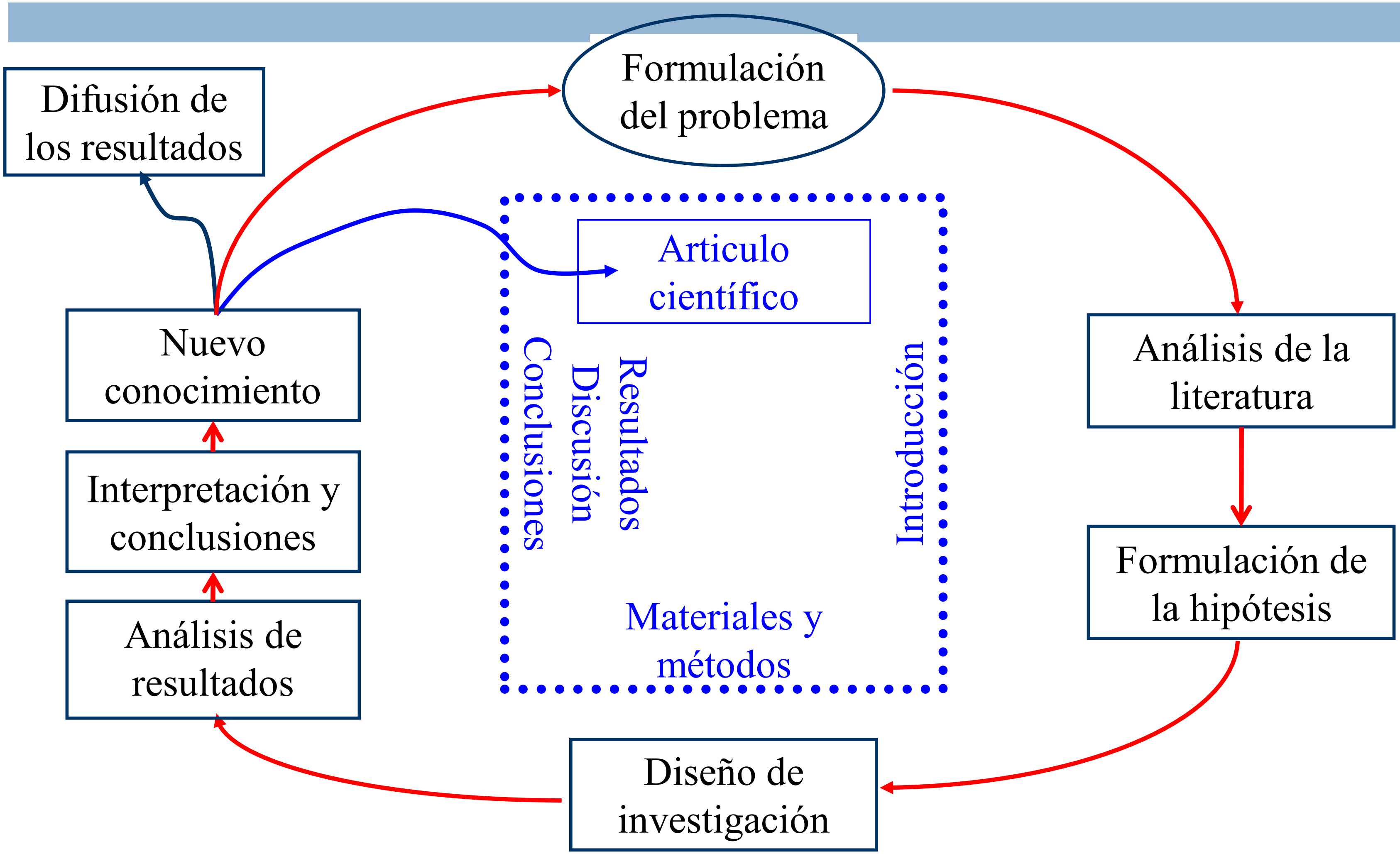
TALLER 2:
Análisis del Estado del Arte

Compilación: Walter Fuertes Díaz, PhD

Módulo I: El protocolo de Investigación

- **Tema:**
  - Taller N° 2: **Análisis de la Literatura**
- **Objetivos:**
  - Estructurar la **línea base** del Marco Teórico de su proyecto de titulación ensamblando los antecedentes de la investigación y las bases teóricas.
  - Estructurar la **línea base** del Estado del Arte de su proyecto de titulación utilizando el SLR propuesto por Bárbara Kitchenham.
- **Se pide:**
  - **Buscar las fuentes bibliográficas** que permitan detectar, extraer y recopilar la información de interés para construir el marco teórico pertinente a su problema de investigación.
  - **Buscar las fuentes bibliográficas mediante la selección de** trabajos relacionados en el tema de su investigación que le permitan tanto sentar las bases del estado del arte como obtener información sobre las tendencias actuales y los desafíos futuros.
- **Entregable:**
  - Trabajo individual. Elaborar un documento en formato PDF, que contenga la línea base del Marco teórico y el Estado del Arte de su proyecto de titulación.
- **Plazo:**
  - Sábado 03 de septiembre de 2020, 17:00 y subirlo a la plataforma virtual.

El Método científico



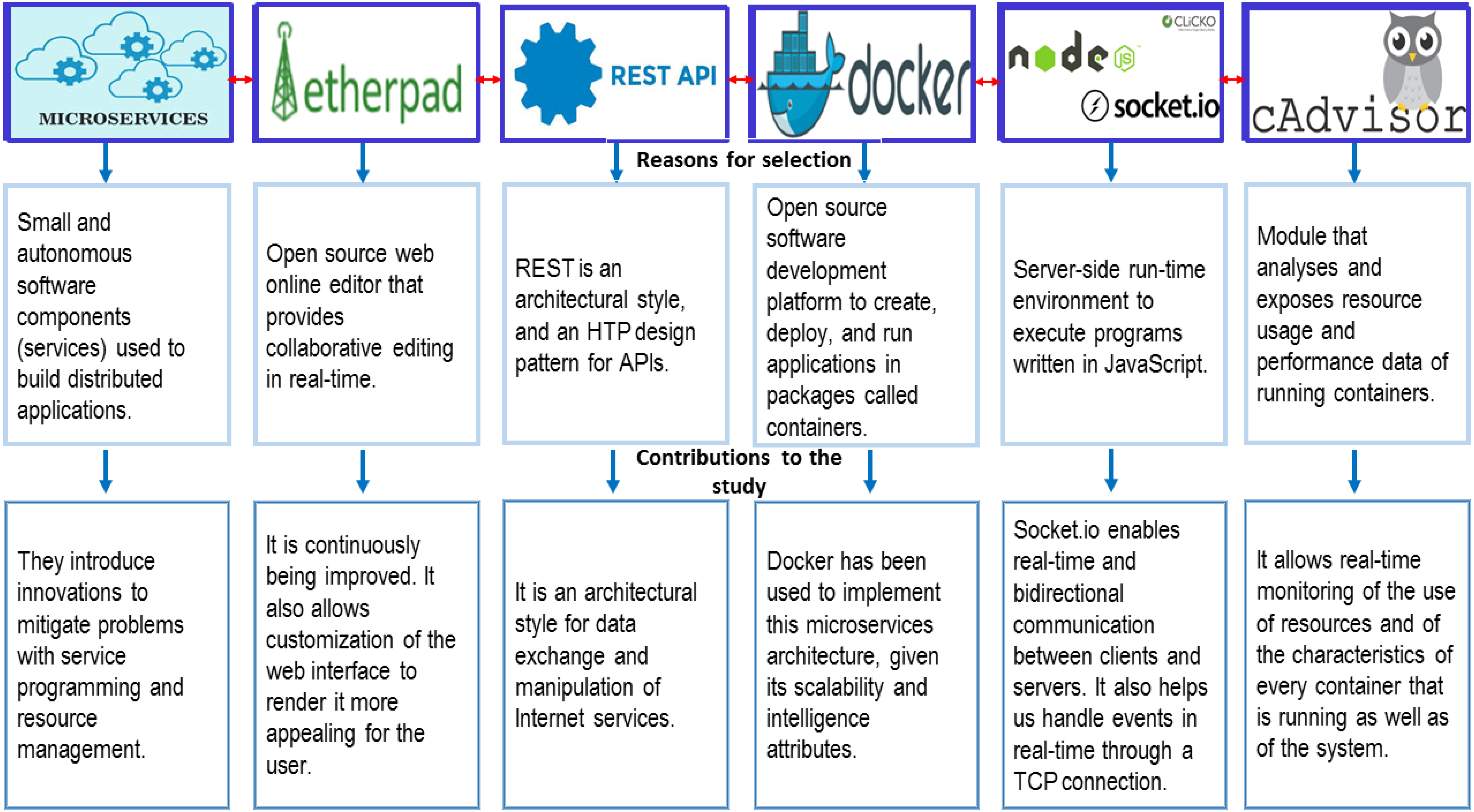
Fuente: Jan Feyen , ¿Cómo elaborar propuestas de investigación?, ESPE-2010

Análisis de la Literatura

- **Antecedentes de la investigación**: Es una revisión bibliográfica crítica de:
  - ¿Qué tanto se ha investigado sobre el tema?
  - ¿Existen estudios previos del que se pretende realizar?
  - ¿Quiénes son los estudiosos mas representativos del tema?
  - ¿Qué metodología, métodos, técnicas, herramientas han utilizado?
  - ¿En que año se ha publicado el estudio y en qué país?
  - ¿Cuáles han sido sus primeros hallazgos”

- **Bases teóricas:** Sirven para entender la realidad y poder explicarla:
  - Variable Dependiente:
    - Definición conceptual
    - Definición Operacional
    - Métricas, dimensiones, Escalas.
  - Variable independiente
    - Definición conceptual
    - Definición Operacional
    - Definición de Instrumentos de Medición
  - La influencia de la variable Independiente sobre la Dependiente.

Marco Teórico Ejemplo



Reasons for selection

Small and autonomous software components (services) used to build distributed applications.

Open source web online editor that provides collaborative editing in real-time.

REST is an architectural style, and an HTP design pattern for APIs.

Open source software development platform to create, deploy, and run applications in packages called containers.

Server-side run-time environment to execute programs written in JavaScript.

Module that analyses and exposes resource usage and performance data of running containers.

Contributions to the study

They introduce innovations to mitigate problems with service programming and resource management.

It is continuously being improved. It also allows customization of the web interface to render it more appealing for the user.

It is an architectural style for data exchange and manipulation of Internet services.

Docker has been used to implement this microservices architecture, given its scalability and intelligence attributes.

Socket.io enables real-time and bidirectional communication between clients and servers. It also helps us handle events in real-time through a TCP connection.

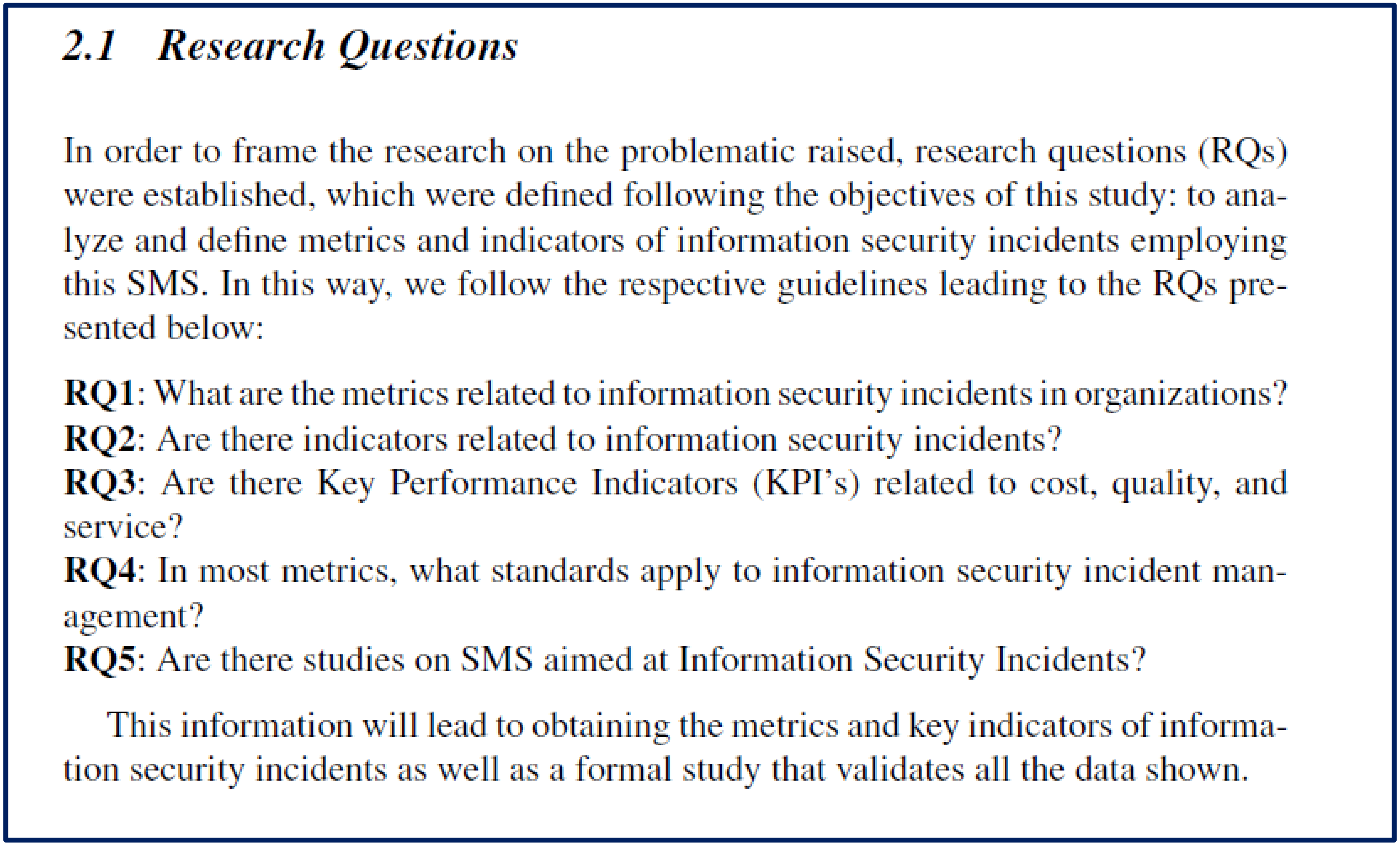
It allows real-time monitoring of the use of resources and of the characteristics of every container that is running as well as of the system.

Revisión Sistemática de Literatura

- **Protocolo:**
  1. Definir las preguntas de investigación;
  2. Definir criterios de inclusión y exclusión para la RSL;
  3. Identificar las bases de datos y motores de búsqueda que se van a utilizar;
  4. Definir los términos de búsqueda;
  5. Buscar en bases de datos científicas;
  6. Fases de Revisión;
  7. Extracción de Datos;
  8. Presentación de Resultados.

Fuente: Revisión Sistemática de la Literatura (SLR). De la Teoría a la Práctica, Eduardo Benavides, julio 2020. E-mail: debenavides@espe.edu.ec

SLR- Ejemplo:



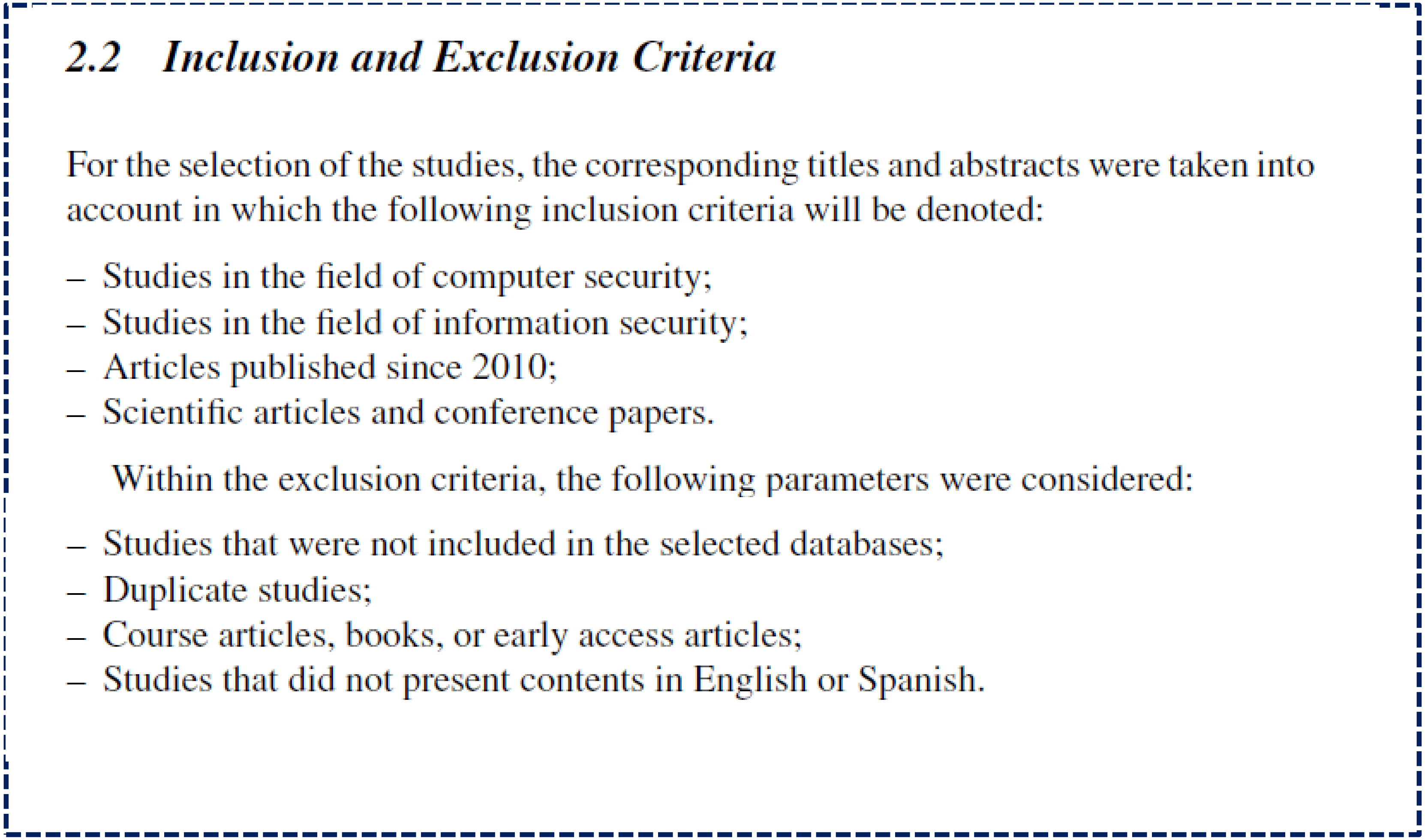
2.1 *Research Questions*

In order to frame the research on the problematic raised, research questions (RQs) were established, which were defined following the objectives of this study: to analyze and define metrics and indicators of information security incidents employing this SMS. In this way, we follow the respective guidelines leading to the RQs presented below:

RQ1: What are the metrics related to information security incidents in organizations?
RQ2: Are there indicators related to information security incidents?
RQ3: Are there Key Performance Indicators (KPI's) related to cost, quality, and service?
RQ4: In most metrics, what standards apply to information security incident management?
RQ5: Are there studies on SMS aimed at Information Security Incidents?

This information will lead to obtaining the metrics and key indicators of information security incidents as well as a formal study that validates all the data shown.

SLR- Ejemplo:



2.2 *Inclusion and Exclusion Criteria*

For the selection of the studies, the corresponding titles and abstracts were taken into account in which the following inclusion criteria will be denoted:

- Studies in the field of computer security;
- Studies in the field of information security;
- Articles published since 2010;
- Scientific articles and conference papers.

Within the exclusion criteria, the following parameters were considered:

- Studies that were not included in the selected databases;
- Duplicate studies;
- Course articles, books, or early access articles;
- Studies that did not present contents in English or Spanish.

SLR- Ejemplo:

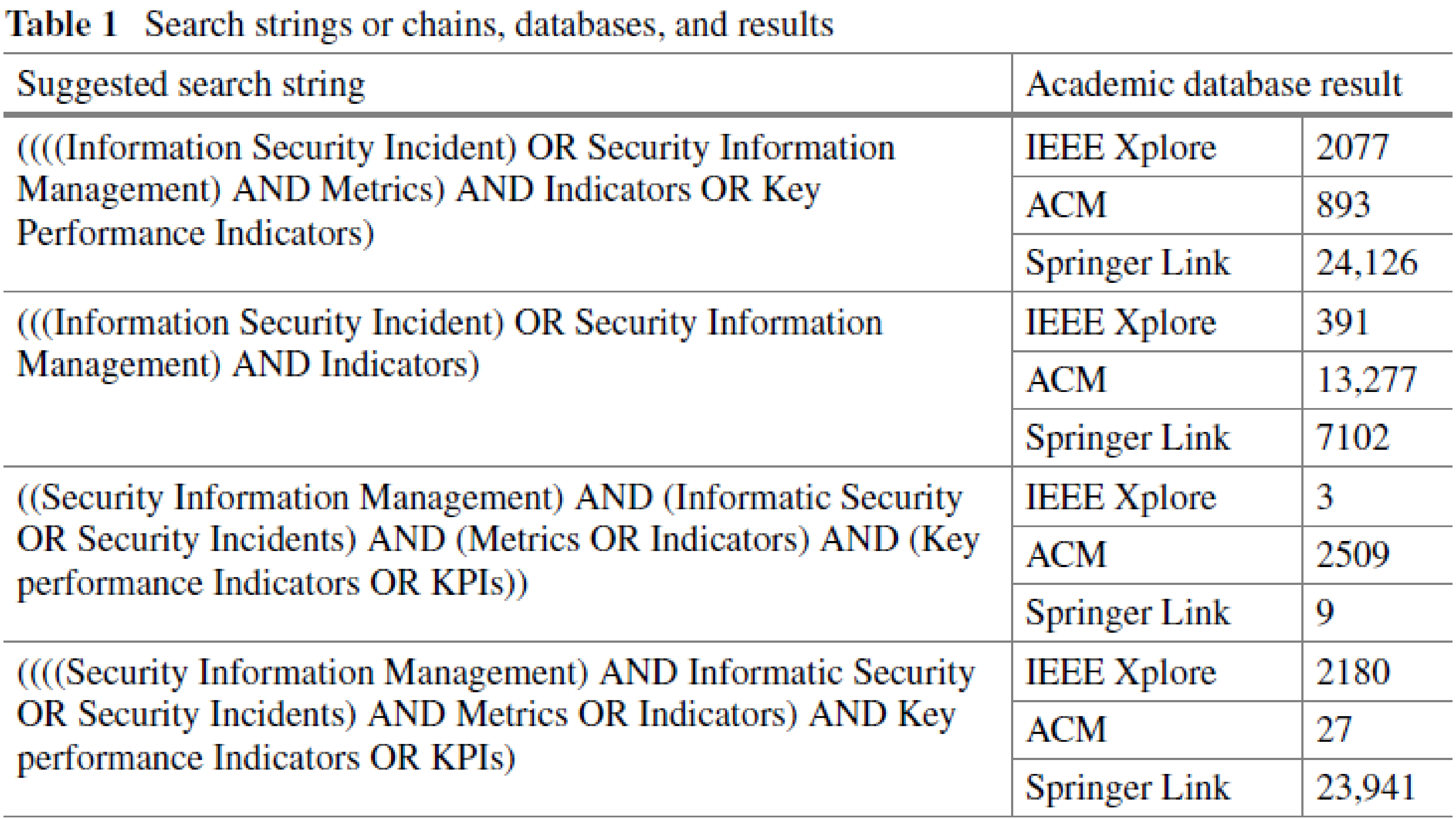


Table 1 Search strings or chains, databases, and results

Suggested search string	Academic database result	
((((Information Security Incident) OR Security Information Management) AND Metrics) AND Indicators OR Key Performance Indicators)	IEEE Xplore	2077
	ACM	893
	Springer Link	24,126
(((Information Security Incident) OR Security Information Management) AND Indicators)	IEEE Xplore	391
	ACM	13,277
	Springer Link	7102
((Security Information Management) AND (Informatic Security OR Security Incidents) AND (Metrics OR Indicators) AND (Key performance Indicators OR KPIs))	IEEE Xplore	3
	ACM	2509
	Springer Link	9
((((Security Information Management) AND Informatic Security OR Security Incidents) AND Metrics OR Indicators) AND Key performance Indicators OR KPIs)	IEEE Xplore	2180
	ACM	27
	Springer Link	23,941

SLR- Ejemplo:

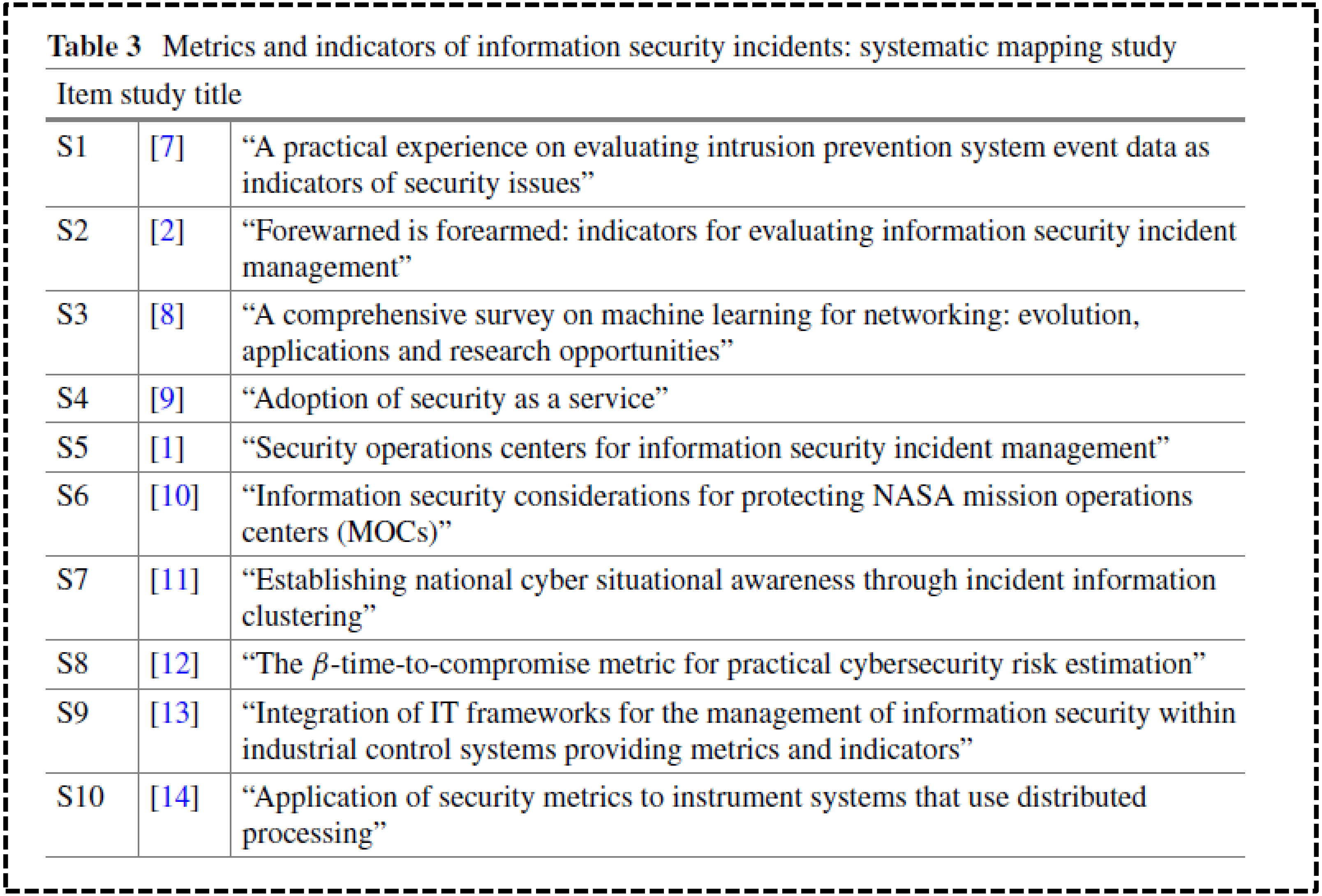


Table 3 Metrics and indicators of information security incidents: systematic mapping study

Item study title		
S1	[7]	"A practical experience on evaluating intrusion prevention system event data as indicators of security issues"
S2	[2]	"Forewarned is forearmed: indicators for evaluating information security incident management"
S3	[8]	"A comprehensive survey on machine learning for networking: evolution, applications and research opportunities"
S4	[9]	"Adoption of security as a service"
S5	[1]	"Security operations centers for information security incident management"
S6	[10]	"Information security considerations for protecting NASA mission operations centers (MOCs)"
S7	[11]	"Establishing national cyber situational awareness through incident information clustering"
S8	[12]	"The β-time-to-compromise metric for practical cybersecurity risk estimation"
S9	[13]	"Integration of IT frameworks for the management of information security within industrial control systems providing metrics and indicators"
S10	[14]	"Application of security metrics to instrument systems that use distributed processing"

SLR- Ejemplo:

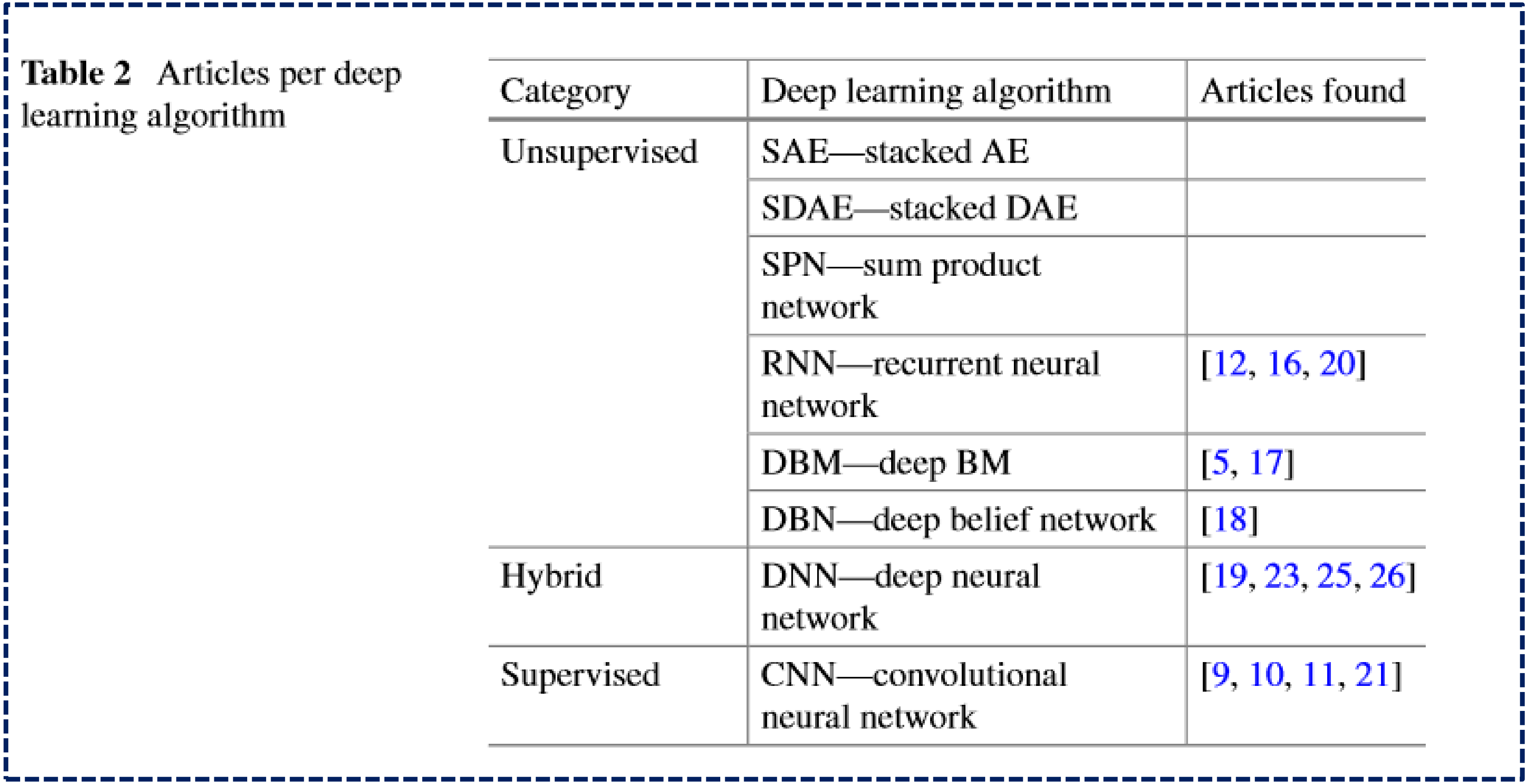
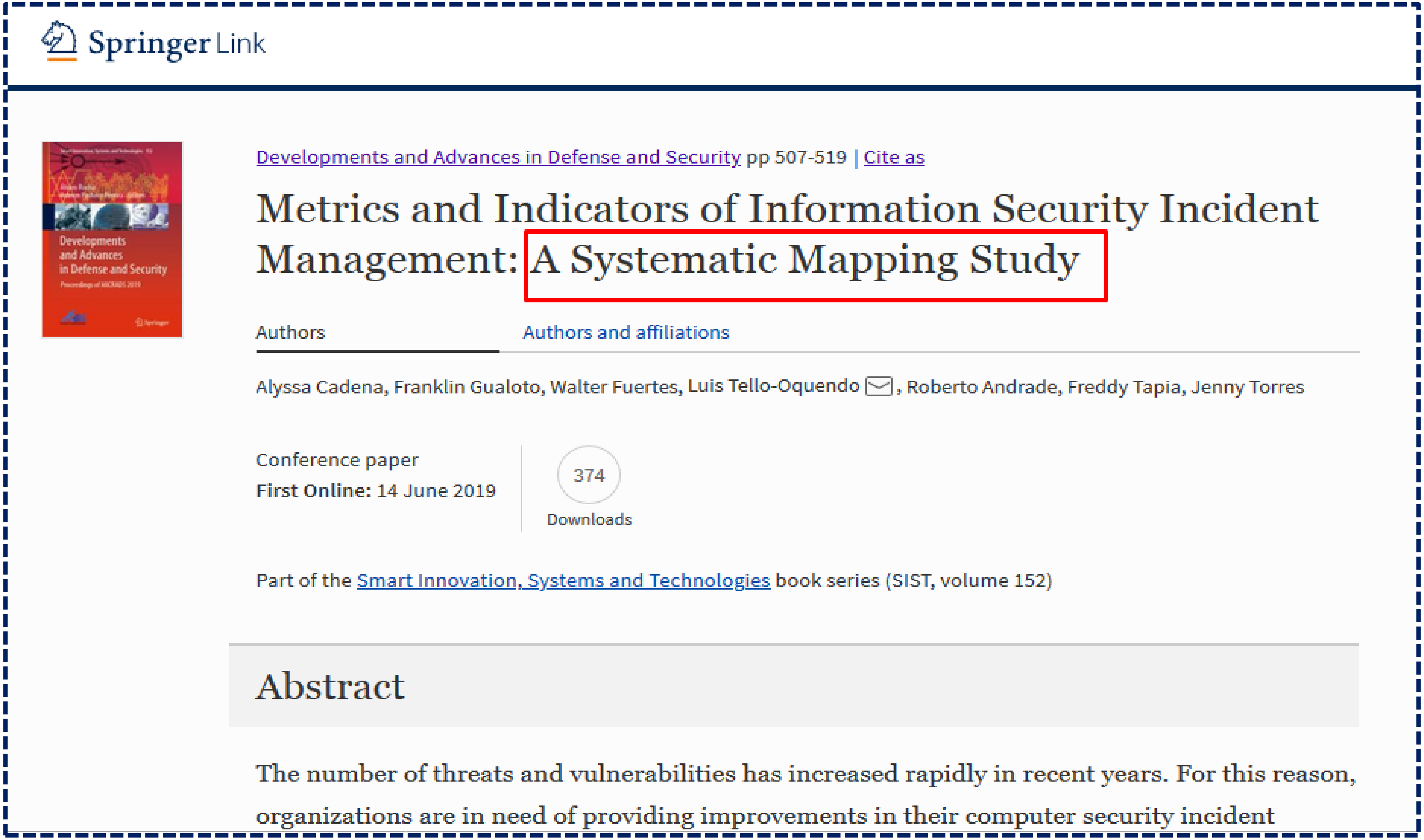


Table 2 Articles per deep learning algorithm

Category	Deep learning algorithm	Articles found
Unsupervised	SAE—stacked AE	
	SDAE—stacked DAE	
	SPN—sum product network	
	RNN—recurrent neural network	[12, 16, 20]
	DBM—deep BM	[5, 17]
	DBN—deep belief network	[18]
Hybrid	DNN—deep neural network	[19, 23, 25, 26]
Supervised	CNN—convolutional neural network	[9, 10, 11, 21]

SLR- Ejemplo:



Developments and Advances in Defense and Security pp 507-519 | Cite as

Metrics and Indicators of Information Security Incident Management: A Systematic Mapping Study

Authors | Authors and affiliations

Alyssa Cadena, Franklin Gualoto, Walter Fuertes, Luis Tello-Oquendo ✉, Roberto Andrade, Freddy Tapia, Jenny Torres

Conference paper
First Online: 14 June 2019

374
Downloads

Part of the Smart Innovation, Systems and Technologies book series (SIST, volume 152)

Abstract

The number of threats and vulnerabilities has increased rapidly in recent years. For this reason, organizations are in need of providing improvements in their computer security incident

Referencias Bibliográficas

- Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering–a systematic literature review. *Information and software technology*, *51*(1), 7-15.
- Tapia, F.; Mora, M.Á.; Fuertes, W.; Lascano, J.E.; Toulkeridis, T., “**A Container Orchestration Development that Optimizes the Etherpad Collaborative Editing Tool through a Novel Management System**”. Electronics 2020, 9, 828. https://doi.org/10.3390/electronics9050828
- Alyssa Cadena, Franklin Gualoto, Walter Fuertes, Luis Tello-Oquendo, Roberto Andrade, Freddy Tapia, and Jenny Torres, “***Metrics and Indicators of Information Security Incident Management: A Systematic Mapping Study”.*** *In: Rocha Á., Pereira R. (eds) Developments and Advances in Defense and Security. Smart Innovation, Systems and Technologies, vol 152. Springer, Singapore.* DOI https://doi.org/10.1007/978-981-13-9155-2_5
- Benavides E., Fuertes W., Sanchez S., and Sanchez M. (2020). “***Classification of Phishing Attack Solutions by Employing Deep Learning Techniques: A Systematic Literature Review***. In: Rocha Á., Pereira R. (eds) Developments and Advances in Defense and Security. Smart Innovation, Systems and Technologies, vol 152. Springer, Singapore. DOI https://doi.org/10.1007/978-981-13-9155-2_5