

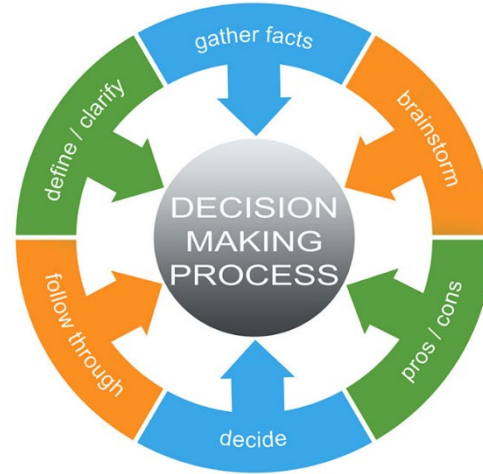
I CONVENCIÓN HEMISFÉRICA DE SEGURIDAD Y DEFENSA



GT 3: Ciberseguridad e Inteligencia Artificial

UN PUNTO DE VISTA DESDE EL ÁMBITO COGNITIVO

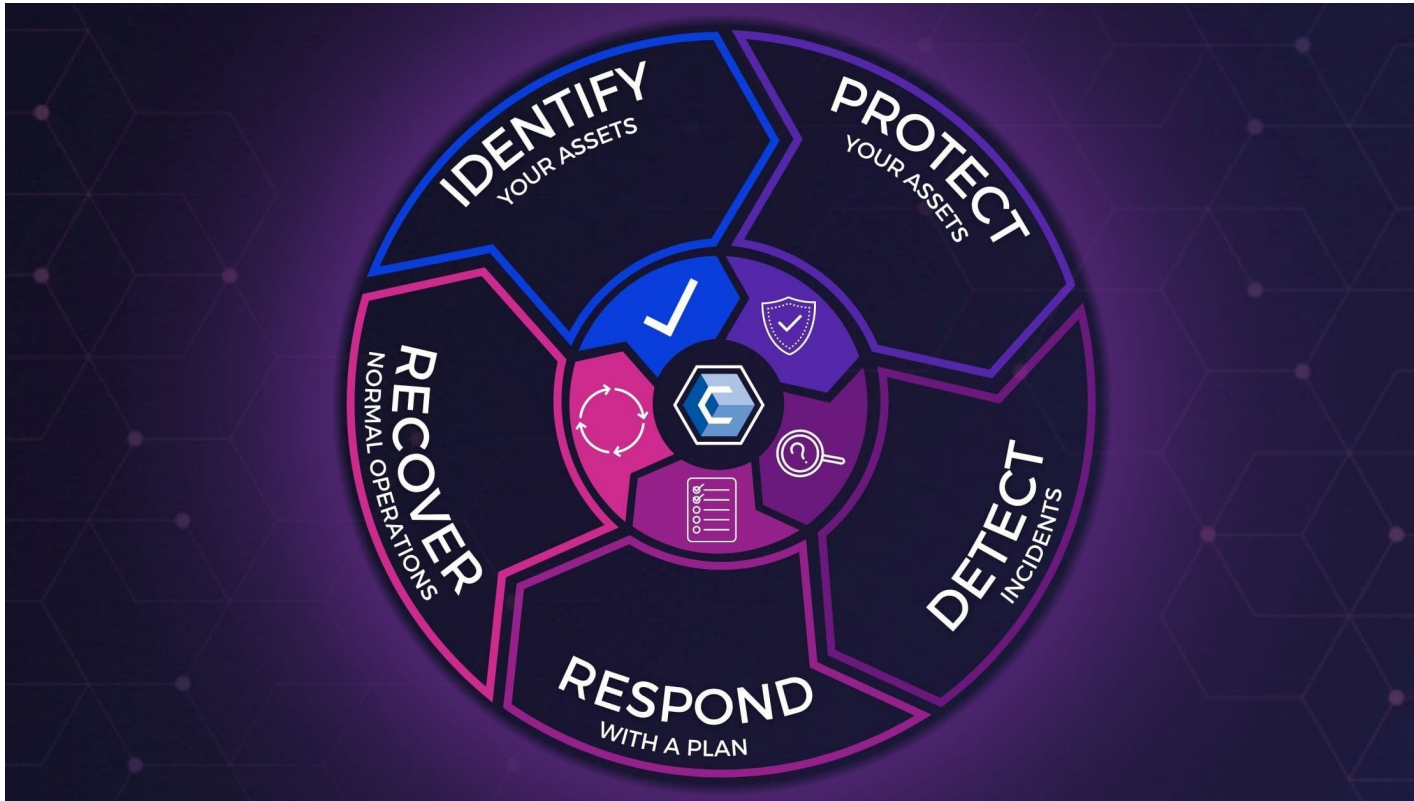
LO QUE OFRECE LA IA EN EL CIBERESPACIO



APLICACIONES DE LA IA



EL CICLO DE LA CIBERSEGURIDAD



La IA puede utilizarse en todas las fases de la ciberseguridad

CONTRIBUYE A LA CIBERRESILIENCIA.

Capacidad de resistir y recuperar en caso de un ciberataque

Facilita colaboración público-privada

PROBLEMAS ENDÓGENOS DE SEGURIDAD Y PROTECCIÓN EN LOS SISTEMAS DE IA

Different types of security vulnerabilities



Unpatched software



Misconfiguration



Weak credentials



Easy-to-phish users



Trust relationship



Compromised credentials



Malicious insider

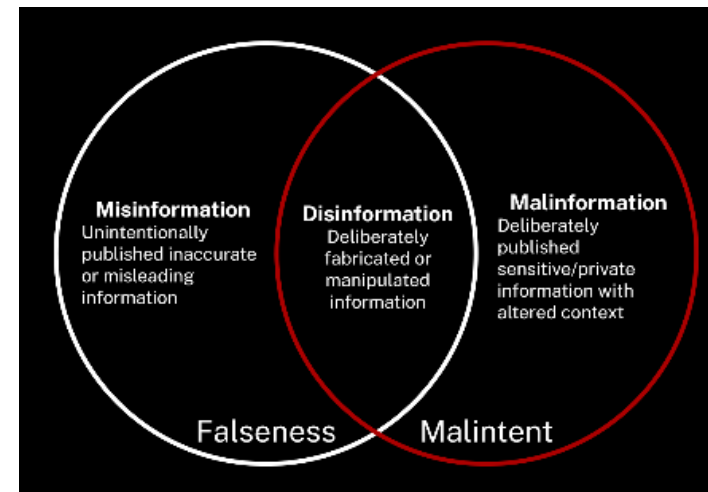


Missing/Poor Encryption



Los sistemas de IA son propensos a sufrir interrupciones, manipulaciones y robos de datos

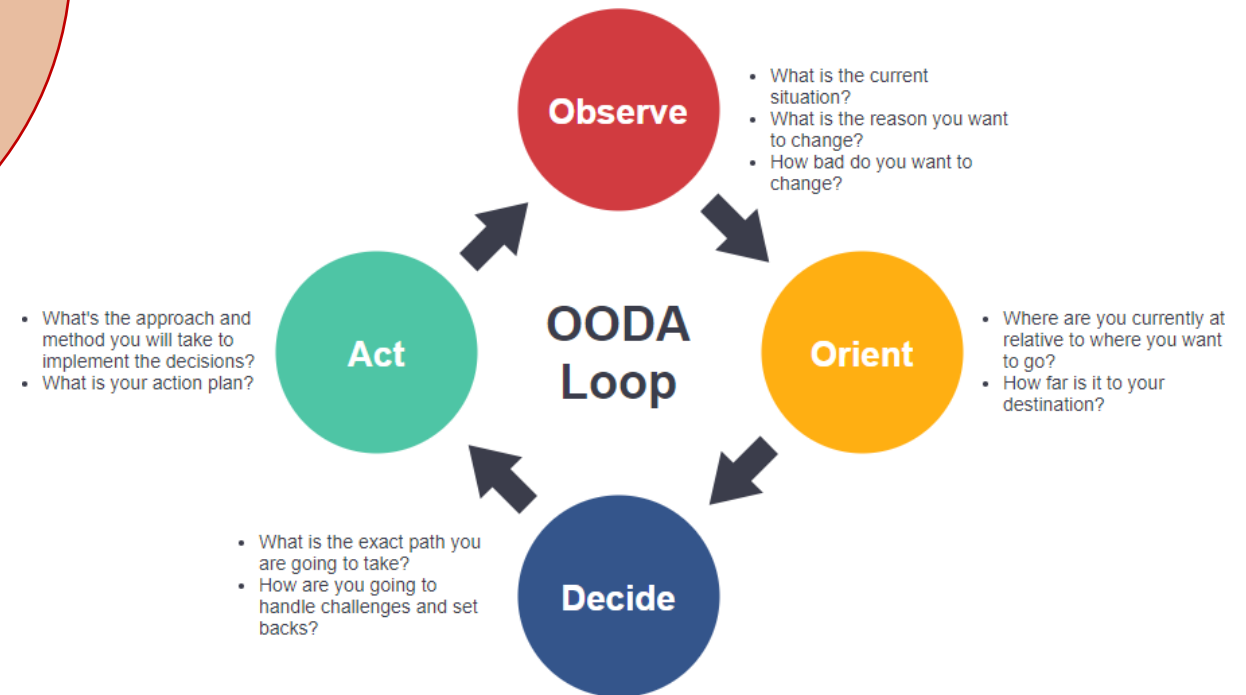
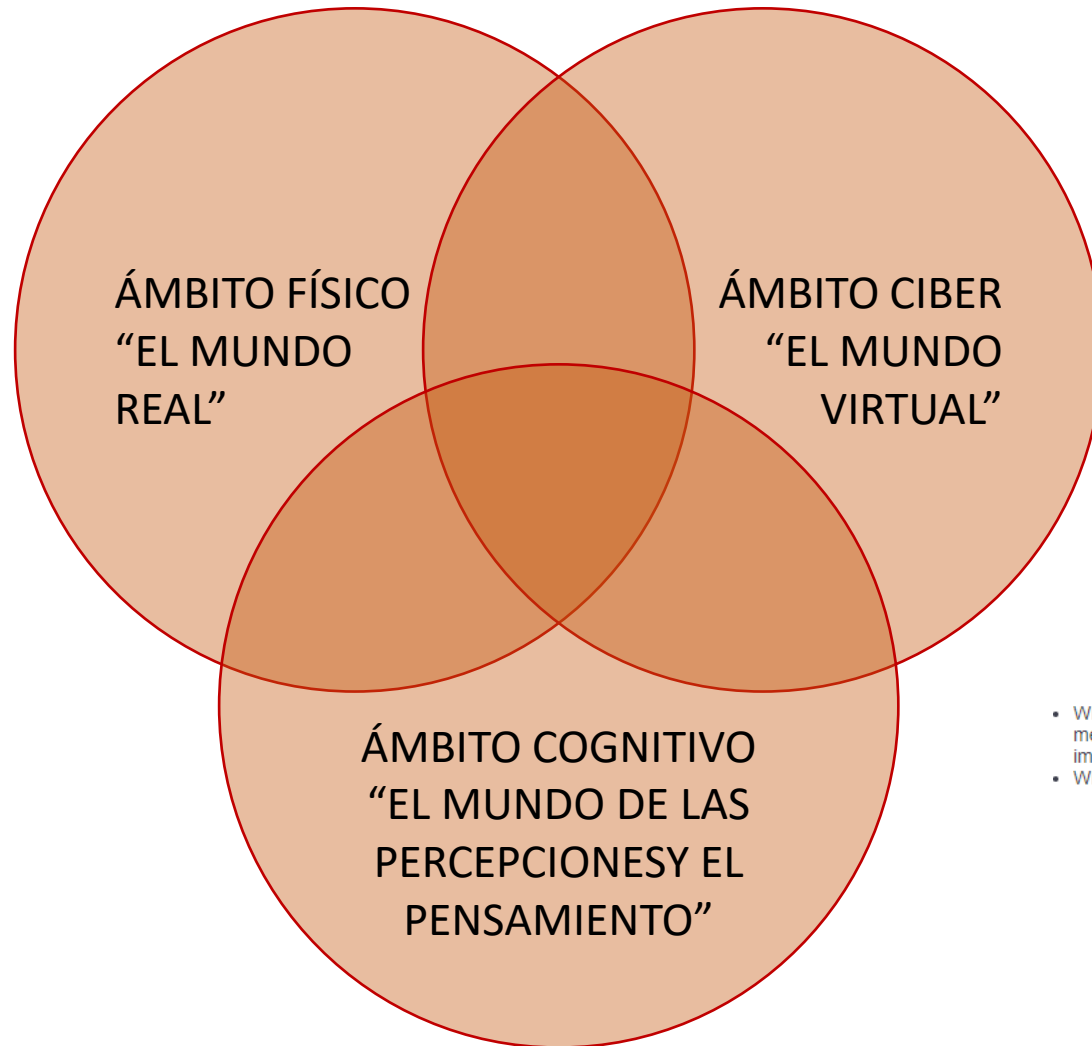
LOS RIESGOS Y AMENAZAS DE LA IA EN EL OODA LOOP (EN SUS TRES ÁMBITOS: FÍSICO, VIRTUAL Y COGNITIVO)



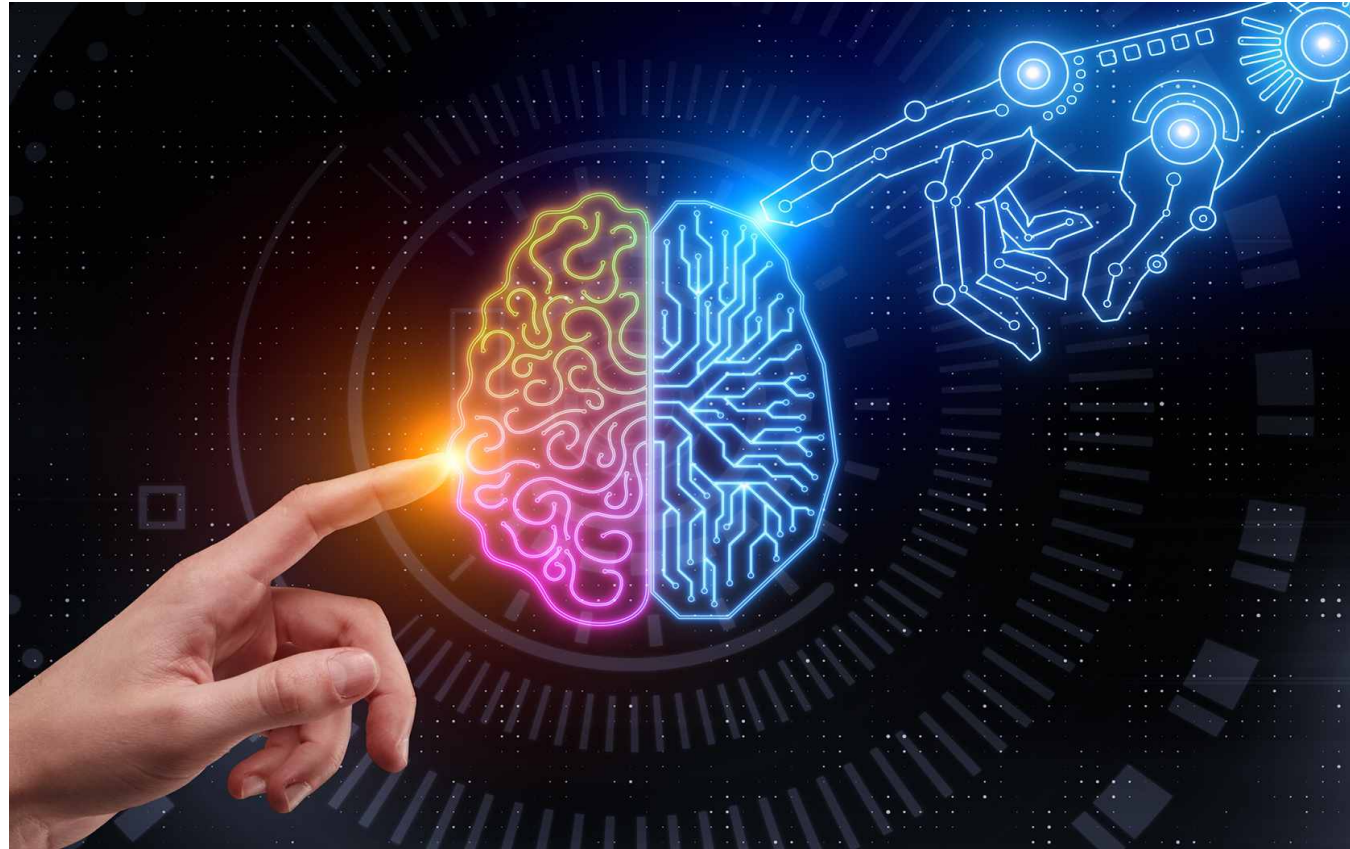
- **HUMAN AGENCY:**
 - Ability and capability of individuals and groups to create and act within the contexts of culture, community, political economy, and/or society.



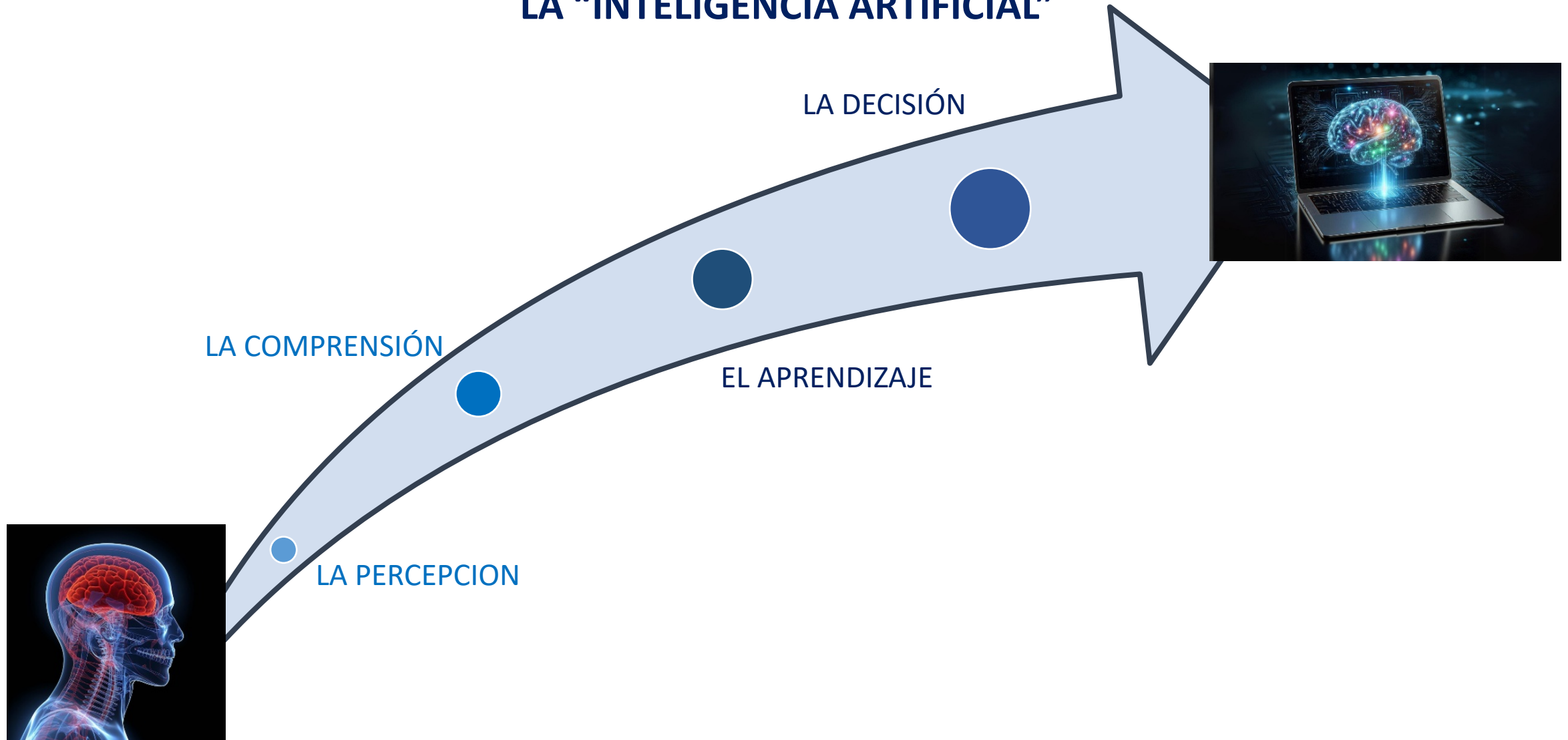
LOS ÁMBITOS DEL OODA LOOP



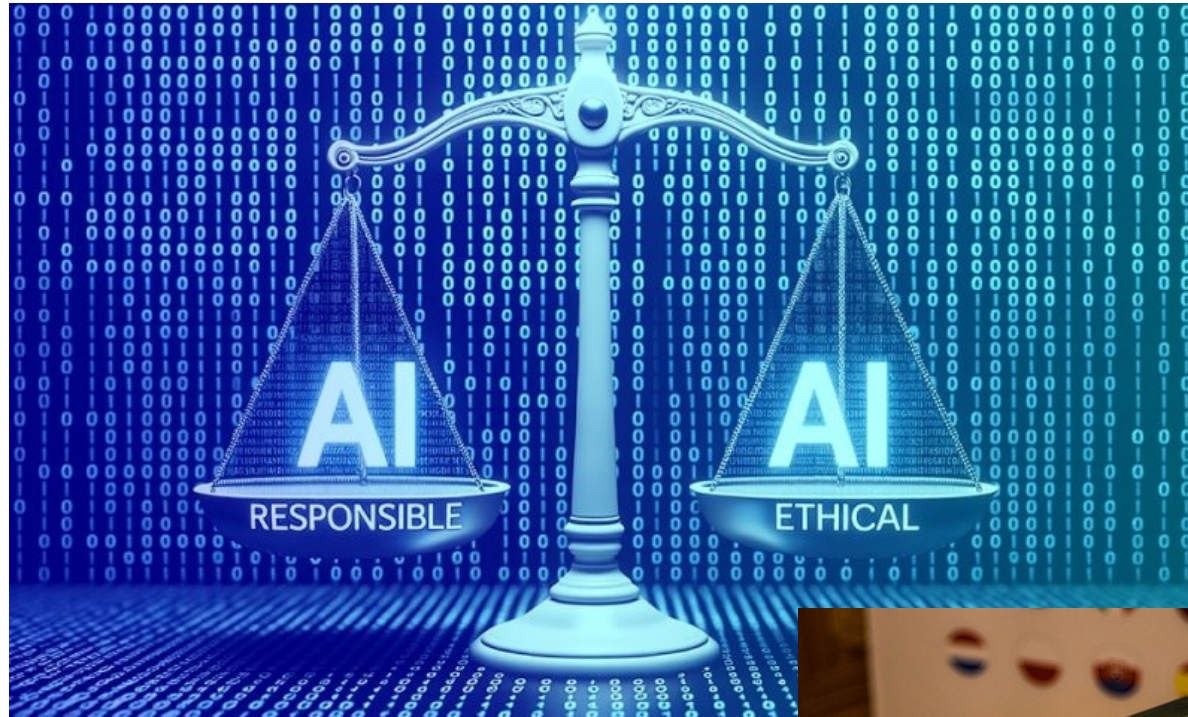
EL APRENDIZAJE Y EL RAZONAMIENTO



LA TRANSICIÓN DE LOS PROCESOS COGNITIVOS HACIA LA “INTELIGENCIA ARTIFICIAL”



EL DEBATE ÉTICO Y NORMATIVO



Directrices UE:

- No disminuir, limitar o desorientar la autonomía humana
- Posibilitar el modificar errores durante todo el ciclo
- Privacidad de los datos personales
- Transparencia basada en la trazabilidad
- Mecanismos que garanticen responsabilidad

Diario Oficial de la Unión Europea 2024/1659 12.7.2024

REGLAMENTO (UE) 2024/1659 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 13 de junio de 2024

por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifica los Reglamentos (CE) n.º 100/2008, (UE) n.º 147/2011, (UE) n.º 168/2011, (UE) 2018/858, (UE) 2018/1119 y (UE) 2019/1144 y las Directivas 2014/60/UE, (UE) 2014/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial)

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular sus artículos 16 y 114,

Vista la propuesta de la Comisión Europea,

Después de consultar al Comité Económico y Social Europeo⁽¹⁾,

Visto el dictamen del Banco Central Europeo⁽²⁾,

Visto el dictamen del Comité de las Regiones⁽³⁾,

De conformidad con el procedimiento legislativo ordinario⁽⁴⁾,

Considerando lo siguiente:

(1) El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme, en particular para el desarrollo, la introducción en el mercado, la puesta en servicio y la utilización de sistemas de inteligencia artificial en los sectores, sistemas de IA en la Unión, de conformidad con los valores de la Unión a fin de promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentalmente consagrados en la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), incluidas la democracia, el Estado de Derecho y la protección del medio ambiente, poner fin a los efectos perjudiciales de los sistemas de IA en la Unión, así como brindar apoyo a la innovación. El presente Reglamento garantiza la libre circulación transfronteriza de mercancías y servicios basados en la IA, con lo que ayuda que los Estados miembros impongan restricciones al desarrollo, la comercialización y la utilización de sistemas de IA, a menos que el presente Reglamento lo autorice expresamente.

(2) El presente Reglamento debe aplicarse de conformidad con los valores de la Unión consagrados en la Carta, lo que refuerza la protección de las personas físicas; los valores, la democracia, el Estado de Derecho y la protección del medio ambiente, y, al mismo tiempo, impulsar la innovación y el empleo y convertir a la Unión en líder en la adopción de una IA fiable.

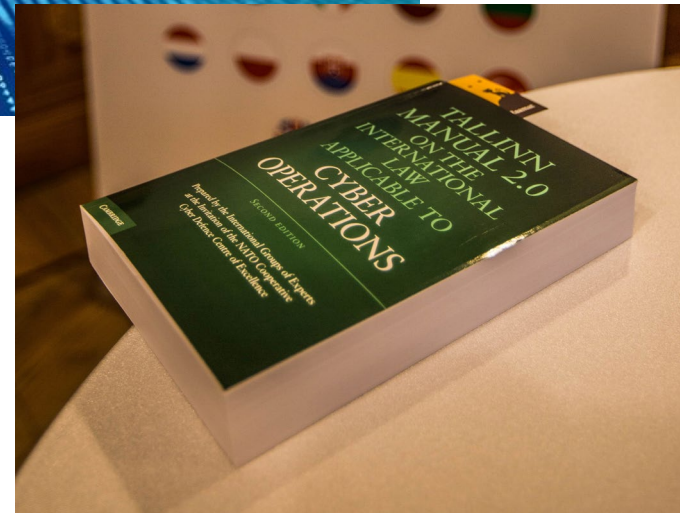
(3) Los sistemas de IA pueden desplegarse con facilidad en sectores muy diversos de la economía y en muchas partes de la sociedad, tangible e intangible, y circular físicamente por toda la Unión. Algunos Estados miembros ya han estudiado la adopción de normas nacionales destinadas a garantizar que la IA sea fiable y segura y se desarrolle y utilice de conformidad con las obligaciones relativas a los derechos fundamentales. La existencia de normas nacionales divergentes puede dar lugar a la fragmentación del mercado interior y reducir la seguridad jurídica de los operadores que desarrollan, importan o utilizan sistemas de IA. Por lo tanto, es preciso garantizar un nivel elevado y uniforme de protección en toda la Unión para lograr una IA fiable, así como erradicar las divergencias que obstaculizan la libre circulación, la innovación, el despliegue y la adopción en el mercado interior de los sistemas de IA y los

(1) DO C 117 de 11.3.2022, p. 6.

(2) DO C 17 de 12.3.2022, p. 4.

(3) DO C 97 de 28.2.2022, p. 60.

(4) Posición del Parlamento Europeo de 13 de marzo de 2024 (quincuésima de publicación en el Diario Oficial) y Decisión del Consejo de 21 de mayo de 2024.



LA INTELIGENCIA ARTIFICIAL DEBE SER UNA HERRAMIENTA DE APOYO



Posibilidad de uso maligno frente a un uso positivo

1956. John McCarthy. La IA: máquinas que ejecutasen tareas características de la inteligencia humana y resolviesen problemas y lograsen objetivos de forma similar a como lo hacen las personas.



REFERENCIAS

- *On challenges of AI to cognitive security and safety*. Ruiyan Huang, Xiaoqing Zheng, Yuting Shang and Xiangyang Xue. Security and Safety, vol 2, 2023012 (2023) <https://doi.org/10.1051/sands/2023012>
- *Cognitive Warfare and Cybersecurity: Strategic Implications for Global Security*. Loukmane Meghraoui and Zakariya Belkhamza. March 2025. International Conference on Cyber Warfare and Security 20(1):257-264 ([PDF](#)) [Cognitive Warfare and Cybersecurity: Strategic Implications for Global Security](#)
- *Cognitive psychology-based artificial intelligence review*. Jian Zhao, Mengqing Wu, Liyun Zhou, Xuezhu Wang and Jian Jia. Frontiers in Neuroscience. October 202216 https://www.researchgate.net/publication/364231996_Cognitive_psychology-based_artificial_intelligence_review
- *Redefining Cognitive Domains in the Era of ChatGPT: A Comprehensive Analysis of Artificial Intelligence's Influence and Future Implications*. Souvik Dubey, Ritwik Ghosh, Mahua Jana Dubey, Subhankar Chatterjee, Shambaditya Das, Julián Benito-León. Med Res Arch. 2024 June ; 12(6). [Redefining Cognitive Domains in the Era of ChatGPT: A Comprehensive Analysis of Artificial Intelligence's Influence and Future Implications – PMC](#)
- *Introduction to 'Cognitive artificial intelligence'*. Alan Bundy, Nick Chater and Stephen Muggleton. Philosophical Transactions of the Royal Society A. 24 July 2023 Volume 381Issue 2251 [Introduction to 'Cognitive artificial intelligence' | Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences](#)
- *The implications of Artificial Intelligence in cybersecurity. Shifting the offense-defense balance*. Jennifer Tang, Tiffany Saade and Steve Kelly. Institute for Security & Technology. October 2024. [The Implications of Artificial Intelligence in Cybersecurity](#)
- *Artificial Intelligence in Cybersecurity: A comprehensive Review and future direction*. Lzzy Ofusori, Tebogo Bokaka & siyabonga Mholongo. Applied artificial Intelligence. An International Journal. December 2024. [Full article: Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction](#)
- La ciberresiliencia: entre la ciberseguridad y la resiliencia. Felix Arteaga y Javier Alonso Lecuit. Real Instituto Elcano ARI 80/2024. Junio 2024. [La ciberresiliencia: entre la ciberseguridad y la resiliencia](#)
- La ciberseguridad y su relación con la inteligencia artificial. Ana Ayerbe. Real Instituto Elcano ARI 128/202. Noviembre 2020. [La ciberseguridad y su relación con la inteligencia artificial](#)
- Implicaciones sobre el uso de la inteligencia artificial en el campo de la ciberseguridad. Javier Alonso Lecuit. Real Instituto Elcano. ARI 50/2019. Mayo 2019. [Implicaciones sobre el uso de la inteligencia artificial en el campo de la ciberseguridad](#)
- AI in Cybersecurity: Key Benefits, Defense Strategies, & Future Trends. What is AI in Cybersecurity? [Artificial Intelligence \(AI\) in Cybersecurity: The Future of Threat Defense](#)