# EJEMPLO 1:

# Efectividad de Modelos de Machine Learning en la detección de intrusos en sistemas de información y su Aplicabilidad en el Contexto del Emprendimiento e Innovación: Una Revisión Sistemática de Literatura

# Introducción

## 1. Contexto

## En el contexto actual de la era digital, la ciberseguridad se ha consolidado como un campo de investigación prioritario dentro de las ciencias de la computación y la ingeniería de sistemas. Desde inicios de la década de 2010, el crecimiento exponencial de dispositivos conectados y la digitalización de procesos críticos han incrementado significativamente la superficie de ataque de las organizaciones, generando un entorno cada vez más complejo y vulnerable. En particular, durante los últimos diez años se ha observado un aumento sostenido tanto en la frecuencia como en la sofisticación de las amenazas cibernéticas, como lo evidencian los informes de Symantec y Data Breach Today, que reportan más de 14 mil millones de registros comprometidos desde 2013 y una proliferación alarmante de ataques de día cero [1][2].Frente a este escenario, los Sistemas de Detección de Intrusos (IDS, por sus siglas en inglés) basados en técnicas de Machine Learning (ML) han adquirido una creciente relevancia en la comunidad científica. Estos sistemas representan una evolución frente a los enfoques tradicionales, permitiendo la detección proactiva de comportamientos anómalos y patrones maliciosos mediante algoritmos capaces de aprender y adaptarse a nuevas estrategias de ataque [3]. Estudios recientes han evidenciado que técnicas como Deep Learning, Random Forests y Support Vector Machines mejoran significativamente la tasa de detección y reducen los falsos positivos en comparación con métodos estáticos [4][5][6]. En su revisión sobre métodos de ML aplicados a IDS, [3] destacan la capacidad de estos enfoques para manejar grandes volúmenes de datos en tiempo real, lo que los convierte en herramientas clave en un entorno de amenazas persistentes. Del mismo modo, investigaciones más recientes como las de [7]y [8] han explorado el uso de redes neuronales profundas para la identificación temprana de ataques, con resultados prometedores en términos de precisión y eficiencia computacional. Asimismo, en [9] proponen arquitecturas híbridas que combinan aprendizaje supervisado y no supervisado, demostrando mejoras notables en entornos dinámicos.

## 2. Problema

## A pesar del notable avance en la aplicación de técnicas de Machine Learning (ML) en los Sistemas de Detección de Intrusos (IDS), persisten desafíos críticos que dificultan su adopción efectiva en contextos reales. La literatura actual ha demostrado el potencial de estos modelos para identificar amenazas con alta precisión [1][2]; sin embargo, esta investigación ha estado mayormente centrada en entornos controlados o en pruebas de laboratorio, lo que deja sin resolver aspectos clave de su implementación práctica.

## Uno de los principales problemas identificados es la falta de evaluaciones comparativas estandarizadas entre distintos modelos de ML. Diversos estudios emplean metodologías, métricas y conjuntos de datos diferentes, lo que dificulta la replicabilidad y la comparación objetiva de resultados [3][4]. Esta situación ha generado un panorama fragmentado, en el que es complejo establecer cuáles enfoques ofrecen el mejor rendimiento en función de criterios como precisión, escalabilidad, eficiencia o adaptabilidad. Adicionalmente, se observa una carencia de investigaciones integradoras que exploren el uso de modelos de ML en IDS desde una perspectiva estratégica de negocio, particularmente en entornos de innovación y emprendimiento. A pesar de que startups y pequeñas empresas constituyen uno de los sectores más vulnerables a ataques cibernéticos, son también los menos preparados en términos de protección digital avanzada [5]. La falta de herramientas accesibles, adaptables y eficientes en costo limita significativamente el aprovechamiento del ML en este tipo de organizaciones.

## 3. Justificación

La presente Revisión Sistemática de Literatura (RSL) se justifica por la creciente importancia **científica y técnica** de aplicar modelos de *Machine Learning* (ML) en Sistemas de Detección de Intrusos (IDS), especialmente en un contexto de amenazas cibernéticas cada vez más complejas. **A nivel económico y social**, este tema es crucial para startups y emprendimientos tecnológicos, los cuales carecen de recursos robustos en ciberseguridad. Aunque existen numerosos estudios individuales, no se han encontrado RSL recientes que aborden de forma integral y aplicada esta temática, considerando aspectos como escalabilidad, viabilidad y transferencia tecnológica. Esta revisión **es necesaria para consolidar el conocimiento disperso** y orientar tanto la investigación académica como el desarrollo de soluciones prácticas en entornos de innovación. Así, se busca identificar modelos de ML con mayor potencial de implementación real, permitiendo cerrar la brecha entre la investigación y su aplicación efectiva en sectores estratégicos .

## 4. Objetivo de la RSL

Esta Revisión Sistemática de Literatura (RSL) tiene como objetivo explorar los modelos de Machine Learning y su efectividad en la detección de intrusos, evaluando su impacto y aplicabilidad en el contexto del emprendimiento e innovación.

.

## Referencias

[1] Symantec Corporation, “Internet Security Threat Report,” Symantec, Mountain View, CA, USA, Rep. 22, 2017. [Online]. Available: <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/istr-22>  
[2] Data Breach Statistics, “Number of Records Exposed in Data Breaches,” 2023. [Online]. Available: <https://www.databreachtoday.com/statistics>  
[3] A. Buczak and E. Guven, “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.  
[4] S. S. Yadav and S. K. Jha, “A Review of Deep Learning Approaches for Intrusion Detection Systems,” *IEEE Access*, vol. 9, pp. 32465–32477, 2021.  
[5] T. S. Ahmed, R. A. Shaikh, and A. S. Rathore, “Machine Learning Algorithms for Intrusion Detection: A Comparative Study,” *International Journal of Computer Applications*, vol. 975, no. 8887, pp. 24–30, 2019.  
[6] M. A. Ambusaidi, X. He, P. Nanda, and Z. Tan, “Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm,” *IEEE Transactions on Computers*, vol. 65, no. 10, pp. 2986–2998, 2016.  
[7] Y. Xiao, X. Xing, K. Liu, and S. Zhang, “An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Network,” *IEEE Access*, vol. 6, pp. 64270–64282, 2018.  
[8] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, “A Deep Learning Approach for Network Intrusion Detection System,” in *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies*, 2016.  
[9] M. López-Martín, B. Carro, A. Sánchez-Esguevillas, and J. Lloret, “Network Traffic Classifier with Convolutional and Recurrent Neural Networks for Internet of Things,” *IEEE Access*, vol. 5, pp. 18042–18050, 2017.

**EJEMPLO 2**

**El método Kaizen en el incremento de la productividad en empresas manufactureras: Revisión sistemática de Literatura**

## Contexto

En la actualidad, la mejora continua de la producción es un objetivo primordial para las empresas manufactureras a nivel global. Si una empresa no implementa una estrategia de mejora continua en sus procesos, a largo plazo puede presentar problemas, tales como: pérdida de competitividad, disminución de la productividad, aumento de los costos de producción por retrabajo y desperdicios, problemas de calidad y satisfacción del cliente, etc. Uno de los enfoques más efectivos para lograr la mejora continua de la producción es la metodología Kaizen, un sistema de gestión japonés que se enfoca en la optimización de los procesos productivos a través de pequeños cambios incrementales. Al adoptar una mentalidad de mejora continua y el involucramiento activo de todos los empleados, las organizaciones pueden identificar y eliminar ineficiencias en sus operaciones y optimizar el flujo de producción.Como indican varios estudios [1], [2], [3], la implementación del método Kaizen muestra resultados significativos en la productividad y la mejora de la eficiencia de los procesos. Por otro lado, para que la implementación de Kaizen en una empresa manufacturera sea sostenible a lo largo del tiempo, es fundamental contar con el firme liderazgo y compromiso de la alta dirección, como indica [4]. Asimismo, se debe implementar un seguimiento y una medición continua de los resultados.

## 2. Problema

A pesar de la creciente aplicación del método Kaizen, muchas empresas no logran mantener su implementación a largo plazo o no obtienen los resultados esperados debido a la falta de compromiso organizacional o a una aplicación inadecuada. Esto refleja una necesidad de estudios que analicen cómo se está aplicando la metodología en diferentes contextos manufactureros y cuáles son los factores que influyen en su éxito o fracaso.

## 3. Justificación

El desarrollo del presente estudio permite analizar los diferentes aspectos que involucran la implementación del método Kaizen en empresas manufactureras de distintos sectores a nivel mundial y sus respectivos resultados.   
Además, busca aportar evidencia concreta que sirva de base para que las empresas puedan tomar decisiones fundamentadas al considerar adoptar Kaizen como herramienta de mejora continua.

## 4. Objetivo

El objetivo de este artículo es comprender cómo la implementación del método Kaizen contribuye a reducir los costos de inventario y disminuir el desperdicio de recursos en empresas manufactureras. Para ello, se realiza una investigación que evalúa los beneficios derivados de dicha implementación a través del análisis de literatura científica especializada.

## 5. Organización del contenido

El documento está estructurado de la siguiente manera:  
En el capítulo 2 (Metodología) se describe la estrategia de búsqueda sistemática de literatura, utilizando la pregunta PICOC, sus componentes, las subpreguntas derivadas, la ecuación de búsqueda aplicada a la base de datos SCOPUS, los criterios de inclusión y exclusión, y el diagrama PRISMA. En el capítulo 3 (Resultados) se presentan las respuestas a las subpreguntas PICOC, acompañadas de gráficos y tablas que sintetizan la información hallada. El capítulo 4 (Discusión) abarca los hallazgos principales del estudio, el análisis de los resultados y su comparación con estudios previos, así como las limitaciones encontradas y propuestas para futuras investigaciones. Finalmente, en el capítulo 5 (Conclusiones) se responde al objetivo de investigación planteado y se describe la contribución que esta RSL hace al campo de estudio.

[1] N. Caso-Murillo, R. Leon Mejia, and J. Quiroz-Flores, "Process Improvement Model based on Lean Manufacturing and Kaizen to Increase Machine Availability at a Plastics Company," *AIP Conference Proceedings*, vol. 2613, 2023. [Online]. https://doi.org/10.1063/5.0119321

[2] C. O. Chan and H. L. Tay, "Combining lean tools application in kaizen: a field study on the printing industry," *Int. J. Productivity and Performance Management*, vol. 67, no. 1, pp. 45–65, 2018. [Online]. https://doi.org/10.1108/IJPPM-09-2016-0197

[3] C. E. Damian-Garcia, D. A. Espiritu-Padilla, J. C. Quiroz-Flores, and S. Nallusamy, "Productivity Enhancement through a Proposed Methodology in the Cutting Process of SMEs," *SSRG Int. J. of Mechanical Engineering*, vol. 10, no. 8, pp. 1–10, 2023. [Online]. https://doi.org/10.14445/23488360/IJME-V10I8P101

[4] F. B. Georgise and A. T. Mindaye, "Kaizen implementation in industries of Southern Ethiopia: Challenges and feasibility," *Cogent Engineering*, vol. 7, no. 1, 2020. [Online]. https://doi.org/10.1080/23311916.2020.1823157