LISA Institute

LISA Challenge

Strategic Analysis #1:

¿Qué innovación tecnológica contemporánea (IA, biotecnología, o cambios epistemológicos) representa el mayor vector de transformación estratégica para la seguridad y defensa?

“IA Generativa y Edge Computing: Vectores Tecnológicos Decisivos para la Transformación Estratégica de la Defensa (2026–2030)”

Autor: TC Julio Enrique PALACIO

Término: 052300 Oct 25 (hora de Madrid).

"IA GENERATIVA Y EDGE COMPUTING: VECTORES TECNOLÓGICOS DECISIVOS PARA LA TRANSFORMACIÓN ESTRATÉGICA DE LA DEFENSA (2026–2030)"

1. INTRODUCCIÓN

a. El Problema.

En el marco de la acelerada transformación tecnológica, las organizaciones militares enfrentan un interrogante estratégico central: ¿qué innovación contemporánea constituye el mayor vector de cambio para la seguridad y defensa?

b. Hipótesis Central

[1]***La integración simultánea de IA generativa y Edge Computing bajo el Marco TEDE puede comprimir el ciclo OODA de Estados Mayores de horas a minutos en operaciones multidominio (2026-2030*).**

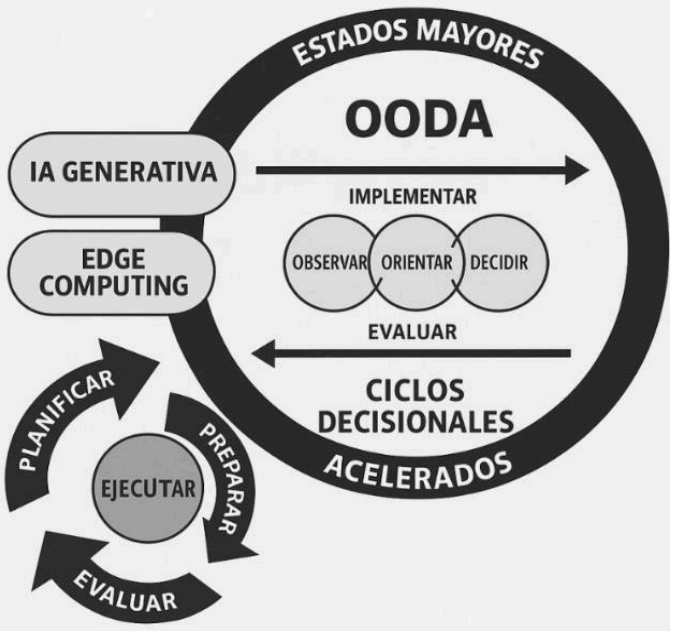


Figura 1: Representación esquemática del ciclo OODA acelerado por IA generativa y Edge Computing en operaciones multidominio.

[1] Esquema gráfico creado específicamente para Strategic Analysis #1, mediante diseño asistido por IA, bajo la

c. Metodología Marco TEDE

Se aplica el marco TEDE (Tecnología–Evaluación–Doctrina–Empleo), método en fase de prueba desarrollado por el autor. Evalúa cuatro dimensiones críticas. Conectando con el análisis prospectivo desarrollado por LISA Institute (2023a).

[2]

Figura 2: Representación esquemática del Marco TEDE (Tecnología–Evaluación–Doctrina–Empleo). Creada específicamente para este análisis, mediante diseño asistido por IA, bajo la dirección y edición del autor.

El Marco TEDE permite evaluar cómo IA generativa y Edge Computing aceleran las fases del ciclo OODA. La prospectiva 2026-2030 identifica cuándo estas capacidades alcanzarán madurez crítica (TRL 8-9) y bajo qué escenarios su adopción será ventaja o rezago estratégico.

[2] Imagen gráfica creada específicamente para Strategic Analysis #1, mediante diseño asistido por IA, bajo la

2. CUERPO DEL ANÁLISIS

a. Marco Conceptual

1) El Ciclo OODA

La velocidad de decisión es factor decisivo para la victoria. El Coronel John Boyd (1987) conceptualizó este ciclo en el cual quien lo completa más rápido desorienta al adversario e impone su iniciativa.

2) Evolución del Tiempo Decisional

Cada salto tecnológico de la guerra, redujo los tiempos del ciclo decisional (Kaushal et al, 2023). La eficacia de un Estado Mayor, se mide por su capacidad ciclos OODA reducidos.

[3]

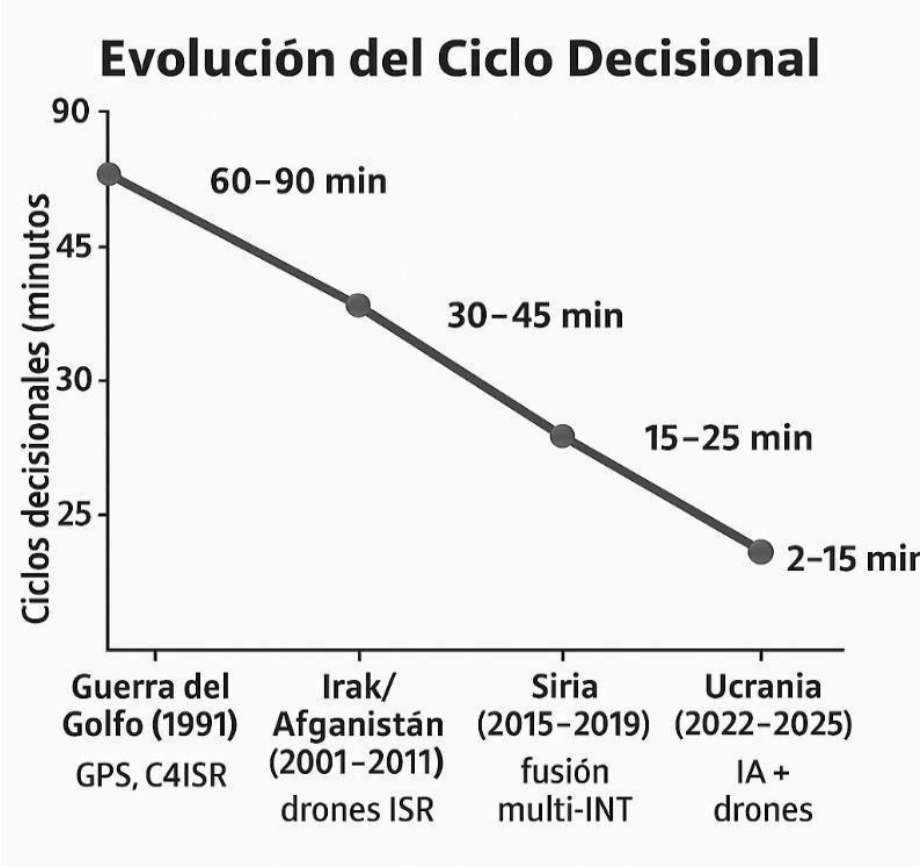


Figura 3: Evolución del Ciclo Decisional en la historia militar reciente.

[3] Gráfico creado específicamente para Strategic Analysis #1, mediante diseño asistido por IA, bajo la dirección y edición del autor.

b. Análisis Tecnológico

El marco TEDE supera el enfoque tradicional de technology push mediante evaluación holística en 4 dimensiones interdependientes (Center for Security and Emerging Technology, 2023):

1) IA Generativa:

Capacidades	Síntesis multi-fuente, generación de Modos de Acción, simulación rápida (Horowitz et al., 2018)
Limitaciones	Sesgos, vulnerabilidad a data poisoning, (Biggio & Roli, 2018) Amenazas como Deep fakes y Brain hacking muestran el impacto de la manipulación cognitiva en la fase Orientar del OODA (LISA Institute, 2024a, 2024b)
Ejemplo	Project Maven redujo un 40% tiempos de análisis, manteniendo decisión humana final (U.S. Army, 2023)

2) Edge Computing:

Ventajas	Baja latencia (<50 ms), resiliencia frente a jamming, reducción de ancho de banda (80–90%), seguridad de datos locales
Estado	TRL 6–7 para nodos tácticos (NATO Science and Technology Organization 2024)

3) Convergencia IA + Edge:

Observar	Sensores procesan localmente, alertas en segundos
Orientar	IA fusiona datos, pero requiere validación humana (Johnson & Kott, 2022)
Decidir	IA propone Modos de Acción.
Actuar	JADC2 sincroniza efectos multidominio en 8–12 min.

c. Evaluación Operacional (TEDE)

Tecnología	IA TRL 7–8 comercial, Edge TRL 6–7 (Center for Security and Emerging Technology, 2023)

Evaluación	Ucrania valida targeting en 2–3 min; OTAN fija meta <10 min al 2027 (NATO Defence Innovation Accelerator for the North Atlantic, 2024) La sinergia entre ciberinteligencia y ciberseguridad resultan esenciales. (LISA Institute, 2023b)
Doctrina	FM 3-0 Multi-Domain Operations (U.S. Army, 2022), JADC2 Strategy (U.S. Department of Defense, 2022), NATO AI Strategy 2024 (North Atlantic Treaty Organization, 2024a)
Empleo	Decisión asistida, control humano permanente (North Atlantic Treaty Organization, 2024b) operaciones 24/7.

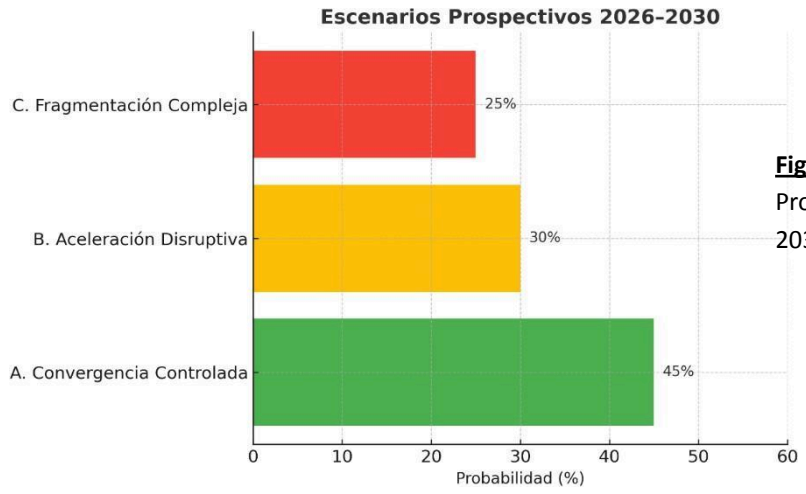
d. <u>Escenarios Prospectivos (2026–2030</u>)

Aplicando método MICMAC, análisis morfológico, de construcción de escenarios de Godet (2007) y Godet y Durance (2011), y la lógica de análisis de amenazas internacionales de LISA Institute (2024c), se identificaron tres escenarios:

A. **<u>Convergencia Controlada (45%)</u>**: Adopción equilibrada, regulación ética, interoperabilidad OTAN. OODA 10–15 min, control humano 100%.

B. **<u>Aceleración Disruptiva (30%)</u>**: Crisis (Ej. Taiwán) acelera ciclo OODA 3–5 min, riesgo de decisiones equivocadas.

C. **<u>Fragmentación Compleja (25%)</u>**: Regulación restrictiva, dividió aliados OTAN. OODA 15–45 min



<u>Figura 4</u>: Escenarios Prospectivos (2026–2030).

4

[4] Gráfico creado específicamente para Strategic Analysis #1, mediante diseño asistido por IA, bajo la dirección y edición del autor

e. Roadmap Estratégico 2030.

1) El Estado Deseado 2030

- OODA <10 min.
- Interoperabilidad OTAN.
- Control humano 100% (U.S. Department of Defense, 2023)
- Capacidades soberanas IA/Edge (IEEE, 2024).

2) Fases Críticas

- 2025 Fundación: TEDE institucionalizado.
- 2026 Consolidación: Doctrina OTAN IA, ejercicios DIANA (NATO Defence Innovation Accelerator for the North Atlantic, 2024)
- 2027 Escalamiento: JADC2-OTAN, OODA <15 min.
- 2028–2030 Optimización: OODA <10 min, IA-nativos.

3) Bifurcaciones Críticas

- 2025–26: Masificación vs. experimentación limitada.
- 2026–27: Aceleración por crisis vs. moratoria regulatoria.
- 2027–28: Soberanía vs. dependencia externa.

Figura 5: Roadmap Estratégico (Backcasting 2030).

[5] Gráfico creado específicamente para Strategic Analysis #1, mediante diseño asistido por IA, bajo la dirección y edición del autor

f. Integración TEDE–FODA.

La integración TEDE–FODA es un enfoque innovador para evaluar maduración tecnológica aplicada a Defensa. El TEDE estructura cuatro dimensiones críticas, mientras el FODA las tensiona en fortalezas, oportunidades, debilidades y amenazas.

Dimensión	Fortaleza/Oportunidad	Debilidad/Amenaza
Tecnología	TRL 7–8 IA; Edge en desarrollo. Adopción temprana 2026–2028	Dependencia externa. Ciberataques
Evaluación	Métricas validadas. Estándar OTAN	Falta de métricas comunes Manipulación adversaria
Doctrina	MDO/JADC2 consolidados. Cooperación OTAN	Falta de TTPs Fragmentación
Empleo	Personal digitalizado, control humano. Capacidades soberanas si hay inversión	Resistencia cultural. Carrera tecnológica China–Rusia

3. CONCLUSIONES.

Del análisis prospectivo estratégico realizado, en el marco TEDE (como innovación metodológica), desarrollado en un horizonte temporal definido, fueron identificados anticipadamente 3 posibles escenarios; pudiéndose determinar que:

- La convergencia de IA generativa y Edge Computing constituye el vector más influyente para la defensa, al comprimir los ciclos decisionales (OODA).

- Las evidencias recientes (Ucrania 2022–2025) muestran que la integración IA+Edge reduce los tiempos de targeting 2/3 minutos, mientras que la OTAN proyecta para 2027 un estándar <10 min.

- La ventaja tecnológica requiere un marco como el TEDE (Tecnología–Evaluación–Doctrina–Empleo), que asegure: métricas operativas, coherencia doctrinal y preservación del control humano.

- El período (2026 – 2030) abre una ventana crítica para fijar estándares, consolidar capacidades tecnológicas soberanas y evitar dependencia tecnológica.

- En la actual carrera armamentista algorítmica, la brecha entre innovadores y rezagados no es gradual, sino exponencial.

ANEXO A. GLOSARIO DE TÉRMINOS.

1. Marco TEDE (Contribución Original).

- **TEDE | Tecnología–Evaluación–Doctrina–Empleo.**
  Marco metodológico original, en fase de prueba, diseñado para evaluar innovaciones tecnológicas militares de manera integral y simultánea, asegurando que el paso del laboratorio al empleo operacional sea coherente y efectivo.
- **Matriz TEDE.**
  Herramienta de análisis que evalúa cada innovación en cuatro dimensiones críticas (tecnología, evaluación, doctrina y empleo), evitando el sesgo del *technology push* carente de marco doctrinal.

2. Metodología Prospectiva.

- **MICMAC**
  Análisis estructural que identifica variables clave del sistema mediante matriz de influencias directas y clasificación por motricidad y dependencia.
- **MACTOR**
  Juego de actores que mapea influencias entre stakeholders, analizando convergencias y divergencias de intereses estratégicos.
- **SMIC**
  Matriz de impactos cruzados que asigna probabilidades a escenarios mediante análisis de coherencia condicional entre hipótesis.
- **Backcasting**
  Metodología prospectiva que parte del estado futuro deseado y retrocede en el tiempo para identificar fases críticas y puntos de bifurcación.
- **Variables Motrices**
  Variables con alta influencia y baja dependencia, que condicionan la evolución del sistema.
- **Variables de Enlace**
  Variables con alta influencia y alta dependencia, que transmiten efectos entre distintos factores del sistema.

3. **Doctrina Militar y Defensa.**

- **OODA | Observe–Orient–Decide–Act**

  Ciclo de decisión militar conceptualizado por John Boyd. Define la guerra como competición de bucles decisionales: quien complete el ciclo más rápido y con mejor orientación impone la iniciativa.

- **MDO | Multi-Domain Operations**

  Concepto operacional que integra capacidades militares en cinco dominios (tierra, aire, mar, espacio y ciberespacio) y tres dimensiones (física, informacional y humana).

- **FM 3-0**

  Manual doctrinal del Ejército de Estados Unidos para operaciones multidominio, actualizado en 2022.

- **JADC2 | Joint All-Domain Command and Control**

  Estrategia del Departamento de Defensa de EE.UU. para conectar sensores, datos y sistemas de todas las fuerzas en una red integrada potenciada por IA.

- **RAI | Responsible Artificial Intelligence**

  Estrategia del DoD para un desarrollo y uso responsable de la IA militar, basada en seis principios fundamentales.

- **PRUs | Principles of Responsible Use (OTAN)**

  Principios para el uso responsable de IA en defensa: Legalidad, Responsabilidad, Trazabilidad, Confiabilidad, Gobernabilidad y Mitigación de Sesgos.

- **C4ISR | Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance**

  Sistema integrado de mando y control que combina comunicaciones, inteligencia, vigilancia y reconocimiento.

4. **Organizaciones y Actores.**

- **DoD | Department of Defense**

  Ministerio de Defensa de Estados Unidos.

- **CDAO | Chief Digital and Artificial Intelligence Officer**

  Oficina del DoD responsable de coordinar políticas de datos e inteligencia artificial.

- **DIANA | Defence Innovation Accelerator for the North Atlantic**

  Acelerador de innovación tecnológica de la OTAN para potenciar la cooperación transatlántica en I+D.

- **OTAN | Organización del Tratado del Atlántico Norte**
  Alianza militar intergubernamental transatlántica fundada en 1949.
- **TRADOC | Training and Doctrine Command**
  Comando del Ejército de EE.UU. encargado de doctrina, adiestramiento y desarrollo conceptual.

5. **<u>Tecnología e Innovación</u>.**
   - **IA Generativa**
     Sistemas de inteligencia artificial capaces de crear contenido nuevo (texto, imágenes, código o planes) a partir de patrones aprendidos.
   - **Edge Computing**
     Procesamiento de datos en el punto de origen (sensores o nodos locales), reduciendo latencias, asegurando resiliencia y minimizando dependencia de redes centrales.
   - **TRL | Technology Readiness Level**
     Escala (1–9) que mide la madurez tecnológica, desde la investigación básica hasta la aplicación operacional.
   - **TEVV | Test, Evaluation, Verification and Validation**
     Marco del DoD para evaluar sistemas de IA mediante pruebas rigurosas, verificación y validación.
   - **Human-in-the-loop**
     Arquitectura que preserva el control humano en decisiones críticas, especialmente en operaciones con IA militar.
   - **Data Poisoning**
     Manipulación maliciosa de conjuntos de datos para degradar o corromper el funcionamiento de modelos de IA.
   - **Sesgos Algorítmicos**
     Distorsiones en los resultados de sistemas de IA causadas por datos de entrenamiento o diseño defectuoso.
   - **Alucinaciones de IA**
     Respuestas falsas o inventadas generadas por sistemas de IA que aparentan ser coherentes pero carecen de veracidad factual.
6. **<u>Acrónimos Operacionales</u>.**
   - **COA | Course of Action**
     Curso de acción que describe una alternativa táctica u operacional.

- **EM | Estado Mayor**

  Órgano de planeamiento, asesoramiento y coordinación en las fuerzas armadas.
- **Estados Mayores IA-nativos**

  Concepto prospectivo que describe Estados Mayores diseñados desde su origen para operar con integración plena de inteligencia artificial.
- **ISR | Intelligence, Surveillance, Reconnaissance**

  Conjunto de capacidades destinadas a obtener información en tiempo real mediante vigilancia e inteligencia técnica y humana.
- **TTPs | Tactics, Techniques, Procedures**

  Tácticas, técnicas y procedimientos que estructuran la acción operacional.
- **C2 | Command and Control**

  Función militar que articula autoridad, dirección y coordinación de fuerzas en operaciones.
- **COCOM | Combatant Command**

  Comandos unificados de EE.UU. con responsabilidad geográfica o funcional a nivel estratégico.

ANEXO B - BIBLIOGRAFÍA INTEGRADA (TEDE + PROSPECTIVA).

1. DOCTRINA Y PUBLICACIONES MILITARES.

a. North Atlantic Treaty Organization. (2024a). *NATO artificial intelligence strategy*. NATO Headquarters. https://www.nato.int/cps/en/natohq/official_texts_213375.htm

b. North Atlantic Treaty Organization. (2024b). *Principles of responsible use of artificial intelligence in defence*. NATO Communications and Information Agency. https://www.nato.int/cps/en/natohq/news_213376.htm

c. NATO Defence Innovation Accelerator for the North Atlantic. (2024). *DIANA challenge programmes 2024*. NATO DIANA. https://www.diana.nato.int/

d. NATO Science and Technology Organization. (2024). *AI in military operations: Opportunities and challenges* (Technical Report TR-IST-217). https://www.sto.nato.int/publications/

e. U.S. Army. (2022). *FM 3-0: Operations*. Headquarters, Department of the Army. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf

f. U.S. Army. (2023). *Project Convergence 2023: After action report*. Army Futures Command. https://www.army.mil/futures/

g. U.S. Department of Defense. (2022). *Joint all-domain command and control (JADC2) strategy*. Office of the Under Secretary of Defense for Acquisition and Sustainment. https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/JADC2_STRATEGY.PDF

h. U.S. Department of Defense. (2023, February 24). *DoD adopts ethical principles for artificial intelligence* [Comunicado de prensa]. https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/

i. Instituto Español de Estudios Estratégicos. (2024). *Inteligencia artificial y defensa: Análisis prospectivo*. Cuadernos de Estrategia 226. Ministerio de Defensa de España. https://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/

2. FUENTES ACADÉMICAS Y CIVILES.

a. Fundamentos Teóricos.

1) Boyd, J. R. (1987). *Organic design for command and control* [Briefing no publicado]. Defense and the National Interest. http://www.dnipogo.org/boyd/organic_design.pdf

2) Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review*, *1*(3), 37-57. https://doi.org/10.15781/T2639KP8R

b. Inteligencia Artificial y Seguridad Internacional.

1) Allen, G. C. (2022). *China's new strategy for waging the AI technology competition*. Center for Strategic and International Studies. https://www.csis.org/analysis/chinas-new-strategy-waging-ai-technology-competition

2) Horowitz, M. C., Allen, G. C., Saravalle, E., Cho, A., Frederick, K., & Scharre, P. (2018). *Artificial intelligence and international security*. Center for a New American Security. https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security

3) Hoadley, D. S., & Lucas, N. J. (2018). *Artificial intelligence and national security* (Report R45178). Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R45178

4) Center for Security and Emerging Technology. (2023). *Technology readiness levels for AI and autonomous systems in defense*. Georgetown University. https://cset.georgetown.edu/publication/trl-ai-defense/

c. Vulnerabilidades y Amenazas Emergentes.

Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition*, *84*, 317-331. https://doi.org/10.1016/j.patcog.2018.07.023

d. Adopción Organizacional y Resistencia al Cambio.

1) Maas, M., & Sweijs, T. (2023). Organizational resistance to AI adoption in military institutions. *Journal of Strategic Studies*, *46*(2), 312-341. https://doi.org/10.1080/01402390.2023.2165432

2) Johnson, J., & Kott, A. (2022). Human–machine teaming in command and control. En A. Kott, D. S. Alberts, & A. Zalman (Eds.), *Autonomous intelligent cyber defense agent (AICA)* (pp. 115-136). Springer. https://doi.org/10.1007/978-3-030-87447-7_6

e. Casos de Estudio y Análisis de Conflictos.

1) Kaushal, S., Watling, J., & Reynolds, N. (2023). *How Ukraine has defended the sky: Air defence lessons from Russia's 2022 invasion* (Special Report). Royal United Services Institute. https://static.rusi.org/409-SR-How-Ukraine-has-Defended-the-Sky-web.pdf

2) Pettyjohn, S. L., & Wasser, B. (2023). *Competing in the gray zone: Russian tactics and Western responses* (Research Report RRA594-1). RAND Corporation. https://doi.org/10.7249/RRA594-1

f. Marco Regulatorio.

Unión Europea. (2024). Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo sobre inteligencia artificial. *Diario Oficial de la Unión Europea*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

3. METODOLOGÍA PROSPECTIVA.

1) Godet, M. (2007). *Prospectiva estratégica: Problemas y métodos* (2.ª ed.). LIPSOR - Laboratoire d'Investigation Prospective et Stratégique. http://www.laprospective.fr/

2) Godet, M., & Durance, P. (2011). *Strategic foresight for corporate and regional development*. Fondation Prospective et Innovation - UNESCO. http://en.laprospective.fr/methods-of-prospective/key-books.html

3) Durance, P., & Godet, M. (2010). Scenario building: Uses and abuses. *Technological Forecasting & Social Change*, *77*(9), 1488-1492. https://doi.org/10.1016/j.techfore.2010.06.007

4) Schwartz, P. (1991). *The art of the long view: Planning for the future in an uncertain world*. Currency Doubleday. https://www.penguinrandomhouse.com/books/

5) Van der Heijden, K. (2005). *Scenarios: The art of strategic conversation* (2.ª ed.). John Wiley & Sons. https://doi.org/10.1002/9780470033234

4. LISA INSTITUTE - PROSPECTIVA Y AMENAZAS EMERGENTES.

1) LISA Institute. (2023a). *Qué es la prospectiva y el análisis prospectivo*. https://www.lisainstitute.com/blogs/blog/prospectiva-analisis-prospectivo

2) LISA Institute. (2023b). *Ciberinteligencia vs ciberseguridad: Diferencias y sinergias*. https://www.lisainstitute.com/blogs/blog/ciberinteligencia-ciberseguridad-diferencias

3) LISA Institute. (2024a). *Brain hacking: La nueva frontera de la manipulación cognitiva*. https://www.lisainstitute.com/blogs/blog/brain-hacking-manipulacion-cognitiva

4) LISA Institute. (2024b). *Deepfakes: Amenaza a la integridad de la información en seguridad nacional*. https://www.lisainstitute.com/blogs/blog/deepfakes-seguridad-nacional

5) LISA Institute. (2024c). *Análisis de amenazas internacionales: Metodologías de inteligencia estratégica*. https://www.lisainstitute.com/blogs/blog/analisis-amenazas-internacionales