

Algoritmos, redes y poder:

las nuevas fronteras del poder geopolítico de las tecnologías emergentes

DOI: 10.29236/sistemas.n180a2

Resumen

La competencia por el poder global se extiende al control de las infraestructuras digitales, los datos y las capacidades de innovación. Este artículo contextualiza cinco campos tecnológicos estratégicos —ciberseguridad, inteligencia artificial, Internet de las cosas, redes 5G y computación cuántica— y explica su relevancia para la economía, la seguridad y las relaciones internacionales. Mediante una revisión de literatura académica e informes institucionales, examina sus principales aplicaciones, los actores que lideran su desarrollo y las dependencias que acompañan su expansión. El análisis muestra que el liderazgo tecnológico comprende distintas capacidades: producir componentes, desarrollar sistemas, desplegar infraestructura y establecer estándares y reglas. Asimismo, aborda la convergencia entre estas tecnologías y sus implicaciones para América Latina. Se concluye que la posición internacional de los países depende tanto del acceso a las innovaciones como de su capacidad para comprenderlas, protegerlas y adaptarlas a sus necesidades. La formación especializada, la cooperación y la continuidad institucional resultan esenciales para convertir la adopción tecnológica en desarrollo y mayores márgenes de autonomía.

Palabras claves:

Tecnologías emergentes; Geopolítica, Poder digital, Soberanía tecnológica, América Latina.

Introducción

Las tecnologías emergentes ocupan un lugar cada vez más relevante en las geopolítica internacional porque transforman las capacidades económicas, científicas y de seguridad de los Estados. Su importancia trasciende la aparición de nuevos productos: intervienen en la organización de la producción, el funcionamiento de los servicios públicos y el control de información estratégica. En este contexto, la competencia tecnológica constituye una dimensión de la disputa por el poder global, donde convergen intereses gubernamentales, empresariales y de la ciudadanía.

La ciberseguridad, la inteligencia artificial (IA), el Internet de las cosas (IoT), las redes 5G y la computación cuántica permiten examinar distintas expresiones de esta transformación. La ciberseguridad protege sistemas y servicios digitales, la IA amplía las posibilidades de analizar información y automatizar tareas, el IoT conecta objetos que recopilan datos sobre el entorno, las redes 5G proporcionan infraestructura de comunicación, y la computación cuántica explora nuevas capacidades de procesamiento para problemas específicos. Aunque presentan diferentes niveles de madurez, estos campos

se relacionan mediante infraestructuras, conocimientos y aplicaciones compartidas (Aguilar Antonio, 2025).

Su relevancia geopolítica reside en las ventajas y dependencias que pueden generar. El acceso a componentes, capacidades de cómputo y personal especializado condiciona las posibilidades de innovación. A su vez, las decisiones sobre proveedores y estándares influyen en la capacidad de los países para operar, proteger y modificar sus sistemas. Las restricciones estadounidenses anunciadas en octubre de 2023 sobre semiconductores avanzados y equipos para fabricarlos ilustran cómo el acceso a determinados recursos tecnológicos se incorpora a los instrumentos de seguridad nacional y política exterior (Bureau of Industry and Security, 2023).

Este artículo contextualiza estas cinco tecnologías y explica su importancia para la competencia internacional, la protección de infraestructura estratégica y la distribución del poder. También, examina sus implicaciones para América Latina, cuya participación depende de la capacidad de convertir la adopción tecnológica en conocimiento, desarrollo productivo y mayores márgenes de decisión.

1. Las tecnologías emergentes en la configuración del poder global

El concepto de tecnología emergente se refiere a desarrollos que introducen cambios significativos y cuyas aplicaciones, beneficios y consecuencias todavía no se encuentran plenamente definidos. Rotolo, Hicks y Martin (2015) identifican cinco atributos para comprender esta condición: novedad radical, crecimiento relativamente rápido, coherencia, impacto destacado e incertidumbre. Esta definición permite distinguir la emergencia tecnológica de la simple actualización de un producto. Una innovación adquiere mayor relevancia cuando puede modificar actividades económicas, prácticas sociales o capacidades institucionales.

Los cinco campos abordados requieren, sin embargo, una distinción. La ciberseguridad constituye un ámbito consolidado que incorpora herramientas emergentes; el IoT y las redes 5G cuentan con aplicaciones comerciales, mientras que la IA reúne tecnologías con distintos grados de desarrollo.

La computación cuántica presenta desafíos científicos y de ingeniería que condicionan sus posibilidades de aplicación. Su análisis conjunto responde a su importancia estratégica y a las relaciones que mantienen, sin atribuirles una madurez equivalente.

Para comprender su dimensión geopolítica resulta necesario observar las condiciones que permiten desarrollarlas. La innovación depende de ecosistemas que articulan investigación, financiamiento, infraestructura y formación especializada. El *AI Index 2024* de Stanford documentó el predominio de la industria en la producción de modelos destacados de IA y el incremento de los costos de entrenamiento de sistemas de frontera (Maslej et al., 2024). Esta evidencia muestra que el conocimiento científico necesita recursos materiales y organizativos para convertirse en capacidades tecnológicas, lo que puede favorecer su concentración.

La infraestructura ocupa un lugar central en esa distribución de capacidades. Los datos requieren redes para circular y sistemas para almacenarse y procesarse. Los dispositivos conectados necesitan mantenimiento y actualizaciones, por su parte, las aplicaciones digitales dependen de componentes y servicios cuya provisión puede concentrarse en determinados proveedores. Por ello, la ubicación física de una infraestructura no garantiza que el país donde se encuentra controle todas sus funciones. También, importan las condiciones de acceso, las responsabilidades operativas y las alternativas disponibles ante una interrupción.

Los estándares y las normas constituyen otra dimensión del poder

tecnológico. Los primeros establecen requisitos técnicos para conectar y proteger sistemas, por eso que sea de suma relevancia para múltiples instituciones o individuos certificarse bajo las normativas de instituciones como la Organización Internacional de Estandarización (ISO) o el Instituto Nacional de Estándares y Tecnología (NIST). En su cancha, las leyes, definen obligaciones y condiciones de uso, y en los hechos solución problemas de delimitación de responsabilidades, crean un marco legal y cimentan las bases de la gobernanza tecnológica. Un caso reciente, por ejemplo, es el Reglamento de Inteligencia Artificial de la Unión Europea de 2024 que organiza obligaciones conforme a los riesgos de determinados sistemas y aplicaciones. Desde una perspectiva geopolítica, la capacidad de establecer condiciones para acceder a un mercado puede influir en las decisiones de empresas y proveedores internacionales (Reglamento UE 2024/1689, 2024)

Estas relaciones permiten entender la autonomía tecnológica como una capacidad gradual para evaluar, adaptar y sostener sistemas, proteger información y negociar condiciones de cooperación. Para América Latina, el desafío consiste en desarrollar competencias que acompañen la adquisición de infraestructura y servicios. La relevancia geopolítica de las tecnologías emergentes depende, en consecuencia, tanto de sus posibilida-

des técnicas como de la capacidad de los Estados para incorporarlas a sus objetivos de desarrollo y seguridad.

2. Ciberseguridad y poder en el espacio digital

La ciberseguridad comprende las medidas, capacidades y procedimientos destinados a proteger sistemas, redes e información frente a accesos no autorizados, alteraciones e interrupciones. Su importancia aumenta conforme las actividades económicas y gubernamentales dependen de servicios digitales. La operación de hospitales, sistemas financieros, redes eléctricas y telecomunicaciones requiere que la información permanezca disponible y conserve su integridad. Por ello, proteger estos sistemas constituye una condición para el funcionamiento del Estado y la continuidad de la vida cotidiana.

La preparación nacional exige una combinación de instrumentos jurídicos, capacidades técnicas, organización institucional, formación y cooperación. Estas dimensiones integran el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones (ITU, 2024). Su enfoque permite comprender que la protección digital depende de políticas sostenidas y responsabilidades definidas, además de equipos y programas informáticos. Sin embargo, el índice evalúa compromisos y capacidades institucionales y sus resultados

no equivalen a una medición de inmunidad frente a ataques ni de poder cibernético ofensivo. Por eso no debe sorprender que incluso los países con los mejores puntajes, como Estados Unidos, Reino Unido, Singapur, Corea del Sur o Alemania, se encuentren entre aquellos que han sido víctimas de incidentes cibernéticos.

La relevancia geopolítica de la ciberseguridad se relaciona con la posibilidad de ejercer presión mediante sistemas digitales. El espionaje informático puede facilitar la obtención de información gubernamental o industrial, mientras que las operaciones dirigidas a interrumpir servicios pueden producir consecuencias económicas y sociales. Estas actividades amplían los instrumentos disponibles para influir sobre otros actores. Su atribución presenta dificultades: identificar una infraestructura utilizada en un ataque no demuestra, por sí mismo, quién lo ordenó o qué gobierno participó.

La protección del espacio digital también incorpora a empresas que administran servicios de nube, redes y plataformas. Sus decisiones sobre acceso, mantenimiento y respuesta a incidentes pueden afectar funciones esenciales. En consecuencia, la seguridad nacional requiere mecanismos de coordinación con operadores privados y condiciones contractuales que permitan conocer las dependencias de los sistemas. La resiliencia, enten-

dida como la capacidad de mantener y recuperar operaciones, adquiere así un valor estratégico.

En los hechos, la ciberseguridad implica para los países la creación de una política nacional permanente de fortalecimiento de capacidades institucionales, que está en estrecha relacionada con la agenda de seguridad nacional y política exterior (Aguilar Antonio, 2021). Desde esta perspectiva, la cooperación internacional resulta relevante cuando fortalece los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) o forma capital humano como especialistas nacionales, facilita el intercambio de información y mejora la respuesta ante incidentes. La ciberseguridad constituye, además, una condición transversal para incorporar las demás tecnologías es la base necesaria que los países deben tener para incorporar el resto de las tecnologías, establecer un marco legal, mecanismos de gobernanza y recibir beneficios de su implementación.

3. IA y competencia por el liderazgo tecnológico

La IA reúne técnicas que permiten a los sistemas informáticos realizar tareas como reconocer patrones, elaborar predicciones y generar contenidos. Sus aplicaciones incluyen el análisis de imágenes médicas, la identificación de fallas industriales, la traducción y el procesamiento de grandes volúmenes

de información. Su relevancia geopolítica deriva de su capacidad para transformar actividades productivas y apoyar funciones gubernamentales, científicas y de seguridad. Los resultados dependen, sin embargo, de la calidad de los datos, del diseño del sistema y de las condiciones en que se utiliza.

El desarrollo de IA requiere personal especializado, infraestructura de cómputo y financiamiento. Aunque sus aplicaciones comerciales pueden difundirse ampliamente, la producción de sistemas de frontera demanda recursos que favorecen la concentración de capacidades. El *AI Index 2024* de Stanford registró que, en 2023, instituciones estadounidenses originaron 61 modelos destacados, frente a 21 de la Unión Europea y 15 de China (Maslej et al., 2024). Estas cifras corresponden a una categoría y un periodo específicos; muestran una dimensión del desarrollo tecnológico, sin establecer una clasificación definitiva de liderazgo. Sin embargo, si enmarcan una disputa geopolítica clara, una competencia entre Occidente, liderado por Estados Unidos, y Oriente, como China como principal actor (Aguilar Antonio, 2025).

La competencia entre Estados Unidos y China también involucra el acceso a los componentes que permiten entrenar y operar sistemas avanzados. Los semiconductores adquieren importancia porque proporcionan capacidad de procesa-

miento. Las restricciones estadounidenses anunciadas en octubre de 2023 sobre chips avanzados y equipos para fabricarlos evidencian la incorporación de estos recursos a la política de seguridad nacional (Bureau of Industry and Security, 2023). Su significado geopolítico reside en que el control de determinados insumos puede condicionar las posibilidades de innovación de otros actores.

Europa participa en esta transformación mediante capacidades científicas, empresariales y regulatorias. El Reglamento de IA (2024) establece obligaciones diferenciadas según los riesgos de determinados sistemas y usos. La regulación puede influir en las prácticas de proveedores que buscan acceder al mercado europeo. De esta manera, la competencia internacional comprende tanto el desarrollo de tecnologías como la definición de condiciones para comercializarlas y utilizarlas.

La IA posee también aplicaciones de doble uso: una capacidad desarrollada para fines civiles puede apoyar actividades de seguridad o defensa. El análisis automatizado puede contribuir al procesamiento de información, la planificación logística y la identificación de patrones. Al mismo tiempo, los errores, los sesgos y la generación de contenidos engañosos plantean problemas de verificación y responsabilidad. La incorporación de estos sistemas a decisiones sensibles

exige evaluar su desempeño y conservar mecanismos de supervisión humana.

4. Internet de las cosas y digitalización del territorio

El IoT conecta dispositivos capaces de recopilar e intercambiar información sobre su entorno. Sensores agrícolas, medidores de electricidad, cámaras y equipos industriales forman parte de este campo. Su funcionamiento permite observar procesos y, en determinados sistemas, activar respuestas automáticas. Un sensor puede advertir una variación de temperatura en una instalación o registrar la humedad del suelo para orientar el riego. Estas aplicaciones vinculan actividades físicas con redes y plataformas digitales.

Su relevancia geopolítica se relaciona con el conocimiento que produce sobre el territorio y la actividad económica. La información generada por dispositivos conectados puede revelar patrones de consumo, movimientos logísticos y condiciones de operación de instalaciones. Cuando estos datos se acumulan y analizan, adquieren valor para empresas y autoridades. Por ello, la expansión del IoT plantea preguntas sobre quién recopila la información, dónde se procesa y en qué condiciones puede utilizarse.

Estados Unidos y China destacan entre los principales actores del IoT, mientras que Alemania, Japón,

Corea del Sur y Singapur sobresalen en aplicaciones industriales y urbanas. El liderazgo estadounidense se apoya en empresas que ofrecen servicios de nube, plataformas digitales y soluciones para conectar y analizar dispositivos. China combina capacidad manufacturera, infraestructura de telecomunicaciones y un amplio mercado para desplegar aplicaciones. Alemania y Japón destacan por la integración de sistemas conectados en manufactura y automatización. Mientras, Corea del Sur articula dispositivos electrónicos y conectividad avanzada y Singapur ofrece un referente de aplicación en servicios urbanos. Estas posiciones representan distintas dimensiones del liderazgo, que no puede reducirse a una clasificación única (Aguilar-Antonio, 2025).

La competencia se desarrolla, por tanto, en varias etapas: fabricación de sensores, provisión de conectividad, administración de plataformas y procesamiento de información. Un país puede destacar en la producción de equipos y depender de servicios externos para analizar sus datos. Esta distribución de funciones permite que actores diferentes ejerzan influencia sobre una misma infraestructura. Controlar la plataforma que integra los dispositivos puede resultar tan relevante como producir los objetos conectados.

La incorporación de dispositivos también amplía los puntos de acce-

so a los sistemas. Un equipo con protección insuficiente puede comprometer información o facilitar una intrusión en la red a la que pertenece. Las orientaciones del NIST identifican capacidades básicas como la protección de datos, el control de acceso y la actualización del software (Fagan et al., 2020). Por su parte, el estándar ETSI EN 303 645 establece una referencia de seguridad para dispositivos conectados de consumo (European Telecommunications Standards Institute, 2020). Estas medidas muestran que la protección debe acompañar el diseño y mantenerse durante la vida útil del producto.

La interoperabilidad constituye otra dimensión estratégica. Esta permite que equipos y plataformas intercambien información y funcionen conjuntamente. Cuando una instalación depende de componentes incompatibles con otras soluciones, sustituir al proveedor puede exigir inversiones adicionales y cambios operativos. La dependencia tecnológica surge entonces de decisiones acumuladas sobre dispositivos, programas y mantenimiento. Disponer de documentación y mecanismos para trasladar los datos contribuye a conservar alternativas.

5. Redes 5G y geopolítica de las telecomunicaciones

Las redes de quinta generación, o 5G, representan una evolución de las comunicaciones móviles. Per-

miten mayores capacidades de transmisión y, bajo determinadas condiciones de despliegue, tiempos de respuesta más cortos y conexión de numerosos dispositivos. Estas características pueden apoyar aplicaciones industriales, servicios digitales y sistemas de monitoreo. Su desempeño depende del espectro disponible, la arquitectura de la red, la infraestructura de transporte y los equipos utilizados. Por ello, contar con cobertura 5G no garantiza disponer de todas sus posibilidades técnicas.

China, Estados Unidos y Corea del Sur destacan por la escala de sus mercados y el desarrollo de redes 5G; Japón y varios países europeos también mantienen capacidades relevantes. China combina despliegue de infraestructura con fabricantes como Huawei y ZTE. En Estados Unidos, operadores como Verizon, AT&T y T-Mobile impulsan la expansión de servicios. Corea del Sur sobresale por su despliegue comercial temprano y la integración de conectividad con su industria tecnológica. Japón cuenta con operadores y empresas que desarrollan aplicaciones para actividades industriales. Estas trayectorias muestran que el liderazgo puede medirse mediante cobertura, adopción, desempeño o capacidad de fabricación, con resultados diferentes según el indicador (Bahia & Amaya Ariza, 2024).

La producción de equipos introduce otra distribución del poder. Erics-

son, de Suecia, y Nokia, de Finlandia, son actores relevantes en infraestructura de telecomunicaciones, junto con Huawei, ZTE y Samsung, de Corea del Sur (Aguilar-Antonio, 2025). La presencia de fabricantes europeos muestra que el tamaño de un mercado nacional no determina por sí mismo la influencia tecnológica. Las empresas que suministran componentes desarrollan soluciones y participan en estándares pueden ocupar posiciones estratégicas en redes instaladas en numerosos países, un caso relevante de esto es Huawei que ha potenciado los modelos “llave en mano” y ha tenido una inserción vertiginosa en múltiples países del Sur Global (Aguilar Antonio, 2026)

La importancia geopolítica de 5G deriva del papel que desempeñan las telecomunicaciones en la organización de la economía. Las redes conectan personas, empresas e instituciones y permiten que circulen datos esenciales para la producción y los servicios. Su construcción requiere inversiones y compromisos de mantenimiento que pueden prolongarse durante años. En consecuencia, las decisiones sobre infraestructura influyen en las posibilidades de modernización y en las relaciones que los países mantienen con proveedores externos.

La selección de proveedores incorpora consideraciones sobre precio, rendimiento, seguridad y continui-

dad del suministro. Desde una perspectiva geopolítica, importa conocer quién controla funciones esenciales de la red y qué alternativas existen si se interrumpe la provisión de componentes o servicios. Estas preocupaciones deben traducirse en evaluaciones técnicas y condiciones contractuales verificables, incluyendo acceso a actualizaciones, documentación y procedimientos de recuperación. Del mismo, las auditorías son mecanismos de evaluación relevantes para los gobiernos y países.

6. Computación cuántica y nuevas fronteras del poder tecnológico

La computación cuántica utiliza propiedades de la mecánica cuántica para procesar información mediante cúbits. A diferencia de los bits convencionales, estos permiten desarrollar formas de cálculo que pueden ofrecer ventajas para determinados problemas. Entre sus aplicaciones potenciales se encuentran la simulación de moléculas, materiales y algunos problemas de optimización. Sin embargo, estas posibilidades no implican que una computadora cuántica pueda resolver cualquier tarea con mayor rapidez. Su desarrollo enfrenta dificultades de estabilidad, corrección de errores y escalabilidad que condicionan su utilidad práctica.

Estados Unidos y China figuran entre los principales actores de la competencia cuántica, mientras

que Alemania, Francia, Reino Unido, Canadá y Japón mantienen importantes capacidades de investigación y desarrollo. El liderazgo presenta distintas dimensiones: producción científica, desarrollo de equipos, formación de especialistas y aplicaciones experimentales. Además, debe distinguirse la computación cuántica de las comunicaciones y los sensores cuánticos, porque los avances en uno de estos campos no demuestran una posición equivalente en los demás (Aguilar Antonio, 2025).

Estados Unidos articula universidades, organismos públicos y empresas mediante iniciativas como la National Quantum Initiative (s.f.), orientada a coordinar investigación y desarrollo de capacidades. China ha otorgado importancia estratégica a las tecnologías cuánticas mediante programas de investigación e infraestructura experimental. En Europa, la cooperación regional busca fortalecer un ecosistema científico e industrial: la Declaración Europea sobre Tecnologías Cuánticas, publicada en diciembre de 2023, reconoce su relevancia para la competitividad y promueve la colaboración entre los países participantes (Comisión Europea, 2023). Estas trayectorias muestran que la competencia depende de esfuerzos sostenidos y no únicamente de un descubrimiento aislado.

Su relevancia geopolítica reside en las ventajas que podrían derivarse

de aplicaciones científicas e industriales y en la posibilidad de establecer nuevas dependencias. El acceso a equipos, componentes especializados y personal capacitado puede condicionar quién participa en esta frontera tecnológica. Los servicios de acceso remoto amplían las oportunidades de experimentación, aunque utilizar una plataforma externa no equivale a controlar su infraestructura ni sus condiciones de disponibilidad.

La protección de información constituye otra implicación estratégica. Una computadora cuántica suficientemente capaz podría comprometer ciertos métodos criptográficos utilizados actualmente. Esto no significa que los sistemas experimentales hayan roto de manera generalizada el cifrado disponible. El riesgo se relaciona con información que necesita permanecer confidencial durante años y que podría ser capturada hoy para intentar descifrarla posteriormente.

En agosto de 2024, el NIST (2024) publicó sus tres primeros estándares finalizados de criptografía poscuántica. Estos utilizan algoritmos diseñados para resistir ataques cuánticos y pueden implementarse en sistemas convencionales. La preparación requiere identificar dependencias criptográficas y planear actualizaciones. De esta manera, la relevancia geopolítica de la computación cuántica combina expectativas de innovación con decisiones presentes sobre la pro-

tección de información estratégica en el futuro.

7. Convergencia tecnológica y posición de América Latina

Las cinco tecnologías analizadas forman parte de una transformación que conecta infraestructura, información y capacidades productivas. Los dispositivos IoT recopilan datos; las redes 5G permiten transmitirlos y la IA puede apoyar su análisis e interpretación. La ciberseguridad protege estos procesos, mientras que la computación cuántica introduce posibilidades de procesamiento y desafíos para ciertos métodos criptográficos. Su convergencia permite comprender que el poder tecnológico depende de la capacidad de integrar sistemas y mantener su funcionamiento.

Para América Latina y el Caribe, esta transformación presenta oportunidades de modernización junto con riesgos de dependencia. Sin embargo, la situación regional es heterogénea. Existen diferencias entre países, sectores productivos e instituciones, por lo que la disponibilidad de una tecnología no garantiza que sus beneficios se distribuyan de manera amplia.

Brasil y México destacan por el tamaño de sus mercados y las oportunidades de aplicación en industria, agricultura y servicios. Chile, Uruguay y Argentina cuentan con capacidades relevantes en determinados componentes de sus eco-

sistemas digitales (Aguilar Antonio, 2025). Estas posiciones deben interpretarse según el campo analizado: el despliegue de telecomunicaciones, la investigación científica y la preparación en ciberseguridad representan capacidades distintas. La región necesita articularlas para transformar la adopción de tecnologías en resultados productivos e institucionales.

La IA ofrece posibilidades para desarrollar aplicaciones ajustadas a necesidades locales, pero requiere datos adecuados, especialistas y mecanismos de evaluación. El IoT puede mejorar procesos agrícolas e industriales, siempre que existan capacidades para mantener los equipos e interpretar la información. Las redes 5G proporcionan infraestructura habilitadora, aunque su aprovechamiento depende de condiciones de inversión, acceso y desarrollo de servicios. El informe de *The mobile economy Latin America 2024* sitúa estos factores dentro de la transición de la economía móvil regional (GSMA, 2024).

En ese sentido, la cooperación regional puede ampliar recursos mediante investigación conjunta, formación especializada e intercambio de información sobre amenazas. La posición geopolítica de América Latina dependerá de su capacidad para convertir la adquisición de tecnologías en aprendizaje y conservar alternativas de operación. La autonomía tecnológica se

construye gradualmente cuando las instituciones pueden evaluar soluciones, proteger información y decidir cómo incorporar la innovación a sus objetivos de desarrollo.

8. Conclusiones

La ciberseguridad, la IA, el IoT, las redes 5G y la computación cuántica adquieren relevancia geopolítica porque influyen en capacidades esenciales de los Estados y sus economías. Su importancia comprende la protección de servicios, el procesamiento de información y la organización de actividades productivas. Estas funciones vinculan la innovación con la seguridad nacional y con las posibilidades de ejercer influencia internacional.

El liderazgo tecnológico presenta distintas dimensiones. La fabricación de componentes, la investigación científica, el despliegue de infraestructura y la definición de estándares pueden distribuirse entre actores diferentes. Por ello, la posición de un país debe evaluarse según las funciones que controla y las capacidades que puede sostener. Las clasificaciones basadas en un solo indicador ofrecen una visión parcial de relaciones tecnológicas más complejas.

La convergencia entre estas tecnologías amplía sus posibilidades y también conecta sus vulnerabilidades. Una infraestructura avanzada puede seguir siendo frágil si depende de mantenimiento externo, care-

ce de protección o no dispone de personal especializado. La capacidad tecnológica requiere continuidad institucional y decisiones que contemplen la vida útil de los sistemas, sus costos y las condiciones de acceso a información estratégica.

Para América Latina, el desafío consiste en fortalecer capacidades que permitan aprovechar las innovaciones y reducir dependencias que limiten sus decisiones. La formación, la cooperación y el desarrollo de aplicaciones pertinentes pueden mejorar su participación internacional. El resultado dependerá de que la modernización tecnológica produzca conocimiento local, servicios sostenibles y mayores posibilidades de elección para los Estados y sus sociedades.

Referencias

- Aguilar Antonio, J. M. (2021). *Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Estudios Internacionales*, 53 (198), 169–197.
<https://doi.org/10.5354/0719-3769.2021.57067>
- Aguilar Antonio, J. M. (2025). *¿Salto tecnológico o retraso tecnológico? La lucha de América Latina por mantenerse al día con las tecnologías emergentes*. Jack D. Gordon Institute for Public Policy, Florida International University.
<https://digitalscholarship.fiu.edu/record/19469?v=pdf>
- Aguilar Antonio, J. M. (2026). *Huawei como vector geopolítico: La disputa por*

la soberanía digital en Centroamérica. Expediente Abierto.
<https://doi.org/10.5281/zenodo.21893927>

Amaya, F., & Bahia, K. (2024, febrero). *The state of 5G 2024: Introducing the GSMA Intelligence 5G Connectivity Index*. GSMA Intelligence.
<https://media-assets-prod.gsmaintelligence.com/content/210224-The-State-of-5G-2024-compressed.pdf>

Bureau of Industry and Security (2023). *Commerce strengthens restrictions on advanced computing semiconductors, semiconductor manufacturing equipment, and supercomputing items to countries of concern*. U.S. Department of Commerce.
<https://www.bis.gov/press-release/commerce-strengthens-restrictions-advanced-computing-semiconductors-semiconductor-manufacturing-equipment>

Comisión Europea (2023). *European declaration on quantum technologies*.
<https://digital-strategy.ec.europa.eu/en/library/european-declaration-quantum-technologies>

GSMA. (2024). *The mobile economy Latin America 2024*.
<https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/06/The-Mobile-Economy-Latin-America-2024.pdf>

Maslej, N., Fattorini, L., Perrault, R., Parli, V., Reuel, A., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Niebles, J. C., Shoham, Y., Wald, R., & Clark, J. (2024). *Artificial intelligence index report 2024*. Stanford Institute for Human-Centered Artificial Intelligence.

<https://hai.stanford.edu/ai-index/2024-ai-index-report>

National Institute of Standards and Technology [NIST]. (2024). *NIST releases first 3 finalized post-quantum encryption standards*.
<https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>

National Quantum Initiative. (s. f.). *The National Quantum Initiative*.
<https://www.quantum.gov/national-quantum-initiative/>

Reglamento (UE) 2024/1689 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 modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). (2024). *Diario Oficial de la Unión Europea, L, 2024/1689*, 12 de julio de 2024.
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

Rotolo, D., Hicks, D., & Martin, B. R. (2015). What is an emerging technology? *Research Policy*, 44 (10), 1827–1843.
<https://doi.org/10.1016/j.respol.2015.06.006>

Unión Internacional de Telecomunicaciones [ITU]. (2024). *Global cybersecurity index 2024* (5.ª ed.).
https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

Juan Manuel Aguilar Antonio. Profesor – investigador en la Facultad de Estudios Superiores Aragón de la Universidad Nacional Autónoma de México (UNAM). Es miembro del Sistema Nacional de Investigadores (SNI), nivel Candidato (2024–2027). Realizó dos estancias posdoctorales en el Centro de Investigaciones sobre América del Norte (CISAN–UNAM) con proyectos centrados en ciberseguridad, inteligencia artificial y tecnologías emergentes. En 2026 recibió el reconocimiento de Xiangshan Young Fellow del 13th Beijing Xiangshan Forum. Fue Becario Fulbright-García Robles para el periodo 2025-2026. Es egresado de los programas “Cyber Policy Development” (2019) y “Combating Transnational Threat Networks in the Americas” (2023) del William J. Perry Center, en la Universidad de la Defensa Nacional, en Washington D.C.

Desde 2013 ha impartido conferencias y clases en instituciones de seguridad pública de los estados de Chihuahua, Tamaulipas, Jalisco, Estado de México y Guanajuato. En la Escuela Superior de Guerra (ESG), el Centro de Estudios del Ejército y la Fuerza Aérea (CEEFA), la Policía Cibernética de la Ciudad de México (CDMX). El Centro Superior de Estudios Navales (CESNAV) de la Armada de México, de la Secretaría de Marina (SEMAR) y el Instituto Mexicano de Estudios Estratégicos en Seguridad de la Defensa Nacional (IMEESDN), y el Centro Nacional de Inteligencia (CNI).

En el ámbito internacional ha impartido clases como mentor senior en el Colegio Interamericano de Defensa (CID), ha sido consultor para la Florida International University (FIU), el U.S. Southern Command, el Instituto de Estudios Estratégicos de Australia (ASPI), la Iniciativa Global contra la Delincuencia Organizada (GITOC) y el Proyecto de Desarrollo e Integración de Mesoamérica. Así como orador en el Foro de Gobernanza Internet (IGF) de la Organización de las Naciones Unidas (ONU) y expositor en Global Conference on Cyber Capacity Building (GC3B) del Global Forum on Cyber Expertise (GFCE). Cuenta con múltiples publicaciones en Journals y/o Revistas Académicas Indexadas de Estados Unidos, México, Colombia, Costa Rica, Chile, Ecuador, España, Guatemala, Colombia y Brasil.