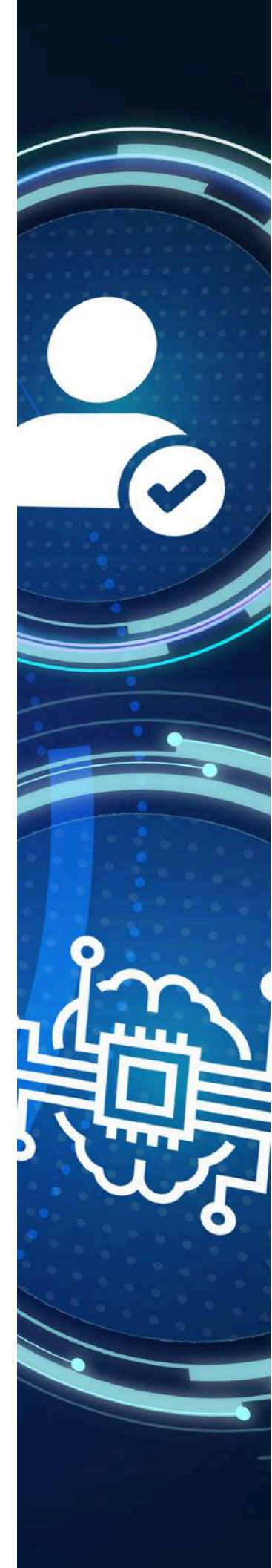


**Ai**

# **LA INTELIGENCIA ARTIFICIAL COMO ARMA DEL CIBERCRIMEN**

Dr. Roberto Morales Estrella  
Profesor Investigador de la UAEM  
05 de enero de 2026



La Inteligencia Artificial (IA), como hoy la conocemos, es resultado de un proceso histórico, cuyas raíces las encontramos en los babilonios, que fueron los que desarrollaron los primeros algoritmos, mediante el método Herón, iterativo grabado en tablillas de arcilla como la BM 85200+, para resolver problemas matemáticos complejos, sentando las bases para la posterior creación de la IA (Knuth, 1972).

La matemática Augusta Ada Byron, mejor conocida como Ada Lovelace, acuñó en 1843, el concepto de algoritmo informático, como parte del desarrollo de la máquina de Charles Babbage, abriendo la posibilidad para ir más allá del simple calculo numérico (Redaccion National Geographic, 2023).

Alan Turing (Rodriguez, 2021) publicó en 1950 su obra "Maquinaria Informática e Inteligencia" para dar respuesta a su pregunta ¿son las máquinas capaces de pensar? conocida como la prueba de Turing, para determinar si una máquina era inteligente, al imitar las respuestas humanas, marcando la pauta para construir una máquina multipropósito (Rene, 2022).

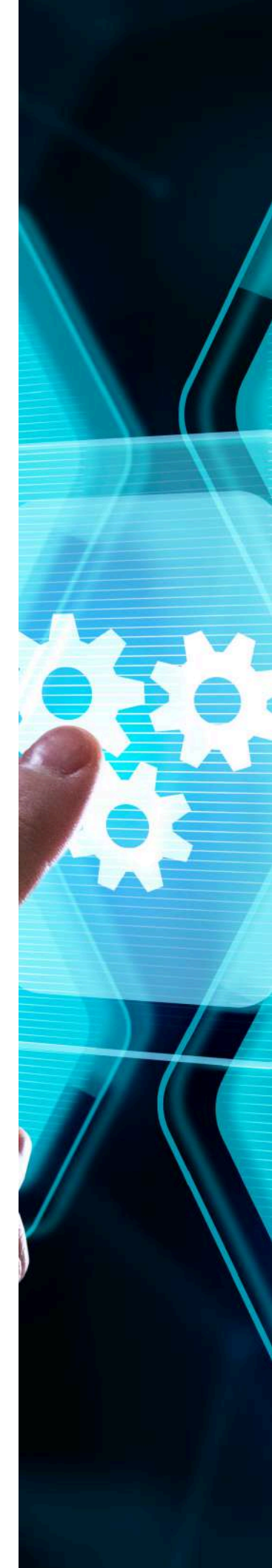
A mitad del siglo XVIII fue surgiendo la primera revolución tecnológica, cuyo escalamiento, después de la segunda guerra mundial marcó la ruta, para que en el siglo XXI la sociedad global viera el surgimiento de los sistemas informáticos y de la IA, con los modelos pre-entrenados (GPT).

La ciberseguridad, es considerada como disciplina, no una ciencia, surge por la necesidad de controlar el acceso a datos sensibles, en el contexto de la guerra fría, donde se dio la creación del ARPANET, por parte del departamento de Defensa Norteamericano, con ello las primeras redes de computadoras.

Fue con el surgimiento del primer gusano informático Creeper, desarrollado por Bob Thomas de BBN Technologies, en 1971 (Norman, 2025), si bien no era malicioso, sí evidenció que podía propagarse en los demás equipos, gracias al internet, mostrando la vulnerabilidad de las redes; por su parte Ray Tomlinson, desarrolló el antivirus Reaper, que eliminaba al Creeper (Pandora, 2024).

Actualmente es tan diversificada la generación de malware, estimándose en más de mil millones los programas maliciosos, tan solo Kaspersky ha detectado un promedio de 500 mil malware diariamente en el 2025. (Kaspersky, 2025).

Existe una gran diversidad de malware, virus y ransomware, (IBM, 2025), como la denegación de servicio distribuido (DDoS) (FORTINET, 2025), sin faltar los gusanos, como el stuxnet o día cero, desarrollado por EEUU en 2010, como arma de guerra cibernética (Escuela de Ingenieria Informatica, 2026), la cibercriminalidad es una industria masiva que representara 10,5 Bdd en 2025 (unico, 2025), (Morgan, 2020), Op. Cit. IBM,25.



En la medida que la tecnología se desarrolla, se acelera la carrera armamentista digital, donde la IA juega un papel determinante, facilitando el incremento de los ciberataques, dotando de velocidad, escala y sofisticación, través de aplicaciones como el vishing (llamadas fraudulentas) y el Deepfakes clonando voz e imágenes.

los hackers utilizando IA, son capaces de crear código malicioso como WormGPT o FraudGPT, y el Malware polimórfico, para reescribir automáticamente el código de un virus propagándolo, además de evadir la Detección y Respuesta de Puntos de Conexión (EDR), para identificar los puntos ciegos y realizar los ataques en momentos de menor vigilancia.

En las etapas anteriores a la era de la IA, la comunicación era humano-humano, pero a partir de la formación de la sociedad de la información, las nuevas tecnologías -como los ordenadores y la IA- han integrado a la humanidad en redes globales de instrumentalidad (Castells, 2000 4ª reimpression, pág. 46). En la actualidad la comunicación es ordenador-ordenador preponderantemente, de forma tal que las cadenas de ordenador a ordenador, pueden funcionar sin la intervención humana (Harari, 2024, págs. 252-253).

Los usuarios de internet, en octubre del 2025, sumaron 6 mil 40 millones de personas, equivalente al 73% de la población mundial (Depto de Investigacion de Statista, 2025), lo que da cuenta de la alta vulnerabilidad, frente a los cibercriminales, por lo que es urgente que los gobiernos, de los más de 100 países, tomen acuerdos para diseñar las estrategias pertinentes, pero la lucha por la hegemonía mundial, no facilita el combate a la cibercriminalidad, incluso las naciones que anhelan la posición hegemónica, la fomentan, creando ciberarmas para abrir frentes de guerra cibernética, como otro elemento de la geopolítica.

#### Bibliografía

- Castells, M. (2000 4ª reimpression). La Sociedad Red (Vol. I / Prologo de La Red y el yo ). Madrid, España: Alianza Editorial.
- Depto de Investigacion de Statista. (1º de diciembre de 2025). statista, estadística. Recuperado el enero de 2026, de [statista.com: https://www.statista.com/statistics/617136/digital-population-worldwide/](https://www.statista.com/statistics/617136/digital-population-worldwide/)
- Escuela de Ingenieria Informatica. (1 de enero de 2026). Universidad de Oviedo. Recuperado el enero de 2026, de [ingenieriainformatica.uniovi.es: https://ingenieriainformatica.uniovi.es/actualidad/noticias/-/asset\\_publisher/XR8d/content/stuxnet-historia-del-primer-arma-de-la-ciberguerra?redirect=%2Factualidad%2Fnoticias%3Fp\\_p\\_id%3D101\\_INSTANCE\\_XR8d%26p\\_p\\_lifecycle%3D0%26p\\_p\\_state%3Dnormal%26p\\_p\\_mode%3D1%26p\\_p\\_col\\_id%3D1%26p\\_p\\_col\\_title%3DHistoria+del+primer+arma+de+la+ciberguerra%26p\\_p\\_col\\_content%3D1](https://ingenieriainformatica.uniovi.es/actualidad/noticias/-/asset_publisher/XR8d/content/stuxnet-historia-del-primer-arma-de-la-ciberguerra?redirect=%2Factualidad%2Fnoticias%3Fp_p_id%3D101_INSTANCE_XR8d%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3D1%26p_p_col_id%3D1%26p_p_col_title%3DHistoria+del+primer+arma+de+la+ciberguerra%26p_p_col_content%3D1)
- FORTINET. (5 de diciembre de 2025). FORTINET. Recuperado el enero de 2026, de [fortinet.com: https://www.fortinet.com/lat/resources/cyberglossary/types-of-cyber-attacks](https://www.fortinet.com/lat/resources/cyberglossary/types-of-cyber-attacks)
- Harari, Y. N. (2024). Nexus Una breve historia de las redes de innformación desde la edad de piedra hasta la IA. Ciudad de México, México : Penguin Random House Grupo Editorial S.A. de C.V.
- IBM. (15 de diciembre de 2025). IBM. Recuperado el enero de 2026, de [ibm.com: https://www.ibm.com/mx-es/think/topics/malware](https://www.ibm.com/mx-es/think/topics/malware)
- Kaspersky. (1 de diciembre de 2025). Kaspersky. Recuperado el enero de 2026, de [kaspersky.com: https://www.kaspersky.com/about/press-releases/the-number-of-the-year-kaspersky-detected-half-a-million-malicious-files-daily-in-2025](https://www.kaspersky.com/about/press-releases/the-number-of-the-year-kaspersky-detected-half-a-million-malicious-files-daily-in-2025)
- Knuth, D. E. (01 de julio de 1972). Ancient Babylonian algorithms. Communications of ACM, 17(7), 671-677.
- Morgan, S. (13 de noviembre de 2020). CIBERCRIME MAGAZINE. Recuperado el enero de 2026, de [cybersecurityventures.com: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/](https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/)
- Norman, J. (28 de diciembre de 2025). Historia de la Información. Recuperado el diciembre de 2025, de [historyofinformation.com: https://www.historyofinformation.com/detail.php?entryid=2860](https://www.historyofinformation.com/detail.php?entryid=2860)
- Pandora, E. d. (11 de marzo de 2024). Pandora Tech Blog. Recuperado el diciembre de 2025, de [pasndorafms.com: https://pandorafms.com/blog/creeper-and-reaper/](https://pandorafms.com/blog/creeper-and-reaper/)
- Redaccion National Geographic. (10 de octubre de 2023). National Geographic/ ciencia. Recuperado el diciembre de 2025, de [nationalgeographicla.com: https://www.nationalgeographicla.com/ciencia/2023/10/fue-la-primer-programadora-de-la-historia-y-predijo-la-existencia-de-la-inteligencia-artificial](https://www.nationalgeographicla.com/ciencia/2023/10/fue-la-primer-programadora-de-la-historia-y-predijo-la-existencia-de-la-inteligencia-artificial)
- Rene, P. (23 de junio de 2022). NIST. EU. Recuperado el diciembre de 2025, de [nist.gov: https://www.nist.gov/blogs/taking-measure/alan-turings-everlasting-contributions-computing-ai-and-cryptography](https://www.nist.gov/blogs/taking-measure/alan-turings-everlasting-contributions-computing-ai-and-cryptography)
- Rodriguez, G. G. (20 de septiembre de 2021). CIIIA (Centro de Innovación Industrial e Inteligencia Artificial. Recuperado el diciembre de 2025, de [ciiia.mx: https://www.ciiia.mx/noticiasciiia/la-prueba-de-turing](https://www.ciiia.mx/noticiasciiia/la-prueba-de-turing)
- unico. (19 de mayo de 2025). unico. Recuperado el enero de 2026, de [unicoid.mx: https://www.unicoid.mx/post/amenaza-global-y-costos-del-cibercrimen](https://www.unicoid.mx/post/amenaza-global-y-costos-del-cibercrimen)