Vol. 9 Núm. 2

ISSN: 2007-5448

RECIBE

Revista electrónica

DE COMPUTACIÓN, INFORMÁTICA, BIOMÉDICA Y ELECTRÓNICA

ReCIBE, Vol. 9 No. 1, Abril 2021

Índice

Computación e Informática

Biomédica

Recibido 27/07/2020 *ReCIBE, Año 9 No. 2, Noviembre 2020*

Aceptado 11/11/2020

Aplicación del internet industrial de las cosas (ioT)en líneas de manufactura por proceso de moldeo por inyección de plástico.

Application of the industrial internet of things (ioT) in manufacturing lines by plastic injection molding process.

Jesus Ivan Aguilar Lugo[1]

jesus.aguilar@uabc.edu.mx

JorgeEduardoIbarraEsquer[1]

jorge.ibarra@uabc.edu.mx

Marlenne Angulo Bernal[1]

mangulo@uabc.edu.mx

[1]Universidad Autónoma de Baja California

Resumen: Las revoluciones industriales han impulsado el desarrollo tecnológico, social y económico. Una de las industrias que se ha beneficiado por los avances tecnológicos es la de moldeo por inyección de plástico, que recientemente ha incorporado tecnologías de la industria 4.0. A partir de esto, el presente documento tiene como objetivo posicionarnos en el contexto de la industria de moldeo por inyección de plástico y el progreso de la industria 4.0 aplicada a sus procesos. Esta industria conlleva un proceso complejo controlado, que requiere el uso de herramientas estadísticas que muestren el comportamiento y resultados del proceso. Los datos se suelen recopilar de forma manual, con fallas u omisiones que generan problemas en diversas áreas. Se plantea entonces utilizar tecnologías de industria 4.0 para aumentar la eficiencia, descifrar tendencias y optimizar recursos y procesos, partiendo de la noción que el uso de estas tecnologías facilita la toma de decisiones acertadas en base a datos extraídos de producción, mejorando el análisis de las causas raíz de la problemática. Por medio de una revisión sistemática de literatura se encuentran casos exitosos de implementación, conceptos en el campo del Internet Industrial de las Cosas y la relación entre la industria de moldeo por inyección y la industria 4.0, con resultados utilizables como referencia para el planteamiento de nuevos proyectos y soluciones por parte de la comunidad interesada en la industria de moldeo por inyección de plástico.

Palabras clave: Internet Industrial, Industria de moldeo por inyección de plástico, Industria 4.0.

Abstract: Industrial Revolutions have been a key part for the technological, social and economic development. Among these industries one that has gained advantage from the technological advances is the plastic injection molding, which recently has integrated Industry 4.0 technologies. From here on the current white paper has the following objective: Positioning on the Industry 4.0 context applied to the Injection molding industry main process. This industry maintains a complex controlled process, which requires the use of statistical methods that display the behavior and outcomes of the process. Data is often acquired manually, which leads to misinformation that could generate issues on different departments. The proposal is to use industry 4.0 technologies to raise efficiency, discover tendencies and optimize resources and processes, starting from the notion that these technologies makes easier the successful decision-making stage based on the data extracted from production, enhancing the root cause analysis for the main issues. By a systematic literature revision, successful cases of integration have been found along with Industrial Internet of things concepts and the relation between industry 4.0 and injection molding industry, the results on the cases can be useful for the injection molding industrial community to integrate this type of solution on their business.

Keywords: Industrial Internet, Plastic injection molding industry, Industry 4.0.

1.- Introducción

1.1 Antecedentes:

Las industrias han impulsado el desarrollo tecnológico, social y económico en la historia del ser humano, con logros que se hicieron tangibles por medio de lo que llamamos revoluciones industriales. Una revolución implica un cambio fuerte y profundo en los sistemas económicos y estructuras sociales, con efectos duraderos o permanentes en los sistemas productivos.

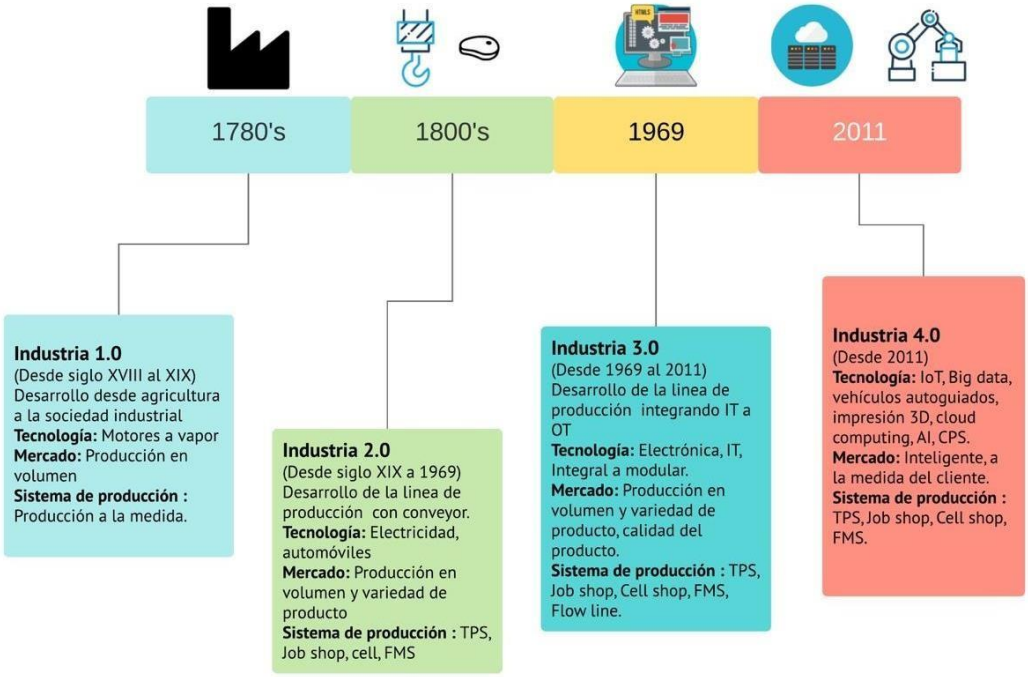


Figura 1. Línea de tiempo de la industria 1.0 - 4.0 basado en (Yong Yin, Kathryn E. Stecke & Dongni Li, 2018).

Como precursora de la revolución industrial se puede considerar a la transición de una cultura nómada a una sedentaria, gracias al establecimiento de un sistema de producción local de alimentos a partir de la agricultura. Esto trajo como consecuencia la necesidad de crear sistemas de transporte, comunicación y modelos económicos entre las diferentes regiones, así como un incremento en la población de estas. A esta etapa siguieron cambios paulatinos hasta llegar a lo que actualmente conocemos como revoluciones industriales, cuyas características más evidentes se muestran en la figura 1 y se describen a continuación (ACATECH, 2013), (Klaus Schwabm, 2016):

- Primera Revolución Industrial fue en el siglo XVIII (1780s) y tuvo lugar en Inglaterra. Las primeras máquinas mecánicas energizadas por medio de vapor hacen su aparición, dejando las casas como fábricas obsoletas para centralizar los negocios en lo que llamamos maquiladoras ocasionando un incremento notable en la productividad.

- Segunda Revolución Industrial, inicia alrededor de 100 años después de la primera (siglo XIX) en las carnicerías de Cincinnati, Ohio, encontró su aplicación más fuerte en las fábricas automovilísticas Ford, en Estados Unidos, al introducir el “Conveyor” o banda automatizada. Así mismo, a partir de esta etapa se involucra la energía eléctrica para la producción en masa.

- Tercera Revolución Industrial, comenzó en el siglo XX (1969) presentándose el primer Controlador Lógico Programable (PLC) y con ello la posibilidad de utilizar programación digital para la automatización de procesos. Además, se introduce la electrónica y el uso de tecnologías de la información. Utilizando estas herramientas de programación de procesos, en la actualidad se ha logrado obtener sistemas automatizados bastante flexibles y eficientes (Drath, R., & Horch, A., 2014), (ACATECH, 2013), (Klaus Schwabm, 2016).

- La Industria 4.0 y su sinónimo Cuarta Revolución Industrial se remonta a Alemania 2011 en la "Hannover Fair" donde se hizo mención del término "Industrie 4.0" como sinónimo de "Cyber-Physical Systems (CPS)" aplicados al dominio de la manufactura o "Cyber-Physical Production Systems (CPPS)". Desde entonces el tema de Industria 4.0 se ha expandido teniendo en cuenta estos principios (Vogel-Heuser, B., & Hess, D., 2016):

  -Servicios de orientación: "CPPS" ofreciendo servicios a través del Internet.

  -Auto organización inteligente: "CPPS" que puedan tomar decisiones propias descentralizadas.

  -Interoperabilidad entre "CPS", hombre y "CPPS": Agregar y representar información para la fácil interpretación de ingeniería y mantenimiento, virtualización del sistema en sus diferentes niveles, información de los datos relevantes en los procesos con posibilidad de verlos en tiempo real.

  -Fácil adaptación y flexibilidad a los cambios de requerimientos, reemplazando o expandiendo módulos.

  -Algoritmos de "Big Data" y tecnologías capaces de procesar en tiempo real.

  -Optimización de procesos de manufactura basados en algoritmos y datos para el incremento de la eficiencia.

  -Integración de datos por medio de ingeniería interdisciplinar a través del ciclo de vida basado en la estandarización de modelos de información.

  -Comunicación segura a través del Internet, en la nube.

1.2 Contexto:

En este documento haremos referencia a muchos conceptos que se hacen mención cuando hablamos de industria 4.0, como lo son:

1.- Cyber-Physical Systems (CPS): Son sistemas inteligentes que incluyen interacción de redes compuestas de componentes físicos y computacionales (Griffor, E. R., Greer, C., Wollman, D. A., & Burns, M. J., 2017). Una definición más completa desde su origen en sistemas de ingeniería y control es: "Es un sistema de elementos computacionales que colaboran para controlar entidades físicas. Cuando un sistema mecánico y eléctrico están en red utilizando componentes de software. Usan conocimiento e información compartida de procesos para controlar de manera independiente la logística y los sistemas de producción" (Greer, C., Burns, M., Wollman, D., & Griffor, E., 2019).

2.- Internet of Things (IoT): El concepto es muy similar a CPS, sin embargo, su origen proviene del punto de vista de redes y tecnología de la información integrando el mundo digital al mundo real. Se han propuesto muchas definiciones para el IoT, pero de manera general, puede describirse como la conjunción de varias tecnologías que permiten el acceso a servicios y aplicaciones basadas en el Internet a partir de dispositivos electrónicos conectados a objetos físicos, o cosas, con el fin de adquirir datos y controlar procesos (Greer, C., Burns, M., Wollman, D., & Griffor, E., 2019).

3.- Industrial Automation & Control Systems (IACS): se describe como un conjunto de sistemas de control e instrumentación de diferente tipo que incluyen dispositivos, sistemas, redes y controles usados para la automatización de procesos industriales (Boyes, H., Hallaq, B., Cunningham, J., & Watson, T., 2018).

4.- Supervisory Control and Data Acquisition (SCADA): se describe como un Sistema que permite al operador, localizado en cualquier parte, poder hacer un cambio en procesos a distancia, así como el monitoreo de ciertas variables o alarmas. Regularmente se compone por un centro de control que monitorea un sistema o maquinaria. Se puede decir que es el precursor al IIoT. Sin embargo, este carece de capacidades como el análisis de información y el nivel de conectividad que se encuentra en aplicaciones IIoT hoy en día (Boyes, H., Hallaq, B., Cunningham, J., & Watson, T., 2018).

5.- Industrial Internet: El consorcio del Internet Industrial de las Cosas (Industrial Internet of Things Consortium o IIC) nos da la definición como:
"Internet of things, machines, computers and people, enabling intelligent industrial operations using advanced data analytics for transformational business outcomes" / "Internet de las cosas, máquinas, computadoras y personas, habilitando operaciones inteligentes que realizan análisis avanzado de datos para la transformación de resultados en negocios."(IIC:PUB:G8:V2.1:PB:20180822).

6.- Industrial Internet of Things (IIoT): El internet industrial es un sistema compuesto por elementos inteligentes conectados, cyber-physical assets, tecnología generadora de información genérica y plataformas opcionales de cómputo en la nube (cloud) o en la rama (edge), que habilitan en tiempo real el acceso, recolección, análisis, comunicación, el intercambio de procesos, productos y/o información de servicios en el entorno industrial, así como la optimización del valor de la producción. Este valor puede incluir; mejora en la entrega del producto o servicio, incremento en la productividad, reducción de costos, reducción de consumo de energía y reducción de ciclos en productos a la medida (Boyes, H., Hallaq, B., Cunningham, J., & Watson, T., 2018).

7.- Sensores: Elemento que transforma una forma de energía a otro tipo de energía, algunos sensores tienen un conjunto de sensores (Greer, C., Burns, M., Wollman, D., & Griffor, E., 2019).

8.- Actuador: Dispositivo que realiza una función de salida para controlar un dispositivo externo, por ejemplo: cilindros, luces, sonido, imágenes, etc... (Greer, C., Burns, M., Wollman, D., & Griffor, E., 2019).

Los conceptos de IoT y CPS tienen puntos en común que hacen que en ocasiones sean utilizadas de forma indistinta, o llevan a representaciones como la que se observa en el diagrama de Venn de la figura 2. Estos traslapes se deben a las capacidades que conllevan conectar el mundo real al que en definición de CPS se toma como la “entidad física o sistemas de ingeniería” o por sus siglas en inglés “Physical”, mientras que en la definición de IoT se toma como “Cosa” o por su sigla en inglés “Thing”. Sin embargo, en este último se denomina como “cosa” también a las entidades virtuales, ya que su objetivo es relacionar lo físico con lo digital, otorgándole una etiqueta a este ente físico.

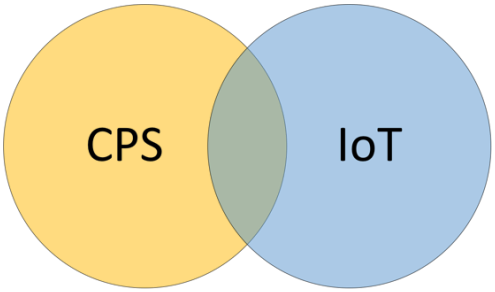


Figura 2. Representación de la visión sobre el traslape entre los conceptos de IoT y CPS (Greer, C., Burns, M., Wollman, D., & Griffor, E., 2019).

Ambos puntos de vista tratan de relacionar el mundo físico con el digital a través de sensores y tecnología interactiva. Sin embargo, la diferencia puede encontrarse en la perspectiva que cada uno le da a sus componentes. El CPS se entiende como un sistema que toma como prioridad el intercambio y retroalimentación de información para el sensado y control de actuadores del mundo físico, buscando establecer un sistema de ciclo cerrado y tomando a la persona como un factor necesario que interactúa con el sistema, lo cual se observa en el diagrama a bloques de la figura 3.

Por otra parte, la perspectiva del IoT es priorizar la interconexión de todas las cosas en el mundo real, brindando la flexibilidad de tener una estructura más abierta. Adicionalmente, esta pretende eliminar la interacción del humano con el sistema y realizar la retroalimentación por medio de algoritmos de inteligencia artificial que realicen las correcciones pertinentes, con una estructura similar a la que se observa en el diagrama de la figura 4 (Greer, C., Burns, M., Wollman, D., & Griffor, E., 2019).

Dado que ambos se encuentran en la categoría de Sistema de Sistemas (SoS), se pueden diseñar e implementar de forma modular. Es decir, uno de estos sistemas puede consistir en múltiples CPS o tecnologías IoT (Greer, C., Burns, M., Wollman, D., & Griffor, E., 2019). A manera de ejemplo, en la figura 4 se tiene un sistema implementado desde el punto de vista de las tecnologías IoT, donde su salida es dirigida hacia un sistema CPS que implementa el bloque de función 2.

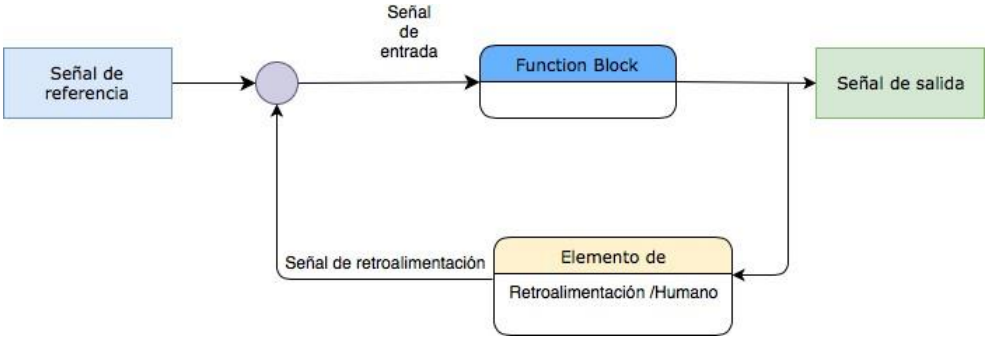


Figura 3. - Sistema desde el punto de vista de tecnología CPS

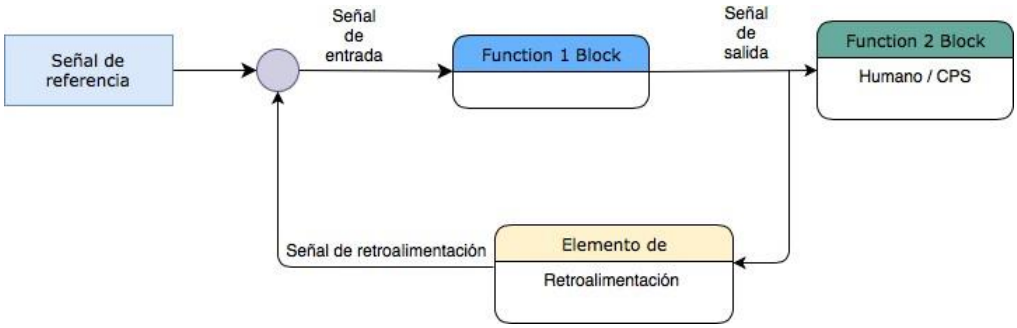


Figura 4. - Sistema desde el punto de vista de tecnología IoT

Se observa entonces que el interés inicial del IoT estaba centrado en ser un punto central de conexión y comunicación para objetos físicos capaces de obtener datos de su entorno, pero ha ido cambiando a un enfoque más completo donde se destaca la importancia para individuos y organizaciones de acceder a dichos datos y administrar sus objetos conectados para así maximizar su producción y beneficios. Las proyecciones que estiman billones de objetos conectados creando enormes cantidades de datos y facilitando monitorear y controlar procesos de forma automatizada generan un enorme interés en establecer al IoT como una tecnología productiva dentro de diferentes sectores, como son:

- Industria: Tomar mejores decisiones de negocio a partir del análisis de datos, realizar un uso más eficiente de sus recursos y explorar oportunidades de nuevos modelos de negocio.

- Academia: Existen varias líneas de investigación vigentes en torno al IoT (Stankovic, 2014) que pueden fomentar y promover la cooperación y vinculación entre grupos de interés pertenecientes tanto a sectores académicos como industriales.

- Sociedad: La promesa de productos y servicios que mejorarán las condiciones de vida y actividades diarias por medio de la integración de tecnologías inteligentes para el hogar, escuelas, hospitales, edificios e incluso ciudades.

En este caso en particular se enfocará en la industria de moldeo por inyección de plástico cuyo proceso se describe a continuación: El ciclo empieza en una tolva donde la resina del polímero es alimentada hacia el proceso. Aquí se muestra la primera variable en el proceso: la termodinámica del polímero se ve afectada por colorantes o resistencia a rayos ultravioleta, así como contaminantes o composición del material en caso de resina reciclada. Después la resina es presionada a través de un cilindro a alta temperatura donde dentro se encuentra un tornillo girando a altas revoluciones, fundiendo y mezclando la resina. En este punto se toma en cuenta como segunda variable a la distribución de la resina en la tolva, ya sea por la geometría de material reciclado o la resina virgen, así como el aire que entra en el cilindro que pudiese afectar la presión y temperatura del proceso de fundición. Cuando se tiene la mezcla lista, esta se hace pasar a través de la nariz del cilindro hacia el bebedero del molde cerrado. Una vez que la cavidad del molde se llena, este se refrigera activamente por medio de agua o aceite, acortando el tiempo del ciclo. Al enfriarse el polímero, se ocasiona una variación en la presión y temperatura, donde el flujo de esta última y el tiempo de enfriamiento tienen un efecto en la calidad del producto. Además, estas variables se pueden ver afectadas de una pieza a otra por situaciones como la solidificación de resina en la entrada de la cavidad, lo que provoca una obstrucción en el punto de inyección, que a su vez ocasiona un cúmulo de presión en el cilindro que afecta a la siguiente parte a producir (Charest, M., Finn, R., & Dubay, R., 2018).

El moldeo por inyección de plástico interactúa principalmente con los siguientes objetos que son los que se tienen que cuidar en un mantenimiento: unidad de inyección, tornillo, nariz y molde, como se puede observar en la figura 5. Es en estos componentes donde se pueden integrar las tecnologías del IIoT para medir las variables que permitan monitorear y controlar el proceso.

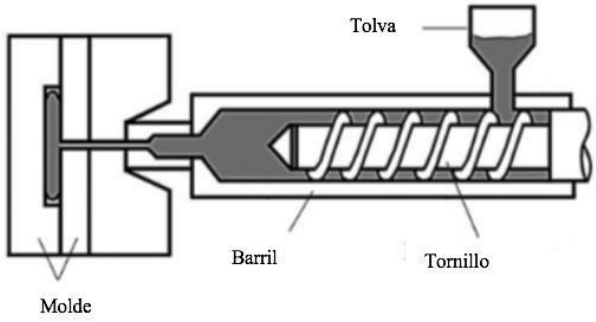


Figura 5. Vista general de componentes fundamentales que componen el moldeo por inyección de plástico (Zheng R., Tanner R.I., Fan XJ., 2011).

El objetivo de realizar esta revisión es documentar experiencias sobre la aplicación de tecnologías de IIoT o Industria 4.0 en el contexto de la industria de moldeo por inyección de plástico. A través de la búsqueda en fuentes de prestigio, se identifican bases científicas y técnicas sólidas empleadas en su implementación.

La revisión sigue las recomendaciones de PRISMA (Urrútia, G., & Bonfill, X., 2010), que guían en la búsqueda ordenada sobre diferentes aplicaciones documentadas en bases de datos de peso en la comunidad científica, donde además no se identificaron estudios de este tipo referentes a este campo de aplicación de la tecnología.

Los resultados que se reportan son útiles para que la comunidad relacionada con esta industria analice las experiencias derivadas de casos de implementación exitosos, y contribuyan a desarrollar una perspectiva de análisis que permita afrontar la problemática día a día en las celdas o líneas de producción, utilizando una visión centrada en el Internet de las Cosas y sus herramientas versátiles.

El resto del artículo está estructurado de la siguiente forma. La sección 2 presenta la metodología utilizada para la búsqueda del estado del arte contenida en el presente artículo, en la sección 3 podemos encontrar los resultados de dicha búsqueda organizado según sea el tipo de aplicación y su fuente de peso donde se puede encontrar la información y en la sección 4 se encuentra las conclusiones obtenidas en base a los casos recopilados, su utilidad y su posible utilización en el futuro.

2.- Metodología

Se plantea la siguiente metodología basada en el modelo PRISMA (Urrútia, G., & Bonfill, X., 2010) que, aunque está diseñada con enfoque en el campo de medicina, su estructura puede ser utilizada para la elaboración de revisiones actualizadas en otras áreas. El apartado de métodos fue implementado de la manera que se expone a continuación:

2.1 Métodos:

2.1.1 Criterios de elegibilidad:

Se busca que las publicaciones de consulta utilizadas cumplan con una antigüedad de no más de 5 años para la búsqueda de conceptos y principios. Con respecto a casos de éxito, el objetivo es recopilar integraciones exitosas para identificar la evolución de esta tecnología, se buscó que se cumplieran algunos principios explicados en la sección anterior. Las publicaciones se obtuvieron utilizando las siguientes cadenas de búsqueda, formuladas para obtener la mayor cantidad posible de resultados y mismas que se adaptaron a las condiciones de cada uno de los motores de búsqueda.

Cadenas de búsqueda:

- Industrial Internet of Things (IIoT)
- Molding 4.0
- Industry 4.0
- Injection Molding & Industry 4.0

2.1.2 Fuentes de información:

Las bases de datos e índices principales que se consideraron para la búsqueda de publicaciones se listan a continuación:

- IEEE Xplore
- Elsevier Science Direct
- Springer Link
- Scopus
- IoP Science
- ACM Digital Library

De manera complementaria, y a fin de encontrar documentos de interés adicionales, se consideraron las siguientes bases de datos auxiliares:

- ResearchGate
- Google Scholar

2.1.3 Búsqueda:

Para la fase de búsqueda y selección de documentos se siguieron los pasos mostrados en el diagrama de la figura 6 (Ibarra-Esquer, J., González-Navarro, F., Flores-Rios, B., Burtseva, L., & Astorga-Vargas, M., 2017), donde:

ST= cadena de búsqueda
SO= Fuente de búsqueda
SD= Documento seleccionado
J= Publicaciones en revistas / Journals
C= Publicaciones en conferencias.

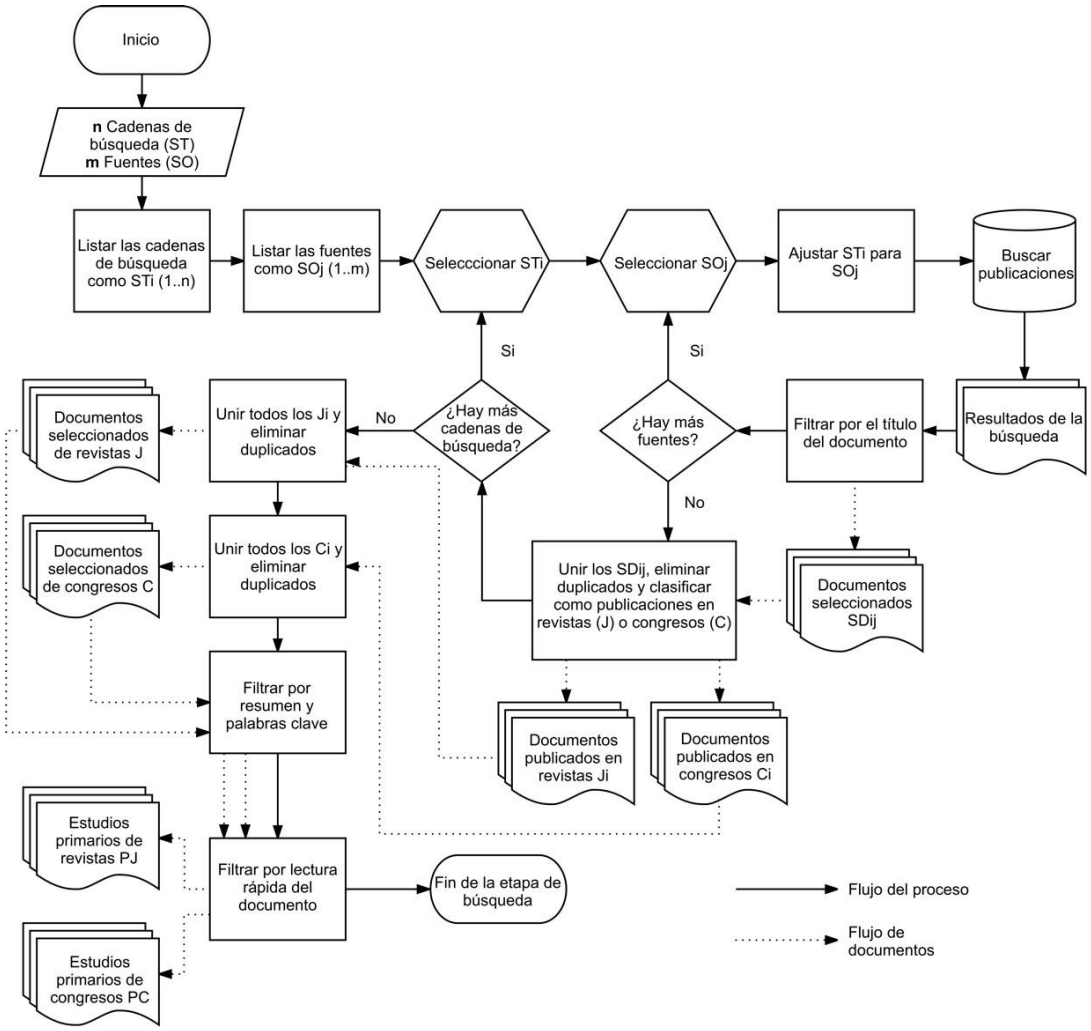


Figura 6. Diagrama de flujo para la etapa de búsqueda de la revisión de literatura (Ibarra-Esquer, J., González-Navarro, F., Flores-Rios, B., Burtseva, L., & Astorga-Vargas, M., 2017).

Se inicia con una lista de cadenas de búsqueda y un conjunto de fuentes de consulta o bases de datos. Cada cadena se adapta a los requerimientos del motor de búsqueda de cada fuente y de los documentos obtenidos se seleccionan aquellos que el título indique un interés potencial. Tras obtener los resultados de todas las fuentes, se identifican documentos duplicados y se eliminan, clasificando además entre documentos publicados en revistas y congresos. La operación se repite para cada cadena de búsqueda.

Al terminar, se integran los resultados de todas las fuentes y nuevamente se identifican y eliminan duplicados. Un segundo filtro consiste en revisar el resumen y palabras clave, llegando así a una selección de documentos más específica para los objetivos de la revisión. Los documentos restantes se someten a un proceso de lectura rápida, tras el cual se llega al conjunto de documentos que se tomará como resultados primarios de la revisión.

3.- Resultados

3.1 Resultados numéricos de búsqueda:

Después de aplicar los filtros se depuran los registros hasta obtener los documentos de interés para la correspondiente investigación, en las tablas se visualizan los resultados después de cada paso en la depuración según lo estipulado en la revisión sistemática de la figura 6, en la tabla 1 se encuentran todos los artículos encontrados con títulos alusivos al tema de interés encontrados en las bases de datos primarias y de soporte; en la tabla 2 se depuran estos resultados al revisar los resúmenes que contienen los documentos y seleccionar los que contienen casos de interés exitosos y en la tabla 3 se seleccionan en base a la revisión completa del contenido de los documentos.

Cadenas de búsqueda	Base de datos						
	IEEE Xplore Search	ScienceDirect	Springer Link	Scopus	IOP Science	Google Scholar	ResearchGate
Molding 4.0	2	6	0	1	0	0	0
Injection Molding & Industry 4.0	1	10	3	3	2	1	0
Industry 4.0	23	6	0	4	0	7	0
IIOT	8	1	0	8	0	4	1

Tabla 1. Artículos seleccionados en base a títulos. Fecha de consulta: Noviembre 2019.

Cadenas de búsqueda	Base de datos						
	IEEE Xplore Search	ScienceDirect	Springer Link	Scopus	IOP Science	Google Scholar	ResearchGate
Molding 4.0	2	6	0	1	0	0	0
Injection Molding & Industry 4.0	1	8	1	3	2	1	0
Industry 4.0	8	3	0	4	0	1	0
IIOT	3	1	0	8	0	4	1

Tabla 2. Artículos seleccionados en base a la revisión del resumen. Fecha de consulta: Noviembre 2019.

Cadenas de búsqueda	Base de datos					
	IEEE Xplore Search	ScienceDirect	Springer Link	Scopus	IOP Science	Google Scholar
Molding 4.0	1	6	0	1	0	0
Injection Molding & Industry 4.0	1	4	0	3	2	1
Industry 4.0	0	0	0	0	0	0
IIOT	1	0	0	0	0	0

Tabla 3. Artículos seleccionados en base a contenido. Fecha de consulta: Noviembre 2019.

Inicialmente se encontraron 90 documentos a partir de las cadenas de búsqueda y tomando como criterio de selección el título. A partir de la revisión de los resúmenes el número de documentos se redujo a 57. Una lectura rápida de los contenidos de los trabajos permitió filtrar y seleccionar los 20 documentos primarios para la revisión de literatura.

3.2 Selección de los estudios:

Siguiendo el diagrama de flujo en la figura 6, de los documentos de interés por contenido se seleccionaron los estudios donde se implementaron tecnologías de industria 4.0 o IIoT para la industria de moldeo por inyección de plástico. Estos se clasificaron cronológicamente para observar más de cerca la evolución que ha tenido la implementación de dichas tecnologías a lo largo del tiempo, así como las diferentes maneras de poder abordar la problemática que se plantea en cada caso de estudio. Los estudios seleccionados se muestran en la tabla 4, incluyendo la fuente de la que fueron obtenidos.

Año	Título de la publicación	Autor	Fuente
2020	Lean Manufacturing 4.0 of Polymeric Injection Molding Products.	Dănuţ-Sorin, I. R., Opran, C. G., & Lamanna, G.	*SCOPUS: Macromolecular Symposia*
2019	In-Mold Sensors for Injection Molding: On the Way to Industry 4.0. *Sensors*	Ageyeva, T., Horváth, S., & Kovács, J. G.	*SCOPUS: Sensors*
2019	AI Based Injection Molding Process for Consistent Product Quality.	Park, H. S., Phuong, D. X., & Kumar, S.	ELSEVIER: *Procedia Manufacturing*
2019	Injection Molding Technology: A New Frontier?: Industry 4.0 is changing the way injection molders fabricate parts.	Romeo, J.	SCOPUS: *Plastics Engineering*
2019	Mold ID Mold Die Tracking System	Balluff	Google Scholar
2018	Integration of artificial intelligence in an injection molding process for on-line process parameter adjustment.	Charest, M., Finn, R., & Dubay, R.	*Annual IEEE International Systems Conference (SysCon)*
2018	A case study on the analysis of an injection moulding machine energy data sets for improving energy and production management.	Rezende, J., Cosgrove, J., Carvalho, S. & Doyle, F.	SCOPUS: Eceee Industrial Summer Study Proceedings.
2018	A Study on Big Data Cluster in Smart Factory using Raspberry-Pi.	Kim, C.-S., & Son, S.-B.	*IEEE International Conference on Big Data (Big Data)*
2018	Real-time parameter optimization based on neural network for smart injection molding.	Lee, H., Liau, Y., & Ryu, K.	*IOP Conference Series: Materials Science and Engineering*
2018	Cloud-based Manufacturing Blockchain: Secure Knowledge Sharing for Injection Mould Redesign.	Li, Z., Liu, L., Barenji, A. V., & Wang, W.	ELSEVIER: *Procedia CIRP*
2018	Optimization of mold thermal control for minimum energy consumption in injection molding of polypropylene parts.	Lucchetta, G., Masato, D., & Sorgato, M.	ELSEVIER: *Journal of Cleaner Production*
2018	Monitoring and Control for Thermoplastics Injection Molding A Review.	Ogorodnyk, O., & Martinsen, K.	ELSEVIER: *Procedia CIRP*
2018	Advanced CPS Service Oriented Architecture for Smart Injection Molding and Molds 4.0.	Siller, H. R., Romero, D., Rabelo, R. J., & Vazquez, E.	IEEE: *International Conference on Intelligent Systems (IS)*

2017	The Implementation of Cloud Platform for Injection Molding Process	Jong, W.-R., Chen, S.-C., Wang, S.-M., Liu, S.-H., Liao, H.-L., Ting, Y.-H., & Chen, H.-T.	ELSEVIER: *Procedia CIRP*
2017	A Framework of a Smart Injection Molding System Based on Real-time Data	Lee, H., Ryu, K., & Cho, Y.	*ELSEVIER: Procedia Manufacturing*
2017	Internet-of-Things Enabled Real-time Monitoring of Energy Efficiency on Manufacturing Shop Floors	Tan, Y. S., Ng, Y. T., & Low, J. S. C.	ELSEVIER: *Procedia CIRP*,
2017	Knowledge elicitation for fault diagnostics in plastic injection moulding: A case for machine-to-machine communication.	Vrabič, R., Kozjek, D., & Butala, P.	ELSEVIER: *CIRP Annals*
2017	A novel vision-based mold monitoring system in an environment of intense vibration	Hu, F., He, Z., Zhao, X., & Zhang, S.	IOP SCIENCE: *Measurement Science and Technology*
2016	Customization of mass-produced parts by combining injection molding and additive manufacturing with Industry 4.0 technologies	Gaub, H.	*ELSEVIER: Reinforced Plastics*
2014	A principal component analysis model-based predictive controller for controlling part warpage in plastic injection molding.	Zhang, S., Dubay, R., & Charest, M.	ELSEVIER: *Expert Systems with Applications*

Tabla 4. Estudios seleccionados para la revisión.

3.3 Proceso de extracción de datos:

Una vez que se recopilan los documentos de interés elegidos por medio del resumen en el paso final, se procede a identificar el objetivo de cada uno de los casos de estudio, ya sea que se tenga un objetivo cuantitativo o cualitativo. También se busca identificar los métodos de aplicación con respecto a las tecnologías de industria 4.0, contratiempos y resultados finales en cada caso.

3.4 Datos, medidas y casos de aplicación:

Como se ha podido apreciar hasta este momento y basados en la teoría anteriormente referida con respecto al proceso de moldeo por inyección de plástico, los principales parámetros que influyen en la calidad de la pieza y en el proceso son temperaturas y presiones. Con temperaturas nos referimos a temperatura en la unidad de inyección, en la materia prima, en la herramienta y al final en la pieza moldeada. Esto define nuestro producto en base a las especificaciones que se buscan cumplir por parte del cliente, requerimientos que se ven priorizados y en control por implementación de industria 4.0.

Dado que esto es foco de interés, se han planteado a lo largo del tiempo diferentes soluciones para controlar estas variables. Resumiendo los resultados de estas implementaciones podemos ver que en (Zhang, S., Dubay, R., & Charest, M., 2014), (Tan, Y. S., Ng, Y. T., & Low, J. S. C., 2017), (Vrabič, R., Kozjek, D., & Butala, P., 2017), (Hu, F., He, Z., Zhao, X., & Zhang, S., 2017), (Siller, H. R., Romero, D., Rabelo, R. J., & Vazquez, E., 2018), (Ogorodnyk, O., & Martinsen, K., 2018), (Lucchetta, G., Masato, D., & Sorgato, M., 2018), (Ageyeva, T., Horváth, S., & Kovács, J. G., 2019), (Park, H. S., Phuong, D. X., & Kumar, S., 2019), (Lee, H., Liau, Y., & Ryu, K., 2018) y (Charest, M., Finn, R., & Dubay, R., 2018) se utiliza tecnología de sensores de temperatura y presiones en las cavidades de los moldes; cada una de las implementaciones ha tomado diferentes medidas en acondicionar las herramientas y las máquinas para poder recopilar los datos, mientras que en los casos donde se ha realizado integración de tecnología, se ha buscado que esta sea la adecuada para obtener los resultados deseados, sobre todo en (Ageyeva, T., Horváth, S., & Kovács, J. G., 2019) donde se proponen diferentes maneras de obtener los datos del comportamiento de plástico por medio de tecnologías diversas.

Existen implementaciones donde se destaca el uso de análisis de datos para optimizar el piso de producción (Gaub, H., 2016), (Lucchetta, G., Masato, D., & Sorgato, M., 2018). Se proponen diferentes arquitecturas o encuadres como marco para el desarrollo de operaciones de acuerdo con un esquema de Industria 4.0, un esquema de arquitectura de comunicación entre maquinarias, el desarrollo de una metodología de manufactura esbelta con enfoque de Industria 4.0 (Dănuţ-Sorin, I. R., Opran, C. G., & Lamanna, G., 2020), (Lee, H., Ryu, K., & Cho, Y., 2017), (Romeo, J., 2019), (Vrabič, R., Kozjek, D., & Butala, P., 2017).

También se encuentran propuestas orientadas a priorizar la calidad del producto en cuestión (Jong, W.-R., Chen, S.-C., Wang, S.-M., Liu, S.-H., Liao, H.-L., Ting, Y.-H., & Chen, H.-T., 2017), así como el planteamiento de toda una plataforma de seguimiento para el desarrollo de nuevos productos desde su inicio hasta el final, recopilando la información completa en una base de datos (Li, Z., Liu, L., Barenji, A. V., & Wang, W., 2018). En términos de implementaciones de tecnología de IIoT o Industria 4.0, los autores en (Kim, C.-S., & Son, S.-B., 2018) plantean que no es necesario un equipo costoso para poder realizar una implementación exitosa, mientras que en (Romeo, J., 2019) se muestra el alcance del beneficio de utilizar estas tecnologías.

Así mismo (Balluff, 2019) ofrece tecnologías de industria 4.0 para la optimización del recurso físico por medio de rastreo de objetos que se virtualizan y propician una entrada al sistema de mantenimiento que se alimenta automáticamente, obteniendo un sistema de gestión de objetos a nivel industrial bastante efectivo.

En la tabla 5 se presentan los casos para cada tipo de implementación encontrada, se observa que mayormente esta tecnología está siendo aplicada para la adquisición de datos dentro de los procesos. Además, para cada caso se menciona el segmento de tecnologías que fueron utilizadas en la implementación.

TIPO DE IMPLEMENTACIÓN	CASO APLICADO	TECNOLOGÍAS 4.0
Aplicación de tecnologías IoT para adquisición de datos en proceso	Ageyeva, T., Horváth, S., & Kovács, J. G. (2019).	• Edge
	Charest, M., Finn, R., & Dubay, R. (2018).	• Edge • A.I. Algorithms
	Hu, F., He, Z., Zhao, X., & Zhang, S. (2017).	• Edge • A.I. Algorithms • Big data processing
	Lee, H., Liau, Y., & Ryu, K. (2018).	• Edge • A.I. Algorithms • Big data processing • Business Intelligence • Real time Monitoring
	Lucchetta, G., Masato, D., & Sorgato, M. (2018).	• Edge
	Ogorodnyk, O., & Martinsen, K. (2018).	• A.I. Algorithms • Real time Monitoring
	Park, H. S., Phuong, D. X., & Kumar, S. (2019).	• Edge • A.I. Algorithms • Big data processing
	Siller, H. R., Romero, D., Rabelo, R. J., & Vazquez, E. (2018).	• Edge • A.I. Algorithms • Big data processing • Cloud computing • Real time monitoring • Business Intelligence
	Tan, Y. S., Ng, Y. T., & Low, J. S. C. (2017).	• Edge • Cloud computing • Real time monitoring • Big data processing
	Vrabič, R., Kozjek, D., & Butala, P. (2017).	• Edge • A.I. Algorithms • M2M • Big data processing

	Zhang, S., Dubay, R., & Charest, M. (2014).	• Edge • A.I. Algorithms
Desarrollo de encuadres y despliegue de arquitectura	Dănuţ-Sorin, I. R., Opran, C. G., & Lamanna, G. (2020).	• Edge • A.I. Algorithms • Big data processing • Cloud computing • Real time monitoring • Business Intelligence
	Lee, H., Ryu, K., & Cho, Y. (2017).	• Edge • A.I. Algorithms • Cloud computing • Real time monitoring • M2M
	Kim, C.-S., & Son, S.-B. (2018).	• Edge • A.I. Algorithms • Big data processing • Cloud computing
	Romeo, J. (2019).	• Edge • A.I. Algorithms • Big data processing • Cloud computing • Real time monitoring • Business Intelligence
	Vrabič, R., Kozjek, D., & Butala, P. (2017).	• Edge • A.I. Algorithms • M2M • Big data processing
Análisis de la información en piso de producción	Gaub, H. (2016).	• Business Intelligence • A.I. Algorithms • Cloud computing
	Lucchetta, G., Masato, D., & Sorgato, M. (2018).	• Edge
	Balluff (2019)	• Edge
Análisis de calidad	Jong, W.-R., Chen, S.-C., Wang, S.-M., Liu, S.-H., Liao, H.-L., Ting, Y.-H., & Chen, H.-T. (2017).	• Edge • A.I. Algorithms • Big data processing • Cloud computing • Business Intelligence
	Tan, Y. S., Ng, Y. T., & Low, J. S. C. (2017).	• Edge • Cloud computing • Real time monitoring • Big data processing
	Rezende, J., Cosgrove, J., Carvalho, S. & Doyle, F. (2018).	• Edge • Real time monitoring • Big data processing
	Li, Z., Liu, L., Barenji, A. V., & Wang, W. (2018).	• Edge • Cloud computing • Big data processing
	Park, H. S., Phuong, D. X., & Kumar, S. (2019).	• Edge • A.I. Algorithms • Big data processing

Tabla 5. Casos por tipo de implementación de tecnologías para IIoT.

En la literatura se encuentran publicaciones relacionadas con Industria 4.0 e IIoT y las definiciones y conceptos que las rodean desde 2011. Así mismo, la utilización de tecnologías que implican estos conceptos aplicados en integraciones para el área de manufactura ha ido en aumento, encontrando más casos conforme pasan los años. En este caso particular, donde el enfoque está en la industria de moldeo por inyección de plástico, se encuentra una evolución desde 2014 trabajando con la definición y en cómo se asimila el encuadre de industria 4.0 a este tipo de industria en particular. Se encuentra evidencia con respecto a la utilización de diversas plataformas o arquitecturas para facilitar el trabajo, así como herramientas de minería de datos aplicadas a la eficiencia del proceso.

3.5 Riesgo de sesgo en los estudios individuales:

Dado que se busca encontrar la evidencia de casos lo más actuales posibles, una cantidad importante de esta indica que se están evaluando prototipos o nuevas propuestas de cómo abordar problemáticas. En este sentido los resultados aún no son muy claros, sin embargo, las propuestas de solución implementando estas nuevas herramientas son de interés para la perspectiva de evolución de tecnologías de Industria 4.0. Por lo anterior, este tipo de información documentada se puede encontrar en bases de datos o fuentes de información de menos peso pero que proporcionan un mayor volumen de resultados y acceso a los mismos, como son Google Scholar o ResearchGate. Su uso es como fuente de información auxiliar, puesto que en estas bases de datos se pueden encontrar estudios realizándose actualmente, avances de implementaciones, prototipos o revisiones de propuestas antes implementadas con nuevos enfoques. Es por lo que, si bien sirven para darnos una guía, se tiene que evaluar un tanto más a fondo las referencias o alcance de los estudios que están reportando dichos resultados.

4.- Conclusiones

La industria 4.0 se ha visto en aumento con el tiempo debido a las ventajas que estas tecnologías proveen para el desarrollo productivo de los negocios. La información que pueden entregar es de suma utilidad, al recopilar en tiempo real los datos que permiten recrear eventos que se llevaron a cabo en un momento especifico de interés. Una de las ventajas en la actualidad con respecto a la implementación de estas tecnologías reside en su valor adquisitivo ya que se mantiene competitivo con dispositivos o integraciones que son simples y no incluyen dichas tecnologías, haciéndose más fácil para los usuarios tomar la decisión de adquirirlas ya sea para su implementación en ambientes hostiles, en ambientes domésticos o de oficina que resultan en un despliegue más económico. Además, para obtener de manera eficaz el método correcto de gestionar los procesos, las herramientas para el procesamiento de grandes volúmenes de información o “big data” se vuelven fundamentales. En este caso en particular, dada la naturaleza de moldeo por inyección de plástico, las herramientas de minería de datos e inteligencia artificial juegan un papel muy importante ya que permiten detectar fallas en el proceso o piezas no conformantes que afectan la cadena de suministro. La revisión presentada en este documento es una compilación de integraciones efectuadas en la industria de moldeo por inyección de plástico desde gestión en el piso de producción, desarrollo de productos en etapas de prototipo o evaluación hasta la mejora del proceso de producción en masa, con el fin de facilitar métodos de ingeniería en procesos útiles en la industria de moldeo por inyección de plástico. Así, esta recopilación funciona como una herramienta de consulta para los campos de ingeniería en la industria de moldeo por inyección de plástico.

5.- Referencias:

1.- Ageyeva, T., Horváth, S., & Kovács, J. G. (2019). In-Mold Sensors for Injection Molding: On the Way to Industry 4.0. *Sensors*, *19*(16), 3551. https://doi.org/10.3390/s19163551

2.- Balluff (2019) Mold ID. Disponible en: https://assets.balluff.com/WebBinary1/LIT_BRO_MOLD_ID_EN_H17_DRW_920549_02_000.pdf Fecha de consulta: Noviembre 2019.

3.- Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, *101*, 1-12. https://doi.org/10.1016/j.compind.2018.04.015

4.- Charest, M., Finn, R., & Dubay, R. (2018). Integration of artificial intelligence in an injection molding process for on-line process parameter adjustment. *2018 Annual IEEE International Systems Conference (SysCon)*, 1-6. https://doi.org/10.1109/SYSCON.2018.8369500

5.- Dănuţ-Sorin, I. R., Opran, C. G., & Lamanna, G. (2020). Lean Manufacturing 4.0 of Polymeric Injection Molding Products. *Macromolecular Symposia*, *389*(1), 1900109. https://doi.org/10.1002/masy.201900109

6.- Drath, R., & Horch, A. (2014). Industrie 4.0: Hit or Hype? [Industry Forum]. *IEEE Industrial Electronics Magazine*, *8*(2), 56-58. https://doi.org/10.1109/MIE.2014.2312079

7.- Forschungsunion, ACATECH (NATIONAL ACADEMY OF SCIENCE AND ENGINEERING). (2013). Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Disponible en: https://en.acatech.de/publication/recommendations-for-implementing-the-strategic-initiative-industrie-4-0-final-report-of-the-industrie-4-0-working-group/. Fecha de consulta: Octubre 2019.

8.- Gaub, H. (2016). Customization of mass-produced parts by combining injection molding and additive manufacturing with Industry 4.0 technologies. *Reinforced Plastics*, *60*(6), 401-404. https://doi.org/10.1016/j.repl.2015.09.004

9.- Greer, C., Burns, M., Wollman, D., & Griffor, E. (2019). *Cyber-physical systems and internet of things* (N.º NIST SP 1900-202; p. NIST SP 1900-202). https://doi.org/10.6028/NIST.SP.1900-202

10.- Griffor, E. R., Greer, C., Wollman, D. A., & Burns, M. J. (2017). *Framework for cyber-physical systems: Volume 1, overview* (N.º NIST SP 1500-201; p. NIST SP 1500-201). https://doi.org/10.6028/NIST.SP.1500-201 Fecha de consulta: Octubre 2019.

11.- Hu, F., He, Z., Zhao, X., & Zhang, S. (2017). A novel vision-based mold monitoring system in an environment of intense vibration. *Measurement Science and Technology*, *28*(10), 105906. https://doi.org/10.1088/1361-6501/aa8537

12.- Ibarra-Esquer, J., González-Navarro, F., Flores-Rios, B., Burtseva, L., & Astorga-Vargas, M. (2017). Tracking the Evolution of the Internet of Things Concept Across Different Application Domains. *Sensors*, *17*(6), 1379. https://doi.org/10.3390/s17061379

13.- Industrial Internet Consortium Vocabulary Task Group in the Technology Working Group, co-chaired by Anish Karmarkar (Oracle) and Robert Martin (MITRE). “The Industrial Internet of Thing, Volume G8: Vocabulary” IIC:PUB:G8:V2.1:PB:20180822. Disponible en:

https://www.iiconsortium.org/pdf/IIC_Vocab_Technical_Report_2.1.pdf . Fecha de consulta: Octubre 2019.

14.- Jong, W.-R., Chen, S.-C., Wang, S.-M., Liu, S.-H., Liao, H.-L., Ting, Y.-H., & Chen, H.-T. (2017). The Implementation of Cloud Platform for Injection Molding Process. *Procedia CIRP*, *63*, 219-223. https://doi.org/10.1016/j.procir.2017.03.117

15.- Kim, C.-S., & Son, S.-B. (2018). A Study on Big Data Cluster in Smart Factory using Raspberry-Pi. *2018 IEEE International Conference on Big Data (Big Data)*, 5360-5362. https://doi.org/10.1109/BigData.2018.8622539

16.- Klaus Schwab (2016), La cuarta revolución industrial, en Penguin Random House Grupo Editorial España, Disponible en: https://www.overdrive.com/search?q=111C4347-2121-4AE1-9B18-7C584195F118 Fecha de consulta: Octubre 2019.

17.- Lee, H., Liau, Y., & Ryu, K. (2018). Real-time parameter optimization based on neural network for smart injection molding. *IOP Conference Series: Materials Science and Engineering*, *324*, 012076. https://doi.org/10.1088/1757-899X/324/1/012076

18.- Lee, H., Ryu, K., & Cho, Y. (2017). A Framework of a Smart Injection Molding System Based on Real-time Data. *Procedia Manufacturing*, *11*, 1004-1011. https://doi.org/10.1016/j.promfg.2017.07.206

19.- Li, Z., Liu, L., Barenji, A. V., & Wang, W. (2018). Cloud-based Manufacturing Blockchain: Secure Knowledge Sharing for Injection Mould Redesign. *Procedia CIRP*, *72*, 961-966. https://doi.org/10.1016/j.procir.2018.03.004

20.- Lucchetta, G., Masato, D., & Sorgato, M. (2018). Optimization of mold thermal control for minimum energy consumption in injection molding of polypropylene parts. *Journal of Cleaner Production*, *182*, 217-226. https://doi.org/10.1016/j.jclepro.2018.01.258

21.- Ogorodnyk, O., & Martinsen, K. (2018). Monitoring and Control for Thermoplastics Injection Molding A Review. *Procedia CIRP*, *67*, 380-385. https://doi.org/10.1016/j.procir.2017.12.229

22.- Park, H. S., Phuong, D. X., & Kumar, S. (2019). AI Based Injection Molding Process for Consistent Product Quality. *Procedia Manufacturing*, *28*, 102-106. https://doi.org/10.1016/j.promfg.2018.12.017

23.- Rezende, J., Cosgrove, J., Carvalho, S. & Doyle, F. (2018). A case study on the analysis of an injection moulding machine energy data sets for improving energy and production management. Eceee Industrial Summer Study Proceedings. Volume 2018-June, 2018, Pages 231-238.

24.- Romeo, J. (2019). Injection Molding Technology: A New Frontier?: Industry 4.0 is changing the way injection molders fabricate parts. *Plastics Engineering*, *75*(4), 32-37. https://doi.org/10.1002/peng.20107

25.- Siller, H. R., Romero, D., Rabelo, R. J., & Vazquez, E. (2018). Advanced CPS Service Oriented Architecture for Smart Injection Molding and Molds 4.0. *2018 International Conference on Intelligent Systems (IS)*, 428-434. https://doi.org/10.1109/IS.2018.8710575

26.- Stankovic, J. (2014, February). Research Directions for the Internet of Things. IEEE Internet of Things Journal, 1(1), 3-9. https://doi:10.1109/JIOT.2014.2312291

27.- Tan, Y. S., Ng, Y. T., & Low, J. S. C. (2017). Internet-of-Things Enabled Real-time Monitoring of Energy Efficiency on Manufacturing Shop Floors. *Procedia CIRP*, *61*, 376-381. https://doi.org/10.1016/j.procir.2016.11.242

28.- Urrútia, G., & Bonfill, X. (2010). Declaración PRISMA: Una propuesta para mejorar la publicación de revisiones sistemáticas y metaanálisis. *Medicina Clínica*, *135*(11), 507-511. https://doi.org/10.1016/j.medcli.2010.01.015

29.- Vogel-Heuser, B., & Hess, D. (2016). Guest Editorial Industry 4.0–Prerequisites and Visions. *IEEE Transactions on Automation Science and Engineering*, *13*(2), 411-413. https://doi.org/10.1109/TASE.2016.2523639

30.- Vrabič, R., Kozjek, D., & Butala, P. (2017). Knowledge elicitation for fault diagnostics in plastic injection moulding: A case for machine-to-machine communication. *CIRP Annals*, *66*(1), 433-436. https://doi.org/10.1016/j.cirp.2017.04.001

31.- Yong Yin, Kathryn E. Stecke & Dongni Li (2018) The evolution of production systems from Industry 2.0 through Industry 4.0, International Journal of Production Research, 56:1-2, 848-861, DOI: 10.1080/00207543.2017.1403664

32.- Zhang, S., Dubay, R., & Charest, M. (2014). A principal component analysis model-based predictive controller for controlling part warpage in plastic injection molding. *Expert Systems with Applications*, *42*(6), 2919-2927. https://doi.org/10.1016/j.eswa.2014.11.030

33.- Zheng R., Tanner R.I., Fan XJ. (2011) Introduction. In: Injection Molding. Springer, Berlin, Heidelberg https://doi.org/10.1007/978-3-642-21263-5

Notas Bibliográficas de los Autores:

Nombre: Jesus Ivan Aguilar Lugo
Adscripción: ivan_lugo
Correo electrónico: jesus.aguilar@uabc.edu.mx

"Ingeniero en Electrónica por la Universidad Autónoma de Baja California, México. Estudiante de Posgrado en Ingeniería y Ciencias por parte de la Facultad de Ingeniería en Universidad Autónoma de Baja California. Actualmente desempeña el cargo de Ingeniero de diseño y manufactura en el área de moldeo por inyección de plásticos donde diseña herramentales, gestiona mejoras en las líneas de producción y automatiza procesos industriales."

Nombre: Jorge Eduardo Ibarra Esquer
Adscripción: jorgeeie
Correo electrónico: jorge.ibarra@uabc.edu.mx

"Ingeniero en Electrónica por el Instituto Tecnológico de Sonora, México. Maestro en Ciencias de la Computación por el Centro de Investigación Científica y de Educación Superior de Ensenada. Doctor en Ciencias de la Computación por la Universidad Autónoma de Baja California.

Profesor de tiempo completo en la Facultad de Ingeniería de la Universidad Autónoma de Baja California, adscrito al programa educativo Ingeniero en Computación.

Responsable de seguimiento a la trayectoria estudiantil en la Facultad de Ingeniería de la Universidad Autónoma de Baja California."

Nombre: Marlenne Angulo Bernal
Adscripción: mangulo
Correo electrónico: mangulo@uabc.edu.mx

"Ingeniero en Electrónica por el Instituto Tecnológico de Sonora, México. Maestra en Ciencias en Electrónica y Telecomunicaciones por el Centro de Investigación Científica y de Educación Superior de Ensenada. Actualmente se encuentra adscrita al programa Ing. en Electrónica de la Facultad de Ingeniería de la Universidad Autónoma de Baja California. Sus áreas de interés están relacionadas con redes de comunicaciones y ciencia de datos."

COMPUTACION E INFORMATICA

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

Aceptado *05/03/2021*

Cybersecurity Ontologies: A Systematic Literature Review

Revisión sistemática de la literatura sobreontologías en ciberseguridad

William Fernando Borja Rivadeneira[2]
william.f.borja.r@pucesa.edu.ec

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

[1]GrIISoft Research Group, Escuela Superior Politécnica de Chimborazo, Riobamba,Ecuador.

[2]Pontificia Universidad Católica del Ecuador Sede Ambato, Ambato, Ecuador

Abstract: Cybersecurity is a young discipline that has gained relevance in our modern society. This research reports the findings of a systematic review of the literature on ontologies in the field of cybersecurity. From an initial set of 214 papers on the subject, 50 relevant papers were selected for this SLR. With these documents we answered research questions related to the domains in which ontologies are reported, the methodologies, tools and languages used, and the verification and validation mechanisms reported. As results, we observed that the largest number of ontologies are classified in the domains of infrastructure and networking, software and human factor. Regarding the papers that report the use of a methodology for developing the ontologies (12%), Methontology is the commonly used one. Protégé, in conjunction with the OWL language, are the preferred tools for ontology development. Regarding verification and validation (V&V) mechanisms, we observe that more than half (62%) report the application of V&V mechanisms to their ontologies.

Keywords: Systematic Literature Review, Ontology, Cyber-security, Cybersecurity Ontologies, ICT.

Resumen: La ciberseguridad es una disciplina joven que ha tomado relevancia en nuestra sociedad moderna. En la presente investigación se reportan los hallazgos de una revisión sistemática de la literatura sobre ontologías en el ámbito de la ciberseguridad. De un conjunto inicial de 214 documentos sobre el tema, para la presente SLR se utilizaron 50 documentos relevantes. Con estos documentos se respondieron preguntas de investigación relacionadas con los dominios en los que se reportan las ontologías, las metodologías, herramientas y lenguajes usados, así como los mecanismos de verificación y validación reportados. Con respecto a los resultados observamos que el mayor número de ontologías se clasifican en los dominios de infraestructura y networking, software y factor humano, dentro del porcentaje de documentos en los que se reporta el uso de alguna metodología para el desarrollo de ontologías (12%), methontology es la metodología comúnmente usada. Protege en conjunto con el lenguaje OWL es la herramienta de preferencia para el desarrollo de ontologías. En cuando a los mecanismos de verificación y validación, observamos que poco más de la mitad (62%) reporta algún mecanismo de V&V.

Palabras Claves: Revisión Sistemática de la Literatura, Ontología, Ciber-seguridad, Ontologías de Ciberseguridad, ICT.

INTRODUCTION

There is no doubt that Information and Communications Technology (ICT) has significantly revolutionized the knowledge society in which we are immersed. Advances in software, hardware and telecommunications have managed to converge in different sectors of our society, offering modern solutions. However, due to the massification of TICs, issues related to vulnerabilities and threats in software, hardware and telecommunications have arisen.

Cybersecurity is a young discipline aimed at protecting vulnerabilities or minimizing threats to technological infrastructure such as software, hardware and telecommunications (Thakur and Pathan, 2014). Although knowledge about cybersecurity issues is mostly held by people involved in the ICT arena, due to massive use of ICT, knowledge about cybersecurity should be extended to the general public (Singer and Friedman, 2014).

Knowledge about cybersecurity has been gradually built up thanks to the diversity of contributions made by different experts in this field. A portion of these contributions have focused on creating ontologies that help to define, represent and organize a vocabulary of concepts (Neches et al., 1991) related to this discipline. These ontologies provide a shared knowledge on the different aspects of cybersecurity. In order to have a better understanding of ontologies reported in the field of cybersecurity, this paper presents the results of a systematic review of the literature on the various ontologies that have been reported in the context of cybersecurity.

The rest of the document is organized as follows: Section II presents some generalities about ontologies; Section III describes the method used in which the research questions to be answered by this systematic review are framed. Section IV presents the results with respect to the specified research questions. Finally, section V discusses the results and presents the conclusions.

ONTOLOGIES

In the origins of Western thought, ontology was considered a discipline related to philosophy. It was oriented to the study of the existing (entities) and their relationships. In a general way, an ontology can be defined as a vocabulary, in which entities, classes, properties, predicates, functions and the relations between these elements are stated. An ontology is important because it enables sharing knowledge regarding a particular domain.

In the literature we can find different approaches or methods to create ontologies (Lenat and Guha, 1990; Uschold and King, 1995; Grüninger and Fox, 1995; Bernaras et al., 1996; Fernandez et al., 1997; Swartout et al., 1997; Staab et al., 2001; KBSI, 1994). For example, in (Lenat and Guha 1990) authors propose an approach for the creation of ontologies that support intelligent systems based on knowledge. Similarly, in (Uschold and King, 1995) authors propose an ontology construction method aimed at capturing knowledge, coding it and integrating it with existing ontologies. In the case of (Grüninger and Fox, 1995), authors propose a methodology that allows the development of systems based on first-order knowledge; in addition, taking advantage of the robustness of classical logic as a guide to transform informal systems into computational ones.

This methodology focuses on identifying the main scenario for the construction of ontologies. On the other hand, in (Bernaras et al., 1996), the Kactus methodology is presented. It focuses on the construction of ontologies considering a knowledge base that uses a process of abstraction, where the context of the entities is specified. One of the widely known methodology is Methontology, proposed by Juristo (Fernandez et al., 1997). It helps to create a new ontology as well as reusing existing ones. This methodology fits into a development process based on the creation of prototypes.

The SENSUS method (Swartout et al., 1997) is another approach, it uses existing ontologies creating an ontology skeleton, the resulting prototype eliminates terms irrelevant to the domain knowledge. Another methodology is Onto-Knowledge (Staab et al., 2001), a project that supports the development of ontologies for knowledge management. Finally, in (KBSI, 1994), authors mention the KBSI IDEF5 method, which is a method that allows and helps in the creation, modification and maintenance of ontologies.

Tools are also relevant in developing ontologies. Examples of these tools are: Ontolingua Server (Farquhar et al., 1997), Ontosaurus (Swartout et al., 1997), Protégé (Noy et al., 2000), WebODE (Arpírez et al., 2003), OntoEdit (Sure et al., 2002), among others. One tool that is commonly used in the creation of ontologies is Protégé (Noy et al., 2000), which is an independent open-source tool that has an extensible architecture. Its main core is the ontology editor, that its functionality can be extended through the use of plug-ins.

Another tool that supports the creation of ontologies is Ontosaurus (Swartout et al., 1997). It consists of two modules: an ontology server that uses a knowledge representation system and a web browser that allows editing and exploring ontologies using HTML. It is worth to note that several of these tools have their own ontology development language. Examples of these languages are: XOL (XML-Based Ontology Exchange Language) (Karp et al., 1999); SHOE (Simple HTML Ontology Extensions) (Luke and Heflin, 2000); which is an extension of HTML, DAML+OIL (Horrocks and van Harmelen, 2001) and OWL (Web Ontology Language) (Dean and Schreiber,2003).

These languages vary according to their use; besides considering that these languages can be integrated through extensions or APIs established by the provider of these languages. OWL (Dean and Schreiber, 2003) is one of the languages commonly used by ontology developers. OWL is aimed at publishing and sharing ontologies developed on the Web. OWL is a derivation of DAML+OIL (Horrocks and van Harmelen, 2001) which shares some of its functionalities.

When an ontology is developed, an important aspect to take into account is the one related to their verification and validation (V&V) (Raad and Cruz, 2015). It can be approached from two perspectives: with regards to its quality and with regards to its correctness (Raad and Cruz, 2015). In the literature we can find some approaches that address the verification and validation of an ontology, such as: the gold standard approach (Ulanov et al., 2010); corpus-based (Brewster et al., 2004); task-based (Welty et al., 2003) and criteria-based (Fernandez et al., 2009). As for the gold standard approach (Ulanov et al., 2010), it focuses on comparing the developed ontology with a reference ontology created with certain criteria.

On the other hand, the corpus-based approach (Brewster et al., 2004), consists in evaluating the coverage of an ontology with one or several ontologies through a corpus in which the determined domain is significantly covered. In the case of the task-based approach (Welty et al., 2003), the evaluation of an ontology is aimed at a specific task, based on the results obtained to improve the knowledge of this task. Another approach consists in validating the ontology according to a desirable criterion (Raad and Cruz, 2015), such as its structure (Fernandez et al., 2009), where for example the number of nodes that an ontology has is used, or more complex criteria may be used.

Another approach is based on experts (Alani and Brewster, 2006), for example, evaluations are based on the coincidences of classes, density and intermediation that are detailed in the ontology. Some support tools for V&V tasks are OntoMetric (Lozano et al., 2004), natural language application metrics (Hartmann et al., 2004), OntoClean (Gangemi et al., 2002); EvaLexon (Spyns et al., 2004) and OOPS! (Poveda et al., 2015). For example, OntoClean (Gangemi et al., 2002), allows the evaluation of an ontology based on its taxonomic structure. Another case is OOPS! (Poveda et al., 2015), a tool that scans an ontology by using a URL to find possible inconsistencies that may affect the modeling of it.

METHOD

The guideline described in (Kitchenham, 2004) was followed in order to conduct the Systematic Literature Review (SLR) here reported. According to (Kitchenham, 2004), the realization of a SLR is divided into three phases: planning, execution and reporting, following we describe each of these phases in our context.
As part of the planning phase, the protocol for this SLR was developed. It sets out the research questions, as well as the objectives of this research. In this phase, the source for searching, the search string, and the inclusion and exclusion criteria are also defined. In the second phase (execution) the protocol is run, in this phase we proceed with the searches of documents with respect to the search string defined in the protocol, we also carry out the discrimination of the documents according to the inclusion and exclusion criteria defined in the protocol, we also carry out the analysis and synthesis of the relevant documents (selected papers). Finally, the third phase corresponds to the presentation of the results of this SLR.

The main objective of this SLR is to gain a better understanding of reported ontologies related to cybersecurity domain. With respect to this objective, the following research questions have been posed.

- RQ1. What areas of cybersecurity are the ontologies reported in?
- RQ2. What methods or approaches have been used for the development of the selected ontologies?
- RQ3. What tools have been used for the construction of the reported ontologies?
- RQ4. Have the reported ontologies been validated?

Identification and selection of the searching source

For the present work, the Scopus database has been chosen. It contains the largest number of abstracts and citations in the scientific literature as well as offers a search engine with advanced searching options.

Definition of the search string

The search string has been defined with different terms based on the subject matter of this SLR, these terms have been combined with logical operators, resulting in the following search string:

TITLE-KEY-ABS(ontology AND (cyber-security OR cybersecurity OR “cyber security”))

Inclusion Criteria(CI) and Exclusion Criteria (CE)

We filtered the selection of primary studies (documents on the subject) in terms of the following inclusion and exclusion criteria. The primary studies were selected based on the title, abstract and keywords in order to determine whether they are identified as relevant ones, documents were selected taking into account compliance with the following inclusion criteria: papers reporting cybersecurity ontologies written in English language. These papers should be published in prestigious indexed venues such as journals, proceedings and book chapters subject to a peer review process. In the same way, those papers that met some of the following exclusion criteria were not considered for this SLR: duplicated papers, papers whose main contribution is not related with cybersecurity ontologies, poster papers, non-English written papers, and short communications such as letters to the editor.

Execution

Once the protocol was defined, we proceeded with the execution phase. The previously defined search string was executed in September 2020, using the Scopus database search engine. It is worth to note that Scopus is one of the biggest abstract and citation database in the arena of scientific literature. Initially 214 document results were obtained after running the search string. After applying the inclusion and exclusion criteria on titles, abstracts and keywords, 72 documents were selected (first filter).

From this selection, the complete content of 69 documents was accessed. After analyzing the content of these documents, 19 were discarded, so finally 50 documents were considered for this review (relevant papers). According to the previously described, we used the Scopus database to run the search string, and the contents of the relevant documents was accessed through their respective publishers such as IEEE, Springer, ACM, Science Direct, among others.

As shown in Figure 1, the first ontology related to cybersecurity was reported in 2004 (Simmonds et al., 2004), from that year onwards, other works sporadically arise, it is from 2014 that the number of ontologies related to cybersecurity increases, for example in 2019 eleven ontologies were reported (Burita, 2019; Vega Barbas et al., 2019; Gasmi et al., 2019; Doynikova et al., 2019; Scarpato et al., 2019; Niyazova et al., 2019; Islam et al., 2019; Baesso Moreira et al., 2019; Katsantonis et al., 2019; Shaaban et al., 2019; Zamfira et al., 2019).

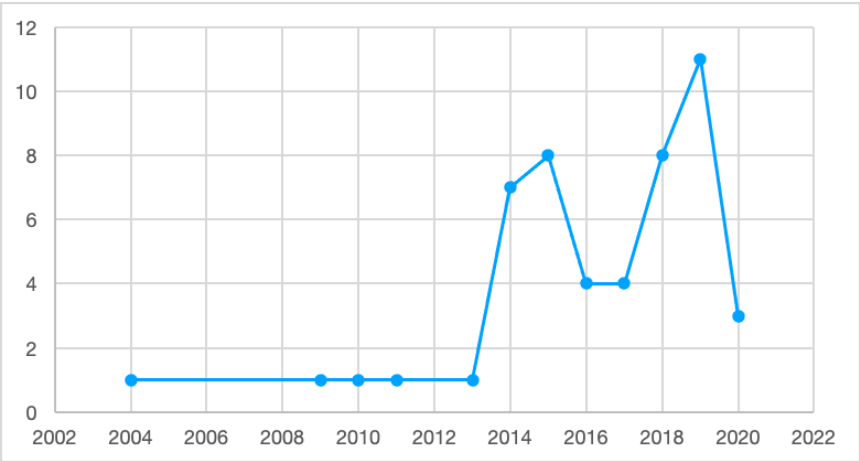


Figure 1. Chronology of ontologies reported in the context of cybersecurity.

It is worth to note that the relevant papers used in this SLR were subjected to a quality assessment. Nine evaluation criteria adapted from (Kitchenham, 2004) were considered, these criteria are related to the year of publication, the type of publication (journal or conference) as well as criteria related to the structure of the selected documents. A Likert scale was used for this purpose, where the maximum evaluation score was set 50 points, Table 1 shows the nine criteria used for the assessment.

TABLE 1. Quality assessment criteria used for this SLR.

The authors of this paper carried out the evaluation of the relevant documents and the results of the evaluation were averaged. As can be seen in Table 2, none of the papers was rejected based on the evaluation criteria used.

Quality percentage score by category	Number of papers	Percentage of papers
Poor (<26%)	0	0%
Regular (26%-45%)	0	0%
Good (46%-65%)	19	38%
Very Good (66%-85%)	26	52%
Excellent (>86%)	5	10%

TABLE 2. Quality assessment outcome.

The total score from each paper was computed using a percentage scale. We observe that all of the relevant papers yielded a quality score that ranges from good to excellent. The average score of this evaluation was 76%, which was considered a good enough quality indicator for this SLR.

RESULTS

This section presents the results of the information synthesis process. These results are structured with respect to the research questions stated for this SLR.

RQ1. What areas of cybersecurity are the ontologies reported in?

Regarding this research question, we have identified four categories in which the ontologies are grouped: General, Networking, Software and Human Factor. The general category refers to those ontologies that involve a mix of concepts related to the other categories, such as networking, software, or the human factor. In the category of networking the ontologies address concepts related to equipment, protocols and network modeling. In the software category, the ontologies are mainly focused on describing cybersecurity concepts from a software development perspective. In the category of human factor are those ontologies that describe concepts related to the personnel involved in aspects of cybersecurity in ICTs. Table 3 presents the ontologies grouped by the categories previously described. As shown in Table 3, the largest number of ontologies analyzed are grouped in the general and networking categories.

Scope / Domain	*Number of papers*	*Percentage of papers*	*References*
General	17	34%	Burita (2019), Vega Barbas et al. (2019), Doynikova et al. (2019), Baesso Moreira et al. (2019), Onwubiko et al. (2018), Zhao et al. (2018), Petrenko and Makoveichuk, (2017), Elnagdy et al. (2016), Falk (2016), Maines et al. (2015), Gcaza et al. (2015), Salem and Wacek (2015), Oltramari et al. (2014), Geller et al. (2014), Van Vuuren et al. (2014), Obrst et al. (2014), Wali et al. (2013)
Networking	16	32%	Chukkapalli et al. (2020), Scarpato et al. (2019), Katsantonis et al. (2019), Shaaban et al. (2019), Zamfira et al. (2019), Zamfira et al. (2018), Mozzaquatro et al. (2018), Zheng et al. (2018), Albalushi et al. (2018), Bergner and Lechner (2017), Oltramari et al., (2015), Iannacone et al. (2015), Laskey et al. (2015), Takahashi et al. (2010), Hieb et al. (2009), Simmonds et al. (2004)
Software	9	18%	Syed (2020), Bataityte et al. (2020), Gasmi et al. (2019), Islam et al. (2019), Ochoa et al. (2018), Alqahtani and Rilling (2017), Syed et al. (2016) Huang et al. (2014), Razzaq et al. (2014)
Human Factor	8	16%	Niyazova et al. (2019), Maathuis et al. (2018), Tseng et al. (2017), Fontenele and Sun (2016), Oltramari et al. (2015), Chun and Geller (2015), Takahashi and Kadobayashi (2014), Takahashi and Kadobayashi (2011)

TABLE 3. Classification of Ontologies according to their scope.

RQ2. What methods or approaches have been used for the development of the selected ontologies?

Regarding this research question, we observe that most of the authors of the reported ontologies (88%,44 papers) do not mention to use existing methods for the development of their ontologies. In other words, the authors describe their own approach that they followed for the development of their ontologies. To a lesser extent we observe that only in six relevant papers (12%), the authors mention following some existing methodology for the development of their ontologies. For example, four authors mention the use of the Methontology methodology (Fernandez et al., 1997), while two authors mention the use of the methodology Ontology Development 101 (Noy and McGuinness, 2001).

Table 4 shows the resulting classification with regards this research question.

Existing Method	***Number of papers***	***Percentage of papers***	***References***
Without Following Existing Methods	44	88%	Syed (2020), Chukkapalli et al. (2020), Bataityte et al. (2020), Burita (2019), Vega Barbas et al. (2019), Gasmi et al. (2019), Doynikova et al. (2019), Scarpato et al. (2019), Niyazova et al. (2019), Islam et al. (2019), Baesso Moreira et al. (2019), Shaaban et al. (2019), Onwubiko et al. (2018), Zamfira et al. (2018), Mozzaquatro et al. (2018), Zheng et al. (2018), Ochoa et al. (2018), Zhao et al. (2018), Albalushi et al. (2018), Alqahtani and Rilling (2017), Tseng et al. (2017), Petrenko and Makoveichuk (2017), Bergner and Lechner (2017), Bergner and Lechner (2017), Fontenele and Sun (2016), Falk (2016), Syed et al. (2016), Maines et al. (2015), Oltramari et al. (2015), Iannacone et al. (2015), Gcaza et al. (2015), Oltramari et al. (2015), Salem and Wacek (2015), Chun and Geller (2015), Laskey et al. (2015), Oltramari et al. (2014), Geller et al. (2014), Takahashi and Kadobayashi (2014), Huang et al. (2014), Wali et al. (2013), Takahashi and Kadobayashi, (2011), Takahashi et al. (2010), Hieb et al. (2009) Simmonds et al. (2004)
Following Existing Methods	6	12%	Zamfira et al. (2019), Maathuis et al. (2018), Obrst et al. (2014), Razzaq et al. (2014), Katsantonis et al. (2019), Van Vuuren et al. (2014)

TABLE 4. Classification of Ontologies according to their methodology.

As shown in Table 4, only six papers report the use of a methodology for developing their ontologies. Methontology approach was reported in four papers (Zamfira et al., 2019; Maathuis et al., 2018; Obrst et al., 2014; Razzaq et al., 2014), whereas the ontology development 101 method was reported in two works (Katsantonis et al.,2019; Van Vuuren et al., 2014).

RQ3.What tools have been used for the construction of the reported ontologies?

In the case of the tools that support the construction of ontologies, 40% of the documents (20 papers) authors mention the use of some tool to support the development of their ontologies. We observe that Protégé is the most used tool for ontology development; its use is mentioned in 16 out of 20 relevant documents that mention the use of a tool. To a lesser extent, the use of other tools is also reported, such as Atom-Tool; Cyber Security Ontology Expert Tool; CYBEX; and IntelMQ. Table 5 shows the ontologies grouped by tools.

Tool	Number of papers	Percentage of papers	References
Protégé	16	32%	Syed (2020), Bataityte et al. (2020), (2019), Katsantonis et al. (201 (2019), Zamfira et al. (2018 (2018), Ochoa et al. (20 Oltramari et al. (201 et al. (2014), (2014), Ra
ATOM-TOOL	1	2%	
Cyber Security Ontology Expert Tool	1		
CYBEX			
IntelM			

TABLE 5. Ontology classification by used tools

The tools used for the ontology development usually incorporate languages that help in the definition of ontologies. We observe that 24% (12 papers) of the relevant documents (Chukkapalli et al., 2020; Vega Barbas et al., 2019; Doynikova et al., 2019; Zheng et al., 2018; Petrenko and Makoveichuk, 2017; Elnagdy et al., 2016; Falk, 2016; Syed et al., 2016; Iannacone et al., 2015; Oltramari et al., 2015; Salem and Wacek, 2015; Laskey et al., 2015) report the use of the OWL language (Dean and Schreiber, 2003).

To a lesser extent, the use of languages such as SPARQL, SWRL, XML and OWL 2 is observed (Baesso Moreira et al., 2019; Onwubiko et al., 2018; Albalushi et al., 2018; Tseng et al., 2017; Bergner and Lechner, 2017; Fontenele and Sun, 2016; Maines et al., 2015; Geller et al., 2014).

RQ4. Have the reported ontologies been validated?

Regarding the evaluation and validation of the ontologies reported in this SLR, we observe that 62% of them (31 primary studies) mention the use of some verification or validation mechanisms. For example, in 18 relevant papers, authors mention the use of information extraction rules similar to those proposed in (Boley et al., 2001). In the case of the ontologies here reported, some authors perform the verification and validation of their ontologies based on the comparison with existing ontologies (3 relevant papers). Another type of validation observed is the validation by experts, approach mentioned in other three relevant papers. The use of tools for assessing ontologies is also mentioned, tools like OntoClean (Gangemi et al., 2002), the OQuare metrics tool (Duque and Fernandez, 2011), and a Protégé extension called HermiT Reasoner (Data and Knowledge Group) are mentioned. We also observe hybrid approaches in which validation is conducted through the use of criteria (Fernandez et al., 2009) and tasks (Welty et al., 2003). Finally, we also observe the use of a metrics-based validation approach. Table 6 shows the resulting classification regarding this research question.

Evaluation / Validation	*Number of papers*	*Percentage of papers*	*References*
Information Extraction Rules	18	36%	Islam et al. (2019), Baesso Moreira et al. (2019), Katsantonis et al. (2019), Shaaban et al. (2019), Ochoa et al. (2018), Zhao et al. (2018), Alqahtani and Rilling (2017), Tseng et al. (2017), Petrenko and Makoveichuk (2017) Elnagdy et al. (2016), Falk (2016), Maines et al. (2015), Salem and Wacek (2015), Laskey et al. (2015), Geller et al. (2014), Takahashi and Kadobayashi (2014), Huang et al. (2014), Takahashi and Kadobayashi (2011)
Comparison with Existing Ontologies	3	6%	Zheng et al. (2018), Syed et al. (2016), Iannacone et al. (2015)
Experts' validation	3	6%	Fontenele and Sun (2016), Chun and Geller (2015), Wali et al. (2013)
OntoClean	3	6%	Zamfira et al. (2019), Zamfira et al. (2018), Razzaq et al. (2014)
OQuare metrics	1	2%	Mozzaquatro et al. (2018)
HermiT Reasoner	1	2%	Maathuis et al. (2018)
Hybrid Approach	1	2%	Syed (2020)
Metrics-based Validation	1	2%	Gasmi et al. (2019)

TABLE 6. Evaluation and validation approaches reported.

DISCUSSION AND CONCLUSIONS

The highest percentage of ontologies reported in the field of cybersecurity are in the general and networking category. The general category addresses a mix of concepts belonging to the networking, software and human factor categories. These findings suggest that work is being done on the definition of ontologies in specific cybersecurity domains. However, we also observe work on the development of ontologies addressing a more general domain of the cybersecurity.

Regarding the methods or approaches used for the development of ontologies, we observe that in most of the relevant documents analyzed, authors do not mention following existing methodologies for developing their ontologies. Only in 12% (six papers) authors mention using some methodology as a reference. From this percentage, the most used methodology is Methontology (Fernandez et al., 1997). These findings seem to suggest a lack of motivation in the use of existing ontology development methodologies. We observe that the most widely used tool for the construction of ontologies is Protégé (Noy et al., 2000).
From the ontologies that report the use of some tool, 32% (16 papers) report the use of Protégé. OWL (Dean and Schreiber, 2003) is the most used language among the ontologies that report the use of a language.

Finally, regarding the use of verification and validation (V&V) mechanisms, we observe that 62% of the primary studies report the use of some verification or validation mechanism, among which the following stand out: the use of information extraction rules, making of comparisons with respect to existing ontologies, validation by experts, validation through the use of metrics, as well as the use of tools for this purpose. We observe that gradually there is interest in applying V&V mechanisms that help to correct deficiencies in the development of ontologies in the field of cybersecurity.

Study Limitations

It is worth to note that secondary studies as the one here reported are subject to interpretation in its different phases, thus implying the presence of bias. In order to minimize a possible bias, we followed the main phases with its activities of the SLR methodology. Although the risk of missing relevant papers was present, we consider that the selected documents for this review (relevant papers) represent a good enough sample of reported cybersecurity ontologies.

In this SLR, we did not consider gray literature, so we assume that good quality grey literature of this subject will be reported in journals or conferences, because of this, possible publication bias may arise due to negative findings are not usually published. We did not consider documents published in a non-English language, although this is not a limitation in our regional context, it can be a reflection of the limitations imposed on us by the available research in this area (updated and peer-reviewed literature is commonly published in English).

Cybersecurity is a young discipline in which disciplines such as telecommunications, electronics and computing have converged. The arrival of different ontologies in the field of cybersecurity has fostered to have more knowledge of the concepts related to this discipline. In this research we have reported the results of a systematic literature review on cybersecurity ontologies. The main contribution of this secondary study is the synthesis of the findings from the different ontologies reported with respect to areas or domains, methodologies, tools and languages used, as well as the V&V mechanisms reported. The results of our work can serve as a reference for future research on this topic.

REFERENCES

Alani, H. and Brewster, C. (2006). Metrics for ranking ontologies.

Albalushi, A., Khan, R., McLaughlin, K. and Sezer, S. (2018). Ontology-based approach for malicious behaviour detection in synchrophasor networks. IEEE Power and Energy Society General Meeting, 1-5.

Alqahtani, S. S. and Rilling, J. (2017). An Ontology-Based Approach to Automate Tagging of Software Artifacts. International Symposium on Empirical Software Engineering and Measurement, 169174.

Arpírez, J., Corcho, O., Fernandez, M. and Gómez, A. (2003). WebODE in a nutshell. AI Magazine.

Baesso Moreira, G., Menditi Calegario, V., Duarte, J. C. and Pereira, Dos Santos, A. F. (2019). Extending the VERIS Framework to an Incident Handling Ontology. 2018 IEEE/WIC/ACM International Conference on Web Intelligence, 8609628, 440-445.

Bataityte, K., Vassilev, V. and Gill, O.J. (2020). Ontological foundations of modelling security policies for logical analytics. IFIP Advances in Information and Communication Technology, 583, 368380.

Bergner, S. and Lechner, U. (2017). Cybersecurity ontology for critical infrastructures. 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, 2, 80-85.

Bernaras, A., Laresgoiti, I. and Corera, J. (1996). Building and reusing ontologies for electrical network applications. Wahlster W (ed) European Conference on Artificial Intelligence (ECAI'96), 298– 302.

Boley, H., Tabet, S. and Wagner, G. (2001). Design Rationale of RuleML: A Markup Language for Semantic Web Rules. In the first Semantic Web Working Symposium.

Brewster, C., Alani, H., Dasmahapatra, S. and Wilks, Y. (2004). Data driven ontology evaluation.

Burita, L. (2019). Model of a Vocabulary. Frontiers in Artificial Intelligence and Applications, 321, 8391.

Chukkapalli, S. S. L., Piplai, A., Mittal, S., Gupta, M. and Joshi, A. (2020). A Smart-Farming Ontology for Attribute Based Access Control. 2020 IEEE 6th Intl Conference on Big Data Security on Cloud, BigDataSecurity 2020, 2020 IEEE Intl Conference on High Performance and Smart Computing, HPSC 2020 and 2020 IEEE Intl Conference on Intelligent Data and Security, 9123052, 29-34.

Chun, S.A. and Geller, J. (2015). Developing a pedagogical cybersecurity ontology. Communications in Computer and Information Science, 178, 117-135.

Data and Knowledge Group. HermiT OWL Reasoner: The New Kid on the OWL Block. Department of Computer Science, University of Oxford, http://www.hermit-reasoner.com/

Dean, M. and Schreiber, G. (2003). OWL Web Ontology Language Reference. http://www.w3.org/TR/owl-ref/

Doynikova, E., Fedorchenko, A. and Kotenko, I. (2019). Ontology of metrics for cyber security assessment. ACM International Conference Proceeding Series, 3341496.

Duque, A. and Fernandez, J. (2011). OQuaRE: A SQuaRE-based Approach for Evaluating the Quality of Ontologies. Journal of Research and Practice in Information Technology.

Elnagdy, S.A., Qiu, M. and Gai, K. (2016). Cyber Incident Classifications Using Ontology-Based Knowledge Representation for Cybersecurity Insurance in Financial Industry. 3rd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2016 and 2nd IEEE International Conference of Scalable and Smart Cloud, SSC 2016, 7545936, 301-306.

Falk, C. (2016). An ontology for threat intelligence. European Conference on Information Warfare and Security, ECCWS, 111-116.

Farquhar, A., Fikes, R. and Rice, J. (1997). The Ontolingua Server: A Tool for Collaborative Ontology Construction. International Journal of Human Computer Studies, 46(6), 707–727.

Fernandez, M., Gomez, A. and Juristo, N. (1997). METHONTOLOGY: From Ontological Art Towards Ontological Engineering. Spring Symposium on Ontological Engineering of AAAI, 33-40.

Fernandez, M., Overbeeke, C., Sabou, M. and Motta, E. (2009). What makes a good ontology? A casestudy in fine-grained knowledge reuse. The semantic web, Springer, 61-75.

Fontenele, M. and Sun, L. (2016). Knowledge management of cyber security expertise: An ontological approach to talent discovery. 2016 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2016, 7502356.

Gangemi, A., Guarino, N., Oltramari, A. and Borgo, S. (2002). Cleaning-up WordNet's Top- Level. 1st International WordNet Conference.

Gasmi, H., Laval, J. and Bouras, A. (2019). Cold-start cybersecurity ontology population using information extraction with LSTM. 2019 International Conference on Cyber Security for Emerging Technologies, 8904905.

Gcaza, N., Von, Solms, R. and Van, Vuuren, J. (2015). An ontology for a national cyber-security culture environment. 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015, 1-10.

Geller, J., Ae Chun, S. and Wali, A. (2014). A hybrid approach to developing a cyber security ontology. 3rd International Conference on Data Management Technologies and Applications, 377-384.

Grüninger, M. and Fox, M. (1995). Methodology for the design and evaluation of ontologies. Skuce D

(eds) IJCAI'95 Workshop on Basic Ontological Issues in Knowledge Sharing, 6.1-6.10.

Hartmann, J., Spyns, P., Giboin, A., Maynard, D., Cuel, R., Carmen, M. and Sure, Y. (2004). Methods for ontology evaluation. Knowledge Web Deliverable D1.2.3, 1.

Hieb, J., Graham, J. and Guan, J. (2009). An ontology for identifying cyber intrusion induced faults in process control systems. IFIP Advances in Information and Communication Technology, 311, 125-138.

Horrocks, I. and van Harmelen F. (2001). Reference Description of the DAML+OIL (March 2001) Ontology Markup Language. http://www.daml.org/2001/03/reference.html

Huang, H., Lee, C., Wang, M. and Kao, H. (2014). IT2FS-based ontology with soft-computing mechanism for malware behavior analysis. Soft Computing, 18, 267-284.

Iannacone, M., Bohn, S., Nakamura, G., Gerth, J., Huffer, K., Bridges, R., Ferragut, E. and Goodall, J. (2015). Developing an ontology for cyber security knowledge graphs. ACM International Conference, 12.

Islam, C., Babar, M.A. and Nepal, S. (2019). An ontology-driven approach to automating the process of integrating security software systems. 2019 IEEE/ACM International Conference on Software and System Processes, 8812856, 54-63.

Karp, P., Chaudhri, V. and Thomere, J. (1999). XOL: An XML-Based Ontology Exchange Language. http://www.ai.sri.com/~pkarp/xol/xol.html

Katsantonis, M. and Mavridis, I. (2019). Ontology-Based Modelling for Cyber Security E-Learning and Training. Computer Science, 11841, 15-27.

KBSI (1994). The IDEF5 Ontology Description Capture Method Overview. KBSI Report.

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. Software Engineering Group Department of Computer Science.

Laskey, K. B., Chandekar, S. and Paris, B. (2015). A probabilistic ontology for large-scale IP geolocation. CEUR Workshop, 1523, 18-25.

Lenat, D. and Guha, R. (1990). Building Large Knowledge-based Systems: Representation and Inference in the Cyc Project. Addison-Wesley

Lozano, A. and Gómez, A. (2004). ONTOMETRIC: A Method to Choose the Appropriate Ontology. Journal of Database Management. Special Issue on Ontological analysis, Evaluation and Engineering of Business Systems Analysis Methods, 15.

Luke, S. and Heflin, J. (2000). SHOE 1.01. Proposed Specification. Technical Report. Parallel Understanding Systems Group. http://www.cs.umd.edu/projects/plus/SHOE/spec1.01.htm

Maathuis, C., Pieters, W. and Van, Den, Berg, J. (2018). A computational ontology for cyber operations.

European Conference on Information Warfare and Security, ECCWS, 278-287.

Maines, C. L., Llewellyn Jones, D., Tang, S. and Zhou, B. (2015). A cyber security ontology for BPMNsecurity extensions. 15th IEEE International Conference on Computer and Information Technology, CIT 2015, 14th IEEE International Conference on Ubiquitous Computing and Communications, IUCC 2015, 13th IEEE International Conference on Dependable, Autonomic and Secure Computing, DASC 2015 and 13th IEEE International Conference on Pervasive Intelligence and Computing, PICom 2015, 7363310, 1756-1763.

Mozzaquatro, B.A., Agostinho, C., Goncalves, D., Martins, J. and Jardim-Goncalves, R. (2018). An ontology-based cybersecurity framework for the internet of things. Sensors, 18(3053).

Neches, R., Fikes, R. E., Finin T., Gruber, T. R., Senator, T. and Swartout, W. R. (1991). Enabling technology for knowledge sharing. AI Magazine, 12(3), 36-56.

Niyazova, R., Aktayeva, Al. and Davletkireeva, L. (2019). An Ontology based Model for User Profile building using Social Network. ACM International Conference Proceeding Series, 21.

Noy, N. F. and McGuinness, D. L. (2001). Ontology development 101: A guide to creating your first ontology. Stanford knowledge systems laboratory technical report KSL-01-05 and Stanford medical informatics technical report.

Noy, N., Fergerson, R. and Musen, M. (2000). The knowledge model of Protege-2000: Combining interoperability and flexibility. Springer-Verlag, 17–32.

Obrst, L., Chase, P. and Markeloff, R. (2014). Developing an ontology of the cyber security domain. CEUR Workshop, 966, 49-56.

Ochoa, O., Steinmann, J. and Lischuk, Y. (2018). Towards eliciting and analyzing security requirements using ontologies through use case scenarios (work-in-progress). 2018 4th International Conference on Software Security and Assurance, ICSSA 2018, 9092285, 1-6.

Oltramari, A., Cranor, L. F., Walls, R. J. and McDaniel, P. (2014). Building an ontology of cyber security. CEUR Workshop, 1304, 54-61.

Oltramari, A., Cranor, L. F., Walls, R. J. and McDaniel, P. (2015). Computational ontology of network operations. IEEE Military Communications Conference MILCOM, 7357462, 318-323.

Oltramari, A., Henshel, D., Cains, M. and Hoffman, B. (2015). Towards a human factors ontology for cyber security. CEUR Workshop, 1523, 26-33.

Onwubiko, C. (2018). CoCoa: An ontology for cybersecurity operations centre analysis process. 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2018, 8551486.

Petrenko, S. A. and Makoveichuk, K. A. (2017). Ontology of cyber security of self-recovering smart Grid. CEUR Workshop, 2081, 98-106.

Poveda, M., Suárez M. C. and Gómez, A. (2015). Did You Validate Your Ontology? OOPS!. ESWC 2012 Satellite Events, 402–407.

Raad, J. and Cruz, C. (2015). A Survey on Ontology Evaluation Methods. Proceedings of the International Conference on Knowledge Engineering and Ontology Development, part of the 7th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management.

Razzaq, A., Anwar, Z., Ahmad, H. F., Latif, K. and Munir, F. (2014). Ontology for attack detection: An intelligent approach to web application security. Computers and Security, 45, 124-146.

Salem, M. B. and Wacek, C. (2015). Enabling new technologies for cyber security defense with the ICAS cyber security ontology. CEUR Workshop, 1523, 42-49.

Scarpato, N., Cilia, N.D. and Romano, M. (2019). Reachability Matrix Ontology: A Cybersecurity Ontology. Applied Artificial Intelligence, 33, 643-655.

Shaaban, A. M., Schmittner, C. and Gruber, T. (2019). Tackling the challenges of IoT security testing using ontologies. IDIMT 2019: Innovation and Transformation in a Digital World - 27th Interdisciplinary Information Management Talks, 411-418.

Simmonds, A., Sandilands, P. and Van Ekert, L. (2004). An ontology for network security attacks. Computer Science, 3285, 317-323.

Singer, P. W. and Friedman, A. (2014). Cybersecurity and Cyberwar What Everyone Needs to Know. Oxford University Press

Spyns, P., Pretorius, A. and Reinberger, M. (2004). Evaluating DOGMA-lexons generated automatically from a text corpus. Proceedings of the EKAW 2004 Workshop on Language and Semantic Technologies to support Knowledge Management Processes, 38 – 44.

Staab, S., Schnurr, H., Studer, R. and Sure, Y. (2001). Knowledge Processes and Ontologies. IEEE Intelligent Systems, 16(1), 26–34.

Sure, Y., Erdmann, M., Angele, J., Staab, S., Studer, R. and Wenke, D. (2002). OntoEdit: Collaborative Ontology Engineering for the Semantic Web. Springer- Verlag, 221–235.

Swartout, B., Ramesh, P., Knight, K. and Russ, T. (1997). Toward Distributed Use of Large- Scale Ontologies. Spring Symposium on Ontological Engineering, 138–148.

Syed, R. (2020). Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. Information and Management, 57 (103334).

Syed, Z., Pädia, A., Finin, T., Mathews, L. and Joshi, A. (2016). UCO: A Unified Cybersecurity Ontology. AAAI Workshop - Technical Report, 195-202.

Takahashi, T. and Kadobayashi, Y. (2011). 3-5 Cybersecurity information exchange techniques: Cybersecurity information ontology and CYBEX. Journal of the National Institute of Information and Communications Technology, 58, 127-135.

Takahashi, T. and Kadobayashi, Y. (2014). Reference Ontology for Cybersecurity Operational Information. Computer Journal, 58, 2297-2312.

Takahashi, T., Kadobayashi, Y. and Fujiwara, H. (2010). Ontological approach toward cybersecurity in cloud computing. 3rd International Conference of Security of Information and Networks, 100109.

Thakur, K. and Pathan, A. (2014). Cybersecurity Fundamentals. CRC Press

Tseng, S., Lin, S., Mao, C., Lee, T., Qiu, G. and Lin, M. (2017). An ontology guiding assessment framework for hacking competition. 10th International Conference on Ubi-Media Computing and Workshops with the 4th International Workshop on Advanced E-Learning and the 1st International Workshop on Multimedia and IoT: Networks, Systems and Applications, 8074131.

Ulanov, A., Shevlyakov, G., Lyubomishchenko, N., Mehra, P. and Polutin, V. (2010). Monte Carlo Study of Taxonomy Evaluation. In Database and Expert Systems Applications (DEXA), 164-168.

Uschold, M. and King, M. (1995). Towards a Methodology for Building Ontologies. Skuce D (eds) IJCAI'95 Workshop on Basic Ontological Issues in Knowledge Sharing, 6.1-6.10.

Van Vuuren, J. J., Leenen, L. and Zaaiman, J. (2014). Using an ontology as a model for the implementation of the national cybersecurity policy framework for South Africa. 9th International Conference on Cyber Warfare and Security 2014, ICCWS 2014, 107-115.

Vega Barbas, M., Villagrá, V. A., Monje, F., Riesco, R., Larriva Novo, X. and Berrocal, J. (2019). Ontology-based system for dynamic risk management in administrative domains.

Wali, A., Chun, S. A. and Geller, J. (2013). A bootstrapping approach for developing a cyber-security ontology using textbook index terms. 2013 International Conference on Availability, Reliability and Security, ARES 2013, 6657291, 569-576.

Welty, C., Mahindru, R. and Chu-Carroll, J. (2003). Evaluating ontological analysis. Semantic Integration Workshop, 92.

Zamfira, A., Fat, R. and Cenan, C. (2019). Applying semantic web technologies to discover an ontology of computer attacks. Scalable Computing, 20, 699-707.

Zamfira, A. C. and Ciocarlie H. (2018). Developing an ontology of cyber-operations in networks of computers. 2018 IEEE 14th International Conference on Intelligent Computer Communication and Processing, ICCP 2018, 8516644, 395-400.

Zhao, Y., Lang, B. and Liu, M. (2018). Ontology-based unified model for heterogeneous threat intelligence integration and sharing. International Conference on Anti-Counterfeiting, Security and Identification, ASID, 11-15.

Zheng, H., Wang, Y., Han, C., Le, F., He, R. and Lu, J. (2018). Learning and Applying Ontology for Machine Learning in Cyber Attack Detection. 17th IEEE International Conference on Trust,

Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018, 8456049, 13091315.

Recibido 26/10/2020 *ReCIBE, Año 9 No. 2, Noviembre 2020*

Aceptado 25/03/2021

Relevamiento y análisis de la evolución de los estándares para la web móvil

Survey and analysis of the evolution of standards for the mobile Web

Rocío Andrea Rodríguez[1]
rocioandrea.rodriguez@uai.edu.ar
Pablo Martín Vera[1]
pablomartin.vera@uai.edu.ar
María Roxana Martínez[1]
roxana.martinez@uai.edu.ar
Mariano Gastón Dogliotti[1]
mariano.dogliotti@uai.edu.ar

[1] Universidad Abierta Interamericana (UAI), Centro de Altos Estudios en Tecnología Informática (CAETI), Montes de Oca 745, Ciudad Autónoma de Buenos Aires, Argentina

Resumen

El World Wide Web Consortium (W3C), es un consorcio internacional que establece estándares para la Web. Esos estándares, llamados recomendaciones, son tomados e implementados por los navegadores Web, permitiendo que los desarrolladores los utilicen. Estas recomendaciones son muy importantes para la portabilidad ya que permiten que cualquier usuario utilice una aplicación Web con todas sus características sin importar el navegador que posea. Este artículo presenta un relevamiento de las recomendaciones del W3C realizando una clasificación de acuerdo con el grado de madurez alcanzado dentro de las categorías propuestas por la misma organización. Sin perder de vista la importancia de la estandarización llevada a cabo por el W3C, se presenta un caso de estudio que evidencia problemas en la evolución entre las diferentes etapas. Las nuevas funcionalidades son implementadas en los navegadores antes de estandarizarse, por lo tanto, surgen las siguientes dudas: ¿Es confiable tomar como base e implementar una tecnología que aún no se ha convertido en recomendación, pero está cerca de serlo? ¿Cuánto tiempo debe un desarrollador esperar para poder usar una nueva tecnología en sus desarrollos? El caso de estudio propuesto dará respuesta a estas preguntas.

Palabras Clave *– Web, Dispositivos Móviles, Estándares, W3C*

Abstract

The World Wide Web Consortium (W3C) is an international consortium that sets standards for the Web. Those standards, called recommendations, are taken up and implemented by Web browsers, allowing developers to use them. These recommendations are very important for portability as they allow any user to use a Web application with all its features regardless of the browser they have. This article presents a survey of the W3C recommendations, classifying them according to the degree of maturity reached within the categories proposed by the same organization. Without losing sight of the importance of the standardization carried out by the W3C, a case study is presented that shows problems in the evolution between the different stages. The new functionalities are implemented in the browsers before being standardized, therefore, the following questions arise: Is it reliable to take as a basis and implement a technology that has not yet become a recommendation, but is close to being so? How long should a developer wait to be able to use new technology in their development? The proposed case study will answer these questions.

Keywords– *Web, Mobile Devices, Standard, W3C*

1. Introducción

La disponibilidad de los dispositivos móviles es alta, principalmente los teléfonos celulares han sido los dispositivos con mayor inserción en el mercado. “Tanto los desarrollos de estándares tecnológicos como la fuerte implantación social en relación al uso cotidiano, la portabilidad y la identidad individual han hecho del teléfono móvil el dispositivo idóneo para aglutinar buena parte de los usos que caracterizan a la Sociedad de la Información” [1].

Es por ello que resulta indispensable tener en cuenta a los dispositivos móviles al momento de diseñar una aplicación. Las pantallas y teclados reducidos son algunas de las limitaciones a las que se deben enfrentar los diseñadores. Así también es importante tomar en cuenta que el usuario móvil no tiene su atención puesta completamente en el dispositivo. Es por ello por lo que las interfaces deben ser simples y directas, para que permitan al usuario alcanzar los principales contenidos/servicios con la mayor facilidad y rapidez posible.

Pero los smartphones incluyen características muy interesantes en cuanto a hardware, como por ejemplo una gran cantidad de sensores que pueden ser aprovechados en el desarrollo de las aplicaciones. Por lo tanto, no se trata tan sólo de pensar en la interfaz que se le presentará al usuario, sino también en el caso de los smartphones como aprovechar el hardware disponible en las soluciones presentadas.

No hace falta que sea puntualmente una solución que requiera hardware para poder funcionar sino simplemente aprovechar el hardware que está disponible para brindar una experiencia de uso más completa al usuario.
Un simple ejemplo es utilizar el motor de vibración presente en los smarthpones para dar una alerta al usuario o dar un feedback de una acción realizada. En el trabajo [2] se presenta un análisis del uso del sensor de proximidad que permite utilizar un teléfono celular por medio de gestos aéreos, esto es un ejemplo de cómo el hardware puede ser integrado a todo tipo de aplicaciones.

Al mencionar integración de hardware es posible presuponer que la aplicación debe ser nativa. Las aplicaciones nativas son aquellas que se desarrollan para un sistema operativo particular, permitiendo el completo acceso al hardware, además tienen la ventaja de que su interfaz tendrá el mismo aspecto al que el usuario está acostumbrado en el resto de las pantallas provistas en el sistema operativo.

Sin embargo, actualmente las aplicaciones Web permiten emular los controles nativos, de esta forma es posible visualmente obtener una interfaz uniforme. ¿Pero qué sucede en cuanto al acceso al hardware? ¿Es necesario desarrollar una aplicación nativa para poder utilizarlo? La respuesta es no, ya que las aplicaciones Web incorporan cada vez más posibilidades de acceso al hardware, achicando la brecha que existía entre aplicaciones Web y nativas [3]. “Las nuevas mejoras realizadas en las tecnologías web permitieron más características y capacidades que antes solo eran posibles en aplicaciones que fueron desarrolladas en forma nativa.” [4]

La principal ventaja de una aplicación Web frente a una aplicación nativa es su portabilidad. Al desarrollar una aplicación web, esta será funcional independientemente del sistema operativo en el cual sea utilizada. “Una de las principales dificultades al desarrollar aplicaciones para móviles es la diversidad de dispositivos y sistemas operativos, teniéndose que construir una versión diferente para cada caso en un lenguaje y una herramienta diferente” [5]. “Si se desea cubrir varias plataformas, se deberá generar una aplicación para cada una de ellas.

Esto conlleva a mayores costos de actualización y distribución de nuevas versiones” [6]. Por lo que algunos desarrolladores recurren a soluciones híbridas usando frameworks tales como PhoneGap [7], encontrando una solución a la portabilidad, teniendo algunas limitaciones propias de la Web como el acceso completo al hardware. Entonces ¿por qué buscar una solución alternativa y no realizar directamente una aplicación Web que aproveche la web a su máximo potencial?

Los Smartphones gracias a HTML 5 [8] cuentan con la posibilidad de ejecutar aplicaciones Web enriquecidas, en las cuales el acceso a la información propia del dispositivo y al hardware es una realidad. “HTML5 se ha concebido con el propósito de simplificar el trabajo de los diseñadores de Web y mejorar el rendimiento de las páginas, especialmente en dispositivos móviles” [9].

2. Estándares del W3C

El W3C es un consorcio web a nivel internacional que establece estándares para la Web en general e incluye a la web móvil [10]. “Los estándares Web son las respuestas más eficaces a la rápida y continua evolución tecnológica que experimenta la red. Adecuarse a ellos hace posible que el trabajo de hoy constituya una base efectiva en el futuro y ayude a evolucionar tecnológicamente con el medio” [11]. “Los estándares Web ofrecen un grupo de posibilidades y sus ventajas clave están en la posibilidad de llegar a un mayor número de usuarios, al expandir el acceso a la información del sistema a un amplio número de navegadores y dispositivos” [11].

El W3C publica periódicamente actualizaciones de un documento al que denominan “Roadmap”, este documento “resume las diversas tecnologías desarrolladas en W3C que aumentan las capacidades de las aplicaciones Web y cómo se aplican más específicamente al contexto móvil” [12].

El documento se encuentra dividido en 12 categorías, que abarcan diversos aspectos, que van desde cuestiones de visualización del sitio Web hasta cuestiones internas que permitan mejorar el funcionamiento e incorporar el uso de hardware en las aplicaciones. Las categorías son:

1. Gráficos y Layout: dedicada a los gráficos y a la distribución de los elementos de la página. Las tecnologías que se analizan en esta categoría son: CSS (Cascading Style Sheets), WOFF (Web Open Font Format), SVG (Scalable Vector Graphics).
2. Adaptación al Dispositivo: Las principales tecnologías de base analizadas en esta categoría son: CSS Media Queries y SVG.
3. Formularios: En esta categoría básicamente se trabaja con los controles propios de formularios que provee HTML, en su actual versión.
4. Almacenamiento de Datos: Trabaja con APIs (Application Programming Interface – Interfaz de Programación de Aplicaciones) que permiten desde el almacenamiento de información hasta la indexación y almacenamiento encriptado.
5. Media: HTML 5 incorpora los tags video y audio, los cuales facilitan todo el trabajo multimedia, no obstante, hay APIs en progreso que tienen que ver con captura de audio/video, streaming desde la Web usando conectividad P2P (punto a punto) en otras tecnologías.
6. Interacción del Usuario: Esta categoría se basa en la interacción y la accesibilidad analizando eventos táctiles, vibración, Notificaciones Web que abren paso a futuros desarrollos como: Método para ingresar texto, Scroll suave, Despertar la pantalla…
7. Sensores e Interacciones Locales: En esta categoría se ubica la API de Geolocalización, junto a otras APIs en progreso como la de sensor de proximidad, estado de la batería…
8. Redes y Comunicaciones: En esta categoría se utilizan tecnologías de AJAX, WebSocket, Eventos iniciados por el servidor…
9. Ciclo de Vida de la Aplicación: Las aplicaciones Web se acercan a las nativas, en el sentido que ya se considera que estas pueden funcionar incluso sin conexión a internet y la importancia de optimizar recursos. Por ello, una de las APIs principales de esta categoría está enfocada en poder detectar si la aplicación está en primer plano o no lo está, para poder optimizar el consumo de recursos.
10. Pagos y Servicios: HTML proporciona ayuda específica para completar automáticamente los detalles de la tarjeta de crédito, lo que facilita el pago una vez que estos datos fueron ingresaron previamente. Distintos grupos del W3C se encuentran trabajando en diversos métodos para solicitar pagos, identificar método de pago, etc.

11. Performance y Ajustes: En esta categoría se analizan mecanismos para supervisar o mejorar el rendimiento de una aplicación Web. Se presentan distintas APIs para poder realizar mediciones tomando tiempos de carga, navegación, etc.
12. Seguridad y Privacidad: Un claro ejemplo de esta categorías el atributo sandbox de HTML5 que permite restringir el tipo de interacciones que pueden realizarse con contenidos incrustados de terceros. También en esta categoría están asociadas las APIs de encriptación de datos (mencionada previamente en la categoría almacenamiento de datos) que permitirán enviar información encriptada desde el sitio Web.

Cada una de estas categorías reúne trabajos que atraviesan diferentes grados de madurez hasta poder convertirse finalmente en estándares. Los estándares para poder consolidarse siguen determinados pasos, los cuales se sintetizan en la tabla 1 (ver paso 1 al paso 6). Los 6 primeros pasos representan las etapas de estandarización del W3C, en donde el grado de madurez va avanzando hasta finalmente convertirse en una Recomendación (paso 6).

Tabla 1. Etapas de estandarización del W3C

Pasos		Nombre de la Etapa	Estado
1.		Editor Draft	Editores
2.		Working Draft	Grupo de Trabajo
3.		Last Call Working Draft	Llamado de Participación a la comunidad
4.		Candidate Recomendation	Implementación
5.		Proposed Recomendation	Se envía al W3C para una última revisión de sus miembros
6.		Recomendation	Aceptada
		Retired	Retirado – Se ha dado de baja
		Living standard	En constante actualización
		Note	Nota – Recomendaciones y Buenas Prácticas

Todo comienza con los borradores de trabajo (pasos 1 y 2) y la convocatoria de participación abierta a la comunidad (paso 3) que permitirá reunir expertos y colaboradores en una determinada categoría y dentro de ella una característica particular a desarrollar. A modo de ejemplo, se presenta el caso del “Cascading Style Sheets Working Group”, este grupo de trabajo tiene actualmente 126 colaboradores [12], los cuales pertenecen a distintas empresas y organismos.

Es de esperarse que al proponerse como recomendación candidata (paso 4), se comience a enviar la propuesta de implementación a los distintos navegadores. No obstante, los grupos de trabajo envían en etapas tempranas los avances para poder ser implementados en los distintos navegadores. A modo de ejemplo, la figura 1 representa una característica particular de la categoría 4 (almacenamiento de datos), que el W3C la ha catalogado como tecnología en proceso.

Puede observarse que su etapa de estandarización es WD (es decir un borrador del grupo de trabajo que según el estado de madurez del W3C, está en el paso 2), no obstante, ha sido enviado para una posible implementación en distintos navegadores.

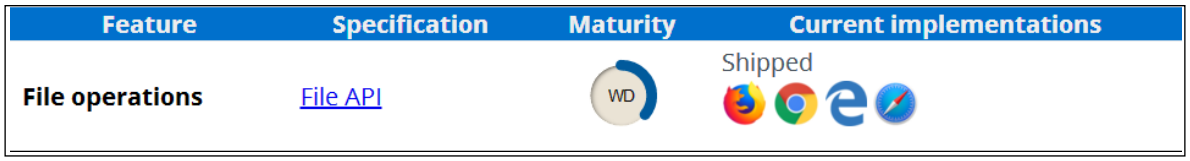


Figura 1. Ejemplo de envío de solicitud de implementación, en etapa de madurez temprana.

Las Recomendaciones Candidatas (paso 4) se someten a pruebas de implementación las cuales están disponibles en el W3C para su consulta y revisión, tal como puede verse a modo de ejemplo en la figura 2.

CSS Backgrounds and Borders Module Level 3

624 Tests

W3C Candidate Recommendation, 17 October 2017

This version:
https://www.w3.org/TR/2017/CR-css-backgrounds-3-20171017/

Latest published version:
https://www.w3.org/TR/css-backgrounds-3/

Editor's Draft:
https://drafts.csswg.org/css-backgrounds/

Previous Version:
https://www.w3.org/TR/2014/CR-css3-background-20140909/

Test Suite:
http://test.csswg.org/suites/css3-background/nightly-unstable/

Editors:
Bert Bos (W3C)
Elika J. Etemad / fantasai (Invited Expert)
Brad Kemper (Invited Expert)

Issue Tracking:
GitHub Issues

Abstract

This draft contains the features of CSS relating to borders and backgrounds. The main extensions compared to level 2 are borders consisting of images, boxes with multiple backgrounds, boxes with rounded corners and boxes with shadows.

CSS is a language for describing the rendering of structured documents (such as HTML and XML) on screen, on paper, in speech, etc.

Status of this document

This section describes the status of this document at the time of its publication. Other documents may supersede this document. A list of current W3C publications and the latest revision of this technical report can be found in the W3C technical reports index at https://www.w3.org/TR/.

Figura 2. Recomendación candidata y sus conjuntos de prueba (Test Suite)

En el paso 5 el W3C hace una última revisión en la que puede dictaminar si finalmente el desarrollo en cuestión será una recomendación (alcanzando el paso 6).

Existen durante el proceso de estandarización tres estados adicionales (representados por las tres últimas filas de la tabla 1), que son excepcionales, pero pueden observarse como símbolo del grado de madurez en alguna de las características en las que se está trabajando: (1) “Retired” con esto se indica que se ha dado de baja lo realizado (esto puede ocurrir mayormente en etapas tempranas del desarrollo), el ícono mostrado en la tabla 1 alertará que dicho documento ha sido desconsiderado. (2) “LS” esta sigla junto con el ícono gráfico presentado en la tabla 1 indicará que el estándar si bien es estable puede sufrir actualizaciones constantes. (3) “Note” tiene que ver con material adicional que puede incluir buenas prácticas, casos de uso, etc.

Las especificaciones se consideran establecidas cuando llegan a la etapa 6, por lo tanto en cada categoría pueden haber trabajos establecidos, trabajos en progreso, trabajos que recién están comenzando a desarrollarse para analizar su factibilidad (exploratorios) y trabajos que ya fueron abandonados o discontinuados. Tomando en cuenta estos 4 estados en la Fig. 3 se presenta una gráfica que presenta la cantidad de especificaciones por categoría.

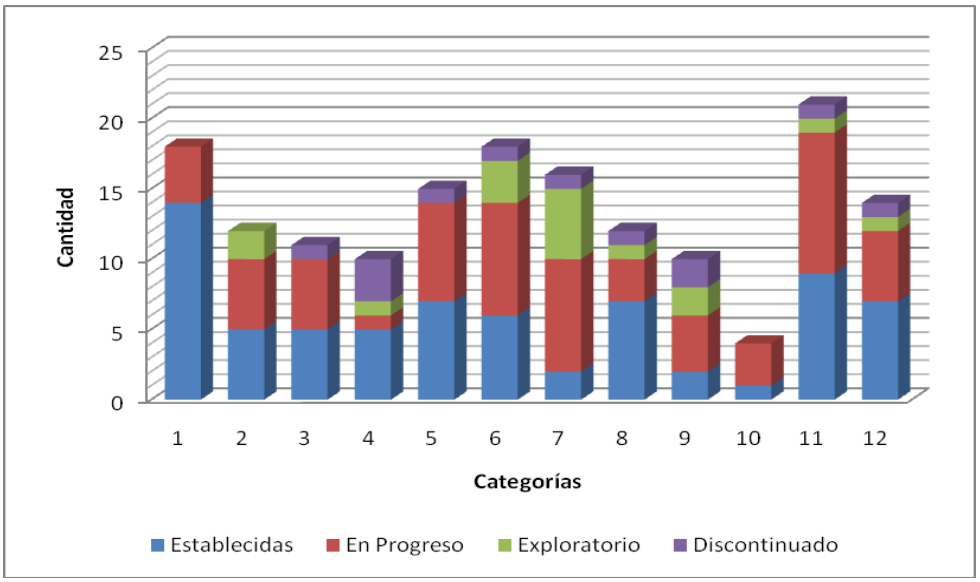


Figura 3. Especificaciones del W3C por categoría

En base a la figura 3 se desprende que:

- La categoría con mayor cantidad de especificaciones establecidas es la 1 (Gráficos y Layout).
- La categoría 11 (Performance y Ajustes) es la que tiene mayor cantidad de especificaciones en total.
- La categoría 4 (Almacenamiento de Datos) es aquella que tiene más especificaciones que han sido discontinuadas. En muchos casos esto se debe a que dichas características serán abarcadas de forma distinta por nuevos trabajos.
- Las categorías 1, 2 y 10 (que corresponden respectivamente a: Gráficos y Layout; Adaptación del Dispositivo; Pagos y Servicios), no tienen especificaciones discontinuadas.
- La categoría con menos especificaciones es la 10 (Pagos y Servicios), que a su vez tiene la mayor parte de sus especificaciones en progreso.

En todas las categorías hay especificaciones ya establecidas y un trabajo continuo que se encuentra en proceso para poder generar nuevas especificaciones.

3. Utilización de los estándares

El W3C pone a disposición estándares que pueden ser utilizados, no obstante, no son siempre implementados por los navegadores o incluso cuando están disponibles en los mismos, los desarrolladores por desconocimiento no los utilizan. “El World Wide Web Consortium (W3C) promulga los estándares…, pero no tiene autoridad para hacer cumplir la adopción de una norma a favor de otra” [14].

Por otra parte, aquellas especificaciones que aún no están establecidas tendrán diversos cambios que harán que las aplicaciones que se generen utilizando dichas funcionalidades queden obsoletas. También en diversas ocasiones las especificaciones están en progreso durante mucho tiempo sin saber si efectivamente serán discontinuadas o bien podrán avanzar para madurar y consolidarse como estándar.

4. Caso de estudio - Evolución en etapas de estandarización

Se toma como caso de estudio la especificación relacionada con el uso del Sensor de Proximidad, la cual está contenida en la categoría 7 (denominada “Sensores e Interacciones Locales”). En el año 2013 el uso del sensor de proximidad se encontraba bajo la especificación de “Eventos de Proximidad” cuyo estado era Recomendación Candidata como puede observarse en la captura de pantalla presentada en la figura 4.

Volviendo a la tabla 1 puede observarse que estando en la etapa 4 (recomendación candidata) faltan tan sólo 2 etapas para convertirse en una recomendación final del W3C. Lo que se analiza con este caso de estudio es ¿Cuánto tiempo llevarán dichas etapas? ¿En qué etapa estará actualmente, habrá llegado a la etapa 6?

Cada documento permite ver el anterior y el siguiente (tal como puede observarse en los links que presenta la figura 4). De este modo se ha hecho un seguimiento del estándar pudiéndose ver que en el 2015 (dos años después) había regresado a ser un borrador de trabajo, es decir a la etapa 2 (ver figura 5), en el 2016 si bien el estado seguía siendo el mismo había cambiado de nombre y pasó a denominarse “Proximity Sensor” (ver figura 6).

Para dar respuesta a la pregunta ¿En qué etapa estará actualmente, habrá llegado a la etapa 6?, basta con mirar la siguiente captura presentada en la figura 7, el último documento corresponde al año 2019, en donde puede observarse que aparece en la etapa 2 (WD - Working Draft) [15], habiendo el año anterior involucionado hacia la etapa 1 (ED - Editor Draft) (ver figura 8).

Figura 4. Sensor de Proximidad seguimiento de la estandarización – 2013

Figura 5. Sensor de Proximidad seguimiento de la estandarización - 2015

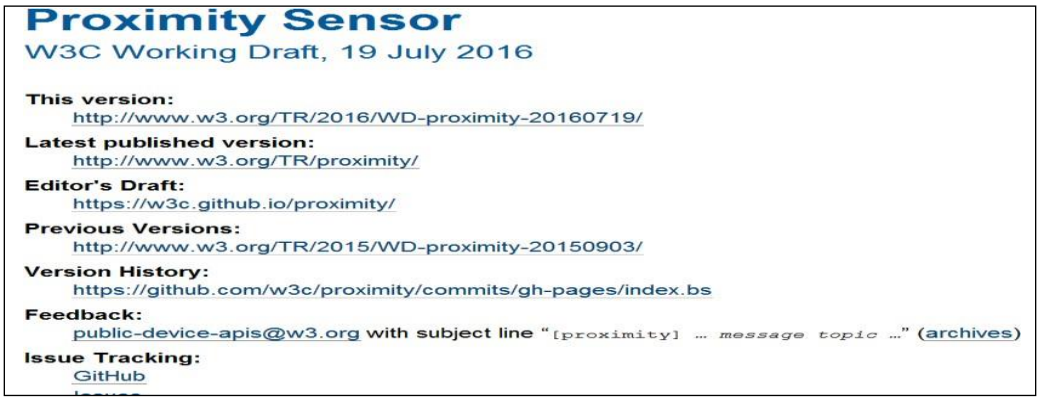


Figura 6. Sensor de Proximidad seguimiento de la estandarización – 2016

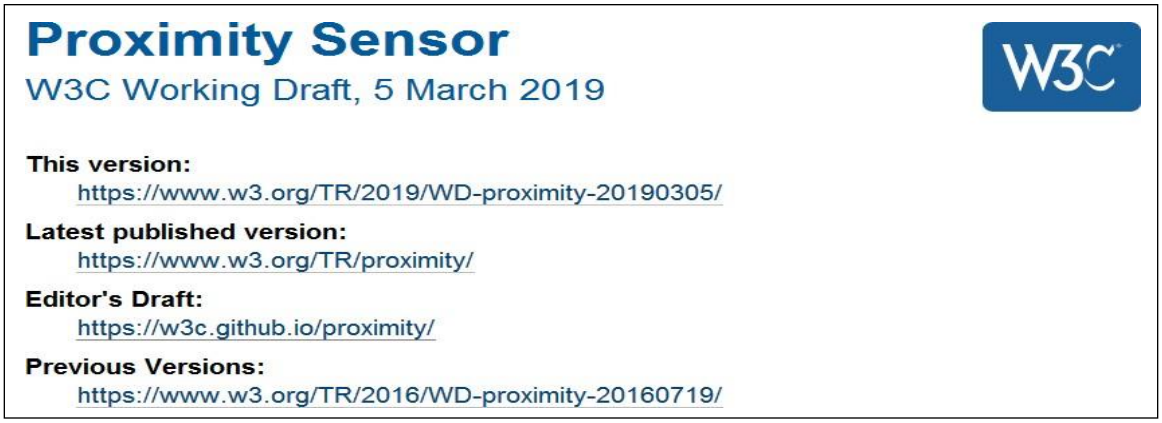


Figura 7. Sensor de Proximidad seguimiento de la estandarización – 2019

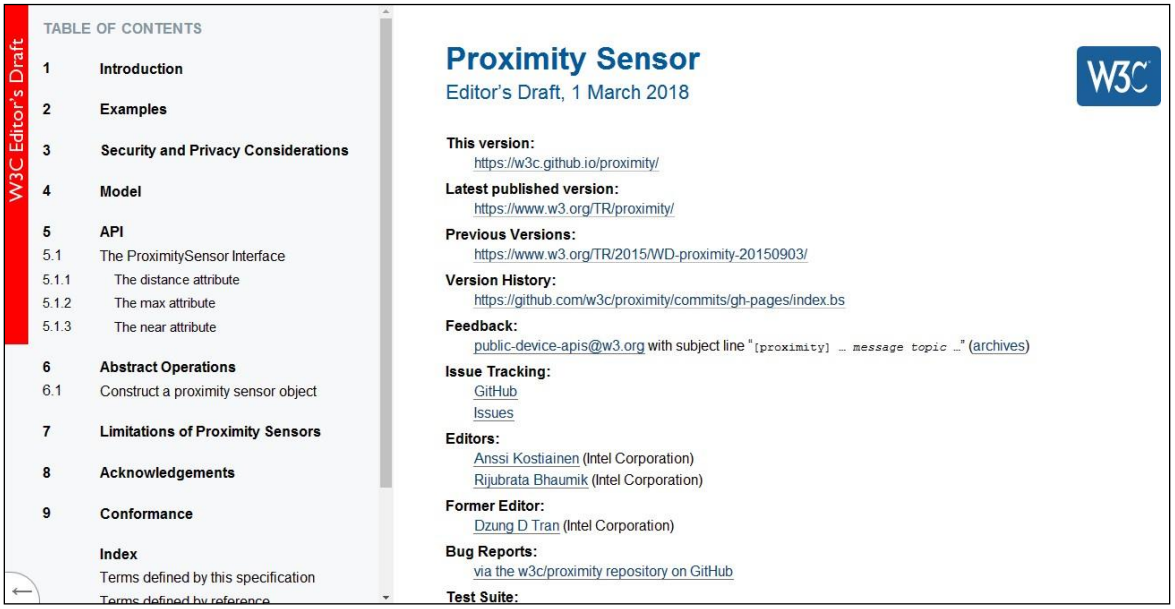


Figura 8. Sensor de Proximidad seguimiento de la estandarización – 2018

En cuanto al otro interrogante planteado ¿Cuánto tiempo llevarán dichas etapas? No hay una respuesta precisa, depende de cada caso en particular, en este caso de análisis han pasado en total 9 años y habiendo estado esta funcionalidad como recomendación candidata en el paso 4 de la estandarización, muy cercano al paso final numerado como 6, ha regresado al paso 1 y actualmente ha vuelto al paso 2. Esto es decepcionante para los desarrolladores que han construido soluciones basadas en la recomendación candidata y ahora se encuentran con que eso ha cambiado y hay un destino incierto.

Se desconoce cómo será la implementación final para poder utilizar el sensor de proximidad y cuánto tiempo más demande tener finalmente la recomendación del W3C (es decir alcanzar el paso 6). Esto debe plantear un nuevo interrogante: ¿Es confiable tomar como base e implementar una tecnología que aún no se ha convertido en recomendación pero que está cerca de estarlo?, dado los importantes cambios que ocurren en los mismos dejando soluciones que se apoyan en estas especificaciones obsoletas, la recomendación es esperar que las especificaciones se asienten y se transformen en recomendaciones (paso 6 del proceso) lo cual no quita que la espera para esto pueda ser verdaderamente larga.

Realizando el seguimiento entre documentos se construye el diagrama de la figura 9, puede observarse que el primer documento accesible data del 2012 y que en un solo año había avanzado de Etapa 2 a Etapa 4. A pesar de este prometedor avance, dos años después vuelve la especificación a etapa 2, tres años después retrocede a la etapa 1 y finalmente se encuentra nuevamente en etapa 2.

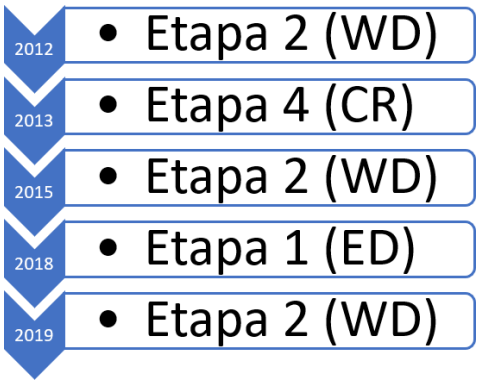


Figura 9. Resumen de fechas y estados de especificación para el uso del sensor de proximidad

Este caso de análisis muestra la dificultad para realizar el seguimiento de una especificación y además deja en evidencia que los pasos a seguir para el proceso de estandarización no siempre avanzan, sino que también pueden implicar un retroceso.

5. Relevamiento por categoría

Habiendo tomado una especificación, como caso de estudio en la sección anterior, se pudo advertir estancamiento en los pasos e involución en los mismos. Entonces surge el interrogante ¿Es este un caso aislado u ocurre en forma general en las especificaciones del W3C? Para dar respuesta a esta pregunta, de las 12 categorías existentes se analizan cuatro (categorías 1, 4 y 10) es decir se considera una muestra del 33%.

A modo de resultados la tabla 2 presenta la cantidad de especificaciones comprendidas en la muestra tomada, clasificadas según su estado actual, en uno de 6 pasos, a lo que se agrega las que fueron retiradas (R), las que están en constante actualización (LS) y las que poseen una nota (N). A continuación, la columna documentos representa la cantidad de documentos que debieron seguirse para poder tener la trazabilidad de las especificaciones de dicha categoría y la columna final muestra el promedio de años de progreso de cada especificación tomando la fecha del primero y el último documento publicado (exceptuándose las especificaciones en estado LS dado que ellas no cuentan con trazabilidad, se muestra sólo la última especificación sin links a las anteriores).

En la última fila se presentan los totales, en donde se ha sumado entre todas las categorías la cantidad de especificaciones por paso, más las tres columnas de estados adicionales, del mismo modo se obtiene el total de documentos analizados y finalmente la última columna representa el promedio de los tiempos de cada categoría. Este relevamiento origino seguir la trazabilidad de 49 especificaciones dando por resultado el análisis de 526 documentos publicados por el W3C. Como puede observarse la mayor cantidad de especificaciones se encuentran en estado 2 (31%), siendo el tiempo promedio en años desde el primer documento hasta el último generado por la especificación es de 7.

Tabla 2. Especificaciones de la muestra indicadas según su estado actual

Categoría	Cantidad por pasos						R	LS	N	Documentos	Promedio
	1	2	3	4	5	6					(años)
1	0	6	0	7	0	5	0	1	0	163	8
4	1	0	0	0	0	3	3	1	1	66	6
7	1	6	0	6	0	1	1	1	0	154	6
10	0	3	0	1	0	0	0	1	0	143	3
Total	**2**	**15**	**0**	**14**	**0**	**9**	**4**	**4**	**1**	**526**	**7**

De las especificaciones que aún no llegaron a ser una recomendación, se analiza cuantos años estuvieron en el estado actual alcanzado (fecha de la última especificación publicada con respecto a la fecha actual). Puede observarse en la Figura 10 que los tiempos se enmarcan a partir de los 2 años hasta los 9 años, el 27% llevan 2 años sin evolución y el 13% 4 años, llama la atención que incluso un 7% de estas especificaciones quedaron estancadas durante 9 años.

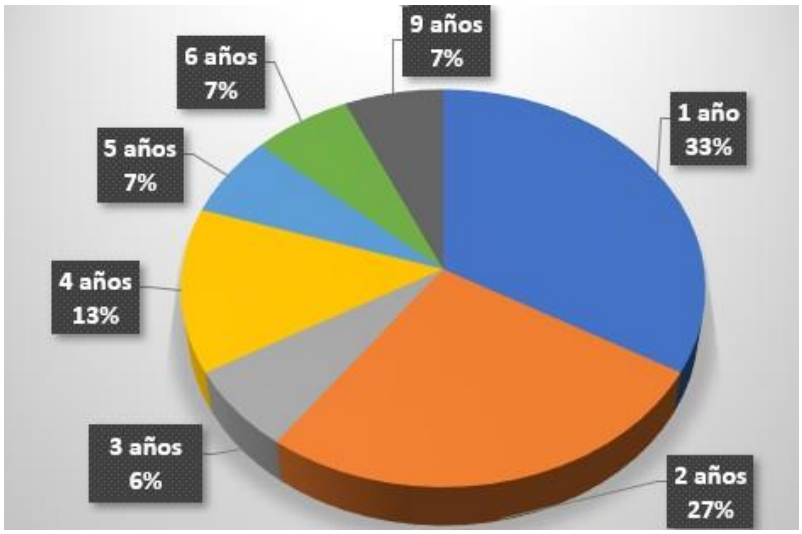


Figura 10. Tiempo de inactividad de las especificaciones

En todas las categorías analizadas se ha encontrado especificaciones que han involucionado, siendo los porcentajes: Categoría 1: 60%, Categoría 4: 50%, Categoría 7: 50%, Categoría 10: 40%. Del total hay un 37% de especificaciones que han involucionado.

Puede observarse en este análisis dos problemas significativos por un lado el estancamiento de las especificaciones que no cambian de estado incluso por 9 años y otras que involucionan retrocediendo de estados.

6. Conclusiones

Es clara la importante actividad que realiza el W3C mediante sus recomendaciones que brindan pautas y consideraciones indispensables para la buena implementación tanto de la Web en general como la Web móvil. El hardware de los dispositivos permite realizar un amplio abanico de aplicaciones que no requieren ser nativas dado que con la llegada de HTML 5 es posible hacer uso del hardware desde la Web mediante el uso de las API.

Pero los tiempos de estandarización del W3C, dificultan esta tarea. No podemos negar que debe existir un proceso que cuente con pasos precisos abiertos a la colaboración de la comunidad para poder tener recomendaciones consolidadas y lo suficientemente probadas. Es de esperarse que en 6 pasos establecidos puedan estancarse algunos trabajos y no logren estandarizarse, también es posible que el avance sea lento.

Pero la dificultad se presenta cuando no sólo las propuestas pueden ser retiradas o actualizadas, sino que estas pueden tener un retroceso tan marcado como el presentado en este artículo con el caso de estudio, en donde habiendo estado en el paso 4, actualmente esté en el paso 2. Solo tomando estas etapas los años van del 2013 al 2021, unos 8 años de involución. Esto es algo completamente desalentador para todo desarrollador que espera utilizar el estándar para su aplicación Web. Creemos que debería haber limitaciones de tiempo para cada uno de los pasos de estandarización y un seguimiento más fácil del grado de madurez, evitando sobre todo retrocesos.
El relevamiento presentado en este artículo, que consideró las 49 especificaciones contenidas en 4 de las 12 categorías, permitió evidenciar que el caso de estudio no era un caso aislado, siendo 7 años el promedio de trabajo por especificación para alcanzar el estado actual, pese a que 35% de ellas se encuentra en el paso 1 o paso 2.

Los tiempos extensos son una complicación clara para el proceso de madurez de las especificaciones.No siendo miembros del W3C, nuestro objetivo fue presentar un relevamiento representativo que permita visibilizar la problemática y alertar a los desarrolladores de software que deben esperar (a pesar de los tiempos) a que las tecnologías estén maduras para trabajar con ellas. Por otra parte, visibilizando la problemática esperamos que el W3C pueda establecer tiempos máximos para el cambio de estado de cada especificación y de este modo alentar a los grupos de trabajo a ser más activos y disminuir el promedio de tiempos.

REFERENCIAS

[1] Aguado, Juan Miguel, and Inmaculada J. Martínez. "El proceso de mediatización de la telefonía móvil: de la interacción al consumo cultural." Zer-Revista de Estudios de Comunicación11.20 (2006).

[2] Rodríguez, R. A., Vera, P. M., Martínez, M. R., Parra Beltrán, F. A., & Alcidor, J. Análisis e implementación de nuevas tecnologías para la web móvil. In XIX Workshop de Investigadores en Ciencias de la Computación (WICC 2017, ITBA, Buenos Aires). 2017

[3] Fortunato, David, and Jorge Bernardino. "Progressive web apps: An alternative to the native mobile Apps." 2018 13th Iberian Conference on Information Systems and Technologies (CISTI). IEEE, 2018.

[4] Charland, A., & Leroux, B. Mobile application development: web vs. native. Communications of the ACM, 54(5), 49-53. 2011

[5] Rodríguez, Camilo, and Héctor Enríquez. "Características del desarrollo en Frameworks multiplataforma para móviles." Ingenium Revista de la facultad de ingeniería 15.30 (2014): 101-117.

[6] Delía, L. N., Galdamez, N., Thomas, P., & Pesado, P. M. (2013). Un análisis experimental de tipo de aplicaciones para dispositivos móviles. In Congreso Argentino de Ciencias de la Computación (CACIC) (Vol. 18).

[7] Adobe PhoneGap, Disponible en: https://phonegap.com/

[8] W3C, HTML 5.[Online]. Disponible en: https://www.w3.org/TR/html52/

[9] Franganillo, Jorge. Htmle: el nuevo estándar básico de la Web. Anuario ThinkEPI, 2011, no 1, p. 261-265. [Online]. Disponible en: https://www.w3.org/standards/webdesign/mobilweb

[10] Claro, Rosendo l. Hernández; Navarro, Deibys Greguas. estándares de diseño web. ciencias de la información, 2010, vol. 41, no 2, p. 69-71.

[11] W3C, Roadmap of Web Applications on Mobile, July 2018. [Online] Disponible en: https://www.w3.org/2018/04/web-roadmaps/mobile/

[12] Cascading Style Sheetsworking group. [Online] Disponible en: https://www.w3.org/Style/CSS/members

[13] Beatty, Patricia; Dick, Scott; Miller, James. Is HTML in a race to the bottom? A large-scale survey and analysis of conformance to W3C standards.IEEE Internet Computing, 2008, vol. 12, no 2.

[14] W3C, Sensors and Local Interactions. January 2018. [Online]. Disponible en: https://www.w3.org/2018/01/web-roadmaps/mobile/sensors.html

[15] W3C, Proximity Sensor - Working Draft, 19 July 2019. [Online]. Disponible en: https://www.w3.org/TR/proximity/

NOTAS BIOGRÁFICAS

Rocío Andrea Rodríguez, Argentina, Ingeniera en Informática (UNLaM - Universidad Nacional de La Matanza). Doctora en Ciencias Informáticas (UNLP - Universidad Nacional de La Plata). Docente de grado en UNLaM, UTN (Universidad Tecnológica Nacional) y UAI (Universidad Abierta Interamericana). Docente de posgrado en UAI. Desde el 2005 realiza investigación académica, actualmente es directora de proyectos en CAETI (Centro de Altos Estudios en Tecnología Informática - UAI). Está categorizada en el Programa de Incentivos al Docente investigador (categoría 2). Dirige tesis de licenciatura, maestría y doctorado. Ha sido jurado en tribunales de tesis, revisora de artículos científicos en congresos y revistas. Se especializa en diversas áreas de investigación en las que se encuentran las tecnologías móviles, redes, gobierno electrónico y educación.

Pablo Martín Vera, Argentino, Ingeniero en Informática recibido en la Universidad Nacional de La Matanza (UNLaM). Obtuvo su título de Doctor en Ciencias Informáticas en la Universidad Nacional de La Plata (UNLP). Actualmente es docente de grado y postgrado en UNLaM, Universidad Tecnológica Nacional (UTN) y en la Universidad Abierta Interamericana (UAI). Adicionalmente a la docencia, se desarrolla como director de proyectos de investigación en CAETI (Centro de Altos Estudios en Tecnología Informática - UAI). Cuenta con más de 100 publicaciones académicas. Es revisor de trabajos científicos en diferentes congresos y revistas. Se especializa en diversas áreas de investigación en las que se encuentran las tecnologías móviles, el desarrollo dirigido por modelos MDD, la gamificación y el gobierno electrónico.

María Roxana Martínez, Argentina, Ingeniera en Sistemas Informáticos (UAI-Universidad Abierta Interamericana). Doctorando en Ciencias Informáticas en la Universidad Nacional de La Plata (UNLP). Magíster en Tecnología Informática (UAI). Docente de grado y posgrado en UAI. Docente de grado en UdeMM (Universidad de la Marina Mercante) y UNQUI (Universidad Nacional de Quilmes). Contenidista en la Universidad Siglo 21. Investigadora en proyectos de investigación en CAETI (Centro de Altos Estudios en Tecnología Informática – UAI). Es autora y expositora de diversos artículos presentados en congresos nacionales e internacionales, como así de revistas. Ha participado como jurado de tesis de grado y posgrado en: UdeMM, UNLAM (Universidad Nacional La Matanza) y UAI. Tutora de tesis de grado. Jurado en congresos nacionales (CONAIISI y TE&ET). Jurado de Python II Maratón Nacional de Programación de Escuelas Estatales 2019, Ministerio de Educación, Cultura, Ciencia y Tecnología. En el ámbito laboral, posee más de 18 años de experiencia en la rama de IT (desarrolladora, analista de sistema, PM, líder, auditora IT, etc.). Actualmente se desempeña como Líder de Procesos IT en la UIF (Unidad de Información Financiera) de Argentina.

Mariano Gastón Dogliotti, Argentino, Licenciado en la Gestión de la Tecnología (UNLaM-Universidad Nacional de La Matanza). Analista Programador en Desarrollo de Aplicaciones (Instituto Superior de Formación Docente y Técnica - ISFDyT N°46). Autor de diversas publicaciones académicas vinculadas con trabajos de I+D (Investigación y Desarrollo). Se desempeña como investigador en proyectos de investigación académica en CAETI (Centro de Altos Estudios en Tecnología Informática) perteneciente a UAI (Universidad Abierta Interamericana). Docente en el profesorado ISFDyT Nº 46. Docente en el instituto privado de educación técnica Monseñor Solari. Se especializa en diversas áreas de investigación en las que se encuentran: Diseño y Modelado 3D, Gamificación, Redes, Tecnologías Móviles y Web.

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.

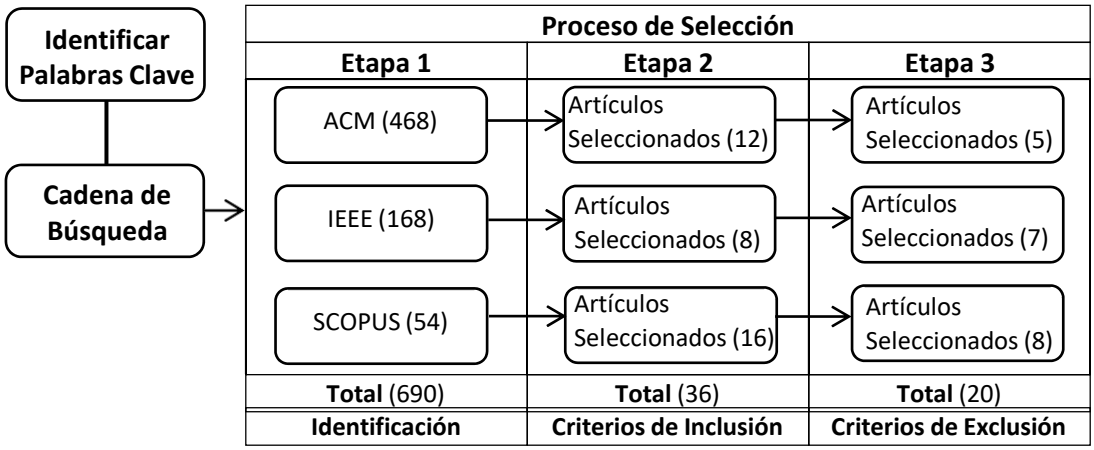


Figura 1. Proceso de selección de estudios primarios.

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.

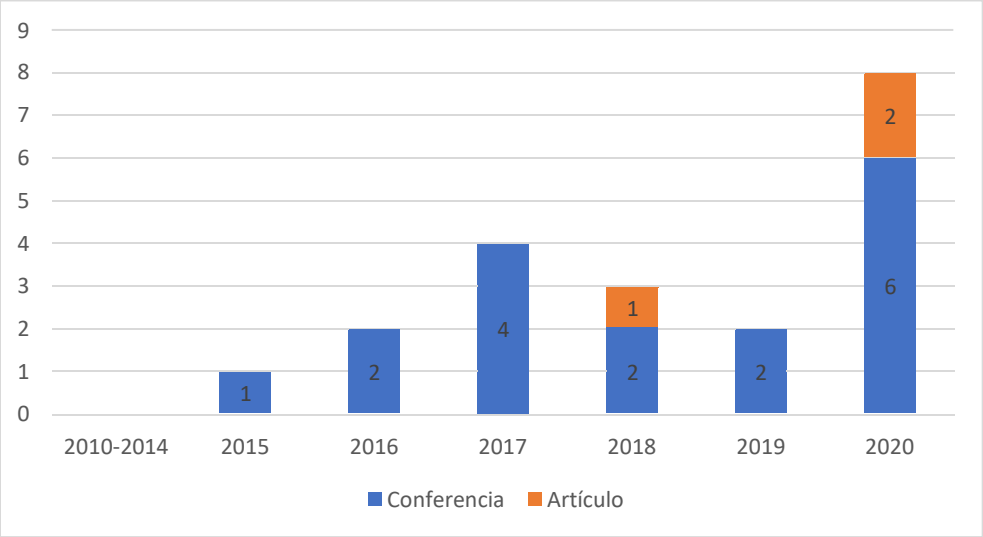


Figura 1. Estudios primarios en la última década.

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.

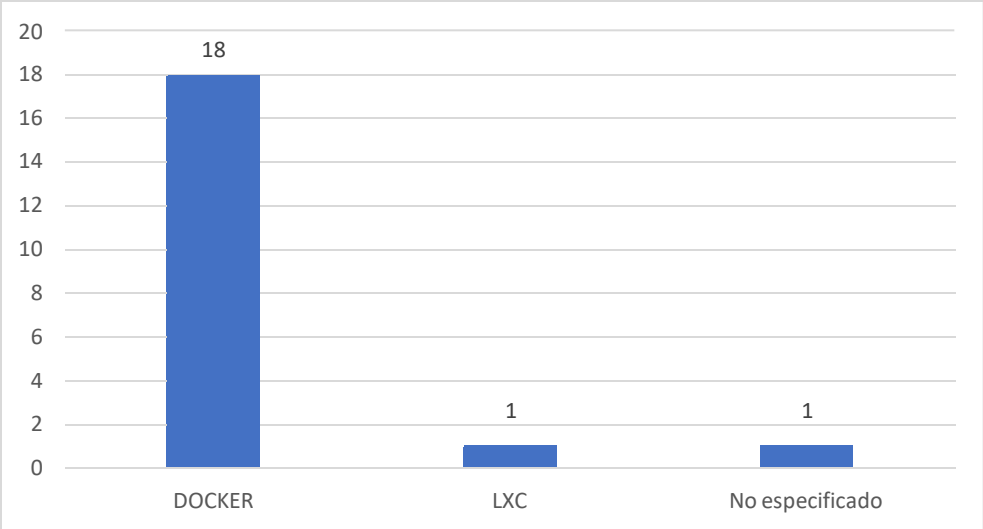


Figura 2. Tipos de contenedores utilizados en el aprendizaje de ciberseguridad.

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	[E03], [E05], [E06], [E07], [E08], [E09], [E11], [E13],
	por lo que es necesario poder desplegar distintos tipos de laboratorios que son posibles gracias a la versatilidad de los contenedores.	[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."

Recibido 21/03/2020 *ReCIBE, Año 9 No. 2, Noviembre 2020*

Aceptado 17/12/2020

Procesamiento embebido de P300 basado en red neuronal convolucional para interfaz cerebro-computadora ubicua

P300 embedded processing based on convolutional neural network for ubiquitous brain-computer interface

José Manuel Macias-Macias[1]
jmmaciasm@itchihuahua.edu.mx

Juan Alberto Ramirez-Quintana[1]
jaramirez@itchihuahua.edu.mx

José Salvador Antonio Méndez-Aguirre[2]
jmendez@upchihuahua.edu.mx

Mario IgnacioChacon-Murguia[1]
mchacon@itchihuahua.edu.mx

Alma Delia Corral-Saenz[1]
adcorral@itchihuahua.edu.mx

[1] Tecnológico Nacional de México / I.T. Chihuahua, Chihuahua, Chihuahua, México.
[2] Universidad Politécnica de Chihuahua, Chihuahua, Chihuahua, México.

Resumen

Se propone un método de bajo costo computacional para detectar la onda P300 en aplicaciones ubicuas de comunicación y control, el cual se denomina Procesamiento Embebido P300 (PE-P300). La entrada de PE-P300 es una señal electroencefalográfica (EEG) de un canal y la arquitectura de este método se basa en redes neuronales convolucionales. Para implementar el método PE-P300, también se presenta un sistema interfaz cerebro-computadora embebida que utiliza cuatro estímulos visuales en forma de recuadro para evocar la onda P300. La interfaz tiene conectividad con una red de Internet de las cosas para el movimiento o control de sistemas mecánicos. Para los experimentos, se generó una base de datos conformada por las señales EEG de 8 sujetos y de acuerdo con los resultados, PE-P300 es capaz de reconocer la onda P300 en las señales EEG de cada sujeto con un desempeño promedio de 96%. Además, PE-P300 requiere solo un electrodo y es posible realizar el procesamiento en tiempo real por su baja complejidad. Como conclusiones, PE-P300 es uno de los métodos más competitivo en la literatura debido a su desempeño de 96%, baja cantidad de electrodos (un electrodo activo) y a que extiende el procesamiento de la onda P300 a sistemas ubicuos utilizados en aplicaciones cotidianas.

Resume

A low computational cost method is proposed to detect the P300 wave in ubiquitous communication and control applications, which is called P300 Embedded Processing (PE-P300). The PE-P300 input is a one channel electroencephalographic (EEG) signal and the architecture of this method is based on convolutional neural networks. To implement the PE-P300 method, an embedded brain-computer interface system is also presented that uses four square visual stimuli to evoke the P300 wave. The interface has connectivity to an Internet of Things network for movement or control of mechanical systems. For the experiments, a EEG database of 8 subjects was generated and according to the results, PE-P300 can recognize the P300 wave in the EEG signals of each subject with an average performance of 96%. Furthermore, PE-P300 requires only one electrode and real-time processing is possible due to its low complexity. In conclusion, PE-P300 is one of the most competitive methods in the literature due to its 96% performance, low number of electrodes (one active electrode), and because it extends the processing of the P300 wave to ubiquitous systems used in everyday applications.

Palabras clave: Onda P300, electroencefalografía, redes neuronales convolucionales, interfaz cerebro computadora.

Keywords: P300 wave, electroencephalography, convolutional neural networks, brain-computer interface.

1. Introducción

La onda P300 es un potencial relacionado a evento que se presenta como una deflexión positiva en la actividad cerebral 300 ms después de la exposición a un estímulo externo. Esta onda se puede estudiar en señales de EEG y se aplica de forma exitosa en comunicación de personas con discapacidad severa, domótica y diagnóstico médico. Para evocar la onda P300, generalmente se recurre al paradigma Oddball, el cual consiste en presentar un estímulo externo en forma aleatoria y repetida entre un grupo de estímulos que se pueden considerar discordantes.

Existen diversos trabajos que recurren al análisis de P300, ya que esta onda tiene un alto porcentaje de reconocimiento (Li et al., 2020) y se puede utilizar en aplicaciones como diferenciación de la edad, medición de alcoholismo (Gamboa & Cruz, 2008; Hamidovic & Wang, 2019), comunicación y control enfocado a personas con Alzheimer (Dal-Bianco et al., 2018; Jervis et al., 2020), esclerosis lateral amiotrófica (McCane et al., 2015), epilepsia (Akramova, 2017; Zhong et al., 2019), parálisis cerebral (Kim & Lee, 2016), etc. Los diversos sistemas de control y comunicación que utilizan la onda P300 son muy variados, por ejemplo, Akman et al. proponen A-BCI (AKMAN AYDIN et al., 2017), un algoritmo para determinar las intenciones de un sujeto para controlar un sistema de internet por medio de 16 electrodos activos que tuvo un 93.71% de desempeño promedio. Corralejo et al. proponen en (Corralejo et al., 2014) el desarrollo de una herramienta para que personas con discapacidad por medio de 8 electrodos activos operen electrodomésticos que logra un desempeño de 74.4%. Masud et al. proponen en (Masud et al., 2017) un sistema de control por 6 electrodos activos para casa inteligente con un clasificador de Random Forest y se logró un desempeño de 87.5%. Lindig-León y Yáñez-Suárez proponen en (Lindig-León & Yáñez-Suárez, 2013) un algoritmo basado en función discriminante lineal (LDA) y decisión bayesiana para un deletreador de Donchin de tiempo reducido con 10 electrodos activos. Como resultado, obtuvieron el mismo desempeño que el deletreador de Donchin clásico, pero con sesiones de menor tiempo. Jijun et al. desarrollaron en (Tong et al., 2015) una interfaz cerebro-computadora basada en P300, una diadema emotiv EPOC® con 14 electrodos activos y una Tablet para generar un sistema que apoye en tareas cotidianas a personas con parálisis cerebral, traumas y esclerosis. El desempeño promedio del sistema fue de 88%. Kamran-Haider et al. hacen un análisis de clasificadores en (Jamshed et al., 2018) de señales EEG de 12 electrodos activos para reducir el ruido en aplicaciones de poligrafía y detección de mentiras. En este análisis, se incluyeron los clasificadores de máquina de soporte de vectores (SVM), función discriminante lineal (LDA), k-vecinos más cercanos (KNN) y redes neuronales artificiales (ANN). Entre estos clasificadores, ANN es el que tuvo mejor desempeño con 89%.

De acuerdo con el análisis de literatura realizado, se observó que la detección de la onda P300 se lleva a cabo mediante algoritmos con un enfoque de aprendizaje automático que tienen una etapa de extracción de características y una de clasificación. Para extraer características, se utilizan los métodos de single-trial (Thigpen & Keil, 2017), análisis de componentes principales (PCA) (Mirghasemi et al., 2006; Swarnkar et al., 2016) y transformada Wavelet (Ghassemzadeh & Haghipour, 2016; Uma & Kumar, 2014; Wang et al., 2014). Estos modelos se utilizan para reducir la cantidad de información cuando se obtiene el P300 con una gran cantidad de electrodos. Para clasificación, es común el uso de los métodos de LDA por partes (Capati et al., 2016; Ghassemzadeh & Haghipour, 2016; Li et al., 2020), SVM (Bhatnagar et al., 2016; Momennezhad et al., 2014; Rakotomamonjy & Guigue, 2008) y redes neuronales convolucionales (CNN) (Carabez et al., 2017; Liu et al., 2018; Vařeka, 2020). LDA por partes es un clasificador popular en múltiples aplicaciones de P300, pero requiere de una cantidad significativa de electrodos (8,16 y 64) para tener resultados aceptables. Los clasificadores basados en SVM y CNN han generado mejores resultados que LDA por partes, pero requieren de varios electrodos y se conforman de varias redes CNN o combinaciones de múltiples SVM.

Consecuentemente, el diseño y prueba de los métodos para procesar señales EEG relacionados a la onda P300 requiere de computadoras costosas con altas capacidades de procesamiento para lograr un buen desempeño. Esta complejidad en los cálculos se debe principalmente a que las señales EEG se adquieren con una cantidad significativa de canales y a mayor cantidad, mayor número de operaciones como es el caso de (Cecotti & Gr, 2011; Rakotomamonjy & Guigue, 2008) donde se utilizan 64 electrodos y desarrollan métodos que requieren costo computacional alto. Además, las señales son ruidosas y las interfaces para evocar el P300 se diseñan con una gran cantidad de estímulos; generalmente el deletreador de Donchin tiene 36 estímulos (Ron-Angevin et al., 2019) y se utilizan las intensificaciones de renglón-columna, lo que provoca un mayor costo en las operaciones de procesamiento en las señales EEG. Sin embargo, ha surgido recientemente una amplia variedad de tecnologías portables y simples de utilizar que obtienen señales EEG con mejor calidad.

Por todo lo mencionado anteriormente, el objetivo de este trabajo es combinar tecnologías de sistemas BCI con la capacidad de generalización de los modelos de aprendizaje profundo, para desarrollar un método de procesamiento embebido de señales EEG de bajo costo computacional. Por lo tanto, en este artículo se propone:

1. Un método con bajo costo computacional para la detección de la onda P300 denominado Procesamiento Embebido P300 (PE-P300).
2. Una interfaz cerebro computadora embebida.
3. Base de datos compuesta por señales EEG.

PE-P300 está orientado al desarrollo de sistemas ubicuos que auxilien a las personas con discapacidad a que realicen tareas por medio de Internet de las cosas (IoT por sus siglas en inglés). Este algoritmo tiene como entrada la información de un solo canal EEG y su procesamiento se basa en una CNN con solo una capa de extracción de características para detectar el P300. Además, para la experimentación y prueba de PE-P300, se propone la implementación de una interfaz cerebro-computadora embebida. Dicha interfaz evoca el P300 mediante cuatro estímulos visuales, tiene una tecnología reciente de adquisición de señales EEG, un procesador embebido portable y una conexión a una red IoT con esquema de computación en la frontera que permite el desarrollo de aplicaciones ubicuas con P300. Con esta interfaz se elabora una base de datos que servirá para ser analizada por PE-P300.

La descripción del artículo se detalla en el sentido de la creación del sistema BCI embebido para generar una base de datos y posteriormente analizarla con PE-P300, por lo que el resto del artículo se organiza de la siguiente manera: la sección 2 presenta los elementos de hardware que componen la interfaz cerebro-computadora embebida, la base de datos desarrollada en este trabajo y la descripción del software o método propuesto PE-P300 que se implementa en la interfaz cerebro-computadora embebida. La sección 3 presenta los resultados, la sección 4 la discusión y la sección 5 las conclusiones.

2. Metodología

2.1 Sistema BCI Embebido

La Figura 1 muestra que el sistema propuesto se compone de una etapa de adquisición de señales EEG, una interfaz gráfica para evocar el P300, un procesador embebido para correr el algoritmo PE-P300 y una aplicación remota que se enlaza mediante una red IoT. La red IoT se basa en el esquema de computación en la frontera (Ning et al., 2019) y permite el desarrollo de aplicaciones del sistema BCI ubicuas.

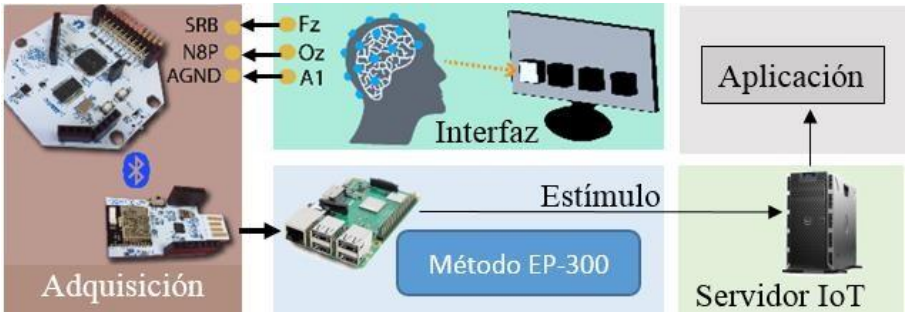


Figura 1. Sistema BCI propuesto.

Para evocar la onda P300, se utilizaron estímulos visuales con forma de recuadros que cambian de negro a blanco (uno a la vez) de manera aleatoria mientras que el sujeto mira fijamente uno de ellos, como muestra la Figura 2. El cambio de color blanco-negro se seleccionó debido a que está demostrado que esta combinación produce mayor amplitud en potenciales evocados (Cao et al., 2012). Para establecer los tiempos de cambios de color en los recuadros, se tomó como base el diagrama de tiempos de la base de datos BCI Competition III dataset II (Blankertz, 2004). El diagrama propuesto se observa en la Figura 2, donde el tiempo de intensificación T_H (solo uno de los cuatro recuadros es color blanco) es de 100 ms o 25 muestras recibidas, mientras que el tiempo donde todos los recuadros permanecen en negro T_L es de 120 ms o 30 muestras recibidas. Se le denomina sesión a la presentación de estímulos a un sujeto, mientras se obtienen señales EEG. Cada sesión se compone de la toma de 1000 muestras, la exposición de sesenta intensificaciones aleatorias entre los cuatro recuadros (3300 muestras) y 250 muestras extra después de la última intensificación, dando como resultado 4550 muestras (18.2 segundos). El número de intensificaciones está basado en la construcción de la base de datos BCI Competition III dataset II que se basa en el deletreador de Donchin propuesto en (Farwell & Donchin, 1988), y este número de intensificaciones se utiliza para evocar la onda P300.

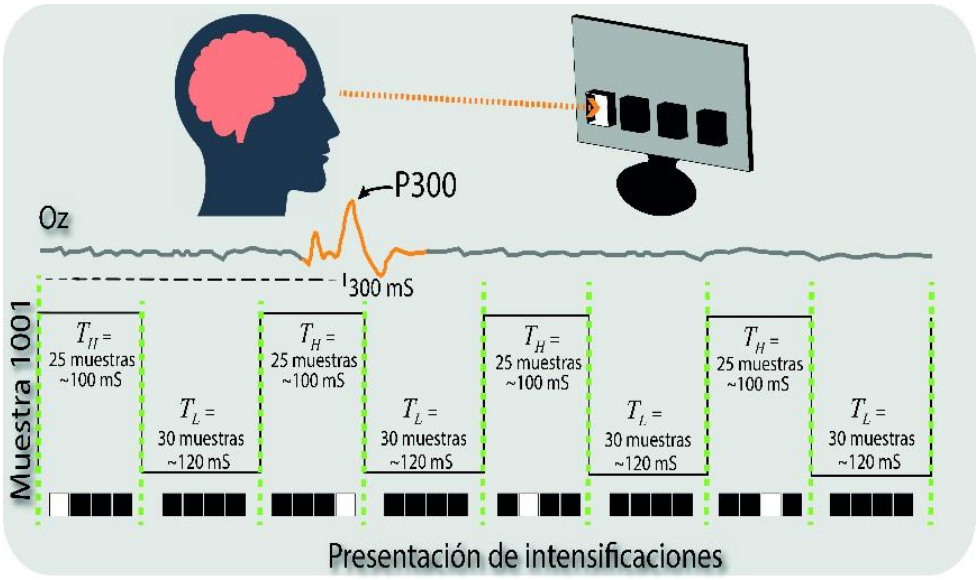


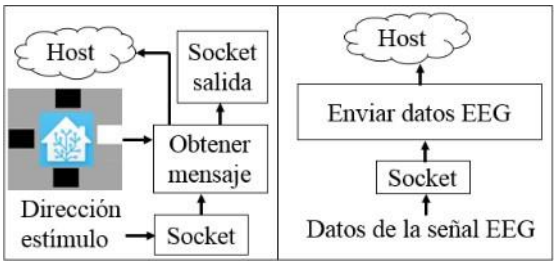
Figura 2. Diagrama de tiempo de los estímulos.

2.1.1 Adquisición de la señal EEG y sistema BCI

La etapa de adquisición está basada en el dispositivo Cyton de OpenBCI® y tres electrodos de copa de oro que se colocan en las posiciones del cuero cabelludo Oz, A1 (tierra) y Fpz (referencia). Los electrodos se conectan a la tarjeta de adquisición Cyton para convertir la actividad EEG del canal Oz a señal digital con una frecuencia de muestro *Fs* de 250Hz. La señal obtenida del electrodo Oz se define como $s(n)$ *donde* n son 4550 muestras tomadas durante 18.2 s. Esta señal se transfiere a la tarjeta embebida Raspberry Pi 3 modelo B+ vía Bluetooth 4.2/BLE para ser analizada por el algoritmo PE-P300 y detectar el estímulo que el sujeto mira fijamente durante la sesión que fue obtenida la señal $s(n)$. La tarjeta Cyton de 32 bits utiliza el conversor análogo digital ADS1299 de Texas Instruments y el microcontrolador PIC32MX250F128B para la digitalización de la señal, además, esta tarjeta fue seleccionada porque es portátil, de bajo costo, se puede utilizar con cualquier plataforma de computación basada en Python y las señales EEG obtenidas presentan poco ruido en comparación con los dispositivos BCI comerciales y clínicos. La Raspberry Pi fue seleccionada ya que se puede programar con Python y se puede utilizar en aplicaciones ubicuas basadas en sistemas embebidos.

Una vez que PE-P300 procesa la señal $s(n)$ (proceso que se explica en la subsección 2.3) la Raspberry utiliza el puerto WiFi para enviar a un servidor local la dirección del estímulo que el sujeto miró fijamente. El servidor es cualquier computadora que tenga instalado el software que se diseñó en este trabajo, el cual se diseñó Python 2.7 y se basó en el esquema hilo-socket. Como requerimiento de hardware solamente es necesario contar con un mínimo de 256 Mb de memoria RAM y 512 Mb de espacio en disco duro. El sistema operativo tiene dos procesos que se muestran en la Figura 3, uno de codificación de mensaje y otro para enviar la señal EEG a la nube. Para la codificación del mensaje, el servidor recibe la dirección del estímulo mediante un socket de entrada. El sistema operativo tiene un hilo que reconoce la interfaz cerebro-computadora utilizada en la sesión y recibe la dirección del estímulo para codificar el mensaje que el sujeto seleccionó de la interfaz (Figura 3a). Dicho mensaje se envía a un host que está en la nube y al socket de salida para controlar alguna aplicación como el driver de un motor, definir una trayectoria de una silla de ruedas, encender/apagar una televisión, un foco o un sistema de aire acondicionado y calefacción.

El proceso de enviar la señal EEG se muestra en la Figura 3b, un socket recibe los datos de la señal EEG para que un hilo los envié a un host de la nube y que cualquier dispositivo móvil pueda tener acceso a ellos. De esta manera, un médico puede monitorear la señal de forma remota.



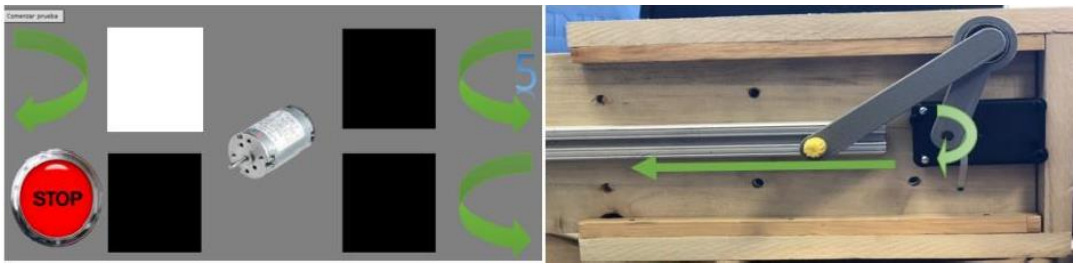
a) b)

Figura 3. Procesos del servidor local. a) Codificar mensaje. b) Enviar los datos EEG.

Estos procesos generados en el servidor local permiten que el sistema BCI embebido tenga una conectividad de computación en la frontera dentro de cualquier red IoT. Esta conectividad permite al sistema BCI funcionar de forma ubicua, es decir que el sistema es portable y funciona en cualquier parte que exista conectividad a WiFi.

2.1.2 Aplicaciones del sistema BCI

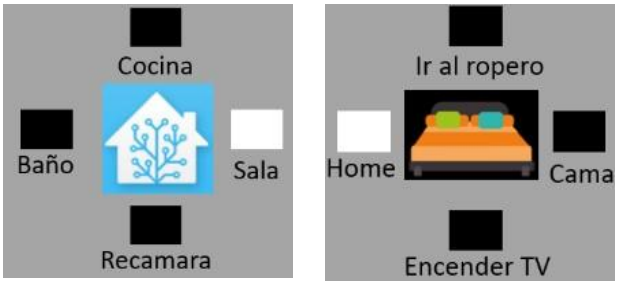
Los recuadros en la interfaz pueden tener un significado que dependerá de la aplicación que se está utilizando. Es decir, los recuadros en la interfaz se muestran en diferentes diseños, por ejemplo, la Figura 4a muestra un diseño para controlar el encendido y giro de un mecanismo compuesto por un motor de corriente directa de la Figura 4b, el cual simula el movimiento de un actuador para prótesis o silla de ruedas. En este caso, el significado que representa cada recuadro está dado por las flechas y el símbolo de stop más cercano a ellos. De esta manera, si el sujeto fija su mirada en el recuadro de la flecha en dirección de las manecillas de reloj, al terminar la sesión y que EP-P300 determine el recuadro en el cual se fijó la mirada, el mecanismo rotativo girará en el sentido de las manecillas del reloj.



a) b)

Figura 4. Diseño de interfaz para control de mecanismo. a) Interfaz para generar estímulos. b) Mecanismo rotativo.

La Figura 5 muestra otro diseño de la interfaz cuya aplicación es un control para domótica que controla una silla de ruedas para llevar a una persona a diferentes ubicaciones dentro de una casa. En este caso, si el sujeto fija su mirada en el recuadro inferior de la Figura 5a, significará que desea trasladarse a la recámara, por lo cual una vez en el lugar, se despliega el menú de la Figura 5b, dando la opción de ir a un lugar más específico en la recámara. Cabe mencionar que este diseño es ilustrativo para demostrar que se pueden realizar varios diseños con la interfaz de 4 recuadros para diferentes aplicaciones.



a) b)

Figura 5. Diseño de interfaz para servicios de domótica. a) Posición de inicio. b) Recámara.

2.2 Base de datos

Para el diseño de algoritmos, se creó una base de datos compuesta de muestras obtenidas bajo un protocolo de adquisición cuya primer etapa es aplicar un cuestionario creado para documentar y validar que el sujeto de pruebas cumpla el perfil para los experimentos (Lee, 2018). A pesar de que se utilizan sujetos sanos para la base de datos, se aseguró que cumplieran algunos requerimientos, por lo que, bajo preguntas, el cuestionario documenta si el sujeto no presenta sueño, cansancio, ingesta de medicamentos y si tiene familiares directos con trastornos o tumores cerebrales. Lo anterior se realiza dado que la respuesta afirmativa de una de estas preguntas está relacionada a alteraciones con la presentación de la onda P300 (Di et al., 2010; Kim & Lee, 2016). En la segunda etapa del protocolo, se colocan los electrodos en las posiciones Oz, Fpz y A1. Posteriormente, se le dan indicaciones al sujeto de prueba de permanecer quieto en una silla cómoda fijando la mirada solamente en uno de los recuadros (estímulo) de la interfaz. La última etapa del protocolo es el procedimiento para la toma de muestras mientras se realiza la exposición de estímulos. En esta etapa, el sujeto mira fijamente solo un estímulo de la interfaz de la Figura 2 mientras estos se intensifican aleatoriamente 15 veces cada uno.

Se generó una base de datos con 8 sujetos sanos de 21-25 años del laboratorio de investigación “Percepción Visual con Aplicaciones en Robótica” del Tecnológico Nacional de México / Instituto Tecnológico de Chihuahua seleccionados voluntariamente, siete de sexo masculino y una del sexo femenino. Del grupo de sujetos, fueron seleccionados con estas características debido a que se utiliza comúnmente este rango de edades y proporciones en la literatura (Kuziek et al., 2017; Samima et al., 2017; Zhang et al., 2016). A cada sujeto se le realizaron 48 sesiones, las cuales generaron 48 señales $s(n)$ y cada una de ellas corresponde en haber fijado la mirada en cada uno de los estímulos. De esta manera, la base de datos es un arreglo compuesto por 48x4550 por sujeto que se refieren a 48 señales de 4550 datos.

Para el análisis de la base de dato se utiliza el algoritmo PE-P300 que se detalla en la sección 2.3 y está basado en un modelo de redes neuronales convolucionales. Este modelo se entrena y valida por sujeto dado que la latencia y amplitud de la onda P300 en cada sujeto es diferente. De esta manera, de las 48 señales por sujeto, se destinan 28 señales para entrenamiento y 20 por sujeto para la validación de la red neuronal convolucional (subsección 2.3.3). Los datos fueron seleccionados de forma aleatoria para cada conjunto. La Figura 6 muestra un ejemplo de lo que se puede obtener con el sistema, una señal $s(n)$ donde se obtiene el P300 y una señal donde solo se tiene ruido (no P300). La señal continua corresponde a una ventana de 200 ms después de que se el sujeto estaba mirando el recuadro que se intensificó, y la discontinua a una ventana después de que se intensificó un recuadro que el sujeto no estaba mirando.

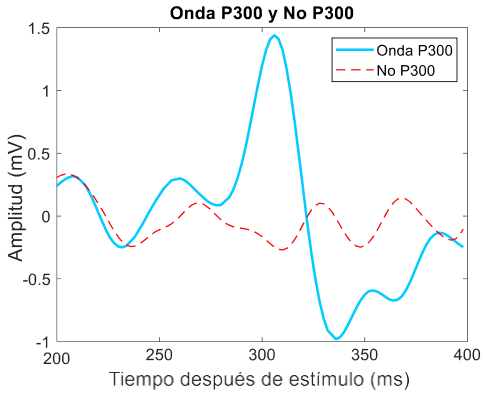


Figura 6. Componente P300 y NoP300 de la señal EEG.

2.3 Método PE-P300

Este método detecta el estímulo que el sujeto mira fijamente y de acuerdo con la Figura 7, tiene cuatro etapas: preprocesamiento, agrupamiento, detección de P300 y clasificación.

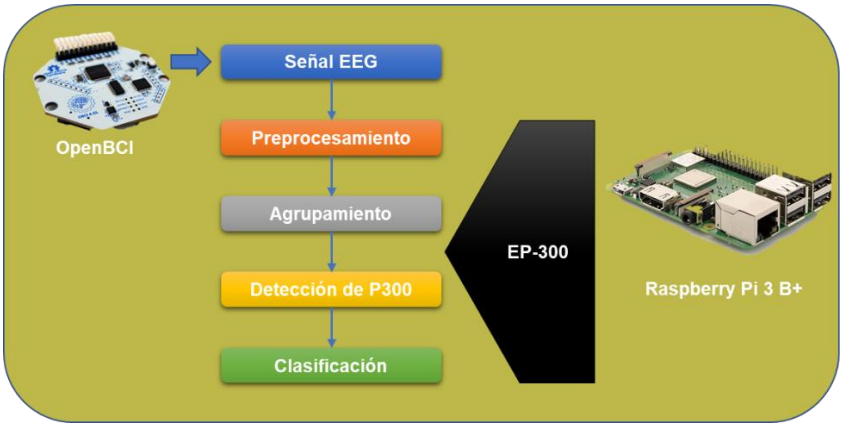


Figura 7. Esquema general de PE-P300.

2.3.1 Preprocesamiento

Esta etapa consiste en un filtrado con un filtro digital Butterworth pasabandas de orden 3 con frecuencias de corte de 1 a 15 Hz. Estas características fueron seleccionadas como base del trabajo (Ramirez-Quintana et al., 2020), además de que este filtro es IIR con la banda de paso más plana y el orden de este filtro presentó la eliminación de ruido suficiente en las señales EEG. El filtro se implementa mediante la siguiente función de transferencia:

$$H(z) = \frac{0.0039 - 0.0118z^{-2} + 0.0118z^{-4} - 0.0039z^{-6}}{1 - 5.27z^{-1} + 11.63z^{-2} - 13.74z^{-3} + 9.17z^{-4} - 3.28z^{-5} + 0.49z^{-6}} \quad (1)$$

El filtro se aplica en la señal debido a que la onda P300 se compone de frecuencias que están en el rango definido por las frecuencias de corte (Rakotomamonjy & Guigue, 2008). El filtro presenta distorsión de fase en las primeras muestras, por lo que el análisis a partir del filtrado se realiza en el intervalo $1001 < n \leq 4550$, además, las intensificaciones comienzan después de la muestra 1000. La salida del filtro se define como $s_f(n)$. Posteriormente, se realiza una normalización con Z-score (Kundu & Ari, 2017) para obtener una señal con media cero y desviación estándar unitaria, lo que hace que las señales de todos los sujetos estén en el mismo rango dinámico de amplitud y media cero. Esta normalización se define por:

$$s_u(n) = \left(s_f(n) - \mu_{sf}\right) / \sigma_{sf} \quad (2)$$

donde $s_u(n)$ es la señal normalizada, μ_{s_f} la media de la señal filtrada y σ_{s_f} la desviación estándar.

2.3.2 Agrupamiento por estímulo

Esta etapa consiste en generar un arreglo de señales promedio que miden la presencia de la onda P300 después de cada estímulo j. Para ello, primero se descompone $s_u(n)$ en 60 fragmentos de 400 ms, que van desde los 100 ms a 500 ms después de la intensificación de cada estímulo. Es decir, cada señal $s_u(n)$ se descompone en 60 fragmentos con intervalos de 400 ms, ya que en ese intervalo de tiempo es cuando se presenta la onda P300 (Samima et al., 2017). Debido a que la frecuencia de muestreo es 250Hz, cada fragmento se compone de 100 muestras. Estos fragmentos se definen como $P_{ij}(m)$ donde $i=1,\ldots,15$ son los fragmentos presentados después de la intensificación del estímulo j, donde $j=1,\ldots,4$. Es decir, $P_{ij}(m)$ se divide en cuatro grupos, donde cada grupo contiene quince fragmentos de la señal $s_u(n)$ después de la presentación de cada estímulo j. Finalmente, el agrupamiento se realiza con el promedio por grupos dado por:

$$X_{Ej}(m) = \frac{1}{15}\sum_{i=0}^{15} P_{ij}(m) \quad m = 1,\ldots,100 \quad (3)$$

donde m es un índice para las muestras en el fragmento de 400 ms, $X_{Ej}(m)$ es un arreglo de 4 señales de 100 datos cada una, las cuales corresponden a los cuatro promedios de los 15 fragmentos luego de la intensificación de cada estímulo. Debido a que el sujeto observa solo un estímulo, una de las señales del arreglo $X_{Ej}(m)$ debe contener la onda P300. De esta forma la señal $X_{Ej}(m)$ representa el vector de características de cada sesión.

2.3.3 Detección con CNN

Esta etapa detecta la presencia de la onda P300 con una red neuronal convolucional basada en la red CNN300 del sistema LEBci de (Ramirez-Quintana et al., 2020). La red CNN300 tiene como entrada los agrupamientos por estímulos de canales EEG O1, Oz y O2 $X_{Ej}(m,c)$, donde c se refiere al canal O1, O2 y Oz. CNN300 extrae características con dos capas de convolución y rectificación lineal y clasifica con una capa totalmente conectada con función de activación softmax. La primera capa de convolución y rectificación reducen la dimensión de las muestras y generan mapas de características, mientras que la segunda capa de ellas reduce a un canal la información de los tres canales EEG. La capa de clasificación encuentra la probabilidad de que las señales EEG contengan la onda P300.

No obstante, PE-P300 utiliza un canal EEG (Oz). Para esta red, la entrada son los agrupamientos $X_{Ej}(m)$ del canal Oz, por lo que solo se utiliza una capa de convolución y rectificación lineal, como se observa en la Figura 8. La clasificación también se compone una capa totalmente conectada y con función de activación softmax.

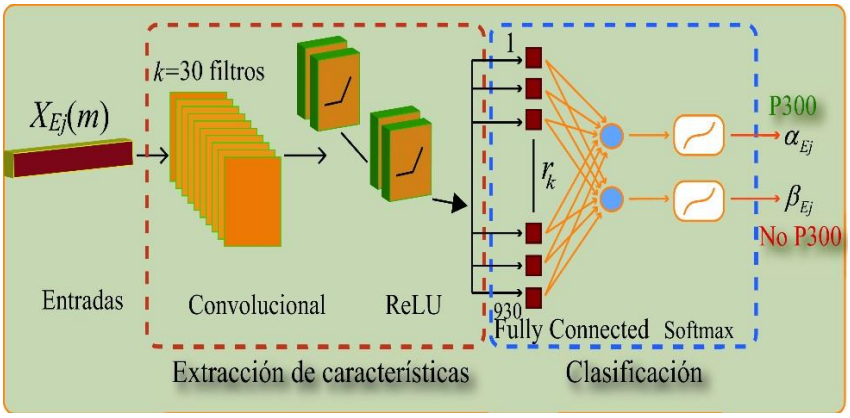


Figura 8. Topología de la red neuronal utilizada para un solo canal.

La capa convolucional realiza treinta mapeos $k=1,\ldots,30$ de cada promedio j de la señal de entrada $X_{Ej}(m)$ en conjuntos de características mediante la convolución espacial con k filtros lineales. Estos filtros se definen por un conjunto de pesos w_k, que fueron definidos variando experimentalmente la longitud, donde finalmente se determinó 1x70 ($q=1,\ldots,70$) dados los mejores desempeños (Pamuła, 2018) y se componen también de la polarización B_k. De esta manera, cada mapeo $c_{kj}(p)$ se define como:

$$c_{kj}(p) = X_{Ej}(m+69) * w_{jk} + B_k \qquad \begin{matrix} m=1,\ldots,100 \\ k=1,\ldots,30 \end{matrix} \tag{4}$$

cada mapeo $c_{kj}(p)$ tendrá una dimensión 1x31 ($p=1,\ldots,31$, resultado de la convolución espacial). La siguiente capa está dada por una función de activación denominada rectificador lineal (ReLU) (Liu et al., 2018). La función característica de esta capa es la siguiente expresión:

$$r_{kj}(p) = \begin{cases} 0, & c_{kj}(p) \le 0 \\ c_{kj}(p), & c_{kj}(p) > 0 \end{cases} \tag{5}$$

Esta etapa ajusta los valores p de $c_{kj}(p)$ para tomar solo aquellos que estimulan a la red de acuerdo con la Ecuación (5), donde se toma el valor de $c_{kj}(p)$ si es positivo, o cero si es negativo. Para la clasificación del modelo de la red propuesta en la Figura 8, se toma cada valor del arreglo $r_{kj}(p)$ y se unen en un nuevo arreglo denominado $u_j(l)$ con dimensión 930 resultado de pxq (l=1,…,930), lo cual se caracteriza por lo siguiente:

$$u_j(l) \equiv r_{kj}(p), \quad l = p + (k-1)P \tag{6}$$

donde $P=100$. El arreglo $u_j(l)$ es la entrada de dos neuronas $v=\{1,2\}$ en la capa totalmente conectada (Fully Connected), caracterizada por lo siguiente:

$$\varphi_{vj} = wf_v(l)u_j(l) + bf_v \tag{7}$$

donde φ_{vj} contiene los valores de salida de la capa totalmente conectada de las dos neuronas.

Finalmente, la función softmax calcula la probabilidad de que φ_{vj} pertenezca a la clase P300 (α_{Ej}) o la clase No P300 (β_{Ej}) . Esta función se describe de la siguiente forma (Ramirez-Quintana et al., 2020):

$$\Phi_{vj} = \frac{e^{\varphi_{vj}}}{\sum_{v=1}^{2} e^{\varphi_{vj}}} \tag{8}$$

donde Φ_{vj} da valores en términos de probabilidad. Si $\Phi_{v=1}$, entonces la salida de la red es el vector α_{Ej} que contiene la probabilidad de presencia de la onda P300 para cada señal EEG de cada estímulo j. Asimismo, si $\Phi_{v=2}$, entonces la salida de la red es el vector β_{Ej} que indica la probabilidad de No P300.

2.4.1 Predicción del estímulo seleccionado

Una vez que se determinan los valores de pertenencia a cada clase de cada agrupación j en $X_{Ej}(m)$, se determina cuál de ellos cuenta con mayor probabilidad de presencia de la onda P300. Para ello, se utiliza el parámetro α_{Ej} que representa a la clase P300, que fue seleccionado debido a que indica la presencia de la onda P300. Para ello, se considera como decisión tomar el valor máximo de probabilidad de los estímulos j de la siguiente manera:

$$e = \max_j \alpha_{Ej} \tag{9}$$

e hace referencia al índice del número de estímulo j al que se fijó la mirada durante la sesión de toma de muestras.

3. RESULTADOS

Esta sección presenta los resultados en referente a la implementación, desempeño de PE-P300 y una comparación del funcionamiento del sistema BCI con método con otros sistemas populares en la literatura que procesan el P300 para tareas cotidianas.

3.1 Implementación de PE-P300

Los tiempos del sistema se presentan en la Tabla 1, donde se especifica que el tiempo de duración de una sesión para evocar el P300 es de 18.2 segundos. Se generaron dos diseños con la interfaz gráfica que evocan el P300 para control de motor, activación de trayectorias en una casa y controles de iluminación, temperatura y televisión. El tiempo de procesamiento de la señal EEG por PE-P300 es de 1.8 s. El resultado del procesamiento es el estímulo que el sujeto seleccionó, el cual es trasmitido por Wifi a un servidor local. El tiempo de envío del estímulo identificado de la Raspberry al servidor es de 86.3 microsegundos.

Tiempo de duración	Sesión	Procesamiento	Estímulo identificado a Host	Señal EEG a Host
PE-P300	18.2	1.8 s	86.3 µS	35.28

Tabla 1. Duración de procesamiento de PE-P300

El servidor local tiene la opción de pedir los datos filtrados EEG de $s_f(n)$ después en recibir el estímulo seleccionado. Esta opción se utiliza para que el servidor local envíe estos datos EEG a un host que encuentra en la nube para seguimiento médico. El tiempo de envío de la señal EEG de la Raspberry al servidor es de 35.28 milisegundos.

Estos tiempos de sesión, procesamiento y trasmisión son factibles para que el sistema BCI embebido funcione correctamente en línea con cualquier aplicación.

3.2 Evaluación de PE-P300

Se elaboró un análisis donde se incluyen las métricas de reconocimiento (R), precisión (P) y F-measure (F1), los cuales se definen en (Yaacoub et al., 2017). Este análisis se describe a detalle en la Tabla 2 e incluye las etapas de entrenamiento y validación para el total de sujetos.

R, P, y F1 tuvieron valores cercanos a uno en el conjunto de entrenamiento, lo que significa que PE-P300 se ajustó correctamente a los datos de dicho conjunto. Sin embargo, en el conjunto de prueba, R bajo a 0.93 y P bajo hasta 0.86. De acuerdo con las definiciones de R, P y F1 de (Yaacoub et al., 2017), esto significa que la red tuvo mejor desempeño en la detección de señales con la onda P300 que en las señales sin P300, es decir, tuvo más falsos positivos que falsos negativos. Esta tendencia a falsos positivos se debe a la composición de las señales de la base de datos, ya que algunos sujetos perdían la concentración momentáneamente debido a que tenían sueño durante las sesiones de adquisición, generándose señales P300 de baja amplitud cuando no se debe presentar esta onda. Esto no se refleja en el entrenamiento ya que la red se ajusta a las señales que se presentan. Sin embargo, si se reflejaba en el conjunto de prueba ya que estas P300 que no se debían presentar varían mucho en amplitud y latencia, causando que estas P300 sean diferentes entre las del conjunto de señales de entrenamiento y las del conjunto de señales de prueba. Lo anterior se ilustra en la Figura 9, con óvalos verdes se denota un ejemplo de señales en la etapa de entrenamiento, mientras que con óvalos verdes señales de la etapa de prueba. La baja cantidad de falsos negativos indican que el ruido generado en la señal EEG no es significativo en el desempeño de PE-P300.

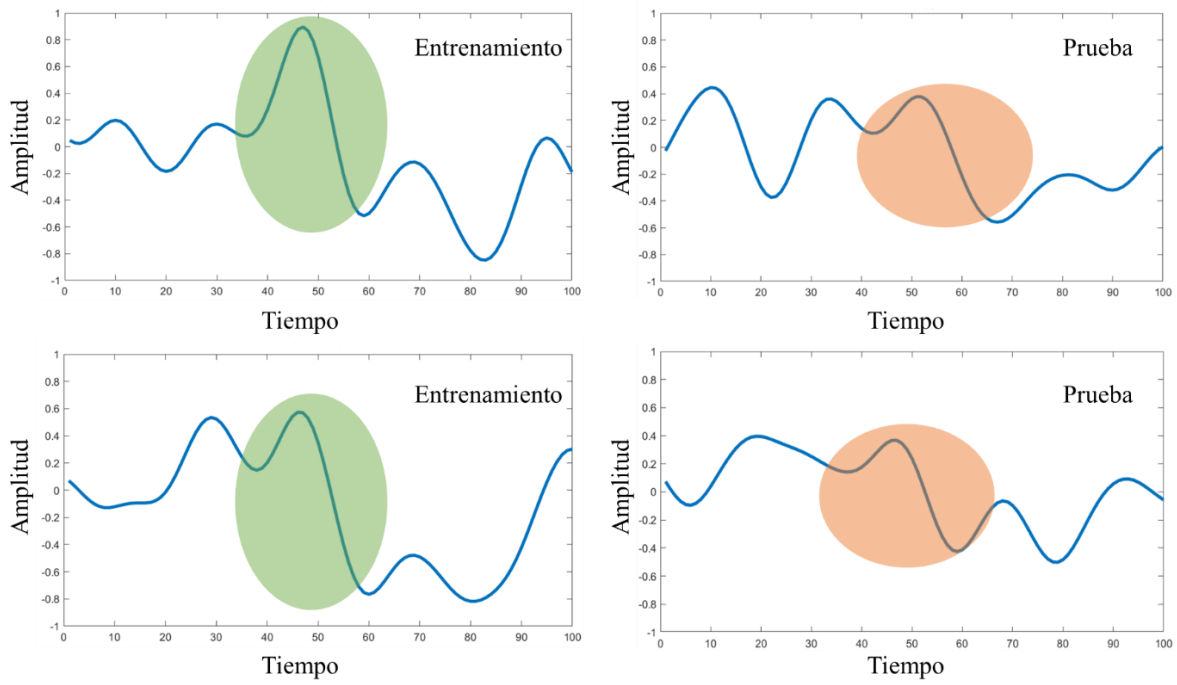


Figura 9. Ejemplo de señales EEG de entrenamiento y prueba con la onda P300 presente.

	Entrenamiento			Prueba		
Sujeto	**Reconocimiento**	**Precisión**	**F-measure**	**Reconocimiento**	**Precisión**	**F-measure**
1	1	1	1	0.94	0.86	0.88
2	0.99	0.97	0.98	0.91	0.81	0.83
3	0.99	1	0.98	0.95	0.94	0.9
4	0.99	1	0.98	0.86	0.74	0.72
5	1	1	1	0.99	0.95	0.98
6	1	1	1	0.86	0.71	0.73
7	1	1	1	1	1	1
8	1	1	1	0.94	0.9	0.87
Promedi	**1**	**1**	**0.99**	**0.93**	**0.86**	**0.86**

Tabla 2. Evaluación de resultados de PE-P300.

La Tabla 3 muestra el número de muestras detectadas correctamente y el desempeño por sujeto. Se puede observar que los sujetos 1, 2, 4 y 6 tienen desempeños menores a 100%, quienes reportaron que haber tenido sueño durante alguna de las sesiones. El resto de los sujetos tuvieron un desempeño de 100% y reportaron haber seguido correctamente el protocolo de adquisición.

Sujeto	**Sesiones correctas**	**Desempeño**
1	18	90%
2	19	95%
3	20	100%
4	18	95%
5	20	100%
6	18	90%
7	20	100%
8	20	100%
Promedio	19.125	96%

Tabla 3. Desempeño de PE-P300.

Se puede observar en las Tablas 2 y 3 que los sujetos con los resultados bajos de P, R y F1 tienen desempeños menores a 100%. Por lo tanto, de acuerdo con estos resultados, PE-P300 puede generar falsos positivos si el sujeto realiza previamente alguna actividad que le cause fatiga mental.

4. Discusión

Para ubicar el desempeño promedio de la Tabla 3, se realizó una comparación del sistema BCI propuesto con otros reportados recientemente en la literatura que se diseñaron para aplicaciones específicas en entornos cotidianos. Esta comparación no considera los métodos probados en BCI Competition de (Cecotti & Gr, 2011; Liu et al., 2018) ya que estos no se pueden implementar en sistemas de baja capacidad de cómputo o embebidos. No existe una metodología de comparación en sistema BCI embebidos o ubicuos, por lo tanto, se generó un esquema de selección de sistemas BCI para aplicaciones específicas que fueran de reciente publicación y reportarán la siguiente información:

Numero de sujetos (NSuj): entre más sujetos se involucren en la evaluación del método propuesto, se conocerá mejor la capacidad de generalización de dicho método, ya que se tiene un universo de muestras más apropiado para el entrenamiento.

Dispositivo de adquisición (Dadq): para desarrollar un sistema BCI embebido y ubicuo se deben considerar el precio comercial, calidad de las señales obtenidas y acceso a ellas en tiempo real. Por ejemplo, un dispositivo costoso es poco factible para personas de escasos recursos.

Número de canales (NCh): al tener la menor cantidad posible de electrodos en el cuero cabelludo, mayor es la comodidad en el uso del BCI y se puede tener un buen desempeño con la menor capacidad de procesamiento posible.

Desempeño (Des): se refiere a la cantidad de muestras correctamente detectadas entre la cantidad total de muestras. Esta métrica es la más utilizada en la literatura para medir la capacidad de clasificación del algoritmo.

Clasificador (Cl): es el algoritmo que se utiliza para determinar en cuál de las señales de entrada se localiza la onda P300.

Variables (M): Relacionado al costo computacional, es el número de variables necesita el algoritmo para analizar una señal de entrada. Se toma a consideración solamente la etapa de clasificación sin tomar en cuenta el preprocesamiento y la extracción de características.

A continuación, se presenta una breve descripción de los métodos seleccionados y en la Tabla 4 se muestra la información de Nsuj, Dadq, NCh, Des, Cl y variables de cada uno.

Método	**Nsuj**	**Nch**	**Dadq**	**Des**	**Cl**	**M**
PE-P300	8	1	OpenBCI	96%	CNN	3062
LEBci (Ramirez-Quintana et al., 2020)	8	3	OpenBCI	96.43%	CNN	80,664
Silla de ruedas (Minguez et al., 2009)	5	16	gUSBamp	93%	SWLDA	125,600
Dispositivo móvil (Anil et al., 2018)	4	8	OpenBCI	67%	Threshold	--
Casa inteligente (Achanccaray et al., 2017)	8	16	gUSBamp	90%	ANFIS	16,000
A-BCI (AKMAN AYDIN et al., 2017)	10	16	V-amp 16	93.71%	LDA	38,416
Navegador web (Martinez-Cagigal et al., 2017)	5	8	g.tec	95.75%	LDA	3600
Submatrix (Shen et al., 2015)	7	10	SynAmp2	96.03%	Pseudokurtosis	--
Sistema de manejo remoto (De Venuto et al., 2017)	5	6	g.tec	80.5%	Threshold	--
Único intento P300 (Haghighatpanah et al., 2013)	2	1	---	65%	LDA	--
Máquina de aprendizaje extremo P300 (Xie et al., 2014)	9	1	NetAmps 300	85.72%	Extreme learning machine	--

Tabla 4. Comparación de PE-P300 con otros métodos populares en la literatura.

LEBci: es un método que analiza señales EEG obtenidas de 8 sujetos con el dispositivo OpenBCI© y el uso de 3 canales. El método procesa las señales con un arreglo EEG de señales promediadas y realiza la clasificación por medio de un modelo CNN. LEBci Se obtiene un desempeño promedio de 96.43% (Ramirez-Quintana et al., 2020).

Silla de ruedas: se presenta una silla de ruedas controlada con P300 que utiliza una interfaz con cinco estímulos que representan los controles de la silla. El procesamiento se basó en análisis discriminante lineal (LDA) (Minguez et al., 2009).

Dispositivo móvil: se propone un BCI basado en P300 que se puede comunicar con un dispositivo móvil con iOS. Para evocar el P300, existe una interfaz en un dispositivo móvil que genera tres estímulos representados con dibujos. El procesamiento se basa en filtros selectivos de frecuencia (Anil et al., 2018).

Casa inteligente: se presenta un control basado en P300 para casa inteligente que consta de seis estímulos con figuras de objetos a controlar (TV, teléfono, radio, persianas, luz y temperatura). El procesamiento se basa en un método ANFIS (Achanccaray et al., 2017).

A-BCI: utiliza una interfaz basada en el paradigma RBP (*Region based paradigm*) para evocar el P300. El procesamiento se lleva a cabo por un análisis discriminante lineal (LDA) (AKMAN AYDIN et al., 2017).

Navegador web: es un sistema para navegar en Internet basado en P300 y tiene una interfaz basada en el paradigma Odbball que contiene una gran cantidad de estímulos que representan caracteres alfanuméricos y acciones para navegar. El método de procesamiento es LDA (Martinez-Cagigal et al., 2017).

Submatrix: se desarrolla un sistema basado en cuatro deletreadores para evocar la onda P300. Estos deletreadores contienen caracteres alfanuméricos. Se ponen a prueba dos algoritmos, valor máximo y pseudo-kurtosis, con los que se obtiene un 96.03% y un 94.81% de desempeño promedio (Shen et al., 2015).

Sistema de manejo remoto: es un sistema que controla remotamente actuadores mecánicos para el manejo de un carro prototipo. La interfaz para evocar el P300 tiene cuatro símbolos que indican dirección y aceleración. El procesamiento se basa en un LDA cuya entrada son cinco características (De Venuto et al., 2017).

Único intento P300: es un método que propone el análisis de la base de datos BCI Competition dataset II en la selección de un único canal; Cz, Fz o Pz. El método puede reconocer la onda P300 en las señales EEG con resultados por debajo del 65% de desempeño promedio. Como métodos de procesamiento se utiliza un análisis de componentes principales basado en un filtro de Wavelet y un LDA como clasificador (Haghighatpanah et al., 2013).

Máquina de aprendizaje extremo P300: se propone un método para el análisis de señales de 9 sujetos con un solo canal, utilizando una máquina de aprendizaje extremo para procesar las señales EEG. El método alcanza un desempeño promedio de un 85.72%. (Xie et al., 2014)

Se puede observar en la Tabla que PE-P300 tiene un mejor desempeño que Silla de ruedas, dispositivo móvil, Casa inteligente, A-BCI, Sistema de manejo remoto, único intento P300 y máquina de aprendizaje extremo P300. Por otro lado, PE-P300 tiene un desempeño similar a Submatrix y el Navegador web, pero a diferencia de estos métodos, PE-P300 utiliza solo un canal EEG. Además, PE-P300 tiene como dispositivo de adquisición a OpenBCI©, el cual es de código abierto y se puede conectar a cualquier computadora o sistema embebido. Los métodos de Silla de ruedas, Casa inteligente, A-BCI, Navegador web, Submatrix y sistema de manejo remoto utilizan dispositivos que se conectan a computadoras de alta capacidad de procesamiento y enfocados a aplicaciones clínicas.

En lo referente a costo computacional, se puede observar que PE-P300 tiene un costo computacional menor que los métodos de (Ramirez-Quintana et al., 2020), (Minguez et al., 2009), (Achanccaray et al., 2017), (AKMAN AYDIN et al., 2017) y (Martinez-Cagigal et al., 2017). Esto se debe a que a pesar de que PE-P300 se basa en una CNN, solamente se procesa $j=4$ estímulos, mientras que los demás métodos procesan utilizan de $j=9$ *a* 45 estímulos. Los métodos de (Anil et al., 2018), (Shen et al., 2015), (De Venuto et al., 2017), (Haghighatpanah et al., 2013) y (Xie et al., 2014) no proporcionan suficiente información para hacer el cálculo de costo computacional, pero (Anil et al., 2018) y (De Venuto et al., 2017) tienen desempeños muy bajos, mientras que (Shen et al., 2015) utiliza 10 electrodos. Aunado a esto, (Haghighatpanah et al., 2013) y (Xie et al., 2014) son métodos que utilizan un solo canal pero tienen desempeños por debajo de un 85.72%, además, fueron elaborados hace 7 y 8 años.

Los algoritmos de procesamiento de todos los métodos reportados en la literatura para procesamiento embebido de P300 se basan en LDA, ANFIS e inferencias de momentos estadísticos. Por otro lado, PE-P300 se adapta a las señales P300 de cada sujeto debido al entrenamiento y el algoritmo que aprovecha las ventajas las redes neuronales convolucionales, pero con un bajo costo computacional.

5. CONCLUSIONES

En este artículo se presentó PE-P300, un método para detectar la onda P300 en un sistema BCI embebido ubicuo con conectividad a una red IoT como sistema de computación en la frontera. El método tiene como entrada los datos de una señal EEG adquirida solo con el electrodo Oz y el procesamiento se basa en la arquitectura de una red neuronal convolucional. PE-P300 tiene un conjunto de interfaces para evocar la P300 que se diseñaron para brindar servicios de comunicación y control. El procesamiento de PE-P300 se basa en un filtro pasabandas de tercer orden, una etapa de promediado de la señal y una red neuronal convolucional. Esta red cuenta con una capa para extracción de características y una capa totalmente conectada con función de activación softmax para determinar la probabilidad de obtener la onda P300. Esta probabilidad es utilizada para determinar el estímulo que el sujeto selecciono.

De acuerdo con los tiempos de sesión, procesamiento y envío al servidor, PE-P300 es factible para aplicaciones de sistemas embebidos y de computación en la frontera. De acuerdo con la evaluación del desempeño, PE-P300 funciona correctamente si el sujeto sigue adecuadamente el protocolo. En caso de que el sujeto pierda la concentración, se pueden tener falsos positivos. El estudio comparativo mostró que el método propuesto tiene uno de los mejores desempeños reportados en la literatura debido a la red neuronal convolucional adaptada a una entrada EEG y a un bajo costo computacional.

Consecuentemente, debido al desempeño y bajo costo computacional, PE-P300 es un método que permite el desarrollo de sistemas BCI embebidos ubicuos que se pueden utilizar en cualquier entorno cotidiano.

Agradecimientos

Este proyecto se realizó bajo el apoyo de Tecnológico Nacional de México con apoyo número 7598.20-P. Los autores agradecen a los voluntarios que participaron en la realización de pruebas.

REFERENCIAS

Achanccaray, D., Flores, C., Fonseca, C., & Andreu-Perez, J. (2017). A P300-based brain computer interface for smart home interaction through an ANFIS ensemble. *IEEE International Conference on Fuzzy Systems*. https://doi.org/10.1109/FUZZ-IEEE.2017.8015770

AKMAN AYDIN, E., BAY, O. F., & Guler, I. (2017). P300 Based Asynchronous Brain Computer Interface for Environmental Control System. *IEEE Journal of Biomedical and Health Informatics*, *2194*(c), 1–1. https://doi.org/10.1109/JBHI.2017.2690801

Akramova, D. (2017). Dependence of the indicators of cognitive potential of p300 to the forms of epilepsy. *Journal of the Neurological Sciences*, *381*(2017), 333. https://doi.org/10.1016/j.jns.2017.08.946

Anil, D. G., Pelayo, P., Mistry, K. S., & George, K. (2018). A tactile P300 based brain computer interface system for communication in iOS devices. *2018 IEEE International Instrumentation and Measurement Technology Conference*, 1–6. https://doi.org/10.1109/I2MTC.2018.8409715

Bhatnagar, V., Yede, N., Keram, R. S., & Chaurasiya, R. K. (2016). A modified approach to ensemble of SVM for P300 based brain computer interface. *2016 International Conference on Advances in Human Machine Interaction, HMI 2016*, 12–15. https://doi.org/10.1109/HMI.2016.7449163

Blankertz, O. B. (2004). Documentation Wadsworth BCI Dataset (P300 Evoked Potentials) BCI Competition III Challenge 2004. *Interface*, 1–8.

Cao, T., Wan, F., Mak, P. U., Mak, P. I., Vai, M. I., & Hu, Y. (2012). Flashing color on the performance of SSVEP-based brain-computer interfaces. *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS*, 1819–1822. https://doi.org/10.1109/EMBC.2012.6346304

Capati, F. A., Bechelli, R. P., & Castro, M. C. F. (2016). Hybrid SSVEP/P300 BCI Keyboard - Controlled by Visual Evoked Potential. *Proceedings of the 9th International Joint Conference on Biomedical Engineering Systems and Technologies*, *January*, 214–218. https://doi.org/10.5220/0005705202140218

Carabez, E., Sugi, M., Nambu, I., & Wada, Y. (2017). Convolutional Neural Networks with 3D Input for P300 Identification in Auditory Brain-Computer Interfaces. *Computational Intelligence and Neuroscience*, *2017*. https://doi.org/10.1155/2017/8163949

Cecotti, H., & Gr, A. (2011). *Convolutional neural networks for P300 Detection with Application to Brain-Computer Interfaces*. *33*(3), 433–445.

Corralejo, R., Nicolás-Alonso, L. F., Álvarez, D., & Hornero, R. (2014). A P300-based brain–computer interface aimed at operating electronic devices at home for severely disabled people. *Medical and Biological Engineering and Computing*, *52*(10), 861–872. https://doi.org/10.1007/s11517-014-1191-5

Dal-Bianco, P., Waser, M., Schmidt, R., Fruehwirt, W., Dorffner, G., Gerstgrasser, M., Benke, T., Grossegger, D., Roberts, S., Ransmayr, G., & Garn, H. (2018). Associations of event-related brain potentials and Alzheimer's disease severity: A longitudinal study. *Progress in Neuro-Psychopharmacology and Biological Psychiatry*, *92*(1), 31–38. https://doi.org/10.1016/j.pnpbp.2018.12.013

De Venuto, D., Annese, V. F., & Mezzina, G. (2017). An embedded system remotely driving mechanical devices by P300 brain activity. *Proceedings of the 2017 Design, Automation and Test in Europe, DATE 2017*, 1014–1019. https://doi.org/10.23919/DATE.2017.7927139

Di, W., Zhihua, C., Ruifang, F., Guangyu, L., & Tian, L. (2010). Notice of Retraction Study on human brain after consuming alcohol based on EEG signal. *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference On*, *5*, 406–409.

Farwell, L. A., & Donchin, E. (1988). Talking off the top of your head: toward a mental prosthesis utilizing event-related brain potentials. *Electroencephalography and Clinical Neurophysiology*, *70*(6), 510–523.

Gamboa, M., & Cruz, J. J. (2008). Potenciales evocados y cognición. *Revista Mexicana de Ingeniería Biomédica*, *29*, 57–63.

Ghassemzadeh, N., & Haghipour, S. (2016). A review on EEG based brain computer interface systems feature extraction methods. *International Journal of Advanced Biological and Biomedical Research*, *4*(2), 117–123. https://doi.org/10.18869/IJABBR.2016.117

Haghighatpanah, N., Amirfattahi, R., Abootalebi, V., & Nazari, B. (2013). A single channel-single trial P300 detection algorithm. *2013 21st Iranian Conference on Electrical Engineering, ICEE 2013*. https://doi.org/10.1109/IranianCEE.2013.6599576

Hamidovic, A., & Wang, Y. (2019). The P300 in alcohol use disorder: A meta-analysis and meta-regression. *Progress in Neuro-Psychopharmacology and Biological Psychiatry*, *95*(April), 109716. https://doi.org/10.1016/j.pnpbp.2019.109716

Jamshed, M. A., Mumtaz, S., Haider, S. K., Jiang, A., & Pervaiz, H. (2018). Performance Enhancement in P300 ERP Single Trial by Machine Learning Adaptive Denoising Mechanism. *IEEE Networking Letters*, 1–1. https://doi.org/10.1109/lnet.2018.2883859

Jervis, B. W., Bigan, C., & Besleaga, M. (2020). New-Onset Alzheimer's Disease and Normal Subjects 100% Separated Statistically by P300 and ICA. *American Journal of Alzheimer's Disease and Other Dementias*, *35*, 1–10. https://doi.org/10.1177/1533317520935675

Kim, T.-W., & Lee, B.-H. (2016). Clinical usefulness of brain-computer interface-controlled functional electrical stimulation for improving brain activity in children with spastic cerebral palsy: a pilot randomized controlled trial. *Journal of Physical Therapy Science*, *28*(9), 2491–2494. https://doi.org/10.1589/jpts.28.2491

Kundu, S., & Ari, S. (2017). Score normalization of ensemble SVMs for brain-computer interface P300 speller. *8th International Conference on Computing, Communications and Networking Technologies*. https://doi.org/10.1109/ICCCNT.2017.8204119

Kuziek, J. W. P., Shienh, A., & Mathewson, K. E. (2017). Transitioning EEG experiments away from the laboratory using a Raspberry Pi 2. *Journal of Neuroscience Methods*, *277*(1), 75–82. https://doi.org/10.1016/j.jneumeth.2016.11.013

Lee, E.-M. (2018). Evoked potential: basic requirements and guidelines for writing reports. *Annals of Clinical Neurophysiology*, *20*(1).

Li, F., Li, X., Wang, F., Zhang, D., Xia, Y., & He, F. (2020). A novel P300 classification algorithm based on a principal component analysis-convolutional neural network. *Applied Sciences (Switzerland)*, *10*(4), 1–15. https://doi.org/10.3390/app10041546

Lindig-León, C., & Yáñez-Suárez, O. (2013). Optimized detection of the infrequent response in p300-based brain-computer interfaces. *Revista Mexicana de Ingenieria Biomedica*, *34*(1), 53–69.

Liu, M., Wu, W., Gu, Z., Yu, Z., Qi, F. F., & Li, Y. (2018). Deep learning based on Batch Normalization for P300 signal detection. *Neurocomputing*, *275*, 288–297. https://doi.org/10.1016/j.neucom.2017.08.039

Martinez-Cagigal, V., Gomez-Pilar, J., Alvarez, D., & Hornero, R. (2017). An Asynchronous P300-Based Brain-Computer Interface Web Browser for Severely Disabled People. *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, *25*(8), 1332–1342. https://doi.org/10.1109/TNSRE.2016.2623381

Masud, U., Baig, M. I., Akram, F., & Kim, T. S. (2017). A P300 brain computer interface based intelligent home control system using a random forest classifier. *2017 IEEE Symposium Series on Computational Intelligence*, *2018-Janua*(978), 1–5. https://doi.org/10.1109/SSCI.2017.8285449

McCane, L. M., Heckman, S. M., McFarland, D. J., Townsend, G., Mak, J. N., Sellers, E. W., Zeitlin, D., Tenteromano, L. M., Wolpaw, J. R., & Vaughan, T. M. (2015). P300-based brain-computer interface (BCI) event-related potentials (ERPs): People with amyotrophic lateral sclerosis (ALS) vs. age-matched controls. *Clinical Neurophysiology*, *126*(11), 2124–2131. https://doi.org/10.1016/j.clinph.2015.01.013

Minguez, J., Iturrate, I., Antelis, J., & Kubler, A. (2009). A NonInvasive Brain-Actuated Wheelchair Based on a P300 Neurophysiological Protocol and Automated Navigation. *IEEE Transactions on Robotics*, *25*(3), 614–627.

Mirghasemi, H., Fazel-Rezai, R., & Shamsollahi, M. B. (2006). Analysis of P300 classifiers in brain computer interface speller. *Annual International Conference of the IEEE Engineering in Medicine and Biology - Proceedings*, 6205–6208. https://doi.org/10.1109/IEMBS.2006.259521

Momennezhad, A., Shamsi, M., & Ebrahimnezhad, H. (2014). *Classification of EEG-P300 Signals Extracted from Brain Activities in BCI Systems Using v -SVM and BLDA Algorithms*. *34*(2), 23–35.

Ning, Z., Kong, X., Xia, F., Hou, W., & Wang, X. (2019). Green and Sustainable Cloud of Things: Enabling Collaborative Edge Computing. *IEEE Communications Magazine*, *57*(1), 72–78. https://doi.org/10.1109/MCOM.2018.1700895

Pamuła, T. (2018). Classification Based on Multilevel Filtering of Image Content Using Convolutional Neural Networks. *IEEE Intelligent Transportation Systems Magazine*, *PP*, 12. https://doi.org/10.1109/MITS.2018.2842040

Rakotomamonjy, A., & Guigue, V. (2008). BCI competition III: Dataset II- ensemble of SVMs for BCI P300 speller. *IEEE Transactions on Biomedical Engineering*, *55*(3), 1147–1154. https://doi.org/10.1109/TBME.2008.915728

Ramirez-Quintana, J. A., Madrid-Herrera, L., Chacon-Murguia, M. I., & Corral-Martinez, L. F. (2020). Brain-Computer Interface System Based on P300 Processing with Convolutional Neural Network, Novel Speller, and Low Number of Electrodes. *Cognitive Computation*. https://doi.org/10.1007/s12559-020-09744-2

Ron-Angevin, R., Garcia, L., Fernández-Rodríguez, A., Saracco, J., André, J. M., Lespinet-Najib, V., & Ahn, M. (2019). Impact of speller size on a visual P300 brain-computer interface (BCI) system under two conditions of constraint for eye movement. *Computational Intelligence and Neuroscience*, *2019*. https://doi.org/10.1155/2019/7876248

Samima, S., Sarma, M., & Samanta, D. (2017). Correlation of P300 ERPs with visual stimuli and its application to vigilance detection. *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 2590–2593. https://doi.org/10.1109/EMBC.2017.8037387

Shen, J., Liang, J., Shi, J., & Wang, Y. (2015). A dynamic submatrix-based P300 online brain-computer interface. *Biomedical Signal Processing and Control*, *15*, 27–32. https://doi.org/10.1016/j.bspc.2014.09.005

Swarnkar, R., Keskar, A. G., Prasad, P. M. S., & Shivprakash, N. C. (2016). A new approach to

detect P300 in a single trial based on PCA and SVM classifier. *2016 IEEE Region 10 Symposium (TENSYMP)*, 355–360. https://doi.org/10.1109/TENCONSpring.2016.7519432

Thigpen, N. N., & Keil, A. (2017). Event-Related Potentials. *Reference Module in Neuroscience and Biobehavioral Psychology*, 1–7. https://doi.org/10.1016/B978-0-12-809324-5.02456-1

Tong, J., Peng, Z., Ran, X., & Lei, D. (2015). The portable P300 dialing system based on tablet and Emotiv Epoc headset. *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS*, *2015-Novem*, 566–569. https://doi.org/10.1109/EMBC.2015.7318425

Uma, K. J., & Kumar, C. S. (2014). *Non-Invasive EEG Based Wireless Brain Computer Interface for Safety Applications Using Embedded Systems*. *2*(1).

Vařeka, L. (2020). Evaluation of convolutional neural networks using a large multi-subject P300 dataset. *Biomedical Signal Processing and Control*, *58*. https://doi.org/10.1016/j.bspc.2019.101837

Wang, Y., Shen, J., Liang, J., & Ji, Y. (2014). Research of P300 feature extraction algorithm based on ICA and wavelet transform. *Proceedings - 2014 6th International Conference on Intelligent Human-Machine Systems and Cybernetics, IHMSC 2014*, *1*, 41–45. https://doi.org/10.1109/IHMSC.2014.18

Xie, S., Wu, Y., Zhang, Y., Zhang, J., & Liu, C. (2014). Single channel single trial P300 detection using extreme learning machine: Compared with BPNN and SVM. *Proceedings of the International Joint Conference on Neural Networks*, *61273250*, 544–549. https://doi.org/10.1109/IJCNN.2014.6889400

Yaacoub, C., Mhanna, G., & Rihana, S. (2017). A genetic-based feature selection approach in the identification of left/right hand motor imagery for a brain-computer interface. *Brain Sciences*, *7*(1). https://doi.org/10.3390/brainsci7010012

Zhang, N., Yu, Y., Yin, E., & Zhou, Z. (2016). Performance of virtual stimulus motion based on the SSVEP-BCI. *IEEE International Symposium on Computer, Consumer and Control*, 656–659. https://doi.org/10.1109/IS3C.2016.169

Zhong, R., Li, M., Chen, Q., Li, J., Li, G., & Lin, W. (2019). The p300 event-related potential component and cognitive impairment in epilepsy: A systematic review and meta-analysis. *Frontiers in Neurology*, *10*(AUG), 1–8. https://doi.org/10.3389/fneur.2019.00943

NOTAS BIOGRÁFICAS

José Manuel Macías Macías. (2016) Obtuvo el grado de Ingeniero Electromédico por la Universidad La Salle Chihuahua. (2019) Recibió el grado de Maestro en Ciencias en Ingeniería Electrónica del Instituto Tecnológico de Chihuahua. Actualmente estudia el Doctorado en Ciencias en Ingeniería Electrónica en el mismo instituto, cuenta con diversas publicaciones en revistas y congresos internacionales. Sus investigaciones están orientadas en el uso de redes neuronales y aprendizaje profundo, en aplicaciones de electroencefalografía, particularmente potenciales evocados y habla imaginada.

Juan Alberto Ramírez Quintana. Recibió los grados de ingeniería (2004), maestría (2007) y doctorado (2014) en ingeniería electrónica del Instituto Tecnológico de Chihuahua, México. Actualmente trabaja como profesor-investigador en el Instituto Tecnológico de Chihuahua, cuenta con diversas publicaciones en revistas y congresos y dirige varias tesis a nivel licenciatura maestría y doctorado. Sus áreas de interés son visión por computadora, procesamiento de señales, aprendizaje automático, percepción visual y sistemas embebidos. El Dr. Ramírez es miembro del Sistema Nacional de Investigadores de México.

José Salvador Antonio Méndez Aguirre. Ingeniero electromecánico por el Instituto Tecnológico de Parral, Maestro en Ciencias en Ingeniería Mecánica por el Centro Nacional de Investigación y Desarrollo Tecnológico (CENIDET) y estudiante de doctorado en el Instituto Tecnológico de Chihuahua II. Actualmente, se desempeña como profesor de tiempo completo en la Universidad Politécnica de Chihuahua, profesor de asignatura de la Universidad LaSalle Chihuahua y profesor invitado de la maestría en mecatrónica del Instituto Tecnológico de Chihuahua.

Mario Ignacio Chacón Murguía. (M’86–SM’04) obtuvo el grado de Ingeniero Industrial en Electrónica, 1982, y el grado de Maestro en Ciencias en Ingeniería Electrónica, en 1985 del Instituto Tecnológico de Chihuahua, México, y el grado de Doctor en Ciencias, 1998, de la Universidad Estatal de Nuevo México, EEUU. Ha desarrollado varios proyectos para varias compañías. Actualmente trabaja como Profesor Investigador en el Instituto Tecnológico de Chihuahua. Ha publicado más de 175 trabajos y publicado 3 libros. Su investigación actual incluye Visión por Computadora y procesamiento de imágenes y señales usando Inteligencia Computacional. El Dr. Chacón es miembro Senior de la IEEE, y miembro de las sociedades IEEE; Inteligencia computacional, Procesamiento Digital de Señales y Miembro del SNI en México.

Alma Delia Corral Sáenz. Recibió el título de Ingeniera en Sistemas Computacionales en Hardware de la Universidad Autónoma de Chihuahua en 1999 y el de Maestra en Ciencias en Ingeniería Electrónica del Instituto Tecnológico de Chihuahua en 2003. Actualmente es profesora y coordinadora del Doctorado y la Maestría en Ciencias en Ingeniería Electrónica en el mismo Instituto, y participa en trabajos de investigación de las áreas de procesamiento de señales y visión por computadora.