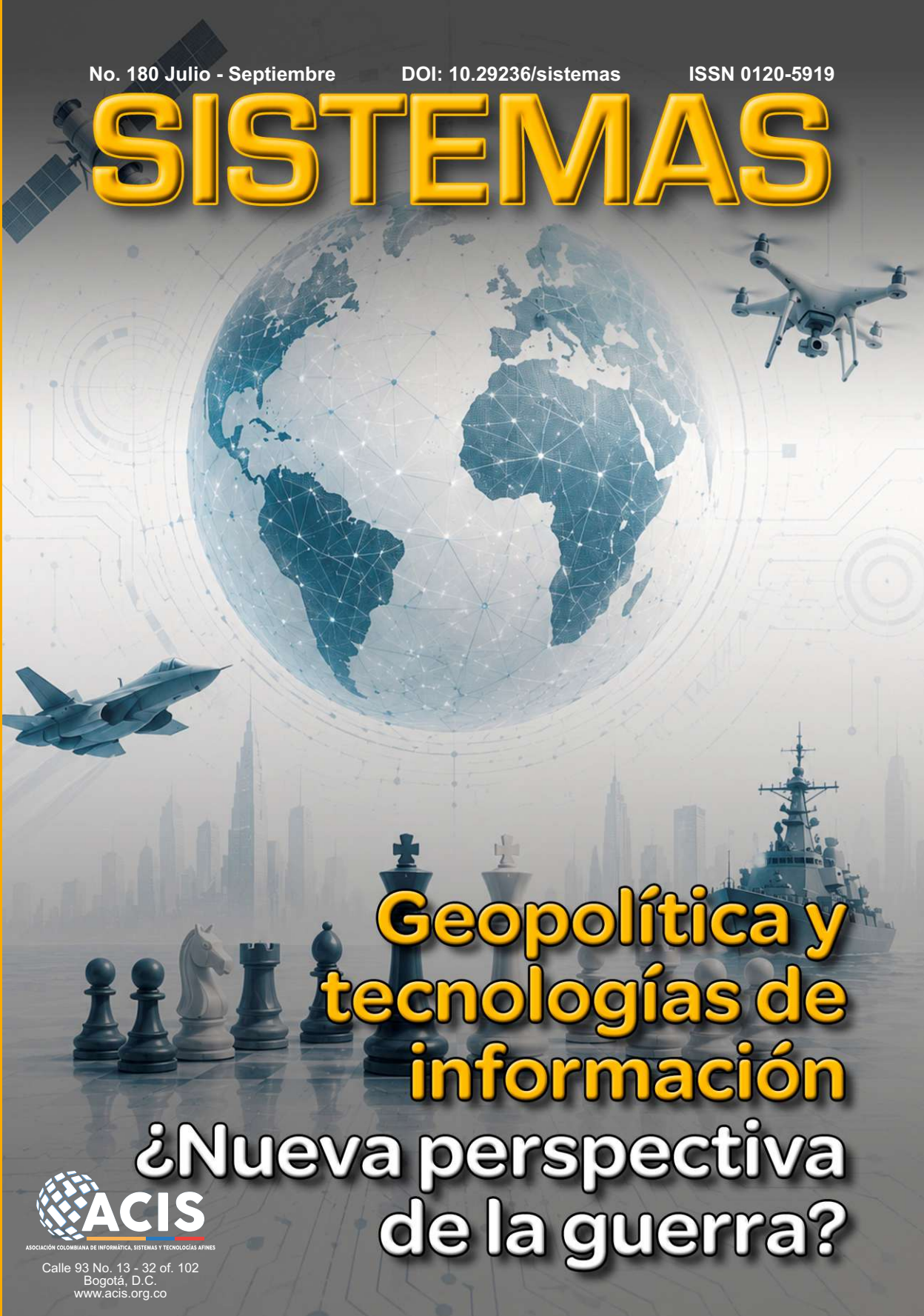
No. 180 Julio - Septiembre DOI: 10.29236/sistemas ISSN 0120-5919

SISTEMAS



Geopolítica y tecnologías de información

¿Nueva perspectiva de la guerra?

ACIS
ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES
Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

REVISTA SISTEMAS

de la Asociación Colombiana de Informática, Sistemas y Tecnologías Afines



https://sistemas.acis.org.co/index.php/sistemas



En esta edición

Editorial 4
El poder se ejerce en bits: ciberdefensa y soberanía digital en la región
DOI: 10.29236/sistemas.n180a1

Columnista Invitado 10
Algoritmos, redes y poder: las nuevas fronteras del poder geopolítico de las tecnologías emergentes
DOI: 10.29236/sistemas.n180a2

Entrevista 24
Panorama tecnológico actual
DOI: 10.29236/sistemas.n180a3

Investigación 30
Soberanía digital: Breve estado del arte global y latinoamericano
DOI: 10.29236/sistemas.n180a4

Uno 41
Defensa persistente avanzada
DOI: 10.29236/sistemas.n180a5

Dos 60
La guerra de los tres días que lleva cuatro años
DOI: 10.29236/sistemas.n180a6

Tres 79
Más allá de las fronteras
DOI: 10.29236/sistemas.n180a7

Cuatro 93
La guerra sin declaración
DOI: 10.29236/sistemas.n180a8

Cinco 101
Conectar los marcos internacionales, coordinar la respuesta: una hoja de ruta para el fortalecimiento de los CSIRT en América Latina
DOI: 10.29236/sistemas.n180a9

Publicación de la Asociación Colombiana de Informática, Sistemas y Tecnologías Afines (ACIS)
Resolución No. 003983 del Ministerio de Gobierno
Tarifa Postal Reducida Servicios Postales Nacional S.A. No. 2015-186 4-72
ISSN 0120-5919
Apartado Aéreo No. 94334
Bogotá D.C., Colombia

Dirección General
Jeimy J. Cano M.

Consejo de Redacción
Francisco Rueda F.
Gabriela Sánchez A.
Manuel Dávila S.
Andrés Ricardo Almanza J.
Emir Hernando Pernet C.
Jorge Eliécer Camargo M.
María Mercedes Corral S.
Johanna Castillo

Editora Técnica
Lina María Patricia Marique Villanueva

Editora
Sara Gallardo M.

Junta ACIS
2026-2028

Presidente
Ricardo Munévar Molano

Junta Directiva
Carlos Andrés Cuesta Yepes
Camilo Rodríguez Acosta
Edgar José Ruiz Dorante
Stalin Rodrigo Chapuel
Jorge Enrique Barbosa Suárez
Héctor Henry Pedraza Piñeros

Directora Ejecutiva
Beatriz E. Caicedo R.

Diseño y diagramación
Bruce Garavito

Los artículos que aparecen en esta edición no reflejan necesariamente el pensamiento de la Asociación. Se publican bajo la responsabilidad de los autores.

Julio - Septiembre 2026
Calle 93 No.13 - 32 Of. 102
Teléfonos 616 1407 - 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co

NASCO
NACIONAL DE COMPUTADORES S.A.

APOYA ESTA PUBLICACIÓN

TEL: 6 06 06 06- CR 15 No 72-73

4-72

Confía en 4-72,
el servicio de envíos
de Colombia

Línea de atención al cliente:
(57 - 1) 472 2000 en Bogotá
01 8000 111 210 a nivel Nacional

www.4-72.com.co

MARATÓN REGIONAL DE PROGRAMACIÓN

Anuncio de los ganadores de la Maratón Nacional de Programación

7 de noviembre de 2026

Innovación, talento y excelencia en la competencia que reúne a las mentes más brillantes de la programación en Colombia.



2 Puesto 2

Sede: Bogotá
Institución: Univ Nacional de Colombia - Bogotá
Equipo:
UN all-in

1 Puesto 1

Sede: Medellín
Institución: EAFIT University
Equipo:
Qué bendición

3 Puesto 3

Sede: Medellín
Institución: Univ Nacional de Colombia - Medellín
Equipo:
UNTreeCiclo

REDIS
RED COLOMBIANA DE PROGRAMAS DE INGENIERÍA DE SISTEMAS Y AFINES

icpc.foundation

CCPL
COLOMBIAN COLLEGIATE PROGRAMMING LEAGUE

ACIS
ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

El poder se ejerce en bits: ciberdefensa y soberanía digital en la región

DOI: 10.29236/sistemas.n180a1

El número 180 de la revista Sistemas de la Asociación Colombiana de Ingenieros de Sistemas (ACIS) es la mejor celebración académica de 50 años, aportando a la información y reflexión al gremio, en el país. La lectura de los artículos es una invitación a continuar con el ejercicio profesional, empresarial e investigativo en un entorno de cambio, cada vez más acelerado. Se inicia con dos miradas complementarias que abren el número para pensar que la guerra informática ya no se declara.

Lina María Patricia Manrique Villanueva

En tiempos donde la soberanía digital se encuentra en disputa, la reconfiguración del nuevo mapa del poder tecnológico y los retos de ciberdefensa para América Latina, los hechos nos invitan a la lectura de la revista Sistemas, que va más allá de los detalles operativos tecnológicos para abrir una gran lente a lo macro, en el mundo de los negocios y las guerras de los universos en torno a las arquitecturas de innovación. A continuación, les comparto lo más interesante y provocador que traen los colaboradores y el director de la revista:

Para empezar, un riguroso estado del arte sobre soberanía digital en manos del doctor Jeimy J. Cano M.

presenta desde su genealogía conceptual hasta la disputa actual por la inteligencia artificial, aplicando una revisión estructurada con método Prisma. El hallazgo central desmonta un lugar común: la soberanía digital no es una categoría jurídica cerrada, sino una práctica discursiva que cada potencia moldea según sus intereses, a partir del enfoque de derechos europeo, el control estatal chino, la lógica de mercado estadounidense, entre otros factores; mientras que América Latina y el Caribe llegan tarde y con dependencia estructural a ese debate. El artículo no se queda en el diagnóstico: propone la interdependencia gestionada como alternativa realista frente a la autarquía, y advierte sobre la "deuda de soberanía" que se acumula cuando la inteligencia artificial pasa de herramienta a capa que planifica y coordina procesos críticos.

Los ingenieros de sistemas en Colombia deben leerlo porque son, en la práctica, quienes toman las decisiones que este artículo problematiza: qué proveedor de nube elegir, dónde alojar los datos, qué tan atrapada queda una organización en un ecosistema tecnológico ajeno, y qué tan auditable y portable es la infraestructura que diseñan. El concepto de "deuda de soberanía", entendido como dependencias ocultas que se contraen hoy y cuestan deshacer mañana, es, en esencia, un problema de arquitectura de sistemas antes que de política pública. Entender el marco de las tres soberanías (datos, sistemas y decisión) le da al ingeniero un lenguaje preciso para evaluar riesgos de dependencia tecnológica en cada decisión de diseño, no solo para discutirlos en el ámbito regulatorio.

En cuanto al artículo de Carlos Alberto Sierra Murillo, éste narra, en orden cronológico y con la mirada de quien viene del mundo de la tecnología, cómo Ucrania pasó de tener siete fabricantes de drones en febrero de 2022 a producir hoy varios millones de unidades al año. Pero el artículo no es un inventario de armas: es una historia de gestión de la innovación bajo presión extrema. Muestra cómo Ucrania resolvió cada restricción con velocidad de iteración, mediante los ciclos de aprendizaje rápidos frente a burocracias que pueden tardar años. Es así, como lo plantea el propio autor, entrega continua, aplicada a la guerra. En otras palabras, es la misma lógica de beta permanente que conocemos en el desarrollo de software, trasladada a la trinchera.

Su lectura es indispensable porque la tesis central invierte la intuición dominante: la ventaja decisiva no fue tecnológica sino organizacional, una lección que interpela directamente a quienes trabajamos en TI y gestión de la innovación. Además, el artículo conecta ese aprendizaje con una realidad que ya no es ajena a nosotros: en Colombia se han documentado 418 ataques con drones armados en

menos de dos años, uno cada 48 horas, y el autor advierte que la respuesta no es un problema de compra de equipos, sino de arquitectura de sistemas, para la detección, clasificación, decisión y mitigación integradas en un mando que responda en segundos. Para cualquier profesional de tecnología, seguridad o defensa en la región, este es un caso de estudio sobre cómo la velocidad de iteración, más que el presupuesto, define hoy quién gana y quién pierde.

Por su parte, el artículo del capitán Diego Edison Cabuya Padilla propone que el ciberespacio no anula la geografía, la estratifica: bajo la ilusión de un mundo sin fronteras se mantienen y propagan los cables submarinos, los centros de datos y las cadenas de semiconductores cuyo control produce dependencia y, con ella, poder. Su modelo de tres vectores: infraestructural, normativo y cognitivo, permite leer episodios como el corte de cables en el Báltico o el ataque a la red Viasat no como hechos aislados, sino como manifestaciones de una misma gramática: persistente, ambigua y calibrada para no cruzar el umbral de la guerra formal. Aplicado a Colombia, el análisis expone una paradoja incómoda: nuestra privilegiada posición bioceánica, con nueve puntos de aterrizaje de cable submarino, es a la vez activo estratégico y superficie de exposición. Para Colombia, contar con las fronteras del Pacífico y el Atlántico sigue siendo una potencia para continuar explorando los recursos y la potencialidad en términos de la Alianza del Pacífico, que se encuentra vigente y constituye una ventana de oportunidad en la proyección Asia Pacífico.

En contraste, Fabricio Cabrera Ortiz lleva la tesis a su expresión más operativa. La hegemonía del siglo XXI, según su artículo, ya no se conquista: se administra tecnológicamente, mediante el control simultáneo de seis dominios, a saber: terrestre, marítimo, aéreo, espacial, cibernético y cognitivo, sincronizados por un mismo motor de semiconductores e inteligencia artificial. Su análisis de la Operación Resolución Absoluta en Venezuela, ejecutada en enero de 2026, ilustra con crudeza cómo la tecnología dejó de acompañar la acción militar para convertirse en la operación misma.

Ambos autores convergen en una advertencia para naciones intermedias como Colombia: sin postura estratégica propia, el riesgo no es la derrota, sino convertirse en terreno de disputas ajenas. Dos lecturas rigurosas, necesarias para entender el tablero de poder que se juega hoy antes del primer disparo.

Desde la perspectiva geopolítica, con frecuencia se habla del debilitamiento del Estado como actor fundamental dentro del escenario de las Relaciones Internacionales en el contexto de globalización, se menciona el rol de las empresas

transnacionales y multinacionales, del capital financiero internacional. Desde otro punto de vista, un diálogo Sur – Sur no aparece tanto en la agenda y "como anotó Mosquera (1994) vivimos en un mundo de "globalización axial" y "zonas de silencio", de manera que, por ejemplo, en muchas situaciones, por ejemplo, de África, los lazos culturales y comunicativos tienden a fluir directamente hacia metrópolis europeas, dejando a muchos países africanos separados los unos de los otros, con vínculos muy tenues entre ellos"[1]. Lo mismo podríamos decir de los países latinoamericanos y del potencial entre nuestros países hispano parlantes y Brasil, con políticas que deberían superar las barreras lingüística, tecnológica y cultural, pensando en términos de interoperabilidad.

En el libro titulado "Poder y Contrapoder en la Era Global", Ulrick Beck, plantea con respecto a la globalización que: "primero, en muchos campos la presión que parte de la globalización es menor de lo que generalmente se supone. Por otro lado, la globalización no es solo una llamada al "menos Estado y ya está, sino que, en muchos campos de la política internacional, los actores que operan transnacionalmente reclaman regulaciones estatales más fuertes y cooperación internacional. Luego está el asunto de la diversidad de reacciones de los sistemas políticos nacionales que muestra que la globalización económica no barre sin más las instituciones históricamente consolidadas y finalmente, la presión de la globalización tiene efectos muy diversos en la capacidad de acción y autonomía de los Estados nacionales"[2].

El escenario está reconfigurando las sociedades receptoras de tecnología y transformándolas para responder a los intereses de los "jugadores locales", frente a los "visitantes". Hay otra dimensión de análisis en esta editorial, para la reflexión del artículo titulado: Defensa persistente avanzada: origen y evolución del concepto.

Este valioso documento nos remite al Atlantic Council (2022) en términos de cuatro brechas de recursos: presupuesto, experticia, capacidad tecnológica e influencia para obtener apoyo externo. Allí el autor, Dr. Jeimy Cano, además realiza un aporte metodológico para tener en cuenta: se trata de un trabajo de carácter teórico-analítico con aplicación a un caso. En él, construye un modelo conceptual, denominado DPA-LAC, a partir de la genealogía doctrinal de la persistencia cibernética, y lo somete a contraste mediante el análisis del caso colombiano comparado con Brasil, Chile

1 Slater, David. *Repensar la especialidad de los movimientos sociales: fronteras, cultura y política en la era global*. pp. 415

2 Grande, Edgar y RISSE, Thomas. *Citados por Ulrick Beck en "Poder y contrapoder". Editorial Paidos. Estado y Sociedad.* 2001. pp. 49

y México, seleccionados por representar posiciones distintas respecto del umbral de pobreza cibernética. El texto se organiza iniciando con la evolución del concepto de defensa persistente avanzada (DPA), luego con la propuesta de modelo de DPA, seguido del caso aplicado a Colombia, la discusión de ventajas y limitaciones del modelo, terminado con algunas conclusiones.

Al final, el hilo que atraviesa estas páginas es uno solo: el poder ya no se declara, se ejerce en silencio, en la arquitectura que elegimos, en los cables que tendemos, en los algoritmos que entrenamos y en las decisiones que postergamos. Los cinco artículos de este número 180, desde la genealogía de la soberanía digital hasta la defensa persistente avanzada, pasando por los drones de Ucrania, los cables del Báltico y la Operación Resolución Absoluta, no son artículo técnicos u operativos. Ellos van a la estrategia y la táctica y constituyen un espejo cóncavo para Colombia y para América Latina: la pregunta de fondo no es si participaremos en esta disputa por el ciberespacio, sino si lo haremos como actores con postura propia o como terreno disponible para el poder de otros.

Cincuenta años después de su fundación, la revista Sistemas sigue cumpliendo la misma función que le dio origen: traducir la complejidad técnica en criterio estratégico para quienes construyen, defienden y gobiernan la infraestructura digital de la región. Que esta edición no se lea como un catálogo de amenazas lejanas, sino como una invitación concreta a la acción: a diseñar con soberanía, a defender con anticipación y a decidir, como gremio y como país, antes de que otros decidan por nosotros. El bit, al final, también es territorio. Y el territorio, ya se sabe, no se protege solo, se ejerce soberanía sobre él.

Referencias

Escobar, Arturo et al. *"Política cultural & Cultura Política".* Editorial Taurus, ICANH.

Grande, Edgar y Risse, Thomas. *Citados por Ulrick Beck en "Poder y contrapoder". Editorial Paidos. Estado y Sociedad. 2001.* pp. 49

Slater, David. *Repensar la especialidad de los movimientos sociales: fronteras, cultura y política en la era global*. pp. 415

Lina María Patricia Manrique Villanueva. *Doctora en Estudios Políticos y Relaciones Internacionales de la Universidad Nacional de Colombia. Máster en tecnologías digitales de la UNED de España. Es la Editora en Jefe de la revista Ciberespacio, Tecnología e innovación. Docente de Ciberdiplomacia en la Maestría en Ciberseguridad y Ciberdefensa y del Doctorado en Estudios Estratégicos en Seguridad y Defensa de la Escuela Superior de Guerra General Rafal Reyes Prieto.*
Oricid: https://orcid.org/0000-0003-3646-4328

CONECTA CON NOSOTROS

@Comunidadacis

ACIS

ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

www.acis.org.co

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 posibilidades 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, entendida 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 Equipo 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 procesamiento. 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. Permiten 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 continuidad 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 auditorias 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 ecosistemas 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, carece 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.

Panorama tecnológico actual

Una mirada a este entorno, por parte de la entrevistada Mónica Flórez Cáceres.

DOI: 10.29236/sistemas.n180a3

Desde la vista de relaciones internacionales y los conflictos actuales ¿cómo ha cambiado la dinámica de los conflictos en el contexto del ciberespacio?

Las dinámicas de los conflictos han cambiado profundamente desde la aparición de nuevas tecnologías, basta con observar las reflexiones de Mary Kaldor hacia finales del siglo XX, para observar cómo los conflictos se transformaban por la erosión de los Estados y el surgimiento de actores asimétricos, así como por la aparición de nuevas herramientas y "espacios" que dieron lugar a lo que en su momento la politóloga denominó guerras virtuales y del ciberespacio.

Así, la consolidación del ciberespacio como quinto dominio de la guerra en la doctrina militar estadounidense y de la OTAN[1], primariamente, ha permitido analizar este escenario desde dos perspectivas: como uno de los ejes transversales de apoyo a los otros dominios (tierra, mar, aire y ciberespacio) y como un

[1] Véase: Fuente, I. (2022). La OTAN y el Ciberespacio: Un nuevo dominio para las operaciones. En: https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/LaOTAN_ciberespacio.pdf

dominio en sí mismo que desafía la triada de Clausewitz referente a la letalidad, la instrumentalización y el objeto político que caracterizan a una guerra tradicional.

No obstante, lo que sí es indiscutible es que ha dado sentido a la hibridez como la descripción exacta del desarrollo de los conflictos actuales, que no solo se valen de medios tradicionales para desestabilizar al oponente, sino que potencializan su actuar con métodos que se tornan contundentes con la mediación de la tecnología, la inexistencia de fronteras en el mundo cibernético, el anonimato de la actuación, la rapidez de los efectos y la masificación de sus efectos.

Siempre traigo a colación el ejemplo del ciberataque a las gasolineras iraníes en diciembre de 2023, el 70% de las gasolineras del país quedaron paralizadas. Así pregunto siempre al público ¿qué sucedería si una sola tarde en su ciudad se dejara de suministrar combustible? Creería que las imágenes apocalípticas han embargado siempre las mentes de mis interlocutores. Ahora bien, al reflexionar sobre las probabilidades de caos total, ha de resaltarse que para ello no hubo necesidad de movilizar tropas, lanzar misiles, volar helicópteros, solo bastó un clic…un solo clic.

Esa es la dinámica que ha cambiado, tal vez ahora no ha sido tan evidente la letalidad de un ciberataque, pero lo que si es cierto es que puede desestabilizar a un país entero si se afecta la infraestructura crítica cibernética, por demás desprotegida en países que no han priorizado la temática dentro de su agenda de seguridad y defensa nacionales.

Adicionalmente, desde el estudio de la geopolítica critica[2] hay un aspecto relevante para el análisis de los conflictos internacionales actuales y es la construcción y masificación de discursos. Es decir, cada acción en el marco de un conflicto va acompañado de la construcción de una narrativa que se masifica gracias a la existencia de las redes sociales, siendo un canal directo para la influencia en la opinión pública, aquella que tanto importa en los procesos electorales y en la legitimación del actuar de los gobiernos o de los tomadores de decisiones.

Las palabras importan, aún más cuando hacen parte de estrategias de “soft power”[3] que moldean las voluntades y los intereses de una audiencia inmersa en un mar de sobreinformación, posverdad, y apasionamientos que polarizan, segmentan y generan fracturas que perpetúan y profundizan las diná-

[2] Véase: Cabrera Toledo, Lester. (2020). Geopolítica crítica: alcances, límites y aportes para los estudios internacionales en Sudamérica. *Foro internacional*, *60*(1), 61-95. Epub 15 de abril de 2020.https://doi.org/10.24201/fi.v60i1.2574

[3] Véase: Ahmed, Shahla. (2025). El poder blando en la era digital. Rn: https://saisreview.sais.jhu.edu/the-role-of-soft-power-in-the-digital-age/

micas conflictuales. Así, podría concluirse, sin ánimo de ser generalistas (porque el debate es profundo, largo y complejo) que el ciberespacio como medio, como fin y como escenario, transforma día a día las dinámicas conflictuales, añadiendo herramientas poderosas que pueden equilibrar la balanza entre actores que tienen diversas capacidades militares y económicas, rediseñándose así el panorama de las guerras y conflictos actuales.

Obsérvese el caso de la guerra ruso-ucraniana, ello ha moderado, incluso, las voces analistas que solían predecir el desenlace de las historias: si bien hay un sinnúmero de factores, indiscutiblemente la mediación de tecnología ha dado un margen de ventaja a la que se consideraba un actor que caería rápida y estrepitosamente ante el poder militar y económico ruso. Hasta la dinámica analítica d ellos conflictos ha cambiado, la prospectiva es tal vez hoy una de las tareas más difíciles de completar.

¿Cómo se observan las tensiones internacionales alrededor de la tecnología? ¿como habilitadores de nuevos conflictos o como aceleradores del desarrollo de armas más avanzadas?

Definitivamente como ambas. Tal y como se planteaba en la respuesta anterior, el ciberespacio puede ser analizado como medio, como fin o como herramienta. Así, bajo las circunstancias planteadas, la facilidad de acceso, el anonimato y el gran alcance de los ciberataques, la desinformación y otras tantas acciones llevadas a cabo en el entorno digital, facilita la escalada de los conflictos a estadios más complejos, violentos y difíciles de desescalar.

A su vez, el perfeccionamiento de ataques que pueden, por ejemplo, amenazar el abastecimiento de energía eléctrica de una ciudad y el funcionamiento de las plantas de suplencia, podría generar caos, inestabilidad e incluso muertes numerosas, pensando, por ejemplo, en el caso de hospitales que tengan pacientes dependientes de maquinaria que pueda verse afectada por este tipo de acciones, incluso, terroristas.

Así mismo, en escenarios de amenaza la innovación se activa, ello se puede constatar en asuntos como la invención del radar o el avance de la aviación que se dio en contextos de guerra, por mencionar algunos ejemplos. En este sentido, la posibilidad de ser atacados y, la clásica paradoja de Relaciones Internacionales del "Dilema de Seguridad"[4], conlleva a que los Estados, en primera medida, y los actores en confrontación, hallen formas de blindarse y superar en poder militar al oponente.

[4] Véase: Jordán, Javier. (2020). El dilema de seguridad en las relaciones internacionales. En: https://global-strategy.org/dilema-seguridad/

Por ello, desde la posibilidad de defenderse y atacar con drones, de realizar ciber espionaje, operaciones cognitivas, ataques a la infraestructura crítica cibernética entre otras, se abre la posibilidad al desarrollo de nuevas armas o su fortalecimiento para adquirir o acumular más poder, en especial en un contexto en el que proliferan los conflictos asimétricos y los actores de diferente estatus al estatal, buscan desestabilizar por diversos medios.

¿Cómo se puede entender estas tensiones de la geopolítica digital en el contexto de Colombia? ¿Estamos poniendo atención a las dinámicas internacionales en estos temas?

Se debe revisar desde la óptica de quien hay atención o no. Es decir, desde la academia y, particularmente, desde el estudio de los conflictos en programas de educación superior, hay un apetito creciente por entender cuáles son las dinámicas conflictivas actuales.

En los anaqueles de las bibliotecas de las universidades del país reposan numerosas investigaciones sobre la temática, pero sin que ello refleje un apetito similar a nivel de la agenda política.

Si bien ha sido creciente el interés de los tomadores de decisiones de diversos sectores sobre la geopolítica actual (tanto en el plano tradicional, como en el ciberespacio), no podría afirmarse que existe un lugar prioritario en la agenda. Las relaciones con socios tradicionales y las actividades, también tradicionales, en la interacción con el sector externo, siguen siendo la prioridad.

De hecho, ha sido objeto de análisis constante el nivel de consciencia geopolítica de los tomadores de decisiones en el país y, particularmente, de quienes han dirigido la política exterior colombiana desde inicios de la vida republicana, no solo por una realidad cambiante y compleja que por largos periodos se ha observado desde la óptica de grandes aliados, sino por el reconocimiento de lo que somos como país.

Por otro lado, para el sector privado existe una preocupación creciente por la ciberseguridad, pero no necesariamente por la geopolítica asociada a las dinámicas conflictivas que derivan en los incidentes de seguridad que vulneran los negocios, probablemente menos del 1% de los encargados de ciberseguridad de las empresas privadas en el país podrían afirmar que la conexión de Hezbollah con algunas redes criminales en Iberoamérica pueden constituirse en una amenaza para la continuidad de su negocio, lo que revela la desconexión entre hechos y causas inmediatas, y contextos algo más profundos y complejos.

Del mismo modo, para el público en general, el tema sigue siendo aún muy desconocido. Si bien la mayo-

ría puede conocer que hay un conflicto entre Palestina e Israel, o entre Rusia o Ucrania, no hay un conocimiento profundo sobre el contexto geopolítico tras aquellos casos, y tras la veintena de conflictos de diversa intensidad que actualmente se documentan en instituciones especializadas como la International Crisis Group.

El conflicto interno y la diversidad de retos que se afrontan como país hacen que la observancia de asuntos internacionales se limite a ciertos sectores, incluso en la academia. Es natural ante un escenario que ya brinda de por si suficientes elementos para estudiar y, por supuesto, para procesar y sobrevivir.

Frente al aumento de ciberataques en diferentes regiones del mundo, y la incorporación de la IA como herramienta dual (defensa y ataque) ¿qué reflexiones se plantean frente a un escalamiento del ciberconflicto que se tiene en la zona gris de las tensiones internacionales?
Podría hacerse un análisis similar al realizado en la post Segunda Guerra Mundial y la consolidación de las armas nucleares como referente de poder militar. Si bien ningún ciberataque ha alcanzado el nivel de destrucción de "Little Boy" y "Fat Man", si se plantearon en su momento serios cuestionamientos sobre la racionalidad de los actores en un escenario de confrontación, sabiendo que es eminente el poder de destrucción total.

Así, retomando la reflexión sobre el dilema de seguridad como un asunto clásico en el estudio de Relaciones Internacionales, el surgimiento de nuevas armas, tácticas y escenarios, remiten a la pregunta sobre qué tan lejos puede ir un actor racional, sin conocer a ciencia cierta cuál podría ser la respuesta de su adversario, precisamente sabiendo que la IA y las nuevas tecnologías son duales.

Por ello una escalada significativa no habría de esperarse si se sigue la lógica del actor racional. Ahora bien, en un complejo tablero geoestratégico, puede haber un error de cálculo que termine en un caos sin precedentes, guiados además por la mera intuición, pues una vez más se reitera: el anonimato en la actuación en el ciberespacio hace casi imposible la atribución a un actor particular de un hecho que pueda abrir el camino a una escalada.

Eventualmente denominaron al orden internacional como un orden del terror, por la posibilidad de una guerra nuclear, infortunadamente se siguen sumando elementos que refuerzan este rotulo y que hacen que la tarea de prospectiva sea un imposible, ante la mutación acelerada de la manera en la que se desarrollan los conflictos.

¿Qué recomendaciones se podría ofrecer a la región latinoamericana frente las operaciones cibernéticas encubiertas y abiertas que los estados desarrollados están desple-

gando en zonas de conflicto en la actualidad?

La primera recomendación es que desde la agenda política y la doctrina militar se aprehenda los conceptos asociados al ciberespacio como amenazas a la supervivencia física y digital del Estado. Si bien la preocupación es creciente, la toma de medidas específicas no permite que la brecha digital se cierre, quedando a merced de la disponibilidad de recursos e información de los aliados estratégicos tradicionales.

Si bien la postura latinoamericana nunca ha sido de ataque, si es necesario entender cómo todas las dinámicas conflictivas globales se interconectan e impactan en un mundo altamente interdependiente. Si bien han sido crecientes los debates sobre la globalización, si es cierto que siguen estando abiertos los canales de intercambio de información, bienes, personas, capitales, etc., lo que de por sí es natural, pero que resulta preocupante cuando hace parte de la estrategia de fortalecimiento del terrorismo internacional y el crimen transnacional, solo por mencionar dos aspectos.

Es menester tener consciencia geopolítica sobre las propias condiciones físicas y ciberespaciales, así como de la vulnerabilidad ante las realidades que cada vez se acercan más al ámbito latinoamericano, entendiendo que hacemos parte de lo que hace unos párrafos recordé como el tablero geoestratégico, en el que podemos quedar en medio de un fuego cruzado o, de unos clics cruzados.

De fondo, la educación y, de manera más avanzada, la voluntad política, podrán priorizar la atención al ciberespacio, no solo desde una mirada meramente exploratoria, para poder entender lo que sucede y cómo podría afectarnos, más que para responder críticamente a favor o en contra de actores extrarregionales, sino para blindarnos frente a los actos y actores que, solo por un efecto colateral, podrían vulnerarnos.

Soberanía digital:

Breve estado del arte global y latinoamericano

DOI: 10.29236/sistemas.n180a4

Jeimy J. Cano M.

Resumen

Este artículo ofrece un estado del arte sobre la soberanía digital, desde sus raíces conceptuales hasta la disputa actual por la inteligencia artificial, con foco en América Latina y el Caribe. Se aplicó una revisión documental estructurada según PRISMA 2020 en versión simplificada, con síntesis narrativa de una base verificada de fuentes académicas e institucionales. Los hallazgos muestran que la soberanía digital funciona más como una práctica discursiva que como una categoría jurídica cerrada, que las grandes potencias siguen modelos distintos y que la región llega tarde y con dependencia estructural al debate. La inteligencia artificial agudiza esa brecha. Las conclusiones son provisionales por la velocidad del cambio tecnológico y el rezago regional, y se proponen caminos concretos de cooperación, gobernanza de datos e interdependencia gestionada para la ciberseguridad y ciberdefensa de América Latina y el Caribe.

Palabras clave

Soberanía digital, gobernanza de datos, inteligencia artificial, América Latina y el Caribe, ciberdefensa.

Introducción

La soberanía digital pasó de ser un término de nicho a ocupar el centro de la política tecnológica y de la ciberdefensa. Gobiernos y empresas la invocan para justificar decisiones sobre datos, redes, nube e inteligencia artificial. El problema es que el término significa cosas distintas según quién lo use. Pohle y Thiel (2020) muestran que se ha convertido en un concepto de uso común y a la vez muy disputado, presente tanto en democracias liberales como en regímenes centralizados.

Esa ambigüedad es un tema relevante. Fratini et al. (2024), tras revisar 271 artículos, concluyen que las distintas versiones del concepto comparten un núcleo común, la idea de control sobre datos e infraestructura, pero divergen en quién ejerce ese control y con qué fin. Cuando un mismo término sirve para proteger derechos o para restringirlos, conviene precisar de qué se habla antes de recomendar o diseñar políticas.

Este trabajo tiene como objetivo hacer una revisión conceptual de la soberanía digital y ubicar en él a América Latina y el Caribe. La revisión se organiza en cuatro ejes. Primero, la genealogía del concepto. Segundo, los modelos que adoptan las principales potencias digitales. Tercero, la situación regional. Cuarto, el papel de la inteligencia artificial como nuevo terreno de tensiones. El enfoque es el de la ciberseguridad y la ciberdefensa, es decir, se pregunta no solo qué significa el concepto, sino qué implica para quien debe proteger activos digitales y tomar las decisiones críticas.

Método

La revisión se realizó siguiendo la declaración PRISMA 2020 (Page et al., 2021) en una versión simplificada. Se conserva el esqueleto de reporte de PRISMA, criterios de elegibilidad, fuentes de información, proceso de selección, extracción y síntesis. Se declara de forma transparente que el método PRISMA 2020 fue diseñado para revisiones de intervenciones en salud, por lo que su uso aquí es una adaptación, no un ajuste literal. En este sentido, se aplica una valoración por tipo de fuente, distinguiendo literatura arbitrada, informes de organismos internacionales y literatura gris de consultoras o centros de pensamiento.

Los criterios de elegibilidad fueron: pertinencia temática con la soberanía digital, idioma español o inglés, y ventana temporal de 2020 a 2024 para las fuentes complementarias, con extensión a 2026 solo en el eje de inteligencia artificial, donde la evidencia reciente es clave. Las fuentes complementarias se identificaron mediante búsquedas en la web y se verificaron cada una de ellas. La síntesis es narrativa y temática, organizada según los cuatro ejes.

Un breve resumen del proceso se presenta a continuación:

- Identificación
  - Búsquedas en la web con las siguientes cadenas: “digital sovereignty systematic review 2020..2024 concept”, “soberanía digital América Latina 2020..2024 revista académica”, “AI sovereignty” OR “sovereign AI” governance compute 2023 2024 peer reviewed, “digital sovereignty Caribbean CEPAL data governance Latin America 2022 2023 2024”
  - Registros recuperados en búsquedas web académicas: ~55
  - Artículos base iniciales: 6

- Filtrado
  - Registros web tras quitar duplicados: ~40
  - Excluidos por duplicación (mismo trabajo en varios repositorios): ~15

- Registros pertinentes al tema: ~25
  - Excluidos por no pertinencia: ~15 (detectores de texto de IA, herramientas, notas de prensa, páginas de listado)

- Elegibilidad - Evaluados por texto o resumen: ~18
  - Excluidos por estar fuera de la ventana temporal o no ser verificables: ~7

- Complementarias incluidas: 10
  - Excluidos por redundancia o carácter secundario: ~9 (literatura gris del eje de IA ya cubierta por otras fuentes)

- Incluidas en la síntesis
  - 10 fuentes complementarias verificadas, 6 referencias base (5 temáticas y 1 guía metodológica) + dos referencias relevantes a notas en internet = 18 en total

Nota: La cifra de ~55 registros es aproximada, por sumar resultados de varias búsquedas antes de depurar; los números intermedios son una reconstrucción del ejercicio de filtrado, no un conteo auditado paso a paso. El resultado final: 10 fuentes complementarias incluidas, 6 básicas y dos referencias a notas en internet. 18 en total.

Resultados

Genealogía del concepto

La soberanía es no es una idea reciente. En el siglo XVI, Bodin la asoció a la autoridad última del gobernante; más tarde, Rousseau la desplazó hacia la soberanía popular, y con el tiempo quedó ligada a la democracia, el Estado de derecho y el territorio (Pohle & Thiel, 2020). En su forma moderna, la soberanía combina independencia frente a otros Estados y poder supremo dentro del propio territorio.

Con la llegada de internet, muchos creyeron que el Estado perdería relevancia. La Declaración de Inde-

pendencia del Ciberespacio de Barlow (1996) expresó esa ilusión: un espacio virtual ajeno al control gubernamental. Pohle y Thiel (2020) llaman a esa corriente excepcionalismo del ciberespacio. A ella se sumó, desde el año 2000, la gobernanza multiactor, que proponía administrar internet mediante la colaboración de los directamente afectados y no de los Estados. Ninguna de las dos cumplió su promesa. La comercialización de internet y la aparición de plataformas dominantes facilitaron, más bien, la observación y el control de los flujos digitales.

El giro decisivo llegó con dos hechos. Primero, la constatación de que el poder que desafía al Estado no está en la red como un todo (internet), sino en corporaciones que controlan infraestructuras vitales y actúan como actores casi soberanos. Segundo, las revelaciones de Snowden en 2013 sobre vigilancia masiva, que dispararon la demanda de control nacional sobre datos y comunicaciones (Pohle & Thiel, 2020). Fratini et al. (2024) sitúan justamente en 2014, el año posterior a esas revelaciones, el punto de arranque de la difusión del concepto.

Couture y Toupin (2019) aportan una advertencia relevante al sostener que la soberanía funciona como un "acto de habla": aparece con fuerza allí donde la autoridad es débil o disputada, mientras que está casi ausente en los Estados Unidos, nación que concentra gran parte del poder de internet. Esta lectura, que entiende la soberanía digital como un discurso antes que como una norma, es hoy la más sólida y guía la presente reflexión.

En esa misma línea, Pohle (2024) invita a "repensar" este concepto y advierte que, debido a su uso constante para fines opuestos, el término corre el riesgo de volverse impreciso y de servir para justificar casi cualquier decisión política o medida regulatoria.

En este sentido, a nivel regional, el discurso de la soberanía tecnológica se erige como un pilar estratégico de estabilidad política, en el cual el control local de la infraestructura crítica y los datos sensibles se vuelve indispensable para asegurar la supervivencia y resiliencia estatal frente a la asimetría de las amenazas externas (Rubio Piñeiro, 2024).

Actores y niveles de reclamo

Quien reclama soberanía digital no siempre es un Estado. Pohle y Thiel (2020) distinguen tres capas de reclamos: la autonomía y seguridad de las infraestructuras nacionales, la autonomía de la economía frente a proveedores extranjeros, y la autodeterminación del individuo como usuario y ciudadano. Couture y Toupin (2019) amplían el mapa con cinco perspectivas, que suman a los Estados los pueblos indígenas, los movimientos sociales y la persona, además de la vieja idea de un ciberespacio autogobernado.

Esa pluralidad importa para la región. En América Latina, colectivos sociales construyen soberanía digital desde abajo, con software libre, servidores propios y prácticas de resistencia frente al internet corporativo, en una línea que enlaza con la soberanía alimentaria y con la crítica al colonialismo digital (Guerra-González et al., 2022). El concepto, por tanto, no pertenece solo a los ministerios; también es una bandera de la sociedad civil.

Modelos de las principales potencias digitales

Las grandes potencias no persiguen la misma soberanía. Fratini et al. (2024) proponen cuatro modelos según cómo y por qué se busca el control: uno basado en derechos, uno orientado al mercado, uno de centralización y uno centrado en el Estado. China fue pionera al reivindicar el control soberano del ciberespacio; la Unión Europea llegó después, apoyándose en la regulación y en la defensa de derechos fundamentales.

El caso europeo es el más citado. Gaia-X, lanzado en 2020, busca una infraestructura de datos federada y conforme a estándares europeos, como alternativa a los grandes proveedores de nube extranjeros (Deloitte, 2025; Pohle & Thiel, 2020). Estados Unidos ofrece el contraste: su ventaja está en las empresas que dominan la nube y los modelos de inteligencia artificial, y su marco legal, con la CLOUD Act de 2018, permite el acceso a datos incluso alojados fuera del país bajo ciertas circunstancias (Arthur D. Little, 2026). Rusia desarrolló una internet soberana que puede aislarse en caso de amenaza, y los países BRICS coordinan esfuerzos para reducir su dependencia de plataformas occidentales (Deloitte, 2025).

Para pasar del discurso a la práctica, Arthur D. Little (2026) propone mirar tres soberanías: la de los datos, referida a dónde residen y qué leyes los gobiernan; la de los sistemas, sobre el control de la infraestructura; y la de la decisión, la capacidad de elegir y sostener las propias decisiones tecnológicas cuando cambian las condiciones. La soberanía, en esta lectura, no es algo que activa o desactiva, sino un conjunto de elecciones deliberadas a lo largo de la cadena tecnológica.

América Latina y el Caribe

La región por lo general resulta alejada de estos debates y más en una postura dependiente. Becerra y Waisbord (2024) documentan la llamativa ausencia de América Latina en el debate mundial sobre soberanía digital y describen dos décadas de un enfoque desregulador que dejó a las plataformas globales operar con pocos límites. El dato institucional acompaña esa lectura: en el índice de gobierno digital para la región, el promedio regional queda muy por debajo del promedio de los países de la OCDE, con avances desiguales entre países (OECD & CAF, 2023).

Esta brecha deja de ser una abstracción regulatoria para convertirse en una vulnerabilidad de seguridad nacional. Por ejemplo, la proliferación de tecnologías extrarregionales vinculadas al Estado chino en la videovigilancia urbana de ciudades inteligentes facilita la recopilación de inteligencia extranjera directa. Un caso crítico de esta exposición geopolítica ocurrió en noviembre de 2024, cuando el grupo de espionaje de origen estatal Flax Typhoon logró infiltrar sistemáticamente la infraestructura de información del Gobierno paraguayo (CEEP, 2024).

Aun así, hay movimiento. La agenda digital regional coordinada por la CEPAL fija prioridades comunes de conectividad, capacidades e innovación, aunque el desarrollo entre países sigue siendo dispar (CEPAL, 2022). En el plano histórico, programas satelitales como el Sistema Morelos de México o el Venesat-1 venezolano de 2008 mostraron que el control de infraestructura orbital también hace parte de la autonomía tecnológica (Deloitte, 2025).

El Caribe merece una revisión especial. Sus pequeños Estados insulares son especialmente vulnerables a desastres naturales, fallos de conectividad y ciberataques. Frente a ello, la CEPAL (2025) estudió las embajadas de datos, arreglos de estatus diplomático que otorgan jurisdicción soberana sobre servidores alojados en el extranjero y garantizan la continuidad del Estado ante una crisis, inspirados en el modelo de Estonia. Es un ejemplo concreto de soberanía de datos adaptada a una realidad regional. La evidencia arbitrada específica sobre el Caribe, sin embargo, es escasa, y se apoya sobre todo en informes de organismos internacionales.

La inteligencia artificial como nuevo campo de disputa soberana

La inteligencia artificial traslada la disputa a un terreno más exigente. Srivastava y Bullock (2024) muestran que Estados y empresas usan la IA para ampliar su poder en tres planos, el instrumental, el estructural y el discursivo, y que la soberanía se juega tanto en el control de las infraestructuras como en la competencia por desarrollarlas. Su tesis central es que la IA no reemplaza al Estado, sino que confunde aún más el poder público con el privado.

Arthur D. Little (2026) añade una alerta operativa. A medida que la IA deja de ser una herramienta de productividad y se convierte en una capa que planifica y coordina procesos, requisitos como la portabilidad, la auditabilidad y la capacidad de salida (*poder abandonar a un proveedor o tecnología y migrar a otro sin quedar atrapado, con rutas de salida diseñadas y probadas de antemano, no solo supuestas*) se vuelven más complejos y costosos de incorporar después. La firma

habla de “deuda de soberanía” para nombrar esas dependencias ocultas que luego cuesta deshacer.

Conviene, sin embargo, no confundir soberanía con autarquía (*forma extrema de autosuficiencia tecnológica que lleva al aislamiento digital, con desconexión de la red global y restricción del acceso a tecnologías externas* (Deloitte, 2025).). Tanner et al. (2026) sostienen que una soberanía de la IA de arquitectura completa es estructuralmente inviable para casi cualquier país, porque la cadena de la IA, desde los minerales y la energía hasta el cómputo y los modelos, cruza fronteras. Proponen una interdependencia gestionada: mapear dependencias por capa (*minerales, energía, chips (cómputo), redes, infraestructura, datos, modelos y aplicaciones, talento y la gobernanza*), diversificar proveedores y socios, y asegurar interoperabilidad mediante estándares y contratos. Este informe procede de un centro de pensamiento que declara como donantes a grandes empresas tecnológicas, dato que conviene tener presente al leer sus recomendaciones. Para América Latina y el Caribe, con capacidades de cómputo limitadas, la interdependencia gestionada parece más realista que la aspiración a una autonomía total.

Este realismo operativo se agudiza al evaluar el Digital Sovereignty Index de la región, el cual evidencia que América Latina y el Caribe mantiene una dependencia estructural casi absoluta de hardware sofisticado, computación de alto rendimiento y nubes extranjeras para desarrollar su propia tecnología, lo que restringe el desarrollo autónomo de soluciones de IA soberanas (Yepes, 2026).

Dimensión organizacional

La soberanía digital también se decide dentro de las organizaciones. Follette et al. (2021) identifica cuatro maneras de gestionar el riesgo geopolítico, desde las empresas que lo tratan como fuente de oportunidad e integran su análisis en la estrategia, hasta las que solo reaccionan de forma defensiva y con procesos mínimos. La diferencia entre unas y otras no es el tamaño, sino la madurez de sus procesos y su disposición a anticiparse.

Ese enfoque conecta con la propuesta de Arthur D. Little (2026) de clasificar los activos por niveles según su criticidad y la viabilidad de reducir la dependencia. No todo requiere el mismo grado de control: algunos activos justifican inversiones estratégicas de largo plazo, mientras que otras dependencias pueden tolerarse como una decisión económica deliberada. Para la ciberseguriad y ciberdefensa regional, esta lógica de priorización es más útil que una consigna de soberanía aplicada a todo por igual.

Dicha priorización es imperativa hoy en día, ya que la línea que separaba la ciberseguridad corporativa del ciberconflicto geopolítico militar

se ha venido desvaneciendo. Al delegar flujos de información críticos a proveedores de nube hiperescalares expuestos a tensiones geopolíticas de sus países de origen, las organizaciones de la región pierden soberanía operativa sobre sus datos de monitoreo, inteligencia y capacidad de respuesta activa.

Discusión

Los resultados de esta revisión dejan tres tensiones de fondo. La primera opone *soberanía y aislamiento*. Tener soberanía digital no significa cerrar fronteras tecnológicas, sino definir las condiciones bajo las cuales se abren; cuando se prohíben servicios extranjeros sin alternativas viables, la soberanía se degrada en aislamiento (Deloitte, 2025). La segunda enfrenta *control y competitividad*: un enfoque rígido de soberanía primero puede encarecer, frenar la innovación y restar competitividad (Arthur D. Little, 2026). La tercera opone *seguridad y derechos*, pues las medidas que refuerzan el control estatal pueden, mal diseñadas, restringir la privacidad y la libertad de expresión en lugar de protegerlas (Pohle & Thiel, 2020).

Para la ciberseguridad y ciberdefensa de América Latina y el Caribe, la implicación es directa. La región combina alta dependencia tecnológica, marcos regulatorios desiguales y poca presencia y capacidad de influencia en los foros donde se fijan las reglas. Pohle y Thiel (2020) advierten que la soberanía digital es un medio, no un fin. Quien la ejerce, sea un gobierno o una empresa, debe responder ante la ciudadanía por cómo la usa. Esto importa aún más donde las instituciones son débiles, porque allí el mismo poder que promete defensa puede terminar usándose para controlar o vigilar sin control.

Limitaciones

La base documental es acotada y la revisión sigue PRISMA en versión simplificada, por lo que no es exhaustiva. Varias fuentes provienen de consultoras y centros de pensamiento, con encuadres comerciales que se han señalado caso por caso. La evidencia arbitrada sobre el Caribe es escasa y se complementa con informes institucionales. Existe además un sesgo de idioma y de publicación, al privilegiar textos en español e inglés.

Por último, en el eje de inteligencia artificial buena parte de la evidencia de 2025 y 2026 es literatura de consultoras o centros de pensamiento, de modo que las conclusiones en ese punto son especialmente provisionales.

Conclusiones y recomendaciones

La soberanía digital se entiende mejor como una práctica discursiva y política que como una categoría jurídica cerrada (Couture & Toupin, 2019; Pohle & Thiel, 2020). Las potencias la ejercen con modelos distintos, desde el enfoque de dere-

chos europeo hasta el control estatal chino (Fratini et al., 2024). América Latina y el Caribe llega con retraso a esa conversación y con dependencia estructural (Becerra & Waisbord, 2024; OECD & CAF, 2023), y la inteligencia artificial amplía la brecha (Srivastava & Bullock, 2024; Tanner et al., 2026).

Estas conclusiones son provisionales. La evolución tecnológica es acelerada, sobre todo en inteligencia artificial, y el rezago de la región es evidente. Lo que hoy parece una recomendación sólida puede quedar desfasado en pocos años, por lo que este estado del arte debe leerse como una fotografía de un momento y no como una guía definitiva.

Con esta anotación, se proponen caminos concretos para la región. No son recetas, sino opciones fundadas en la evidencia revisada:

Cooperación regional. Actuar en bloque a través de la agenda digital coordinada por la CEPAL para superar la escala pequeña de los mercados nacionales (CEPAL, 2022).

- **Gobernanza de datos sensata.** Regular residencia y acceso a los datos sin caer en el aislamiento, distinguiendo soberanía de autarquía (Deloitte, 2025).

- **Interdependencia gestionada.** En inteligencia artificial, mapear dependencias, diversificar proveedores y asegurar interoperabilidad, en lugar de perseguir una autonomía total inviable (Tanner et al., 2026).

- **Resiliencia para el Caribe.** Explorar mecanismos como las embajadas de datos para asegurar la continuidad del Estado en los pequeños Estados insulares (CEPAL, 2025).

- **Priorización por criticidad.** Concentrar los esfuerzos de soberanía donde el valor en riesgo es mayor, clasificando los activos por niveles (Arthur D. Little, 2026).

- **Talento e infraestructura local.** Invertir en formación y en infraestructura propia como base de la autonomía, tanto en el sector público como en el privado (Deloitte, 2025).

- **Enfoque de derechos y participación.** Fundar las políticas en los derechos digitales y participar activamente en los foros de gobernanza de la IA para evitar nuevas formas de dependencia (Fratini et al., 2024; Guerra-González et al., 2022).

Referencias

Arthur D. Little. (2026). *The trade-offs of digital sovereignty: A practical framework for implementing the right strategy*. *Arthur D. Little*. https://capital-riesgo.es/es/articles/the-trade-offs-of-digital-sovereignty-a-practical-framework-for-implementing-the-right-strategy/

Barlow, J. (1996). A Declaration of the Independence of Cyberspace. https://www.eff.org/cyberspace-independence

Becerra, M., & Waisbord, S. (2024). Soberanía y nacionalismo en entornos digitales: la llamativa ausencia de América Latina en el debate mundial. *Signo y Pensamiento, 43*. https://revistas.javeriana.edu.co/index.php/signoypensamiento

Follette, C., Gilbert, M., Haris, I., McAdoo, M. & Seshadri, P. (2021). *Turning geopolitical risk into strategic advantage*. BCG. https://www.bcg.com/publications/2021/advantages-of-geopolitical-risk-management-organizations-and-processes

Centro de Estudios Estratégicos del Ejército del Perú - CEEEP (2024). https://dialogo-americas.com/es/articles/soberania-digital-en-latinoamerica-desafios-de-vigilancia-geopolitica-y-riesgo-del-crimen-organizado/

Comisión Económica para América Latina y el Caribe. (2022). *Una senda digital para el desarrollo sostenible de América Latina y el Caribe*. CEPAL. https://repositorio.cepal.org/handle/11362/48461

Comisión Económica para América Latina y el Caribe. (2025). *Data embassies: An innovative approach to strengthening digital resilience in the Caribbean* (LC/TS.2025/99). CEPAL. https://hdl.handle.net/11362/84445

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society, 21*(10), 2305–2322. https://doi.org/10.1177/1461444819865984

Deloitte. (2025). *Soberanía digital como estrategia nacional: un enfoque holístico*. Deloitte. https://www.deloitte.com/latam/es/industries/tmt/perspectives/soberania-digital-como-estrategia-nacional.html

Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. *Digital Society, 3*(3). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4816020

Guerra-González, J. T., Suárez-Estrada, M., & Cerratto-Pargman, T. (2022). Construyendo soberanía digital en América Latina: un análisis de las iniciativas de cuatro colectivos sociales. *Chasqui. Revista Latinoamericana de Comunicación*, (149), 227–242. https://doi.org/10.16921/chasqui.v1i149.4628

Organisation for Economic Co-operation and Development, & CAF. (2023). *Digital government review of Latin America and the Caribbean: Building inclusive and responsive public services*. OECD Publishing. https://doi.org/10.1787/29f32e64-en

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., … Moher, D. (2021). Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas. *Revista Española de Cardiología, 74*(9), 790–799. https://doi.org/10.1016/j.recesp.2021.06.016

Pohle, J. (2024). Unthinking digital sovereignty: A critical reflection on origins, objectives, and practices. *Policy & Internet*. https://doi.org/10.1002/poi3.437

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review, 9*(4). https://doi.org/10.14763/2020.4.1532

Rubio Piñeiro, G. J. (2024). Soberanía Tecnológica - Ciberseguridad. *DERROTERO*, *18*(02), 1–13. https://doi.org/10.70554/Derrotero2024.v18n02.03

Srivastava, S., & Bullock, J. (2024). *AI, global governance, and digital sovereignty* [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2410.17481

Tanner, B., Kerry, C. F., Wyckoff, A. W., Kyosovska, N., Renda, A., & Tabassi, E. (2026). Is AI sovereignty possible? Balancing autonomy and interdependence. *Brookings Institution y CEPS*. https://www.brookings.edu/articles/is-ai-sovereignty-possible-balancing-autonomy-and-interdependence/

Yepes, L. (2026). La inteligencia artificial avanza en América Latina, pero la región enfrenta un nuevo desafío: la soberanía digital. *Infobae*. https://www.infobae.com/america/inhouse/2026/08/03/la-inteligencia-artificial-avanza-en-america-latina-pero-la-region-enfrenta-un-nuevo-desafio-la-soberania-digital/

Jeimy J. Cano M., Ph.D, Ed.D., CFE, CICA. *Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia; Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*

Defensa persistente avanzada

Un modelo multinivel de ciberdefensa para latinoamérica

DOI: 10.29236/sistemas.n180a5

Resumen
El ciberespacio ha evolucionado hacia un entorno de competencia geopolítica permanente, lo que exige transitar de una defensa estática hacia la Defensa Persistente Avanzada (DPA). No obstante, en América Latina, la implementación de este paradigma enfrenta obstáculos estructurales derivados de la fragmentación institucional y la posición de los Estados respecto a la "línea de pobreza cibernética". Este concepto, adaptado del nivel organizacional al nivel Estatal, define un umbral de suficiencia basado en cuatro brechas: presupuesto, talento, tecnología e influencia. Este estudio propone el modelo DPA-LAC, cuya innovación radica en una secuencia de implementación invertida que prioriza el "componente cero" o base mínima de suficiencia nacional. A través de un análisis comparado de Brasil, Chile, México y Colombia, se evidencia una marcada dispersión de capacidades que imposibilita la integración regional uniforme. Se concluye que el éxito estratégico regional reside en la elevación de la base mínima común de capacidades cibernéticas y en la resiliencia como estrategia defensiva viable y costo-efectiva para la región ante sus limitaciones presupuestarias.

Palabras clave: defensa persistente avanzada, línea de pobreza cibernética, ciberdefensa, América Latina, resiliencia estratégica

Introducción

El ciberespacio dejó de comportarse como un dominio de crisis coyunturales para consolidarse como un escenario de competencia continua. Buchanan (2020) documenta que los ataques cibernéticos no se materializaron en el equivalente digital de una guerra nuclear, sino en una forma de baja intensidad y alta frecuencia de la competencia geopolítica, en la que los Estados moldean el entorno estratégico mediante espionaje, sabotaje y desestabilización antes que mediante señalización coercitiva. Este contexto desplaza el eje del debate: si la agresión es permanente, la defensa no puede ser intermitente.

De este escenario surge la Defensa Persistente Avanzada (DPA), concepto formulado por Abdul Rahman (2026) como visión complementaria de la amenaza persistente avanzada. En su formulación original, la DPA articula tres funciones en el plano organizacional: recolección de inteligencia e intercambio de información, monitoreo activo para la cacería de amenazas y respuesta orientada a mitigar el impacto, y las proyecta hacia los planos nacional y regional, exigiendo coherencia interna de los enfoques estatales y coordinación entre defensores civiles y militares. El caso que sustenta la propuesta es el del Sudeste Asiático, con Singapur como referente de madurez y las normas internacionales sobre comportamiento responsable de los Estados como marco común.

La propuesta, sin embargo, descansa sobre precondiciones que no son universales. La DPA supone un proceso de integración digital formalizado, la existencia de un Estado fuerte capaz de exportar capacidades hacia sus vecinos y arquitecturas regionales de ciberseguridad ya operativas. América Latina no reúne ninguna de las tres. El problema no es solo de rezago tecnológico: es de arquitectura institucional y de distribución desigual de capacidades entre Estados que comparten un mismo espacio de exposición.

Este artículo sugiere que la variable explicativa de esa asimetría es la posición estructural de los Estados respecto de la línea de pobreza cibernética. El concepto fue acuñado por Nather y Ellis (2013) para designar el umbral por debajo del cual una organización no puede defenderse eficazmente de los incidentes cibernéticos, y fue sistematizado posteriormente por el Atlantic Council (2022) en términos de cuatro brechas de recursos: presupuesto, experticia, capacidad tecnológica e influencia para obtener apoyo externo. Su formulación es organizacional; su traslado al nivel estatal constituye una extensión

analítica que este estudio asume de manera explícita para plantear una propuesta de defensa persistente.

El argumento se despliega en cuatro movimientos. Primero, la extensión de escala del umbral, que permite pensar la capacidad soberana en términos de suficiencia defensiva. Segundo, el diagnóstico regional por dispersión antes que por déficit uniforme. Tercero, la demostración de que la secuencia descendente del modelo original resulta inviable en contextos de alta variación de capacidades, lo que obliga a invertirla. Cuarto, la reformulación del criterio de éxito, que abandona la paridad de capacidades y adopta la elevación de la base mínima requerida, esto es mejoramiento de las capacidades cibernéticas básicas disponibles.

Metodológicamente, el trabajo es de carácter teórico-analítico con aplicación a un caso. Construye un modelo conceptual, denominado DPA-LAC, a partir de la genealogía doctrinal de la persistencia cibernética, y lo somete a contraste mediante el análisis del caso colombiano comparado con Brasil, Chile y México, seleccionados por representar posiciones distintas respecto del umbral de pobreza cibernética. El texto se organiza iniciando con la evolución del concepto de defensa persistente avanzada (DPA), luego con la propuesta de modelo de DPA, seguidamente el caso aplicado a Colombia, la discusión de ventajas y limitaciones del modelo, terminado con algunas conclusiones.

Defensa persistente avanzada: origen y evolución del concepto

La genealogía de la DPA no comienza en 2026. Su antecedente doctrinal directo es la noción de persistencia cibernética formulada por Nakasone (2019), quien argumentó que el concepto estratégico de una fuerza de respuesta: mantener capacidades en reserva para responder después del hecho, resultaba análogo a la doctrina naval anterior a 1945 y cedía la iniciativa estratégica a adversarios dispuestos a operar de manera continua. La alternativa propuesta fue la persistencia: competir globalmente y a escala, operar por debajo del umbral del uso de la fuerza y defender hacia adelante, sustituyendo relaciones transaccionales con el sector privado por colaboración operativa continua.

Esta doctrina fue objeto de una revisión crítica por parte de Hurel y Mott (2025). Los académicos identifican cinco escuelas en el debate sobre disuasión cibernética: la analogía nuclear, el escepticismo, el compromiso persistente, la resiliencia sobre la disuasión y la disuasión transdominio. Su análisis señala que los supuestos de la disuasión clásica, señalizar umbrales precisos, atribuir con rapidez y demostrar represalia creíble, rara vez se satisfacen en el ciberespacio, donde los adversarios explotan la

ambigüedad de los umbrales y externalizan operaciones a intermediarios. La escuela de la resiliencia se distancia de la centralidad de la disuasión y propone construir sistemas capaces de absorber, adaptarse y recuperarse con disrupción mínima, negando al atacante el efecto buscado.

Ese giro hacia la resiliencia adquiere una orientación organizacional en Nobrega et al. (2024), quienes proponen la noción de ciberdefensa integral. Su argumento central es que la exposición se ha ampliado por la conectividad extendida y que la respuesta exige sincronizar práctica y teoría a través de múltiples actores: profesionales de seguridad, usuarios, reguladores y proveedores, en lugar de confinar la defensa al perímetro técnico de cada organización. La DPA hereda de esta corriente su carácter multiactor y se aparta de la separación entre defensa técnica y gobernanza institucional.

Un cuarto pilar es la atribución. Rid y Buchanan (2015) establecieron que la atribución no es un problema binario de identificación técnica, sino un proceso graduado que combina evidencia forense, análisis operacional y juicio político, y cuyo resultado admite grados de confianza antes que certezas. Hedling y Ördén (2025) extienden el argumento al terreno político: distinguen entre atribución pública, que impone costos sociales y señala capacidad y resolución, y no atribución, entendida como decisión deliberada de no asignar responsabilidad pese a disponer de evidencia. La atribución deja así de ser un acto técnico para constituirse en instrumento de política exterior cuyo uso depende de la resiliencia social percibida.

El cuarto vector proviene de la inteligencia artificial y altera los supuestos del modelo. Maschmeyer (2026) sostiene que existe una brecha de automatización entre ofensiva y defensiva: la ofensiva depende de la creatividad y del engaño, tareas en las que los modelos actuales rinden mal, mientras que la defensiva depende del reconocimiento de patrones, donde sobresalen. La consecuencia es que la defensiva obtiene ganancias superiores de eficiencia y eficacia, y que la brecha se ensancha a medida que aumentan las apuestas. Dotterrer et al. (2026) matizan esta conclusión al identificar un déficit de control: la automatización ofensiva puede ser desplegada por actores individuales con infraestructura mínima, mientras que la automatización defensiva exige integración, validación y coordinación organizacional extensas. Esta asimetría de requisitos institucionales es clave para las reflexiones de este estudio.

Rosen y Kraprayoon (2026) advierten que los agentes autónomos representan una categoría nueva de amenaza para la seguridad nacional, y observan que las institu-

ciones que sostienen infraestructura crítica suelen operar con sistemas obsoletos, recursos insuficientes y experticia interna limitada. El Instituto Nacional de Ciberseguridad (2026) traduce ese diagnóstico a medidas concretas, subrayando que el acortamiento de los tiempos de detección de vulnerabilidades exige acelerar los procesos de actualización y parches, para los cuales muchas organizaciones no están preparadas.

La dimensión cognitiva completa la revisión. Whyte et al. (2020) muestran que las campañas de guerra de información habilitadas por medios cibernéticos operan bajo una lógica de involucramiento antes que de disrupción indiscriminada, y que su conceptualización sigue siendo insuficiente en la literatura sobre disuasión. Jaidka et al. (2025) documentan cómo la inteligencia artificial generativa reduce las barreras para producir y difundir desinformación, dificulta la atribución de fuentes y erosiona la confianza incluso hacia medios reconocidos, lo que sitúa la resiliencia informacional como componente de la defensa y no como asunto separado.

La convergencia de estas siete corrientes permite formular la DPA no como una innovación aislada, sino como la materialización representativa de un desplazamiento acumulado. El movimiento va de la respuesta a la persistencia (Nakasone, 2019), de la disuasión a la resiliencia (Hurel y Mott, 2025), del perímetro técnico a la coordinación multiactor (de Nobrega et al., 2024), de la atribución técnica a la atribución política (Hedling y Ördén, 2025; Rid y Buchanan, 2015) y de la presunta ventaja ofensiva a la ventaja defensiva estructural condicionada (Dotterrer et al., 2026; Maschmeyer, 2026). La Tabla 1 sintetiza esta genealogía. Lo que la DPA aporta es la integración de estos desplazamientos en un mismo marco y su proyección a los planos nacional y regional. Lo que no aporta es una teoría de las condiciones materiales que hacen posible esa integración, y es precisamente ese vacío el que la línea de pobreza cibernética permite ocupar.

Finalmente, la dimensión material. Kajander et al. (2025) evidencian que los requisitos de ciberseguridad para sistemas de armas permanecen fragmentados y en gran medida clasificados, y que no existe una disposición explícita de derecho internacional que los imponga. Gopal Chari (2025) sitúa este vacío en el marco del desacoplamiento de cadenas de suministro y de la búsqueda de soberanía tecnológica, señalando que las economías emergentes de África y América Latina enfrentan obstáculos considerables para acceder a estas tecnologías mientras permanecen dependientes de proveedores extranjeros. Es en ese punto donde la línea de pobreza cibernética adquiere pertinencia analítica: la

dependencia tecnológica no es solo una condición económica, sino un determinante de la capacidad defensiva soberana.

Modelo DPA-LAC y sus componentes

El modelo DPA-LAC se construye sobre una premisa que lo distingue de su matriz asiática: la línea de pobreza cibernética no es un dato contextual, sino la variable que ordena la secuencia de implementación. En consecuencia, el modelo incorpora un componente cero que opera como precondición de los demás.

El primer movimiento del argumento es la extensión de escala. La línea de pobreza cibernética, formulada por Nather y Ellis (2013) para organizaciones y sistematizada por el Atlantic Council (2022) en cuatro brechas de recursos, se traslada aquí al nivel estatal. Existe un umbral de capacidad: presupuestal, de talento, tecnológica y de influencia, por debajo del cual un Estado no puede sostener defensa persistente, sino únicamente respuesta reactiva y coyuntural. La analogía es justificable porque las cuatro brechas originales tienen equivalentes soberanos directos: el presupuesto de defensa cibernética, la disponibilidad de talento especializado formado localmente, la capacidad tecnológica no dependiente de proveedores externos y la

Tabla 1
Genealogía doctrinal de la Defensa Persistente Avanzada

Corriente	Fuente	Aporte conceptual a la DPA
Persistencia cibernética	Nakasone (2019)	Sustitución de la respuesta por la iniciativa continua; defensa hacia adelante y colaboración operativa permanente.
Debate sobre disuasión	Hurel y Mott (2025)	Delimitación de cinco escuelas y reconocimiento de la resiliencia como denegación de efecto.
Ciberdefensa integral	de Nobrega et al. (2024)	Fundamento multiactor y sincronización entre práctica organizacional y teoría.
Atribución graduada	Rid y Buchanan (2015)	Atribución como proceso con grados de confianza, no como identificación binaria.
Política de la atribución	Hedling y Ördén (2025)	Distinción entre atribución pública y no atribución como decisiones estratégicas.
Brecha de automatización	Maschmeyer (2026)	Ventaja estructural de la defensa derivada de la asimetría entre engaño y detección.
Déficit de control	Dotterrer et al. (2026)	Condicionamiento de esa ventaja a la integración organizacional del defensor.
Dimensión cognitiva	Whyte et al. (2020); Jaidka et al. (2025)	Incorporación de la integridad informacional al perímetro de la ciberdefensa.

Nota. Elaboración propia a partir de las fuentes citadas.
El orden es cronológico-conceptual y no jerárquico.

influencia para obtener asistencia internacional en condiciones favorables.

El segundo movimiento es el diagnóstico regional por dispersión. América Latina no se sitúa uniformemente bajo el umbral: presenta niveles de variación de capacidades. Este hecho desplaza el problema. Si todos los Estados estuvieran igualmente por debajo, la solución sería la transferencia externa de capacidad. Si todos estuvieran por encima, la cooperación sería un asunto de coordinación. La dispersión genera un problema distinto: los Estados con mayor capacidad carecen de incentivos para vincular sus arquitecturas a las de sus vecinos, porque la integración importa riesgo sin aportar capacidad, mientras que los Estados con menor capacidad carecen de los prerrequisitos institucionales para absorber la asistencia que se les ofrece.

El tercer movimiento se deriva de lo anterior. La lógica del eslabón más débil que Abdul Rahman (2026) aplica al Sudeste Asiático resulta excesiva bajo alta dispersión: un diseño regional que presuponga capacidades nacionales homogéneas carece de base material. De ahí la inversión de secuencia. En el modelo original, el marco regional orienta y disciplina los enfoques nacionales. En el DPA-LAC, la persistencia se construye desde el nivel nacional hacia el subregional y solo después hacia el regional, y la cooperación regional deja de ser el punto de partida para convertirse en el mecanismo de elevación del umbral.

El cuarto movimiento reformula el criterio de éxito. La métrica no puede ser la paridad de capacidades con potencias cibernéticas, que resulta inalcanzable y estratégicamente irrelevante para Estados de capacidad media. La métrica pertinente es doble: elevación de la base común y reducción de la variación de capacidades intrarregional. Esta reformulación tiene una consecuencia doctrinal precisa. La resiliencia deja de ser una alternativa entre otras dentro del debate sobre disuasión, tal como la presentan Hurel y Mott (2025), y pasa a ser un mecanismo relevante y costo-efectivo bajo restricción presupuestal.

Sobre esta base, el modelo se compone de seis elementos y dos ejes transversales. El componente cero, umbral de suficiencia defensiva, define la línea base nacional: marco normativo vigente, equipo de respuesta operativo, inventario de infraestructura crítica y canal de comunicación civil-militar establecido, sin el cual los demás componentes carecen de sustento. El componente uno, inteligencia anticipatoria compartida, se concibe como mecanismo de transferencia de capacidad y no solo de intercambio de indicadores, siguiendo la lógica multiactor de Nobrega et al. (2024). El componente dos, cacería persistente de amenazas, es escalable

según la posición del Estado respecto del umbral, y admite implementaciones mínimas basadas en monitoreo centralizado antes que en capacidades distribuidas.

El componente tres, atribución graduada y decisión política, incorpora la distinción de Rid y Buchanan (2015) entre grados de confianza y la de Hedling y Ördén (2025) entre atribución pública y no atribución. En contextos de capacidad media, la atribución forense completa tiene un costo exagerado para un Estado individual, lo que la convierte en candidata natural a bien público regional. El componente cuatro, resiliencia como sustituto funcional de la disuasión, traduce el argumento del tercer movimiento en capacidades concretas de continuidad operativa, respaldos inmutables y recuperación verificada, en línea con las medidas propuestas por el Instituto Nacional de Ciberseguridad (2026). El componente cinco, gobernanza normativa y confianza, adopta las normas internacionales y los marcos hemisféricos como sustituto funcional de una integración formal que en América Latina no existe.

Los dos ejes transversales atraviesan todos los componentes. El eje de inteligencia artificial y automatización es ambivalente: la brecha identificada por Maschmeyer (2026) favorece estructuralmente a la defensa, pero el déficit de control descrito por Dotterrer et al. (2026) implica que capitalizar esa ventaja exige integración organizacional importante, precisamente el recurso más escaso bajo el umbral. La automatización puede, por tanto, reducir o ampliar la distancia al umbral según la capacidad institucional previa. El eje cognitivo reconoce que la desinformación constituye el vector de menor costo contra Estados situados bajo el umbral, dado que explota la confianza institucional antes que la infraestructura técnica (Jaidka et al., 2025; Whyte et al., 2020; Erendor, 2024).

La Tabla 2 sintetiza la arquitectura resultante. Conviene subrayar que el orden de los componentes no es jerárquico sino secuencial: expresa una precedencia de implementación y no una escala de importancia. Un Estado situado claramente por debajo del umbral que invirtiera en cacería persistente de amenazas sin haber consolidado el componente cero obtendría capacidad técnica sin una base institucional para sostenerla, patrón que la literatura sobre cooperación en seguridad documenta con frecuencia bajo la forma de capacidades donadas que se degradan una vez concluida la asistencia externa. Inversamente, un Estado que consolidara el componente cero sin avanzar hacia los siguientes permanecería en la respuesta reactiva y coyuntural que el modelo busca superar. La utilidad del DPA-LAC reside, por tanto, en ordenar decisiones de inversión bajo restricción presupuestal antes que en prescribir una dotación completa de capacidades.

Tabla 2
Componentes del modelo DPA-LAC y su función respecto del umbral de suficiencia defensiva

Código	Componente	Función respecto del umbral
C0	Umbral de suficiencia defensiva	Define la línea base nacional; precondición de operabilidad de los componentes restantes.
C1	Inteligencia anticipatoria compartida	Opera como mecanismo de transferencia de capacidad y no solo de intercambio de indicadores.
C2	Cacería persistente de amenazas	Escalable según la posición del Estado respecto del umbral; admite implementaciones mínimas.
C3	Atribución graduada y decisión política	Bien público regional ante el costo individual exagerado de la capacidad forense completa.
C4	Resiliencia como sustituto funcional de disuasión	Estrategia dominante bajo restricción presupuestal; denegación de efecto al atacante.
C5	Gobernanza normativa y confianza	Normas internacionales como sustituto funcional de una integración formal inexistente.
Eje A	Inteligencia artificial y automatización	Reduce o amplía la distancia al umbral según la capacidad institucional previa.
Eje B	Dimensión cognitiva	Vector de menor costo contra Estados situados por debajo del umbral.

Nota. Elaboración propia. La numeración expresa precedencia de implementación y no jerarquía de importancia.

Modelo DPA-LAC: Caso aplicado a Colombia

La aplicación del modelo a Colombia exige situarla primero en el contexto regional. El Índice Mundial de Ciberseguridad de la Unión Internacional de Telecomunicaciones (2024) ofrece una medida comparable de compromiso estatal en cinco pilares: jurídico, técnico, organizacional, desarrollo de capacidades y cooperación, y clasifica a los países en cinco niveles. En América Latina, Brasil es el único Estado clasificado como modelo de referencia; México y Ecuador se ubican en el nivel de avance; Chile, Colombia, Costa Rica, Panamá y Perú, entre otros, en el nivel de establecimiento; y una porción sustancial de la región permanece en niveles de evolución o construcción. Esta distribución confirma empíricamente el segundo movimiento del argumento: el problema regional no es un déficit uniforme, sino una dispersión que abarca cuatro de los cinco niveles disponibles.

Brasil opera por encima del umbral en la mayoría de las dimensiones. Su escala demográfica y económica sostiene un presupuesto de defensa cibernética sin equivalente regional, cuenta con industria nacional de defensa y con un comando militar cibernético consolidado, y su clasificación como modelo de referencia refleja madurez homogénea en los cinco pilares. Su limitación no es de capacidad sino de vocación: la asimetría con sus veci-

nos reduce los incentivos para vincular su arquitectura a esquemas regionales que aportarían poco a su postura y añadirían exposición (OEA-BID, 2020).

Chile representa el caso de mayor densidad normativa. La Ley 21.663 estableció un marco general de ciberseguridad y creó la Agencia Nacional de Ciberseguridad, con obligaciones específicas para operadores de importancia vital, incluidos sistemas de gestión de seguridad de la información, designación de oficiales de ciberseguridad y plazos escalonados de reporte de incidentes (Congreso Nacional de Chile, 2024). Este diseño resuelve institucionalmente el componente cero del modelo y establece una línea base verificable. Su clasificación en el nivel de establecimiento sugiere, no obstante, que la maduración normativa aún no se ha traducido plenamente en capacidad técnica y operativa.

México ilustra la brecha entre exposición y arquitectura. Su clasificación en el nivel de avance convive con una fragmentación institucional persistente y con la ausencia de una ley marco equivalente a la chilena, en un contexto de integración productiva profunda con Norteamérica que amplifica las consecuencias de cualquier compromiso en su infraestructura crítica. Es el caso que mejor ilustra por qué la posición respecto del umbral no se deduce del tamaño económico (OEA-BID, 2020).

Colombia se ubica en el nivel de establecimiento y presenta un perfil característico de Estado en torno al umbral. Dispone de los elementos formales del componente cero: una política nacional de seguridad digital que define roles y responsabilidades de gobernanza, un equipo de respuesta a emergencias cibernéticas con función de punto de contacto nacional, un centro cibernético policial y capacidades de ciberdefensa militar bajo un comando conjunto cibernético (CONPES, 2020), además de regulación sectorial específica en el ámbito financiero que exige pruebas periódicas de ciberresiliencia. La política nacional de inteligencia artificial adoptada en 2025 incorporó lineamientos de ciberseguridad y privacidad como condición habilitante, lo que conecta el eje transversal de automatización con la agenda de política pública (CONPES, 2025).

El diagnóstico por componentes revela, sin embargo, brechas consistentes. En el componente uno, el intercambio de inteligencia opera predominantemente entre entidades estatales y con un flujo limitado hacia el sector privado y las entidades territoriales, lo que reproduce internamente la lógica de dispersión que caracteriza a la región: la capacidad se concentra en el nivel central mientras los municipios y las pequeñas y medianas empresas permanecen claramente bajo el umbral. En el componente dos, la cacería persistente de amenazas depende de capacidades concen-

tralizadas y no de una función distribuida, lo que limita su alcance a los activos de mayor visibilidad.

En el componente tres, la atribución constituye la brecha más marcada. El costo de una capacidad forense y analítica completa excede lo que un Estado de capacidad media puede sostener de manera autónoma, y la dimensión política de la atribución que describen Hedling y Ördén (2025) añade una restricción adicional en un entorno regional donde la asignación pública de responsabilidad tiene consecuencias diplomáticas inmediatas.

En el componente cuatro, la resiliencia muestra avances sectoriales, notablemente en el ámbito financiero, donde la exigencia regulatoria de pruebas periódicas ha generado capacidad verificable, pero desigualdad marcada entre sectores.

El componente cinco encuentra su principal limitación en la ausencia de un equivalente latinoamericano al andamiaje regional asiático. No existe un equipo regional de respuesta ni un centro de excelencia de ciberdefensa comparable, y los mecanismos hemisféricos operan con mandatos amplios y recursos limitados. La condición de Colombia como socio global de la Organización del Tratado del Atlántico Norte introduce un elemento distintivo: le proporciona acceso a marcos de interoperabilidad y a estándares de ciberseguridad para sistemas de armas cuya ausencia documentan Kajander et al. (2025), pero también la sitúa en una posición particular dentro de un entorno regional donde tal vinculación no es la norma.

Los dos ejes transversales operan con signo opuesto. En el eje de automatización, la ventaja estructural de la defensa que identifica Maschmeyer (2026) es teóricamente accesible, pero su realización depende de la integración organizacional que Dotterrer et al. (2026) señalan como requisito, y esa integración es precisamente lo que la fragmentación institucional colombiana dificulta. En el eje cognitivo, la exposición es alta: el entorno regional presenta condiciones propicias para operaciones de información, y la reducción de barreras para producir desinformación mediante inteligencia artificial generativa (Jaidka et al., 2025) amplifica un vector que no requiere superioridad técnica del atacante.

La Tabla 3 sintetiza el análisis comparado. El patrón que emerge es consistente con el segundo movimiento del argumento: los cuatro Estados examinados ocupan tres niveles distintos de clasificación y presentan configuraciones institucionales no equivalentes, de modo que ninguna arquitectura regional podría aplicarles obligaciones uniformes sin excluir de facto a los que se sitúan más abajo. Colombia, en particular, ilustra la condición de Estado en torno al umbral: dispone

de instituciones formales suficientes para operar los componentes básicos del modelo, pero no de la integración organizacional necesaria para capitalizar la ventaja defensiva que la automatización ofrece.

Ventajas y limitaciones para la aplicación del modelo

La primera ventaja del modelo es su realidad secuencial. Al establecer un componente cero como precondición explícita, el DPA-LAC evita el error recurrente de las agendas de cooperación regional que presuponen capacidades nacionales inexistentes. La secuencia invertida: nacional, subregional, regional, permite que cada Estado identifique su posición respecto del umbral antes de comprometerse con obligaciones que no puede sostener, lo que reduce el riesgo de acuerdos formales sin implementación efectiva, un patrón frecuente en la cooperación latinoamericana en materia de seguridad.

La segunda ventaja es la reformulación del criterio de éxito. Al sustituir la paridad de capacidades por la elevación de la línea base común y la reducción de la variación de capacidades, el modelo ofrece métricas alcanzables y verificables.

Un Estado puede demostrar progreso mediante el ascenso de nivel en índices comparables o mediante la incorporación de entidades territoriales al perímetro de protección nacional, sin necesidad de compararse con actores cuya escala presupuestal es inalcanzable. Esta

Tabla 3

Análisis comparado de capacidades de ciberdefensa: Colombia, Brasil, Chile y México

Estado	Nivel UIT (2024)	Rasgo institucional distintivo	Brecha principal respecto del DPA-LAC
Brasil	Modelo de referencia	Escala presupuestal, industria nacional de defensa y comando militar cibernético consolidado.	Ausencia de incentivo para vincular su arquitectura a esquemas regionales (C5).
México	Avance	Integración productiva profunda con Norteamérica; alta exposición de infraestructura crítica.	Fragmentación institucional sin ley marco equivalente (C0).
Chile	Establecimiento	Ley 21.663 y Agencia Nacional de Ciberseguridad con rectoría concentrada.	Traducción incompleta de la madurez normativa en capacidad operativa (C2).
Colombia	Establecimiento	Política nacional de seguridad digital, colCERT, centro cibernético policial, comando conjunto cibernético y regulación sectorial financiera.	Atribución autónoma y cacería distribuida de amenazas (C2, C3).

Nota. Clasificación tomada de la Unión Internacional de Telecomunicaciones (2024); análisis institucional de elaboración propia.

reformulación tiene además un efecto político: convierte la ciberdefensa en una agenda de desarrollo institucional antes que en una carrera armamentista digital.

La tercera ventaja es la coherencia con la evidencia sobre automatización. Si la brecha identificada por Maschmeyer (2026) es correcta, los Estados que inviertan en automatización defensiva obtendrán ventajas crecientes sobre los que prioricen la automatización ofensiva. Para Estados de capacidad media, esta conclusión es estratégicamente favorable: sugiere que la inversión defensiva ofrece mayor retorno marginal que el desarrollo de capacidades ofensivas, cuyo costo y cuyos riesgos de escalamiento son considerablemente mayores.

La cuarta ventaja es la utilización de las normas internacionales como sustituto funcional de la integración formal. Dado que América Latina carece de un acuerdo de integración digital comparable al asiático, las normas internacionales sobre comportamiento responsable de los Estados ofrecen un lenguaje común que no requiere cesión de soberanía ni creación de instituciones nuevas, y que puede adoptarse de manera incremental y asimétrica según la capacidad de cada Estado.

Así mismo se presentan algunas limitaciones del modelo que se precisan a continuación. La primera y más importante es de orden epistemológico: la extensión de la línea de pobreza cibernética del nivel organizacional al estatal es una analogía, no una equivalencia demostrada. Las organizaciones enfrentan un umbral definido por la disponibilidad de recursos en un mercado; los Estados enfrentan restricciones adicionales de soberanía, legitimidad democrática y economía política que no tienen equivalente organizacional, que ilustran los retos de las naciones en este contexto.

La segunda limitación es la operacionalización del umbral. El modelo postula un componente cero, pero no se detalla valores concretos que permitan determinar con precisión si un Estado se sitúa por encima o por debajo. Los índices comparados disponibles miden compromiso declarado y marcos institucionales antes que capacidad operativa efectiva, y su metodología descansa en autoreporte verificado. Una operacionalización concreta exigiría indicadores de desempeño: tiempos de detección y contención, cobertura efectiva de infraestructura crítica, densidad de talento especializado, que actualmente no se recopilan de manera comparable en la región.

La tercera limitación es el problema del incentivo asimétrico. El modelo propone que los Estados de mayor capacidad actúen como mecanismos de transferencia, pero no resuelve por qué habrían de hacer-

lo. En el caso asiático, la vinculación de la ciberseguridad a un acuerdo de integración económica genera un interés material directo. En América Latina, la ausencia de ese vínculo deja la cooperación dependiente de la voluntad política, históricamente volátil y sujeta a los ciclos electorales de cada Estado.

La cuarta limitación concierne a la atribución como bien público regional. La propuesta es analíticamente atractiva pero políticamente difícil: compartir capacidad de atribución implica compartir inteligencia, y ello exige un nivel de confianza intergubernamental que la región no ha construido. La distinción de Hedling y Ördén (2025) entre atribución y no atribución profundiza el reto, pues un mecanismo compartido obligaría a coordinar decisiones políticas sobre asignación pública de responsabilidad que cada Estado prefiere reservarse.

La quinta limitación es temporal. El modelo propone una secuencia ascendente que requiere años, mientras que la evolución de las capacidades ofensivas automatizadas transcurre en meses. Rosen y Kraprayoon (2026) advierten que el margen disponible se mide en años y no en décadas. Existe, por tanto, un riesgo real de que la construcción secuencial del umbral sea superada por la velocidad de la amenaza, escenario en el cual el modelo describiría correctamente el problema comprometiendo la oportunidad de la solución.

La sexta limitación es de alcance empírico. El caso aplicado se sustenta en fuentes documentales, normativas e índices comparados, sin trabajo de campo ni acceso a información operativa clasificada, que es precisamente donde reside buena parte de la capacidad real. Kajander et al. (2025) advierten que la naturaleza clasificada de los requisitos de ciberseguridad para sistemas de armas hace difícil establecer qué han implementado efectivamente los Estados. Esta opacidad afecta a cualquier evaluación externa y aconseja tratar los resultados como aproximaciones antes que como mediciones.

En conjunto, las ventajas del modelo se concentran en su capacidad de ordenar decisiones bajo restricción, y sus limitaciones en la ausencia de una teoría del incentivo que explique por qué los Estados de mayor capacidad deben participar. Esta asimetría entre lo que el modelo resuelve y lo que deja abierto no invalida la propuesta, pero delimita su alcance: el DPA-LAC es un instrumento de diseño de política pública nacional con proyección regional, y no un mecanismo de cooperación autoejecutable. Su valor práctico depende de que los Estados que lo adopten reconozcan su propia posición respecto del umbral antes de comprometerse con obligaciones externas, y de que las agencias de cooperación ajusten sus instrumentos de asistencia a esa secuencia en lugar de replicar modelos diseñados para

contextos con precondiciones distintas.

En la tabla 4 se resumen las ventajas, limitaciones y tensiones resultantes propias del modelo DPA-LAC.

Conclusiones

La Defensa Persistente Avanzada constituye una respuesta conceptualmente válida a la realidad de que la agresión en el ciberespacio es continua. Su traslado a América Latina, sin embargo, no puede ser

Tabla 4.
Ventajas y limitaciones del modelo DPA-LAC

Dimensión	Ventaja	Limitación	Tensión resultante
Diseño secuencial (C0)	Realismo: el umbral de suficiencia como precondición explícita evita agendas que presuponen capacidades inexistentes.	Sin valores de corte cuantitativos; los índices miden compromiso declarado, no capacidad operativa.	El modelo ordena la secuencia pero no permite determinar con precisión en qué punto se encuentra un Estado.
Criterio de éxito	Métricas alcanzables: elevación de la línea base común y reducción de la variación de capacidades en lugar de paridad.	Alcance empírico restringido: sin trabajo de campo ni acceso a información clasificada.	Las métricas son verificables en principio, pero la evidencia disponible es indirecta.
Cooperación regional (C5)	Las normas internacionales operan como sustituto de una integración formal inexistente, sin cesión de soberanía	Incentivo asimétrico: no explica por qué los Estados de mayor capacidad pueden ayudar a otros.	Ofrece el lenguaje de la cooperación sin resolver el reto de fondo.
Atribución (C3)	Concebirla como bien público regional resuelve el costo individual de un Estado.	Exige compartir inteligencia y coordinar decisiones políticas que cada Estado reserva.	Solución económicamente racional, políticamente inviable en baja confianza.
Automatización (Eje A)	Ventaja estructural de la defensa; mayor retorno marginal que la inversión ofensiva.	Capitalizarla exige integración organizacional, el recurso más escaso bajo el umbral.	La ventaja teórica se invierte en la práctica para quienes más la necesitan.
Horizonte temporal	Secuencia ascendente adaptada a	Requiere años; las capacidades ofensivas automatizadas evolucionan en meses.	Riesgo de que el diagnóstico sea correcto y la solución llegue tarde.
Dimensión	**Ventaja**	**Limitación**	**Tensión resultante**
	restricción presupuestal real.		

Nota. Elaboración propia.

una operación de importación doctrinal. Las precondiciones que sostienen su formulación original: integración digital formalizada, un Estado fuerte con capacidades cibernéticas y arquitecturas de ciberseguridad operativas, son limitadas en la región, y esa ausencia no es contingente sino estructural.

Esta reflexión ha argumentado que la variable que explica la asimetría es la posición de los Estados respecto de la línea de pobreza cibernética. La extensión de este concepto del nivel organizacional al estatal, asumida explícitamente como aporte analítico, permite reconceptualizar el problema: la capacidad de sostener defensa persistente depende de un umbral de suficiencia por debajo del cual solo es posible la respuesta reactiva y coyuntural.

El diagnóstico regional resultante desplaza el foco tradicional de los análisis. El obstáculo principal para una arquitectura latinoamericana de ciberdefensa no es la carencia absoluta de capacidades, sino su dispersión. La clasificación comparada muestra a la región distribuida en cuatro de los cinco niveles disponibles, con Brasil como modelo de referencia y una porción sustancial de Estados en niveles iniciales.

Esta variación en las capacidades genera un problema de incentivos que ninguna transferencia de recursos resuelve por sí sola.

De ello se sigue la inversión de secuencia que constituye la contribución central del modelo DPALAC. Mientras el diseño original procede del marco regional hacia los enfoques nacionales, el modelo propuesto invierte el orden y convierte la cooperación regional en mecanismo de elevación del umbral antes que en punto de partida. El componente cero: umbral de suficiencia defensiva, opera como precondición explícita de los cinco componentes restantes y de los dos ejes transversales.

El caso colombiano confirma el diagnóstico. Colombia dispone de los elementos formales del componente cero pero presenta brechas consistentes en inteligencia compartida, cacería distribuida de amenazas y atribución, junto con avances sectoriales significativos en resiliencia. Su posición en torno al umbral la sitúa en una condición ambivalente: suficientemente desarrollada para operar los componentes básicos, insuficientemente integrada para capitalizar la ventaja defensiva que ofrece la automatización.

Tres implicaciones se desprenden del análisis. Primera, para Estados de capacidad media la resiliencia no es una opción doctrinal, sino un mecanismo costo-efecto y sostenible en el tiempo. Segunda, la ventaja estructural que la inteligencia artificial otorga a la defensa no es automática: depende de una inte-

gración organizacional que constituye precisamente el recurso más escaso bajo el umbral. Tercera, la métrica de éxito debe reformularse en términos de elevación de la línea base común y reducción de la variación de capacidades.

Las limitaciones identificadas delimitan el alcance de estas conclusiones. La analogía entre umbral organizacional y umbral estatal permanece requieren demostración empírica; el componente cero demanda valores de corte mínimos esperados; el problema del incentivo asimétrico no encuentra solución dentro del modelo; y la velocidad de evolución de las capacidades ofensivas automatizadas puede superar la secuencia ascendente propuesta.

La agenda de investigación que se abre es tiene dos elementos. En el plano conceptual, corresponde someter a prueba la validez de la extensión del modelo mediante estudios comparados que incorporen indicadores de desempeño operativo y no solo de compromiso declarado. En el plano aplicado, corresponde examinar si mecanismos de atribución compartida son viables en contextos de baja confianza intergubernamental, cuestión de la que depende buena parte de la factibilidad del modelo propuesto.

Referencias

Abdul Rahman, M. F. B. (2026). Securing ASEAN cyberspace: A case for Advanced Persistent Defence (IDSS Paper No. IP26074). S. Rajaratnam School of International Studies, *Nanyang Technological University*. https://rsis.edu.sg/rsis-publication/idss/ip26074/

Atlantic Council. (2022). Buying down risk: Cyber poverty line. Cyber Statecraft Initiative. https://www.atlanticcouncil.org/content-series/buying-down-risk/cyber-poverty-line/

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.

Congreso Nacional de Chile. (2024). Ley 21.663, Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información. Biblioteca del Congreso Nacional de Chile.

Consejo Nacional de Política Económica y Social - CONPES. (2020). Documento CONPES 3995: Política Nacional de Confianza y Seguridad Digital. *Departamento Nacional de Planeación*. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf

Consejo Nacional de Política Económica y Social - CONPES. (2025). Documento CONPES 4144: Política Nacional de Inteligencia Artificial. *Departamento Nacional de Planeación*. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/4144.pdf

de Nobrega, K. M., Rutkowski, A.-F., & Saunders, C. (2024). The whole of cyber defense: Syncing practice and theory. *The Journal of Strategic Information Systems*, *33*(4), Article 101861. https://doi.org/10.1016/j.jsis.2024.101861

Dotterrer, K., Hauptman, A. I., Richoux, B. P., & Corbett, M. L. (2026). Grand cha-

llenges in agentic AI for cyber operations: A research agenda. *The Cyber Defense Review*, *11*(3), 1–28. https://doi.org/10.55682/cdr/gcai-agda

Erendor, M. E. (Ed.). (2024). *Cyber security in the age of artificial intelligence and autonomous weapons*. CRC Press. https://doi.org/10.1201/9781003441700

Gopal Chari, S. (2025). Power, pixels and politics: The geopolitics of emerging technologies in the digital age. *London Journal of Research in Humanities and Social Science*, *25*(2), 1–95. https://journalspress.com/LJRHSS_Volume25/Power-Pixels-and-Politics-The-Geopolitics-of-Emerging-Technologies-in-the-Digital-Age.pdf

Hedling, E., & Ördén, H. (2025). Disinformation, deterrence and the politics of attribution. *International Affairs*, *101*(3), 967–985. https://doi.org/10.1093/ia/iiaf055

Hurel, L. M., & Mott, G. (2025). Rethinking cyber deterrence in a multipolar world: Emerging insights. *Royal United Services Institute for Defence and Security Studies*. https://www.rusi.org/explore-our-research/publications/emerging-insights/rethinking-cyber-deterrence-multipolar-world

Instituto Nacional de Ciberseguridad - INCIBE. (2026). Medidas de ciberseguridad y ciberresiliencia ante modelos de IA de frontera: Información para entidades. *INCIBE-CERT*. https://www.incibe.es/incibe-cert/blog/medidas-de-ciberseguridad-y-ciberresiliencia-ante-modelos-de-ia-de-frontera

Jaidka, K., Chen, T., Chesterman, S., Hsu, W., Kan, M.-Y., Kankanhalli, M., Lee, M. L., Seres, G., Sim, T., Taeihagh, A., Tung, A., Xiao, X., & Yue, A. (2025). Misinformation, disinformation, and generative AI: Implications for perception and policy. *Digital Government: Research and Practice*, *6*(1), Article 11. https://doi.org/10.1145/3689372

Kajander, A., Liivoja, R., & Naagel, M. (2025). Cybersecurity of weapon systems. *Journal of Cybersecurity*, *11*(1). https://doi.org/10.1093/cybsec/tyaf017

Maschmeyer, L. (2026). Deception and detection: Why artificial intelligence empowers cyber defense over offense. *International Security*, *50*(3), 86–126. https://doi.org/10.1162/ISEC.a.398

Nakasone, P. M. (2019). A cyber force for persistent operations. *Joint Force Quarterly*, 92, 10–14. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1736950/a-cyber-force-for-persistent-operations/

Nather, W. & Ellis, A. (2013). Living below the security poverty line: coping mechanism. Akamai - 451 Research. *RSA Conference 2013*. https://www.infosecuritymagazine.nl/files/2fb0642808f57f0f9831532ae8f7e8fd.pdf

Organización de los Estados Americanos & Banco Interamericano de Desarrollo – OEA-BID. (2020). Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte de Ciberseguridad 2020. *OEA-BID*. http://dx.doi.org/10.18235/0002513

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382

Rosen, B., & Kraprayoon, J. (2026). Cyberwar's new frontier. *Foreign Affairs*. https://www.foreignaffairs.com/united-states/cyberwars-new-frontier

Unión Internacional de Telecomunicaciones – UIT. (2024). Global cybersecurity index 2024. UIT. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

Whyte, C., Thrall, A. T., & Mazanec, B. M. (Eds.). (2020). *Information warfare in the age of cyber conflict*. Routledge.

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia; Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*

La guerra de los tres días que lleva cuatro años

Cómo los drones de Ucrania reescribieron las reglas de la guerra y de la geopolítica.

DOI: 10.29236/sistemas.n180a6

Resumen

En febrero de 2022, el segundo ejército más poderoso del mundo se lanzó sobre un país que tenía siete fabricantes de drones. Cuatro años después, ese país produce diez millones de aparatos al año, exporta tecnología de defensa a las monarquías del Golfo y firma con la Unión Europea la primera alianza industrial de su historia. Este artículo narra esa transformación en orden cronológico, desde el ensayo que Vladimir Putin publicó en julio de 2021 hasta la crisis de combustible que hoy sacude a Rusia. En el camino examina lo que a mi juicio constituye la verdadera lección: la ventaja decisiva de Ucrania no fue tecnológica sino organizacional. Un ciclo de aprendizaje que itera en semanas frente a burocracias que iteran en años; un mercado digital que asigna equipos según resultados verificados en video; una base industrial distribuida entre cientos de fabricantes. Es, en lenguaje de nuestra profesión, entrega continua aplicada a la guerra. Y es una historia que ya llegó a Colombia, donde se han documentado 418 ataques con drones armados: uno cada 48 horas.

Palabras claves

Drones, guerra electrónica, geopolítica, producción distribuida, innovación tecnológica

Introducción

Hay guerras que se recuerdan por una batalla y guerras que se recuerdan por una tecnología. La Primera Guerra Mundial dejó la ametralladora y el alambre de púas; la Segunda, el portaaviones y la bomba atómica; Vietnam, el helicóptero. La guerra de Ucrania quedará asociada a un objeto que hasta hace poco vendíamos en almacenes de electrónica de consumo: un cuadricóptero con una cámara, una batería de litio y un enlace de radio.

A comienzos de 2026, el presidente ucraniano dio el dato que resume todo: más del 80 % de los impactos exitosos contra fuerzas rusas se ejecutan hoy con sistemas no tripulados. Ochenta por ciento. La artillería, a la que la doctrina soviética llamó durante un siglo el dios de la guerra, fue desplazada por un aparato de cuatrocientos dólares que se arma en un galpón.

Lo que sigue es esa historia contada en orden, desde el principio. La cuento así a propósito. Para quienes trabajamos en tecnología, el valor de este episodio no está en el inventario de armas sino en la secuencia: cada capacidad nueva nació de una restricción, y cada restricción se resolvió con velocidad de iteración antes que con superioridad de recursos. Es una lección de gestión tecnológica escrita con la peor tinta posible.

Tengo muy presente haberle dicho a mi equipo en Axede, antes de la llegada de Tribeca, que avanzáramos a la mayor velocidad posible; que yo prefería que nos equivocáramos rápido y corrigiéramos, y no que nos estancáramos por exceso de prudencia.

Una advertencia metodológica antes de empezar: buena parte de las cifras disponibles proviene de fuentes beligerantes y no es verificable de manera independiente. A lo largo del texto se contrastan, cuando existen, con estimaciones de terceros.

Julio de 2021: la promesa que estaba a punto de romperse

En julio de 2021, Vladimir Putin publica un ensayo de siete mil palabras sobre la unidad histórica de rusos y ucranianos. No es un discurso ni un comunicado: es un texto firmado por él, largo, casi académico, en el que sostiene que Ucrania no existe como nación, que es una invención administrativa de Lenin, que rusos y ucranianos son un solo pueblo separado por un accidente. Los analistas occidentales lo leen como nostalgia imperial de un hombre de sesenta y ocho años. Era una declaración de intenciones, y estaba a la vista de todos.

Veintisiete años antes, en diciembre de 1994, Ucrania había hecho algo que ningún país volvió a hacer: entregar voluntariamente el tercer arsenal nuclear del planeta. Cerca de mil novecientas ojivas heredadas del derrumbe soviético, misiles intercontinentales, bombarderos estratégicos. Las devolvió a Rusia a cambio de una firma. El Memorando de Budapest comprometía a Rusia, Estados Unidos y el Reino Unido a respetar la integridad territorial y la independencia de Ucrania, y a abstenerse de amenazarla con la fuerza. Ucrania cumplió su parte en 1996. Rusia empezó a incumplir la suya en 2014.

Porque para entonces ya había ensayado. Crimea se anexó en marzo de 2014 en tres semanas, con soldados sin insignias que la prensa bautizó «hombrecitos verdes», sin prácticamente disparar un tiro, sin bajas dignas de mención y con un costo internacional que se limitó a un paquete de sanciones que Moscú absorbió sin despeinarse. Fue la lección equivocada aprendida a la perfección: se puede tomar territorio europeo y el mundo protestará durante unas semanas.

Lo que Putin no podía tolerar no era la riqueza de Ucrania —en 2021 era uno de los países más pobres del continente, con un ingreso por habitante inferior al que tenía al independizarse—, sino su dirección. Un país eslavo, ortodoxo, de lengua hermana, encaminándose hacia la Unión Europea y coqueteando con la OTAN, era un experimento peligroso: si aquello funcionaba, la pregunta que se harían los rusos al otro lado de la frontera sería insoportable.

Faltaba una pieza, y se colocó en septiembre de 2021. Ese mes se completó Nord Stream 2, el gasoducto que corre por el fondo del mar Báltico y que le permitía a Rusia vender su gas a Alemania sin tocar suelo ucraniano. Durante décadas, los tubos que cruzaban Ucrania habían sido su mejor seguro de vida: atacarla era cortarle el suministro a media Europa. Ese seguro llevaba años venciéndose —el tránsito había caído de más de ciento cuarenta mil millones de metros cúbicos anuales a unos cuarenta mil— y el nuevo gasoducto lo canceló. Putin no invadió a pesar de la energía. Invadió cuando la energía dejó de proteger a Ucrania.

Después de eso, solo quedaba mirar los números, y los números eran una humillación. Rusia gastaba unos sesenta y seis mil millones de dólares anuales en defensa; Ucrania, menos de seis mil. Rusia mantenía novecientos mil efectivos activos; Ucrania, doscientos mil. Rusia tenía más de mil aviones de combate; Ucrania, poco más de un centenar. Rusia tenía la Flota del Mar Negro; Ucrania había perdido casi toda su armada en Crimea siete años antes. Y en el dominio que terminaría decidiéndolo todo, el desequilibrio era casi cómico: cuando empezó la invasión, Ucra-

nia tenía siete fabricantes de drones. Siete.

El plan, entonces, era simple y no requería genialidad alguna. Tomar Kiev en setenta y dos horas, instalar un gobierno afín, aguantar el chaparrón internacional durante un par de meses y presentarle al mundo un hecho consumado.

Todo estaba calculado, y todo estaba mal.

La noche en que el mundo dio por terminada a Ucrania

En enero de 2022, Estados Unidos hace algo inusual en la historia del espionaje: publica lo que sabe. Fotografías satelitales, cifras, mapas, evaluaciones. Ciento noventa mil hombres desplegados en un arco que va desde Bielorrusia hasta Crimea. Hospitales de campaña montados. Reservas de sangre tras-ladadas al frente, que es el detalle que no admite otra lectura, porque nadie mueve bancos de sangre para un ejercicio. Washington advierte que la invasión es inminente. Buena parte de Europa no lo cree. Berlín ofrece cinco mil cascos. En Kiev, el propio gobierno ucraniano pide calma para no espantar a la economía.

Con las intenciones a la vista y sin nada más que ocultar, Putin da la orden. El 24 de febrero de 2022, a las cinco de la mañana, el segundo ejército más poderoso del mundo se lanza sobre Ucrania. Misiles de crucero contra radares, baterías antiaéreas y centros de mando; columnas mecanizadas cruzando la frontera por el norte, el este y el sur. Y sobre el aeropuerto de Hostomel, a treinta kilómetros de Kiev, una operación aerotransportada de manual: paracaidistas de élite descendiendo de helicópteros para capturar la pista y abrir un puente aéreo que descargaría tropas rusas a las puertas de la capital en cuestión de horas. Era la jugada maestra del plan, la que hacía innecesario el resto.

Los paracaidistas tomaron el aeropuerto. No lograron retenerlo. La artillería ucraniana destruyó la pista y contraatacó, y el puente aéreo hacia Kiev nunca se abrió. Todo lo que Rusia quisiera meter en la capital tendría que entrar rodando por una carretera.

El 25 de febrero la guerra está en las calles de Kiev. Se combate en Obolón, al norte de la ciudad; hay comandos rusos infiltrados con listas de nombres. Ese día, fuerzas amigas le ofrecen a Volodímir Zelenski una evacuación segura, y él responde con la frase que se convertiría en el símbolo de la resistencia ucraniana: la pelea está aquí, necesito municiones, no un aventón.

Publicó un video esa noche, filmado con un teléfono en la calle, rodeado de su gabinete, sin chaleco, señalando el edificio a su espalda para demostrar dónde estaba. El pueblo ucraniano no necesitó

más. Se pusieron de pie todos: reservistas, jubilados, programadores, campesinos, filas de horas en los puestos de reclutamiento y en los centros de donación. Lo que Moscú había planeado como una operación policial se convirtió en una guerra nacional en cuarenta y ocho horas.

Y entonces el ejército más temido de Europa empezó a fallar de las maneras más humillantes. Las vías estaban en mal estado y el deshielo de finales de febrero había convertido el campo en un lodazal que obligaba a los blindados a marchar sobre el asfalto, en fila, sin poder desplegarse. Los camiones cisterna no alcanzaban. Los neumáticos, mal mantenidos durante años, estallaban. Los soldados descubrían por radio abierta que no estaban en un ejercicio. Y por esas radios abiertas —sin cifrado— los ucranianos escuchaban.

Al norte de Kiev se formó entonces la imagen que definió el mes: una columna de sesenta y cuatro kilómetros de tanques, camiones y artillería, detenida en una sola carretera, sin combustible, sin cobertura aérea suficiente, sin poder avanzar ni retroceder. Contra ella no operaban divisiones acorazadas, sino partidas de tres o cuatro hombres con tubos desechables al hombro.

El Javelin pesa unos veintidós kilos y lo carga un soldado. Su misil sube casi vertical y cae sobre el techo del blindado, donde el acero es más delgado y donde ningún tanque diseñado en la Guerra Fría esperaba recibir un golpe. Dispara y olvida: el operador no tiene que mantener la puntería, se marcha antes de que el proyectil impacte. El NLAW, británico-sueco, pesa doce kilos, cuesta una fracción, se dispara desde ventanas y se descarta después de usarlo. Cada uno de esos tubos costaba decenas de miles de dólares. Cada tanque que destruían costaba entre dos y cinco millones.

El 14 de abril, en el mar, dos misiles Neptune de fabricación ucraniana hunden el crucero Moskvá, buque insignia de la Flota del Mar Negro. Nadie lo llamó así en ese momento, pero ahí estaba escrito el principio que gobernaría los cuatro años siguientes: en esta guerra, lo caro muere a manos de lo barato.

A finales de marzo, Rusia anunció que «completaba las tareas» en el eje de Kiev y se retiró hacia el este. Era una derrota, la primera. La guerra de tres días llevaba cinco semanas y apenas empezaba.

Un misil en el blanco vale más que una lluvia sin puntería

El mundo se moviliza. Zelenski aprende a hablarle a cada parlamento en su propio idioma —les recuerda a los británicos a Churchill, a los alemanes el muro, a los estadounidenses Pearl Harbor— y el mundo se rinde no ante sus discursos sino ante un hecho más sim-

ple: ni él ni su familia se fueron de Kiev.

Las armas ligeras ya estaban llegando desde antes de la invasión, pero en junio de 2022 aterriza algo distinto: los HIMARS. Un camión de seis ruedas con un contenedor de seis cohetes guiados por GPS, alcance de ochenta kilómetros, error de pocos metros. Lo que cambia no es la potencia —un cohete de estos lleva noventa kilos de explosivo, nada extraordinario— sino la relación entre lo que se dispara y lo que se destruye. La artillería soviética resolvía la imprecisión con volumen: cientos de proyectiles sobre una cuadrícula, con la esperanza estadística de que alguno cayera donde importaba. El HIMARS hace lo contrario. Un solo cohete sobre el depósito de municiones. Y el depósito, con sus veinte mil proyectiles, deja de existir.

En seis meses, los ucranianos destruyeron más de un centenar de depósitos y puestos de mando. Rusia tuvo que retirar su logística más allá de los ochenta kilómetros, alargar las líneas de suministro y bajar el ritmo de fuego de su artillería. Ese fue el primer derrotero del avance técnico ucraniano, y es una idea que atraviesa toda esta historia: un misil en el blanco vale más que una lluvia desordenada sin precisión. La información vale más que la masa.

El 1.º de julio de 2022 ocurre algo que en su momento nadie consideró noticia militar. La plataforma de recaudación UNITED24, junto con el Estado Mayor y el Ministerio de Transformación Digital que dirige Mykhailo Fedorov —un exdirector de marketing digital de treinta y un años—, lanza el programa Army of Drones. Su objetivo inicial es modestísimo: comprar doscientos drones tácticos de reconocimiento. Pero el diseño del programa es lo interesante, porque no es una compra: es un ciclo completo. Adquisición, reparación, reemplazo inmediato del aparato perdido y, sobre todo, formación de pilotos. Se admiten donaciones en dinero y también donaciones del propio dron del ciudadano —una palabra nueva, dronation—; se recibe en cualquier sucursal de la empresa de correos diciendo simplemente que es para el ejército.

Fedorov no se imagina el alcance de lo que acaba de encender. En nueve meses el programa contrata 3.200 sistemas y entrena a siete mil operadores. En un año, la producción y adquisición de drones se multiplica por cien.

En abril de 2023 llega la segunda pieza, y esta es de arquitectura institucional: Brave1. Un clúster estatal de tecnología de defensa que reúne en una sola mesa al Ministerio de Defensa, al Estado Mayor, al Ministerio de Transformación Digital y al sector privado. Su función es eliminar los tres cuellos de botella que ahogan a cualquier innovador frente a un Estado: encontrar quién

compra, obtener capital semilla y conseguir la certificación oficial que permite vender. Brave1 otorga microsubvenciones, organiza pruebas de campo, conecta al desarrollador con la unidad que tiene el problema y codifica el producto para que el ejército pueda adquirirlo. Hacia 2025 tendrá mil quinientas empresas registradas y miles de productos en su catálogo. Es, en lenguaje de nuestro oficio, una incubadora estatal con acceso directo al usuario final. El usuario final está en una trinchera y responde en veinticuatro horas.

Mientras tanto, en el mar, sucede algo que al principio nadie entiende. En septiembre de 2022 aparece varado en una playa cerca de Sebastopol un artefacto extraño: una especie de kayak con cámara, antenas y una carga en la proa. Los rusos lo fotografían con curiosidad, casi con burla. El 29 de octubre, una decena de esos artefactos entra al puerto de Sebastopol —el fondeadero histórico de la Flota del Mar Negro, protegido desde tiempos zaristas— y avería a la fragata insignia. Los oficiales rusos en el frente no alcanzan a sospechar el alcance que tendrá esa tecnología. Ucrania no tiene armada. Acaba de inventar una que no necesita marinos.

En el verano de 2023, la contraofensiva tan anunciada choca contra la realidad. Rusia había tenido ocho meses para preparar la defensa y los usó bien: campos minados de veinte kilómetros de profundidad, trincheras, dientes de dragón, artillería registrada. Las brigadas ucranianas entrenadas por la OTAN avanzaron unos pocos kilómetros y se detuvieron entre minas. Fue el momento más bajo de la guerra para Ucrania, y también la lección más cara: el asalto mecanizado clásico, tal como se enseña en las academias occidentales, ya no funciona bajo observación permanente.

La escasez inventa un modo de guerra

A finales de 2023 el golpe se vuelve doble. El Congreso estadounidense bloquea la ayuda y estalla la crisis de munición de artillería: hay sectores del frente donde los rusos disparan diez proyectiles por cada uno ucraniano. Y ahí Zelenski y su grupo de mando toman la decisión que define el resto de la guerra: jugársela por los drones.

Las cuentas son claras y brutales. Un proyectil de 155 milímetros cuesta entre tres mil y ocho mil dólares, hay que dispararlo desde un obús que Occidente entrega con cuentagotas, y su precisión depende de la corrección del observador. Un dron FPV —first person view, un cuadricóptero de carreras pilotado con gafas de video— cuesta cuatrocientos dólares, lo lleva un soldado en una mochila y no necesita corregir nada: el operador ve el blanco por la cámara y lo persigue hasta el impacto. No sustituye a la artillería en todo, pero sí en lo esencial, y

con una precisión que la artillería no alcanza. La producción nacional estaba entonces en unos pocos miles de unidades anuales, en manos de siete fabricantes.

En febrero de 2024, mientras todo eso empieza a moverse, el mar entrega su titular. Drones navales de la serie Magura V5 hunden al Ivanovets, una corbeta lanzamisiles, y al Tsezar Kunikov, un buque de desembarco de cuatro mil toneladas. Es la primera vez en la historia que vehículos no tripulados de superficie hunden buques de guerra. Se escriben las primeras páginas del manual moderno de la guerra, y las escribe un país sin flota, con embarcaciones de un cuarto de millón de dólares contra barcos de decenas de millones.

Ante el asedio continuo, Rusia hace algo que no había hecho desde 1783: sacar su flota de Sebastopol. Los buques se repliegan a Novorosíisk, a cuatrocientos kilómetros. Y ese movimiento —una decisión militar defensiva— tiene una consecuencia que se siente en los mercados de todo el planeta: se reabre el corredor de granos ucraniano. El trigo vuelve a salir por el Mar Negro y la presión sobre los precios de los alimentos cede desde El Cairo hasta Bogotá. Unos botes teledirigidos acababan de alterar la seguridad alimentaria global.

En 2024 llega la pieza que convierte la improvisación en sistema: Army of Drones Bonus. El mecanismo es de una elegancia casi comercial. Cada unidad graba el video de su ataque, lo carga en la plataforma de conciencia situacional Delta, y una central lo analiza, lo verifica y lo clasifica según la importancia del blanco: no vale lo mismo un camión que un lanzacohetes o un sistema de guerra electrónica. El resultado se convierte en puntos. Y con esos puntos —no con presupuesto, no con solicitudes por el conducto regular— la unidad compra el equipo que quiere en un catálogo digital.

El modelo ruso, construido sobre la opacidad y la jerarquía, no tiene con qué responder a eso. Aquí los recursos van a los frentes que mejores resultados obtienen, no a los que llevan más tiempo esperando ni a los que tienen mejores padrinos. Los videos, además, sirven de material de entrenamiento: lo que una unidad descubre en Pokrovsk el martes lo replican doce unidades en Járkiv el viernes. Y hay un tercer efecto que suele pasar inadvertido y que a mí me parece el más importante. El Estado obtiene por fin evidencia real de qué equipo funciona, en qué sector del frente y contra qué amenaza. La adquisición militar deja de decidirse por lobby y pasa a decidirse por telemetría.

La respuesta rusa no se hace esperar. Rusia tiene una tradición de sesenta años en guerra electrónica y la despliega en serio: pronto el espectro radioeléctrico sobre el

campo de batalla es una sopa imposible de navegar. Los drones pierden conexión, se estrellan, caen antes de llegar. Rusia ha eliminado la amenaza.

Hasta que alguien —no un laboratorio, alguien— ata un carrete de hilo de fibra óptica a un dron y lo echa a volar. El hilo se desenrolla en el aire, kilómetro tras kilómetro, y se convierte en el nuevo cordón umbilical entre el aparato y su operador. Video en alta definición, control absoluto, cero radiofrecuencia que interferir. La guerra electrónica queda fuera de juego de un solo golpe. Los carretes llegan hasta veinte kilómetros. La solución cunde de frente en frente y los drones recuperan su intensidad.

La innovación de la fibra óptica prueba la eficacia del modelo ucraniano mejor que cualquier estadística. Prueba y error iterando en días y semanas, en talleres, frente a ciclos rusos anclados en grandes factorías y procesos industrializados. El paradigma del producto terminado ha sido eliminado incluso de la guerra. Todos los que trabajamos en operaciones de TI modernas sabemos que vivimos en el beta eterno: lanzar, probar, mejorar, lanzar, y vuelve y juega. Resulta que la trinchera llegó a la misma conclusión del despliegue continuo, y por las mismas razones.

A este respecto me ocurrió que un cliente me reclamó porque nuestro producto está siempre en evolución. Debí explicarle que el ciclo de innovación, la competencia y la propia demanda de los clientes nos obligan a incorporar cosas nuevas a la solución todos los días.

La telaraña, y la primera rendición ante una máquina

El 1.º de junio de 2025, Ucrania asesta el golpe psicológico más importante de la guerra hasta ese momento. Durante dieciocho meses, el Servicio de Seguridad de Ucrania había introducido en Rusia camiones con casetas prefabricadas en el techo. Los conductores eran civiles contratados, que no sabían nada. Ese domingo, los techos de las casetas se abrieron por control remoto en cinco puntos distintos del país, separados por cinco husos horarios, y ciento diecisiete drones FPV despegaron sobre cuatro bases aéreas estratégicas.

Ucrania reclamó cuarenta y un aeronaves alcanzadas, entre ellas bombarderos nucleares Tu-95 y Tu-22M3 y aviones de alerta temprana A-50; la OTAN estimó entre diez y trece completamente destruidos; el daño calculado, unos siete mil millones de dólares. Lo verdaderamente irreparable es otra cosa: esos bombarderos no se fabrican desde la caída de la Unión Soviética. No hay línea de producción que los reponga. Un aparato de mil dólares acababa de causar una pérdida que ningún presupuesto de defensa puede recuperar, y lo había hecho desde un camión estacionado en una carretera rusa.

Ese mismo verano, la unidad robótica NC13 de la 3.ª Brigada de Asalto toma una posición fortificada en el óblast de Járkiv empleando únicamente drones aéreos y vehículos terrestres. Los soldados rusos, sin infantería enemiga a la vista y sin posibilidad de evacuación, levantaron un cartón escrito a mano: queremos rendirnos. Fueron conducidos al cautiverio guiados por drones. Se escribe la segunda página del manual moderno de la guerra: por primera vez, soldados en combate se rinden ante una máquina.

Conviene entender que nada de esto fue capricho tecnológico. Fue aritmética. En una guerra de desgaste, Ucrania no podía permitir que la relación de bajas siguiera siendo de uno a uno, por la sencilla razón de que tiene la tercera parte de la población rusa: un intercambio parejo la liquidaba primero. El dron introduce distancia entre el soldado y el combate, y esa distancia es exactamente la diferencia entre perder un operador y perder un pelotón. La apuesta era imponer bajas sustancialmente mayores que las propias. Y lo logró: hacia abril de 2026 el presidente finlandés Alexander Stubb estimaba públicamente una relación de cinco a uno a favor de Ucrania (Gosselin-Malo, 2026a).

Pronto los drones generaron sobre el frente una franja que se bautizó death zone. Una zona donde nadie puede permanecer sin exponerse a una explosión teledirigida; donde un vehículo que se mueve es detectado en minutos y destruido en diez; donde el reabastecimiento se hace de día, a pie, o no se hace. Las cámaras infrarrojas cancelaron el último refugio, que era la oscuridad. Se escribe la tercera página del manual: los drones generan supremacía aérea de baja altura. Nadie sobrevive dentro de su zona de control, que llegó a extenderse veinte kilómetros a cada lado de la línea de contacto. El frente dejó de ser una línea y se volvió un espesor.

Para finales de 2025, aquellos siete fabricantes de principios de la guerra se han convertido en cerca de quinientos. La producción de drones entregados a las fuerzas armadas ese año superó los tres millones de unidades, con una capacidad instalada estimada entre ocho y diez millones anuales (Just Security, 2026).

De siete fábricas y unos pocos miles de drones al comenzar, a tres millones al terminar 2025.

2026: la estrategia del judo

Llega 2026, y Ucrania ya no es el país que pedía armas.

El camino hasta ahí incluyó un episodio que merece contarse, porque revela quién juega realmente en este tablero. Durante los primeros años, los drones ucranianos eran, en lo esencial, ensamblajes de piezas chinas: baterías de litio, controladoras de vuelo, motores, cáma-

ras térmicas, módulos de navegación. Cerca del noventa y siete por ciento de los componentes venía de China. Y Pekín, que se proclama neutral, empezó a apretar. Controles de exportación en 2023, ampliados en 2024, endurecidos en 2025 hasta bloquear envíos de electrónica a países europeos si sospechaba que terminarían en Kiev. Las piezas que sí salían llegaban con precios triplicados. Mientras tanto, los mismos componentes seguían fluyendo hacia Rusia por una frontera terrestre de cuatro mil kilómetros que ningún control alcanza.

El estrangulamiento fue real y dolió. Pero produjo el efecto contrario al buscado. Ucrania se lanzó a fabricar lo que no sabía fabricar: circuitos impresos, motores, baterías, hélices. En marzo de 2026, el New York Times documentó la escena que resume el esfuerzo —talleres en sótanos, decenas de trabajadores con linternas frontales soldando placas que un año antes el país no producía— y el hito que la acompaña: Ucrania ya puede construir un dron sin una sola pieza china. La participación de componentes chinos cayó del noventa y siete por ciento a cerca del treinta y ocho (Kyiv Post, 2026a). La producción masiva a ese estándar todavía tomará años, pero la dirección es inequívoca. Una empresa, Motor-G, entrega doscientos mil motores al mes. Y hay una ironía deliciosa en su origen: adquirió el conocimiento pagándoles diez mil dólares a fabricantes chinos por una transferencia de tecnología. Ese es el país que en 2026 exporta lo que en 2022 mendigaba.

Con capacidad propia y alcance creciente, Zelenski y su equipo de mando enfrentan la pregunta que define toda campaña militar: ¿qué atacar?

Y ahí hacen algo que no es táctica sino estrategia en el sentido más puro. En lugar de buscar las debilidades del enemigo, examinan sus ventajas, aquellas de las que Rusia se ufanaba al comenzar la guerra, para convertirlas en su ruina. Judo aplicado a la guerra: usar el peso del adversario contra él mismo.

La primera ventaja rusa era su economía energética. Petróleo, gasolina y gas vendidos a un mundo ávido de consumir hasta la última gota, con un as adicional en la manga: en el cálculo de 2022, la propia guerra encarecía el crudo, de modo que el conflicto financiaba el conflicto. Un gana-gana perfecto. La segunda ventaja era demográfica: tres veces la población de Ucrania significa soportar mucho mejor las bajas, y Moscú lo sabía y contaba con ello.

La decisión es atacar el aparato de refinación y exportación de hidrocarburos, y con él los centros logísticos de Wildberries, el Amazon ruso. El primer objetivo es transparente: cortar el ingreso de rublos limitando la capacidad de refinar y exportar, y el segundo perturbar la

operación del gigante del comercio electrónico. Pero el efecto clave es el político. Los dos blancos pinchan la burbuja de falsa seguridad en la que vive el ciudadano ruso: el que llena el tanque de su auto y el que espera un paquete. La ventaja convertida en debilidad. Jaque al rey.

Y luego está Sun Tzu, que lo escribió hace veinticinco siglos: un ejército sin bagajes está perdido; sin provisiones está perdido; sin bases de abastecimiento está perdido.

La R-280 es una carretera costera de setecientos kilómetros que sale de Rostov del Don, bordea el mar de Azov, pasa por Mariúpol, Berdiansk y Melitópol, y entra a Crimea. Las autoridades de ocupación la rebautizaron «Novorossiya» y la convirtieron en la arteria principal de suministro del sur, precisamente porque desde los ataques al puente de Kerch en 2022 el transporte de combustible por el puente está prohibido. Es el cordón umbilical de doscientos cincuenta mil soldados rusos.

Los ucranianos la llaman la carretera de la muerte.

Desde abril de 2026, la 414.ª Brigada de Aviación de Ataque No Tripulado —«los Pájaros de Madyar», al mando de Robert Brovdi— y otras unidades de las Fuerzas de Sistemas No Tripulados ejecutan sobre ella una campaña de «golpe medio»: ataques entre veinte y doscientos kilómetros detrás de la línea de contacto, contra camiones cisterna, convoyes, locomotoras, puentes y transbordadores. Drones merodeadores que sobrevuelan la ruta esperando tráfico. El 9 de junio, Brovdi reporta que el flujo de carga militar por la R-280 cayó un setenta y uno por ciento en dos semanas (Kyiv Post, 2026b). Desde finales de mayo, la vía está prácticamente cerrada al tráfico civil. El registro de ACLED contabiliza trescientos sesenta y un ataques en ese corredor durante el primer semestre (ACLED, 2026). Veinte trenes atacados desde enero, muchos de ellos cisternas de combustible.

La carretera se convirtió en una death zone de setecientos kilómetros. Y en Crimea, la península que Putin anexó como joya de su proyecto imperial, empiezan las compras de pánico, se vacían los anaqueles y aparecen las filas.

El 28 de febrero de 2025, en el Despacho Oval, Donald Trump había arrinconado a Zelenski frente a las cámaras del mundo con una frase que dio la vuelta al planeta: no tienes las cartas. Fue el momento más humillante de la guerra para Kiev, y no ocurrió en un campo de batalla.

La baraja se repartió de nuevo. En marzo de 2026, mientras Estados Unidos e Israel libran su propia guerra contra Irán y los drones Shahed llueven sobre el Golfo, Zelenski aterriza sin anuncio previo en Yeda.

El 27 firma con Arabia Saudita un acuerdo de cooperación en defensa antidrón, el primero de Ucrania con una monarquía del Golfo; al día siguiente firma con Emiratos Árabes Unidos y con Catar. Son acuerdos a diez años, con transferencia de tecnología, y despliega asesores en los tres países. La lógica que convenció a Riad es puramente económica y es la misma que atraviesa esta guerra: derribar un Shahed de ciento treinta mil dólares con un misil de varios millones es insostenible; hacerlo con un interceptor ucraniano de diez mil, no. Arabia Saudita, socio histórico de Moscú en la OPEP+, eligió a Ucrania para defenderse de las armas que fabrica el aliado de Rusia.

En 2022, Rusia era el segundo exportador de armamento del mundo. Hoy los países cancelan pedidos a Moscú mientras cierran acuerdos con Kiev.

Y el 15 de julio de 2026, en la plaza de San Miguel, la presidenta de la Comisión Europea viaja a Kiev para firmar la primera alianza industrial de defensa entre la Unión Europea y Ucrania. Mil millones de euros desembolsados de inmediato para drones, diez mil millones adicionales habilitados, diecinueve socios industriales fundadores. Y von der Leyen dice en voz alta lo que hace cuatro años habría sonado absurdo: Europa tiene capacidad industrial, pero no tiene el conocimiento probado en combate que Ucrania forjó. Zelenski responde con una cifra: hacemos diez millones de drones al año. Y serán veinte (Euronews, 2026).

El invitado que llegaba a pedir ayuda se convirtió en el invitado con el que hay que hablar de la defensa tecnológica de todo el continente.

Julio de 2026: las filas de gasolina

Mientras termino de escribir este artículo, los números son estos. Ucrania ha golpeado instalaciones petroleras rusas más de trescientas veces desde el inicio de la invasión, y solo desde marzo de 2026 ha atacado más de dos docenas de refinerías, incluidas ocho de las diez mayores del país. Kapotnia, la que abastece a Moscú, fue alcanzada dos veces en junio. Omsk, la mayor de Rusia, a dos mil quinientos kilómetros de la frontera, cayó el 7 de julio.

¿Cuánta capacidad de refinación está fuera de servicio? Depende de a quién se le pregunte. El Estado Mayor ucraniano reclama un 42,7 %; los analistas independientes se quedan entre el 20 % y el 25 %. La Agencia Internacional de Energía, que no tiene bandera en esta pelea, calificó la perturbación como sin precedentes en el conflicto (Kyiv Post, 2026c; RFE/RL, 2026). Lo que sí es incontrovertible es lo que se ve en la calle. La producción de gasolina corre cerca de un veinte por ciento por debajo de la deman-

da interna. Al 24 de junio, cincuenta y cinco de las ochenta y tres entidades federales rusas habían impuesto restricciones a la venta de combustible, y semanas después prácticamente todas. Unos cincuenta millones de ciudadanos afectados. Filas kilométricas en ciudades importantes. Los residentes de Crimea vaciando los supermercados.

Y las bodegas de Wildberries ardiendo: tres oleadas en menos de una semana en julio, en las regiones de Moscú, Tambov y San Petersburgo, con columnas de humo visibles a doscientos kilómetros y pérdidas de mercancía estimadas por la prensa en decenas de miles de millones de rublos. La justificación militar es la llamada zona gris del suministro: por esos centros circulan insumos de doble uso —chalecos, visores térmicos, baterías, fibra óptica, componentes de dron— que terminan en el frente, comprados en línea por los propios soldados. Los ataques también dejaron muertos y decenas de heridos entre trabajadores civiles, y eso abre una discusión jurídica seria sobre el principio de distinción del derecho internacional humanitario. Es una zona gris que esta guerra está ampliando en ambas direcciones, y ninguna narrativa triunfalista debería omitirlo.

Entonces las encuestas del propio Kremlin empiezan a moverse. La Fundación de Opinión Pública, que trabaja para el gobierno, registra entre el 10 y el 12 de julio una caída de la aprobación de Putin del setenta y uno al sesenta y seis por ciento: cinco puntos en una semana, el desplome más pronunciado desde la movilización parcial de 2022. Por segunda semana consecutiva, los rusos identifican la escasez de combustible como el problema más importante del país, diecinueve por ciento, por encima de la guerra misma. El índice de confianza del consumidor del Centro Levada cae a su nivel más bajo desde octubre de 2022 (Kyiv Post, 2026d; Meduza, 2026). Y son cifras de encuestadoras controladas, lo que significa que la realidad detrás de ellas es probablemente peor.

La estrategia de judo está dando frutos. En Polymarket, los apostadores asignan cerca de un veintiocho por ciento de probabilidad a que Ucrania y Rusia firmen un acuerdo de paz antes de 2027.

Es una probabilidad baja. Pero hace dos años era cero, y la conversación no era sobre si Rusia negociaría, sino sobre cuánto tiempo aguantaría Ucrania.

Conviene, eso sí, resistir la tentación del pronóstico. De la erosión del apoyo a un levantamiento popular hay una distancia que la evidencia no autoriza a recorrer: Rusia carece de canales de protesta viables, con gobernadores designados de facto por el Kremlin, oposición excluida de las elecciones y una ciudadanía que históricamente

elige la adaptación sobre la confrontación. Y sobre el terreno, Rusia no ha sido expulsada de ningún lado; sigue avanzando, lentamente y a un costo altísimo. Lo que la campaña de ataques profundos busca no es derribar a Putin, sino algo más modesto y más alcanzable: elevar el costo interno de sostener la guerra hasta hacerlo políticamente incómodo, erosionando el contrato social que cambió libertades por estabilidad material.

Esta historia continuará…

Conclusiones / Reflexiones finales

Primera. Los drones no ganaron la guerra, porque la guerra no está ganada. Lo que hicieron fue cambiar tres cosas que difícilmente volverán a su lugar: el campo de batalla se volvió transparente y hoy casi nada se mueve sin ser visto; la ecuación de costos entre atacante y defensor se invirtió; y el modelo industrial que sostiene el esfuerzo bélico dejó de parecerse a una fábrica de armas y empezó a parecerse a una industria de software. Sobre la segunda vale la pena detenerse un momento. Un dron de quinientos dólares destruye un tanque de cinco millones. Un bote no tripulado de doscientos cincuenta mil amenaza a una fragata de quinientos millones. Un artefacto de mil dólares alcanza a un bombardero estratégico que ya nadie fabrica. Cuando el atacante gasta tres órdenes de magnitud menos que el defensor, ningún presupuesto resiste indefinidamente. Ha nacido un arma nueva, la dronería, junto a la infantería, la artillería, la caballería y la fuerza aérea.

Segunda, y para mí la principal. La ventaja decisiva de Ucrania no fue tecnológica sino organizacional. Sus drones no son mejores que los de nadie en particular. Su ciclo de aprendizaje sí. Un requerimiento nace en una trinchera, llega al fabricante en días, se modifica y vuelve al frente en semanas, y el resultado se mide en video verificado que alimenta tanto la asignación de recursos como la decisión de escalar o descartar el producto. Cualquier CIO reconocerá la descripción sin necesidad de que se la traduzcan: entrega continua, telemetría de producción, decisiones basadas en datos de uso real. En entornos de alta incertidumbre, la velocidad de iteración le gana a la sofisticación. Como suele decir Elon Musk, si las cosas no están fallando, no se está innovando lo suficiente.

En el caso de Axede fue evidente la velocidad que ganamos cuando nos separamos de Alcatel. Las decisiones pasaron de estar controladas por la burocracia de la multinacional a tomarse en una conversación de pasillo, y eso nos valió una enorme ventaja estratégica.

Tercera. La arquitectura distribuida es una decisión estratégica, no solo técnica. Cientos de proveedores con interfaces comunes resisten lo

que una planta única no resiste. Pero la resiliencia se pierde si la dependencia se traslada al eslabón de componentes, y el episodio chino lo demuestra con claridad: quien controla la cadena de suministro tiene voto en el resultado de una guerra sin disparar un tiro. Es una lección directa para cualquier país que hable de soberanía tecnológica sin mirar de dónde vienen sus piezas.

Cuarta, y menos cómoda. Esta guerra está normalizando la gamificación de la letalidad y acelerando el paso del control humano hacia la autonomía, precisamente porque la guerra electrónica hace inviable el enlace permanente con el operador. La presión técnica empuja hacia armas que seleccionan objetivos por sí mismas. Quienes construimos software de visión, clasificación y navegación tenemos una responsabilidad en ese debate, y sería ingenuo suponer que la frontera entre lo civil y lo militar seguirá existiendo en un mercado de componentes duales.

Quinta. Para Colombia, el asunto ya no es prospectivo. Entre abril de 2024 y febrero de 2026 se documentaron 418 ataques con sistemas aéreos no tripulados cargados con explosivos, con unas 935 granadas lanzadas y 328 afectaciones entre civiles y miembros de la Fuerza Pública (El Tiempo, 2026a). Uno cada cuarenta y ocho horas. En el Catatumbo, informes de organizaciones sociales y de prensa reportan el uso sistemático de esta modalidad por parte del ELN y de disidencias de las FARC, con ataques en enjambre y afectación directa a la población civil (El Tiempo, 2026b). Entre tanto, la prensa ha documentado que los sistemas antidrón contratados para el Ejército no estaban operativos en las fechas previstas. La brecha entre la velocidad de adopción del atacante y la del defensor institucional es, aquí, el problema central.

Y es un problema de ingeniería de sistemas, no de compra de equipos. Ahí quiero ser enfático, porque es el error que veo repetirse. La contramedida efectiva no es un dispositivo sino una cadena completa. Empieza por la detección multiespectral, que combina radiofrecuencia, radar de baja sección, acústica y electroóptica. Sigue con la identificación y la clasificación asistidas por aprendizaje automático. Continúa con una decisión gobernada por reglas de enfrentamiento claras. Y termina en una mitigación escalonada que va de la inhibición y la suplantación de señal a la captura o la interceptación cinética. Todo eso tiene que estar integrado en un mando y control que responda en segundos, no en minutos. Añádase que la interferencia electromagnética indiscriminada afecta aviación civil, telecomunicaciones y servicios de emergencia en zonas pobladas, y lo que queda es un problema de arquitectura, no de catálogo. Lo mismo aplica a la infraestructura crítica. Su-

bestaciones eléctricas, refinerías, aeropuertos, centros de datos y torres de telecomunicaciones fueron diseñados para resistir una intrusión terrestre. Nadie los pensó contra una amenaza aérea de cuatrocientos dólares.

Esta reescritura de las reglas de la guerra que está haciendo Ucrania nos obliga a repensar las formas de enfrentar el conflicto interno en nuestro país. Tal vez no necesitamos más helicópteros Black Hawk ni más aviones, sino conseguir una superioridad a baja altura con una estrategia basada en drones, justamente la más apropiada para el tipo de reto que enfrentamos.

Hay una buena noticia en todo esto, y es que lo mismo que vuelve peligrosa a esta tecnología, su bajo costo y su base comercial, la vuelve accesible para quien decida defenderse. Los componentes se compran. Los equipos se contratan. Lo único que no viene en ningún contrato es el ciclo de aprendizaje. Ese hay que construirlo, y toma años.

Referencias

ACLED. (julio de 2026). Ukraine's drone campaign is dismantling Russia's military supply network in the occupied south. Armed Conflict Location & Event Data Project. https://acleddata.com/report/ukraines-drone-campaign-dismantling-russias-military-supply-network-occupied-south

Al Jazeera. (27 de marzo de 2026). Ukraine announces 'mutually beneficial' defence deal with Saudi Arabia. Al Jazeera. https://www.aljazeera.com/news/2026/3/27/ukraine-announces-defense-pact-with-saudi-arabia

CNN. (6 de julio de 2026). Almost every Russian region hit by fuel crisis, as Ukraine escalates drone attacks. CNN. https://www.cnn.com/2026/07/06/europe/russia-fuel-crisis-ukraine-drone-attacks-intl-vis

Counteroffensive.pro. (22 de febrero de 2025). Deep dive: Ukraine's decentralized 3D-printing war goods industry. The Counteroffensive. https://newsletter.counteroffensive.pro/p/deep-dive-ukraine-s-decentralized-3d-printing-war-goods-industry

Defense News. (24 de abril de 2026). Ukraine to field 25,000 ground robots in push to replace soldiers for frontline logistics. Defense News. https://www.defensenews.com/unmanned/2026/04/24/ukraine-to-field-25000-ground-robots-in-push-to-replace-soldiers-for-frontline-logistics/

El Tiempo. (25 de febrero de 2026a). En 22 meses se registraron 418 ataques con drones cargados con explosivos. El Tiempo. https://www.eltiempo.com/justicia/conflicto-y-narcotrafico/en-22-meses-se-registraron-418-ataques-con-drones-cargados-con-explosivos-3535498

El Tiempo. (julio de 2026b). El informe que revela cómo los drones con explosivos cambiaron la guerra en el Catatumbo. El Tiempo. https://www.eltiempo.com/justicia/conflicto-y-narcotrafico/el-informe-que-revela-como-los-drones-con-explosivos-cambiaron-la-guerra-en-el-catatumbo-3569847

Euromaidan Press. (3 de julio de 2026). Ukraine reports 1,150% increase in

deep strikes. Euromaidan Press. https://euromaidanpress.com/2026/07/03/ukraine-reports-1150-increase-in-deep-strikes/

Euronews. (15 de julio de 2026). Von der Leyen and Zelenskyy sign EU-Ukraine drone deal. Euronews. https://www.euronews.com/my-europe/2026/07/15/von-der-leyen-and-zelenskyy-sign-eu-ukraine-drone-deal

Gosselin-Malo, E. (14 de abril de 2026a). 1:5 kill ratio: Ukraine inflicts heavy Russian losses using drones, says Finnish president. Breaking Defense. https://breakingdefense.com/2026/04/15-kill-ratio-ukraine-inflicts-heavy-russian-losses-using-drones-says-finnish-president/

Gosselin-Malo, E. (17 de julio de 2026b). EU, Ukraine sign drone deal to fast-track unmanned systems production. Breaking Defense. https://breakingdefense.com/2026/07/eu-ukraine-sign-drone-deal-to-fast-track-unmanned-systems-production/

Institute for the Study of War. (1 de julio de 2026). Russian offensive campaign assessment, July 1, 2026. Critical Threats Project. https://www.criticalthreats.org/analysis/russian-offensive-campaign-assessment-july-1-2026

Just Security. (1 de junio de 2026). How Ukraine became a drone superpower. Just Security. https://www.justsecurity.org/138164/ukraine-drone-superpower/

Kyiv Independent. (3 de junio de 2025). Ukraine confirms 41 Russian aircraft hit during Operation Spiderweb. The Kyiv Independent. https://kyivindependent.com/ukraines-general-staff-confirms-striking-41-russian-bombers-other-aircraft-in-june-1-mass-drone-attack/

Kyiv Post. (11 de junio de 2026b). Bridge strikes, drone swarms: Ukraine targets Russia's key Crimea supply route. Kyiv Post. https://www.kyivpost.com/post/77980

Kyiv Post. (11 de marzo de 2026a). Ukraine cuts reliance on Chinese drone components. Kyiv Post. https://www.kyivpost.com/post/71701

Kyiv Post. (julio de 2026c). Ukrainian defense forces disable 43% of Russia's total oil refining capacity. Kyiv Post. https://www.kyivpost.com/post/79574

Kyiv Post. (julio de 2026d). Putin's approval rating sees biggest weekly drop since 2022 amid fuel crisis. Kyiv Post. https://www.kyivpost.com/post/80486

Meduza. (17 de julio de 2026). Putin's approval rating just posted its steepest drop since Russia invaded Ukraine. Meduza. https://meduza.io/en/news/2026/07/17/putin-s-approval-rating-just-posted-its-steepest-drop-since-russia-invaded-ukraine

Meduza. (4 de junio de 2025). Ukraine's 'Spiderweb' operation damaged 40 Russian aircraft, destroying at least 10-13, senior NATO official says. Meduza. https://meduza.io/en/news/2025/06/04/ukraine-s-spiderweb-operation-damaged-40-russian-aircraft-and-destroyed-10-30-senior-nato-official-says

RFE/RL. (24 de junio de 2026). Russia is grappling with its worst nationwide fuel shortages in years. Here's where. Radio Free Europe/Radio Liberty. https://www.rferl.org/a/ukraine-russia-oil-refinery-fuel-shortages-kremlin/33787903.html

Royal United Services Institute. (2025). Drones win battles, components win wars. RUSI Commentary.

https://www.rusi.org/explore-our-research/publications/commentary/drones-win-battles-components-win-wars

Ukrainska Pravda. (27 de abril de 2026). Drones every day: How Ukraine has caught up with Russia in long-range UAV numbers. Ukrainska Pravda. https://www.pravda.com.ua/eng/articles/2026/04/27/8032007/

UNITED24. (2022). Ukraine raises an Army of Drones. UNITED24. https://u24.gov.ua/news/army_of_drones

War on the Rocks. (7 de enero de 2026). Gamified war in Ukraine: Points, drones, and the new moral economy of killing. War on the Rocks. https://warontherocks.com/gamified-war-in-

Carlos Alberto Sierra Murillo. *Ingeniero y empresario colombiano, estratega, fundador de Axede S.A.S., compañía de integración tecnológica en redes, ciberseguridad y automatización, y fundador de MindX Corp, plataforma de automatización conversacional con inteligencia artificial. Autor del libro «Axede y el Tribeca Way». Ha liderado durante más de tres décadas proyectos de transformación tecnológica para grandes clientes corporativos en Colombia y América Latina.*

Más allá de las fronteras

El ciberespacio como nuevo escenario del poder geopolítico

DOI: 10.29236/sistemas.n180a7

Resumen

El ciberespacio dejó de ser un soporte técnico de la vida social para convertirse en un escenario donde se disputa el poder entre Estados. Este artículo sostiene que la digitalización no anula la geografía política: la estratifica. Bajo la aparente desterritorialización de los flujos de datos persiste una geografía densa —cables submarinos, puntos de aterrizaje, centros de datos, cadenas de suministro de semiconductores— cuyo control produce dependencia y, por lo tanto, poder. A partir de una revisión de literatura especializada, doctrina militar, instrumentos de gobernanza internacional y evidencia empírica del periodo 2022-2026, se propone un modelo de análisis articulado en tres vectores de ciberpoder: infraestructural, normativo y cognitivo. El modelo se aplica al caso colombiano, una potencia media bioceánica con nueve puntos de aterrizaje de cable submarino, alta dependencia tecnológica externa y capacidades institucionales en consolidación. Se concluye que el ciberespacio no inaugura una guerra distinta, sino una gramática distinta del conflicto: persistente, ambigua y situada por debajo del umbral del ataque armado. Para las potencias medias, la autonomía estratégica dependerá menos de la fuerza acumulada que de la capacidad de anticipación.

Palabras clave

Geopolítica; ciberespacio; ciberpoder; soberanía digital; infraestructura crítica cibernética.

Introducción

Durante más de un siglo, la geopolítica pensó el poder desde la geografía. Mahan situó la clave del predominio en el control de las líneas de comunicación marítima; Mackinder (1904) la desplazó al corazón continental euroasiático; Spykman la reubicó en los bordes. Distintas como son, estas tradiciones comparten una intuición: el poder no se distribuye de manera uniforme sobre el espacio, sino que se concentra en aquellos lugares por donde necesariamente deben pasar los flujos que sostienen la vida económica y militar de las naciones.

El ciberespacio parecía haber roto esa lógica. La promesa fundacional de la red era la de un dominio instantáneo, ubicuo y desterritorializado, ajeno a la soberanía de los Estados. "Los gobiernos del mundo industrial —escribía Barlow (1996)— no son bienvenidos entre nosotros.

No tienen soberanía donde nos reunimos". Tres décadas después, el diagnóstico se invirtió. Los Estados regresaron al ciberespacio, no como intrusos, sino como sus principales arquitectos: legislan sobre datos, subsidian semiconductores, tienden cables, patrullan lechos marinos y desarrollan capacidades militares específicas para el dominio (Perafán Del Campo et al., 2021). Lo que parecía un espacio sin geografía resultó ser un espacio con una geografía nueva, superpuesta a la anterior y no menos disputada, donde emergen "fronteras virtuales" que no coinciden con las líneas del mapa, pero organizan identidades, flujos y lealtades (García-Jiménez et al., 2010).

Este artículo sostiene una tesis deliberadamente contraintuitiva: la digitalización no anula la geografía política, la estratifica. La aparente inmaterialidad de los datos descansa sobre una infraestructura físicamente localizada, jurídicamente sometida a jurisdicciones concretas y económicamente concentrada en pocas manos. Quien controla esa infraestructura no domina un territorio, pero sí determina las condiciones de posibilidad de la actividad ajena. Esa es, en sentido estricto, una forma de poder geopolítico.

La pregunta que anima este número —si las tecnologías de la información inauguran una nueva perspectiva de la guerra— admite una respuesta matizada. El argumento que aquí se desarrolla es que el ciberespacio no produce una guerra distinta, sino una gramática distinta del conflicto: persistente en el tiempo, ambigua en la atribución y deliberadamente situada por debajo del umbral que activa las respuestas del derecho internacional. Menos una nueva guerra que una

nueva manera de competir sin declararla.

El texto avanza en cinco movimientos: el marco conceptual y el modelo de los tres vectores de ciberpoder, la materialidad del dominio, el debate sobre su carácter bélico, la disputa por las reglas globales y la aplicación al caso colombiano.

De Mackinder al Heartland cibernético: tres vectores de ciberpoder

La doctrina militar describe el ciberespacio como un dominio operacional compuesto por tres capas interdependientes: una capa física —cables, servidores, dispositivos, con coordenadas y propietarios—, una capa lógica —protocolos, direccionamiento, software— y una capa ciber-persona, donde residen las identidades digitales de individuos y organizaciones (United States Joint Staff, 2018). Esta arquitectura estratificada es más que una convención técnica: es el punto de partida de cualquier análisis geopolítico serio, porque cada capa habilita un tipo distinto de poder y admite un tipo distinto de disputa.

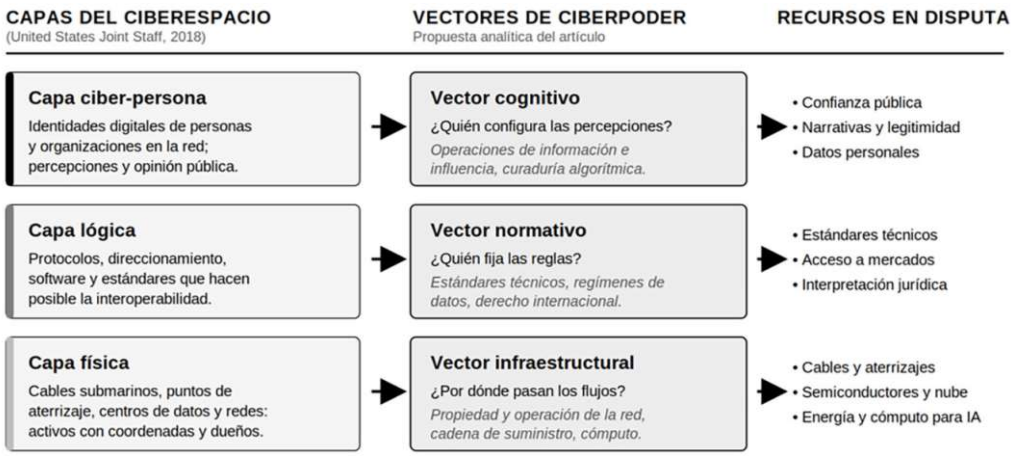
Prado (2018) propuso leer esta configuración en clave mackinderiana y hablar de un *Heartland* cibernético: el conjunto de nodos cuyo control confiere ventaja estructural sobre la red. La analogía es fértil, pero exige una precisión. El Heartland euroasiático era un dato de la naturaleza; el cibernético es un artefacto que se construye, se financia, se traslada y a veces se destruye. Esa reversibilidad es justamente lo que lo convierte en objeto de política pública y de estrategia, y no solo de descripción.

Sobre esta base es posible ordenar analíticamente el ciberpoder —la capacidad de un actor de obtener resultados preferidos mediante el uso de recursos electrónicamente interconectados (Nye, 2011)— en tres vectores complementarios, que constituyen la propuesta analítica de este artículo y se sintetizan en la Figura 1. La agregación de estos vectores es lo que los índices comparados intentan capturar cuando ordenan a los Estados por capacidad e intención cibernéticas (Voo et al., 2022), y lo que la literatura latinoamericana reciente ha discutido bajo las categorías de ciberpoder, cibersoberanía y ciberdiplomacia (Bartolomé, 2023).

El **vector infraestructural** opera sobre la capa física y responde a la pregunta por dónde pasan los flujos: propiedad de cables submarinos y puntos de aterrizaje, localización de centros de datos, control de la cadena de suministro de semiconductores y disponibilidad de cómputo para inteligencia artificial. Es el vector más cercano a la geopolítica clásica y, por eso mismo, el más subestimado por los análisis que insisten en la inmaterialidad de lo digital.

El **vector normativo** opera sobre la capa lógica y responde a la pre-

Figura 1. Modelo de análisis geopolítico del ciberespacio: capas, vectores de ciberpoder y recursos en disputa.



Nota. Elaboración propia a partir de la arquitectura de capas de United States Joint Staff (2018) y del concepto de ciberpoder de Nye (2011).

gunta quién fija las reglas: estándares técnicos, regímenes de protección de datos, condiciones de acceso a mercados digitales, posición de cada Estado sobre el derecho internacional aplicable y presencia en los foros donde eso se negocia. Bradford (2020) mostró que la capacidad regulatoria se proyecta extraterritorialmente sin coerción alguna: basta con controlar el acceso a un mercado suficientemente grande para que las normas propias se vuelvan estándar ajeno.

El **vector cognitivo** opera sobre la capa ciber-persona y responde a la pregunta quién configura las percepciones: operaciones de información e influencia, manipulación algorítmica de la conversación pública y uso de la desinformación como herramienta de política exterior. Es donde la asimetría es mayor: actores con recursos modestos generan efectos desproporcionados sobre sociedades altamente conectadas.

Estos vectores no son compartimentos estancos: su valor analítico reside en la interacción. El sabotaje de un cable submarino (infraestructural) resulta rentable porque la ambigüedad jurídica sobre su calificación (normativo) impide una respuesta contundente, mientras la incertidumbre alimenta narrativas de vulnerabilidad (cognitivo). El ciberpoder efectivo es el producto, no la suma, de los tres.

La materialidad del poder: cables, chips y nubes

Nada revela mejor la persistencia de la geografía que la infraestructu-

ra submarina. Aproximadamente el 99 % del tráfico mundial de internet viaja por más de quinientos sistemas de cable de fibra óptica tendidos sobre el lecho marino, no por satélite; solo en 2024 se instalaron cerca de 200.000 kilómetros de cable nuevo, y en 2025 se ejecutaron más de 170 reparaciones, un promedio cercano a cuatro fallas por semana (Unión Internacional de Telecomunicaciones, 2025).

Esta arquitectura reproduce, con notable fidelidad, los cuellos de botella de la geografía marítima clásica: el mar Rojo, el estrecho de Malaca, el canal de Sicilia o el golfo de Finlandia concentran haces de cables cuya interrupción simultánea produce efectos regionales inmediatos.

Los años recientes convirtieron esa vulnerabilidad teórica en un problema operacional. Entre el 17 y el 18 de noviembre de 2024, los cables BCS East-West Interlink (Lituania-Suecia) y C-Lion1 (Finlandia-Alemania) fueron seccionados en el mar Báltico; las investigaciones señalaron al buque *Yi Peng 3*, que había apagado su sistema de identificación automática durante siete horas y media al cruzar la zona del incidente. En febrero de 2025 se registraron nuevos daños en la misma cuenca. La respuesta fue instructiva: en enero de 2025 la OTAN activó la misión *Baltic Sentry* para la protección de infraestructura crítica submarina, desplegando medios navales, aéreos y sistemas no tripulados en una tarea que hasta hace poco se habría considerado ajena a una alianza militar (Organización del Tratado del Atlántico Norte, 2025). La protección de un cable de telecomunicaciones se volvió, literalmente, una misión de defensa colectiva.

Lo relevante de estos episodios no es el daño causado —los cables fueron reparados en días o semanas— sino su gramática: acciones de bajo costo, ejecutadas por medios civiles, jurídicamente ambiguas, difícilmente atribuibles y con efectos económicos y psicológicos desproporcionados. Es el patrón característico de la conflictividad contemporánea en el ciberespacio.

El vector infraestructural no se agota en los cables. La disputa por los semiconductores avanzados —donde un puñado de empresas concentra diseño, fabricación y maquinaria litográfica— convirtió los controles de exportación en instrumento de política exterior de primer orden, y algo análogo ocurre con el cómputo para inteligencia artificial y la nube, cuya concentración hipoteca la autonomía de Estados enteros. La Ruta de la Seda Digital china y las iniciativas occidentales de conectividad segura compiten por equipar las redes del Sur global, incluida América Latina, sabiendo que quien instala la infraestructura fija los estándares y accede a los datos durante décadas (Rivas, 2021; Mata-Sánchez, 2023).

Para las potencias medias la implicación es incómoda: la conectividad, presentada como bien público y factor de desarrollo, es a la vez un vector de dependencia. No hay soberanía digital sin respuesta explícita a quién construye, opera y puede interrumpir la infraestructura sobre la que descansa la economía nacional.

¿Una nueva perspectiva de la guerra?

La pregunta por el carácter bélico del ciberespacio tiene ya dos décadas de debate. Rid (2013) argumentó que ninguna operación cibernética conocida satisface los tres criterios clausewitzianos de la guerra —violencia, instrumentalidad y carácter político atribuido— y que lo observado es sabotaje, espionaje y subversión potenciados por medios digitales. Kello (2017) replicó que esa conclusión, técnicamente correcta, oscurece el fenómeno relevante: un estado intermedio de "paz inestable" que erosiona el orden internacional sin cruzar el umbral de la guerra. Valeriano y Maness (2015) documentaron un patrón de contención: los Estados usan estas capacidades con moderación calculada, porque su valor coercitivo depende de no emplearlas de forma catastrófica.

La evidencia reciente respalda una lectura sintética. La operación contra la red satelital KA-SAT de Viasat, ejecutada el 24 de febrero de 2022 —día de la invasión rusa a Ucrania— mediante el *wiper* AcidRain, inutilizó al menos 27.000 módems y dejó fuera de servicio durante semanas 5.800 aerogeneradores en Alemania; fue atribuida oficialmente a Rusia por la Unión Europea, el Reino Unido y Estados Unidos el 10 de mayo de 2022 (CCDCOE, 2022). Es el ejemplo más nítido de una ciberoperación integrada a una campaña militar convencional: preparó el terreno, degradó comunicaciones y generó efectos transfronterizos no deseados sobre terceros Estados neutrales, lo que ilustra con precisión los dilemas jurídicos que plantea el uso de la fuerza en el ciberespacio (Llorens, 2017; García Vázquez, 2021). Pero también muestra los límites del instrumento: no decidió la campaña ni sustituyó al fuego.

Más inquietante para el análisis geopolítico es un fenómeno distinto: el preposicionamiento. Las campañas asociadas a los actores designados como *Volt Typhoon* y *Salt Typhoon* revelaron accesos persistentes en infraestructura crítica y en redes de telecomunicaciones de Estados Unidos y de otros países, sin objetivos de extracción inmediata evidentes (Congressional Research Service, 2025). Su lógica no es el ataque, sino la opción de ataque: la construcción anticipada de una capacidad que solo se activaría en una crisis futura. Esto altera la naturaleza del problema estratégico. La disuasión clásica supone capacidades visibles y umbrales claros; el preposicionamiento opera sobre lo invisi-

ble y genera un dilema de seguridad permanente, en el que cada actor debe asumir que sus redes ya están comprometidas.

A ello se suma la inteligencia artificial como acelerador del ciclo ofensivo. Las proyecciones para 2026 anticipan una carrera armamentística algorítmica, con automatización creciente del reconocimiento, la explotación de vulnerabilidades y la ingeniería social, y una correlativa automatización de la defensa (Google Cloud, 2025). El efecto neto no es necesariamente más ataques exitosos, sino una compresión drástica del tiempo para decidir.

El resultado es una conflictividad con reglas propias, que la Tabla 1 contrasta con la guerra interestatal clásica. No se trata de una guerra nueva, sino de una competencia estratégica continua, deliberadamente calibrada para permanecer bajo el umbral del artículo 2(4) de la Carta de las Naciones Unidas, donde el derecho internacional sigue aplicándose —así lo reconoce el consenso reflejado en el *Manual*

Tabla 1. Gramáticas comparadas del conflicto: guerra interestatal clásica y conflictividad ciberespacial.

Dimensión	Guerra interestatal clásica	Conflictividad en el ciberespacio
Umbral	Declaración formal o acto de fuerza reconocible bajo el artículo 2(4) de la Carta de la ONU.	Calibrada deliberadamente por debajo del umbral del uso de la fuerza y del ataque armado.
Temporalidad	Episódica: inicio, desarrollo y terminación identificables.	Persistente: competencia continua, sin estado final ni armisticio.
Atribución	Directa e inmediata; el autor suele ser evidente.	Técnica, lenta y probabilística; atribuir es una decisión política costosa.
Actores	Fuerzas armadas estatales, con cadena de mando definida.	Estados, proxies, grupos criminales, empresas tecnológicas e individuos.
Efecto buscado	Destrucción de capacidades y control del territorio.	Degradación, denegación, manipulación y, sobre todo, dependencia.
Terreno	Geografía física: dada, estable y de titularidad pública.	Infraestructura construida: reversible, deslocalizable y mayoritariamente privada.
Disuasión	Basada en capacidades visibles y umbrales explícitos.	Erosionada por la opacidad de las capacidades y el preposicionamiento.
Reversibilidad	Daño físico permanente y costoso de revertir.	Efectos con frecuencia reversibles, pero repetibles a muy bajo costo.

Nota. Elaboración propia a partir de Rid (2013), Valeriano y Maness (2015), Kello (2017), Schmitt (2017) y United States Joint Staff (2018).

de Tallin 2.0 (Schmitt, 2017)— pero donde su aplicación práctica se enfrenta al problema de la atribución.

La disputa por las reglas: gobernanza, fragmentación y modelos en competencia

Si el vector normativo es tan decisivo como el infraestructural, los foros donde se negocian las reglas son escenarios geopolíticos de pleno derecho, y el periodo 2024-2026 fue particularmente denso en ese frente.

El Grupo de Trabajo de Composición Abierta de las Naciones Unidas sobre seguridad en el uso de las tecnologías de la información concluyó su mandato el 11 de julio de 2025 con la adopción de un informe final por consenso, y dio paso a un **Mecanismo Global** de carácter permanente, cuya sesión organizativa debía celebrarse a más tardar en marzo de 2026 (Naciones Unidas, 2025). El acuerdo consolidó el Directorio Global de Puntos de Contacto y priorizó la implementación de las normas voluntarias ya existentes sobre la creación de otras nuevas —una señal clara de que el consenso alcanzable se agotó, por ahora, en el terreno declarativo. Paralelamente, el 25 de octubre de 2025 se abrió a la firma en Hanói la Convención de las Naciones Unidas contra la Ciberdelincuencia, suscrita ese día por 65 Estados, entre ellos Colombia, y que entrará en vigor noventa días después del depósito del cuadragésimo instrumento de ratificación (Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC], 2025).

Estos avances conviven con una fragmentación creciente. Tres modelos de ordenamiento compiten por definir el ciberespacio del futuro, y la elección entre ellos —o la negativa a elegir— constituye hoy una decisión de política exterior. El primero, de matriz estadounidense, privilegia la libertad de flujo de datos y la autorregulación del mercado. El segundo, de matriz china, articula la doctrina de la cibersoberanía: el ciberespacio como extensión del territorio nacional, sujeto a control estatal pleno sobre contenidos, datos e infraestructura (Vargas-Chaparro, 2022). El tercero, europeo, construye una tercera vía basada en derechos fundamentales y proyección regulatoria extraterritorial (Bradford, 2020).

Para una potencia media, la disyuntiva no es adherir a un bloque, sino evitar quedar atrapada en la infraestructura de uno y en la regulación de otro sin haberlo decidido.

El riesgo de esta competencia no es la victoria de un modelo, sino la consolidación de bloques tecnológicos incompatibles —el fenómeno descrito como *splinternet*—, con estándares, cadenas de suministro y regímenes de datos divergentes.

Para países que dependen simultáneamente de tecnología de ambos

polos, la fragmentación no es una abstracción: es un costo directo de transacción y una restricción a la autonomía.

Conviene, no obstante, evitar el determinismo. El Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones (2024) documenta un progreso agregado significativo: 139 países cuentan con equipos de respuesta a incidentes —frente a 109 en 2021—, 132 tienen estrategias nacionales y 177 regulan la protección de datos. La capacidad estatal se está difundiendo, de manera desigual pero real, y eso reduce el margen de las grandes potencias para imponer reglas por defecto.

Colombia: geopolítica cibernética de una potencia media

Colombia ofrece un caso analíticamente valioso porque combina una posición geográfica privilegiada con una dependencia tecnológica estructural. Su condición bioceánica se traduce, en el vector infraestructural, en aproximadamente diez sistemas de cable submarino activos y nueve puntos de aterrizaje distribuidos entre Buenaventura, Tolú, Cartagena, Puerto Colombia, Barranquilla, Parque Isla Salamanca, Santa Marta, San Andrés y Riohacha (Portafolio, 2023). Esa dotación, notable para la región, es a la vez activo estratégico y superficie de exposición: la conectividad internacional depende de pocas instalaciones costeras cuya protección involucra a autoridades marítimas, operadores privados y fuerzas militares, sin un régimen integrado de responsabilidad. La experiencia báltica sugiere que conviene cerrar esa brecha antes, y no después, del primer incidente.

En el plano de las amenazas, las cifras oficiales muestran una evolución favorable, pero requieren lectura cuidadosa. Colombia gestionó 1.427 incidentes cibernéticos en 2024 y 697 en 2025, una reducción del 48,84 %, en un periodo en el que el ColCERT amplió su capacidad de vigilancia de 31 a cerca de 1.300 entidades y logró por primera vez el monitoreo de infraestructura crítica en los 32 departamentos (Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC], 2026). El fraude concentró el 79,83 % de los casos del bienio, con el *phishing* (835 casos) y el acceso no autorizado a cuentas de correo (784 casos) como vectores dominantes. Ahora bien, una caída de incidentes gestionados en un contexto de expansión del perímetro de monitoreo admite dos lecturas: mejora real de la postura defensiva o cambio en los criterios de registro. El propio informe advierte un incremento de amenazas persistentes avanzadas sobre sectores estratégicos —energía, salud, defensa, transporte, finanzas y telecomunicaciones—, lo que sugiere sustitución de volumen por sofisticación. Geopolíticamente esa es la transición decisiva: del cibercrimen oportunista a la presencia de actores con patrocinio estatal.

En el vector normativo, el país ha construido una arquitectura institucional apreciable. Los documentos CONPES 3701 de 2011, 3854 de 2016 y 3995 de 2020 establecieron sucesivamente los marcos de ciberseguridad, gestión de riesgo y confianza digital (Departamento Nacional de Planeación, 2020); el Decreto 338 de 2022 definió la gobernanza de la seguridad digital (Presidencia de la República de Colombia, 2022); y la Estrategia Nacional de Seguridad Digital 2025-2027 (Presidencia de la República de Colombia, 2025) organiza la acción estatal en torno a cuatro objetivos: gobernanza, resiliencia nacional, talento y adecuación regulatoria. A ello se suman la adhesión al Convenio de Budapest mediante la Ley 1928 de 2018 (Congreso de la República de Colombia, 2018), la firma de la Convención de Hanói en 2025 y, particularmente relevante para el análisis geopolítico, la publicación de la Posición Nacional sobre la Aplicación del Derecho Internacional al Ciberespacio (Ministerio de Relaciones Exteriores de Colombia, 2025), que sitúa al país entre el grupo todavía reducido de Estados que han fijado públicamente su interpretación jurídica del dominio. El desafío, señalado desde hace años por la literatura especializada, no está en la producción normativa sino en su implementación efectiva y en la articulación entre instrumentos de política, capacidades técnicas y decisión estratégica (Saavedra & Parraguez, 2018). Publicar una posición nacional no es un gesto declarativo: es un acto de ciberdiplomacia que aumenta la previsibilidad y reduce el margen de ambigüedad (Patiño Orozco, 2019; Riordan, 2019).

Las brechas persisten en tres frentes. La dependencia tecnológica: casi todo el hardware, el software de base y los servicios de nube que sostienen la infraestructura crítica nacional son de origen extranjero, lo que limita la autonomía en detección, respuesta y análisis forense (Cabuya-Padilla et al., 2022). El talento: la demanda de perfiles especializados supera con amplitud la oferta formativa y el sector público compite en desventaja por retenerlos (Cujabante Villamil et al., 2020). Y la capacidad de anticipación, menos discutida: la producción científica regional en modelamiento y simulación aplicados a la ciberdefensa es limitada y las herramientas propias para explorar escenarios de crisis son incipientes (Cabuya-Padilla & Castañeda-Marroquín, 2024). Los modelos de propagación de ciberataques sobre infraestructura marítima (Cabuya-Padilla et al., 2025b) y los ejercicios híbridos de mesa apoyados en simulación matemática (Cabuya-Padilla et al., 2025a) apuntan en esa dirección: permiten ensayar decisiones estratégicas antes de que la crisis obligue a improvisarlas.

Frente a estas brechas, Colombia dispone de márgenes de maniobra

reales. En lo regional, su trayectoria institucional le permite aspirar a referente en política pública de seguridad digital y en la cooperación operativa entre CSIRT nacionales. En lo multilateral, su participación en el Mecanismo Global y su condición de firmante temprano de la Convención de Hanói le dan legitimidad para promover una agenda de creación de capacidades útil al conjunto de las potencias medias. En lo interno, la cooperación cívico-militar —rasgo distintivo del modelo colombiano (Cujabante Villamil et al., 2020)— es un activo replicable, siempre que se acompañe de salvaguardas democráticas explícitas sobre el uso de capacidades cibernéticas.

Reflexiones finales

El ciberespacio no derogó la geografía: produjo una geografía adicional, superpuesta a la física y regida por lógicas propias. Bajo la retórica de la nube persisten cables, puntos de aterrizaje, jurisdicciones y cadenas de suministro cuya distribución es tan desigual —y tan políticamente significativa— como la de los estrechos marítimos que ocuparon a la geopolítica clásica. Reconocer esa materialidad es la primera condición de cualquier estrategia seria de soberanía digital.

A la pregunta que da título a este número, la respuesta que aquí se ha sostenido es negativa en la forma y afirmativa en el fondo. El ciberespacio no ha producido una guerra nueva: las operaciones cibernéticas, por sí solas, no han decidido ningún conflicto ni han sustituido al empleo de la fuerza. Pero sí ha producido una nueva perspectiva sobre la guerra, en tres sentidos precisos. Primero, ha extendido la competencia estratégica a un tiempo continuo, sin distinción nítida entre paz y guerra. Segundo, ha desplazado el centro de gravedad del conflicto desde la destrucción hacia la dependencia: hoy importa menos lo que un adversario puede destruir que aquello de lo cual puede privarnos. Tercero, ha convertido la ambigüedad en un recurso deliberado, lo que erosiona los mecanismos de disuasión construidos sobre la claridad de umbrales y atribuciones.

Para una potencia media como Colombia, esto define un margen de acción específico. No puede competir en acumulación de capacidades ofensivas ni aspirar a la autosuficiencia tecnológica en el horizonte previsible, pero sí en tres terrenos donde la asimetría de recursos pesa menos. En resiliencia, con protección integrada de sus infraestructuras críticas cibernéticas y atención prioritaria a los puntos de aterrizaje de cable submarino, hoy en zona gris de responsabilidad. En diplomacia, con voz activa en el Mecanismo Global y posiciones regionales que eleven el costo político de las operaciones contra Estados pequeños. Y en anticipación, invirtiendo en modelamiento, simulación y juegos de gue-

rra que permitan probar decisiones estratégicas antes de que la crisis las imponga.

La lección de fondo es que la geopolítica del ciberespacio no premia la fuerza, sino la comprensión. En un dominio donde las capacidades se deprecian con cada parche y las alianzas se reconfiguran con cada cambio tecnológico, la ventaja duradera pertenece a quien entiende mejor el sistema que habita. Para los Estados que no pueden dominar el terreno, entenderlo es la forma más realista de ejercer poder sobre él.

Referencias

Barlow, J. P. (1996). *A declaration of the independence of cyberspace*. Electronic Frontier Foundation. https://www.eff.org/es/cyberspace-independence

Bartolomé, M. (2023). *Ciberseguridad, geopolítica y relaciones internacionales* (Global Strategy Report 5/2023). Global Strategy, Universidad de Granada.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Cabuya-Padilla, D. E., Alvarado Carvajal, C. F., Carrascal Ortiz, R. A., Escandón Bernal, S. P., Riola Rodríguez, J. M., & Fajardo-Toro, C. H. (2022). Ciberseguridad y ciberdefensa marítima: análisis bibliométrico años 1990-2021. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (E49), 197-210.

Cabuya-Padilla, D. E., & Castañeda-Marroquín, C. A. (2024). Marco de referencia para el modelamiento y simulación de la ciberdefensa marítima - MARCIM: estado del arte y metodología. *DYNA*, 91(231), 169-179. https://doi.org/10.15446/dyna.v91n231.109774

Cabuya-Padilla, D. E., Díaz-López, D., & Castañeda-Marroquín, C. (2025a). Hybrid tabletop exercise (TTX) based on a mathematical simulation-based model for the maritime sector. En *Actas de las X Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2025)* (pp. 37-44). Universidad de Zaragoza.

Cabuya-Padilla, D. E., Díaz-López, D., Martínez-Páez, J., Hernández, L., & Castañeda-Marroquín, C. (2025b). SERDUX-MARCIM: Maritime cyberattack simulation using dynamic modeling, compartmental models in epidemiology and agent-based modeling. *International Journal of Information Security*, 24(3), 122. https://doi.org/10.1007/s10207-025-00985-6

CCDCOE. (2022). *Viasat KA-SAT attack (2022)*. Cyber Law Toolkit, NATO Cooperative Cyber Defence Centre of Excellence. https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_(2022)

Congressional Research Service. (2025). *Salt Typhoon hacks of telecommunications companies and federal response implications* (CRS Report IF12798). Library of Congress.

Congreso de la República de Colombia. (2018). *Ley 1928 de 2018, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado en Budapest el 23 de noviembre de 2001*. Diario Oficial No. 50.664.

Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible

modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova*, 18(30), 357-377. https://doi.org/10.21830/19006586.588

Departamento Nacional de Planeación. (2020). *Documento CONPES 3995: Política nacional de confianza y seguridad digital*. Consejo Nacional de Política Económica y Social.

García Vázquez, B. (2021). El derecho internacional frente a los nuevos medios y espacios en que desarrollar la guerra: la ciberguerra. *Revista Chilena de Derecho y Tecnología*, 10(2), 43-68. https://doi.org/10.5354/0719-2584.2021.57077

García-Jiménez, A., Beltrán Orenes, P., & Núñez Puente, S. (2010). Una aproximación al concepto de frontera virtual. Identidades y espacios de comunicación. *Revista Latina de Comunicación Social*, (65), 214-221. https://doi.org/10.4185/RLCS-2010-894-214-221

Google Cloud. (2025). *Cybersecurity forecast 2026*. Google Cloud Security.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Llorens, M. P. (2017). Los desafíos del uso de la fuerza en el ciberespacio. *Anuario Mexicano de Derecho Internacional*, 17, 785-816. https://doi.org/10.22201/iij.24487872e.2017.17.11052

Mackinder, H. J. (1904). The geographical pivot of history. *The Geographical Journal*, 23(4), 421-437. https://doi.org/10.2307/1775498

Mata-Sánchez, G. (2023). Relaciones internacionales y geopolítica: conflicto y poder en el ciberespacio. *Relações Internacionais no Mundo Atual*, 3(41).

Ministerio de Relaciones Exteriores de Colombia. (2025). *Posición nacional de Colombia sobre la aplicación del derecho internacional al ciberespacio*. Gobierno de Colombia.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2026, 2 de abril). *Colombia fortalece su soberanía digital: durante 2025 logró reducir en un 48 % los incidentes cibernéticos*. MinTIC. https://www.mintic.gov.co/portal/715/w3-article-433511.html

Naciones Unidas. (2025). *Final report of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025*. Asamblea General de las Naciones Unidas.

Nye, J. S. (2011). *The future of power*. PublicAffairs.

Oficina de las Naciones Unidas contra la Droga y el Delito. (2025). *Convención de las Naciones Unidas contra la Ciberdelincuencia*. UNODC.

Organización del Tratado del Atlántico Norte. (2025). *Baltic Sentry: NATO steps up patrols in the Baltic Sea to safeguard critical undersea infrastructure*. Allied Maritime Command. https://mc.nato.int/media-centre/news/2025

Patiño Orozco, G. A. (2019). El sistema internacional cibernético: elementos de análisis. *Oasis*, (30), 163-186. https://doi.org/10.18601/16577558.n30.10

Perafán Del Campo, E. A., Polo Alvis, S., Sánchez Acevedo, M. E., & Miranda Aguirre, C. (2021). Estado y soberanía en el ciberespacio. *Via Inveniendi et Iudicandi*, 16(1). https://doi.org/10.15332/19090528.6480

Portafolio. (2023, 6 de marzo). *Así está el mapa de los cables submarinos que llegan al país*. Portafolio. https://www.portafolio.co/innovacion/cables-submarinos-este-es-el-panorama-en-colombia-579498

Prado, B. (2018). Geopolítica del ciberespacio: hacia el Heartland cibernético. *Revista Geografía y Sistemas de Información Geográfica (GeoSIG)*, 10, 1-13.

Presidencia de la República de Colombia. (2022). *Decreto 338 de 2022, por el cual se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital*. Diario Oficial No. 51.973.

Presidencia de la República de Colombia. (2025). *Estrategia nacional de seguridad digital de Colombia 2025-2027*. Gobierno de Colombia.

Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.

Riordan, S. (2019). *Cyberdiplomacy: Managing security and governance online*. Polity Press.

Rivas, S. M. (2021). El ciberespacio como zona de control geopolítico y papel de las potencias por la supremacía cibernética: China y Estados Unidos. *Revista Relaciones Internacionales*, 3(1), 89-107.

Saavedra, B., & Parraguez, L. (2018). La ciberseguridad: análisis político y estratégico. *Fuerzas Armadas*, (243), 44-51. https://doi.org/10.25062/0120-0631.737

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations* (2.ª ed.). Cambridge University Press.

Unión Internacional de Telecomunicaciones. (2024). *Global cybersecurity index 2024*. ITU Publications.

Unión Internacional de Telecomunicaciones. (2025). *Submarine cable resilience*. ITU. https://www.itu.int/en/mediacentre/backgrounders/Pages/submarine-cable-resilience.aspx

United States Joint Staff. (2018). *Cyberspace operations* (Joint Publication 3-12). Department of Defense.

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press.

Vargas-Chaparro, N. E. (2022). La cibergeopolítica de China: un interés estratégico de Estado. *Estudios en Seguridad y Defensa*, 17(33), 201-222. https://doi.org/10.25062/1900-8325.328

Voo, J., Hemani, I., & Cassidy, D. (2022). *National cyber power index 2022*. Belfer Center for Science and International Affairs, Harvard Kennedy School.

Diego Edison Cabuya Padilla. *Capitán de Fragata de la Armada de Colombia y Doctor en Ciencias del Mar de la Escuela Naval de Cadetes "Almirante Padilla", con investigación doctoral en ciberseguridad y ciberdefensa marítima. Magíster en Ciberseguridad y Ciberdefensa, en Gestión de la Información (Universitat Politècnica de València, España) y en Logística; ingeniero electrónico y profesional en ciencias navales. Ha servido en el Comando Conjunto Cibernético de las Fuerzas Militares y fue visiting scholar Fulbright en el William J. Perry Center for Hemispheric Defense Studies (National Defense University). Actualmente es Director de Investigación de la Academia Naval de Estudios Estratégicos. ORCID: 0000-0001-5338-9943.*

La guerra sin declaración

Cómo la tecnología redefine el poder antes del primer disparo.

DOI: 10.29236/sistemas.n180a8

Resumen

La geopolítica del siglo XXI ya no se decide únicamente en tratados o en despliegues visibles de tropas, sino en el control silencioso de semiconductores, satélites, algoritmos y percepciones. Este artículo sostiene que la "nueva guerra" no lo es en su naturaleza —dominar la voluntad del adversario sigue siendo el objetivo de siempre—, sino en su arquitectura: hoy opera de forma multidominio, simultánea y frecuentemente indetectable hasta el momento mismo de su ejecución. Se examina la carrera tecnológica entre bloques —semiconductores e inteligencia artificial— como el verdadero campo de batalla previo al conflicto armado declarado, y se conecta cada uno de los seis dominios reconocidos de la guerra —terrestre, marítimo, aéreo, espacial, cibernético y cognitivo— con el motor tecnológico específico que hoy lo transforma. Se ilustra con la Operación Resolución Absoluta, ejecutada en Venezuela en enero de 2026, como caso empírico de sincronización simultánea de los seis dominios en una sola acción de pocas horas. Se concluye que la hegemonía ya no se conquista: se administra tecnológicamente, y que las naciones sin postura estratégica propia corren el riesgo de convertirse en terreno de disputa ajena, y no en actores de su propia seguridad.

Palabras clave

Geopolítica tecnológica; guerra multidominio; hegemonía digital; dominio cognitivo; ciberdefensa.

Introducción

Durante siglos, la geopolítica se explicó a partir de variables tangibles: territorio, población, recursos naturales y capacidad de movilización militar. En el siglo XXI esa ecuación ha cambiado de naturaleza sin cambiar de propósito. El poder sigue buscando lo mismo de siempre —imponer voluntad, proteger intereses, sostener hegemonía—, pero el terreno donde se disputa ya no es exclusivamente físico: es el control de semiconductores, redes satelitales, algoritmos de inteligencia artificial y, en última instancia, de la percepción humana.

Este artículo parte de una pregunta incómoda para la doctrina clásica de la guerra: ¿sigue siendo útil distinguir tajantemente entre "guerra" y "paz" cuando el control sobre un adversario —o sobre un aliado— puede ejercerse de forma permanente, silenciosa y tecnológica, sin que medie jamás una declaración formal de hostilidades? La carrera tecnológica entre bloques —Estados Unidos, China, la Unión Europea— no es un telón de fondo económico de las tensiones internacionales actuales: es, en sí misma, la disputa central por la hegemonía del siglo XXI.

La tesis central de este artículo es que la guerra contemporánea ha dejado de tener un inicio y un final claramente delimitados, para convertirse en un continuo de competencia tecnológica que se activa —de forma cinética y visible— solo cuando el desequilibrio de capacidades lo permite. Se desarrollan cuatro niveles de análisis, de lo macro a lo específico: primero, la carrera estructural por el control de la infraestructura tecnológica crítica entre bloques; segundo, el motor tecnológico que hoy transforma cada uno de los seis dominios reconocidos de la guerra —terrestre, marítimo, aéreo, espacial, cibernético y cognitivo—; tercero, la traducción operativa de ese marco en un caso real y reciente, la Operación Resolución Absoluta en Venezuela; y cuarto, una profundización del dominio cognitivo, que no es nuevo en su esencia pero sí en su escala y velocidad de ejecución. Se cierra con una reflexión sobre el lugar de naciones intermedias como Colombia en este nuevo tablero.

1. La nueva materia prima del poder: semiconductores, inteligencia artificial y bloques

En 2026 la soberanía de una nación ya no se mide solamente por sus reservas de crudo o por su capacidad de movilización militar convencional, sino también por su acceso a semiconductores avanzados (Yılmaz, 2026). Estos componentes son de naturaleza dual: sostienen tanto la economía digital como la precisión de los sistemas

de armas modernos y la eficacia de la guerra electrónica. La industria de los chips, que durante décadas fue percibida como un triunfo silencioso de la globalización, se ha revelado hoy como su vulnerabilidad más evidente: la fabricación de los nodos más avanzados se concentra en un puñado de instalaciones, en su mayoría en Taiwán, bajo presión geopolítica creciente.

Peters documenta cómo la Ley CHIPS and Science de Estados Unidos representa una ruptura deliberada respecto al libre mercado neoliberal, en favor de una estrategia de ciencia y tecnología dirigida y sostenida desde el nivel federal, con el objetivo explícito de reducir la dependencia de una cadena de suministro internacional fácilmente disruptible (2023). China, por su parte, no ha permanecido pasiva, impulsa arquitecturas abiertas como RISC-V[1] para reducir su dependencia de la propiedad intelectual estadounidense (ARM, x86), y compite no por frontera tecnológica absoluta, sino por velocidad y costo de despliegue. En el plano regional, Ruck muestra cómo la Unión Europea reorganiza sus propias cadenas de valor en semiconductores mediante lo que denomina un "geoeconomic fix", evidenciando que la disputa ya no es bilateral, sino de bloques que compiten por autonomía tecnológica (2026).

A esta carrera se suma la disputa por la inteligencia artificial, que Yılmaz (2026) caracteriza como una nueva dimensión del poder geopolítico que trasciende lo económico. La IA influye directamente en cómo los Estados proyectan autoridad, regulan la innovación y negocian normas globales. El estudio identifica tres paradigmas de gobernanza en competencia —el modelo liberal orientado a la innovación (Estados Unidos), el modelo autoritario de control estatal (China) y el modelo regulatorio orientado a la ética (Unión Europea)— y advierte que la IA intensifica asimetrías de poder, generando "jerarquías algorítmicas" que refuerzan la dependencia digital, particularmente en el Sur Global (Yılmaz, 2026).

Conviene precisar, sin embargo, que esta tercera posición europea es de naturaleza distinta a las otras dos: mientras Estados Unidos y China compiten de forma directa por volumen de inversión y capacidad de cómputo —los cientos de miles de millones de dólares referidos más arriba—, la Unión Europea no dispone de un competidor propio a esa escala de capital, y ejerce su influencia geopolítica en la IA no como tercer polo de inversión, sino como poder regulatorio: sus normas, como la Ley de IA europea, tienden a convertirse en estándar

[1] *Reduced Instruction Set Computer* ("Computador de Conjunto de Instrucciones Reducido"). Es una filosofía de diseño de procesadores que usa instrucciones simples y pocas, en lugar de instrucciones complejas y numerosas (el enfoque contrario se llama CISC, usado por ejemplo en x86 de Intel). La ventaja de RISC es que los chips resultan más simples, rápidos, eficientes en consumo de energía y más fáciles de personalizar.

de facto global por el llamado "efecto Bruselas", dado que muchas empresas prefieren cumplir la norma más exigente una sola vez para todo el mercado mundial.

Akram et al. (2025) refuerzan el punto estructural al mostrar cómo los clústeres de innovación en inteligencia artificial —Silicon Valley, Shenzhen, Tel Aviv— funcionan hoy como nuevos centros de influencia geopolítica, y cómo la soberanía de datos se ha convertido en una dimensión crítica de la seguridad nacional y de la palanca diplomática de los Estados. El resultado estructural es la formación de bloques tecnológicos de facto, alianzas de suministro, de infraestructura y de gobernanza que se parecen cada vez más a los bloques geopolíticos tradicionales, pero cuya moneda de cambio ya no es únicamente territorio o tratados militares, sino acceso garantizado a chips, datos y capacidad computacional.

2. Los seis dominios de la guerra y su motor tecnológico

La doctrina militar contemporánea reconoce seis dominios de la guerra: terrestre, marítimo, aéreo, espacial, cibernético y cognitivo. Lo que este artículo sostiene es que, si bien los seis han existido conceptualmente por décadas —los tres primeros desde siempre, el espacial desde la Guerra Fría, el cibernético desde finales del siglo XX y el cognitivo desde que existe la guerra misma—, hoy cada uno está siendo transformado por un motor tecnológico específico, y es precisamente esa transformación simultánea la que redefine el carácter de la guerra contemporánea.

En el dominio terrestre, el motor son los vehículos no tripulados de combate y reconocimiento, los exoesqueletos que amplían la capacidad física del combatiente, y los sistemas C4ISR de campo que integran mando, control, comunicaciones e inteligencia en tiempo real hasta el nivel de escuadra, junto con munición de precisión guiada que reduce drásticamente el margen de error operativo. En el dominio marítimo, la transformación llega de la mano de drones navales y submarinos autónomos, sensores de fondo marino para vigilancia persistente, y una nueva forma de vulnerabilidad estratégica: la guerra de cables submarinos, por donde transita más del noventa por ciento del tráfico de datos intercontinental y que hoy constituye un objetivo de sabotaje de alto valor, tan crítico como cualquier estrecho marítimo tradicional.

El dominio aéreo se transforma con la aviación de quinta y sexta generación, los enjambres de drones capaces de saturar defensas antiaéreas mediante numerosidad más que mediante sofisticación individual, y la guerra electrónica aérea que ciega sensores y radares antes de que el adversario perciba la amenaza. El dominio espacial depende hoy de constelaciones de satélites de observación e inteligencia, de la

capacidad de mando integrada como la que ejerce el Comando Espacial estadounidense (SPACECOM), y de una competencia creciente por capacidades anti-satélite que podrían inutilizar en minutos la infraestructura orbital de un adversario, incluyendo constelaciones comerciales de conectividad masiva que ya se emplean con fines militares.

El dominio cibernético, sostenido por comandos especializados como el Comando Cibernético de Estados Unidos (CYBERCOM), ha probado su capacidad de sabotear infraestructura crítica —energía, comunicaciones, sistemas financieros— sin disparar un solo proyectil, y hoy incorpora inteligencia artificial ofensiva capaz de identificar y explotar vulnerabilidades a una velocidad que ningún equipo humano de ciberdefensa puede igualar. Finalmente, el dominio cognitivo, que se desarrolla con mayor profundidad en la sección tercera de este artículo, encuentra en la inteligencia artificial generativa, los deepfakes y el targeting psicográfico su motor de transformación: la capacidad de moldear percepciones de forma masiva, personalizada y en tiempo real.

La implicación central de este marco es que ningún conflicto contemporáneo de relevancia estratégica se libra hoy en un solo dominio. La ventaja decisiva pertenece a quien logra sincronizar los seis de forma simultánea, no a quien es superior en uno de ellos de manera aislada. El caso que se desarrolla a continuación —la Operación Resolución Absoluta en Venezuela— constituye, hasta la fecha, el ejemplo más completo y mejor documentado de esta sincronización multidominio ejecutada en pocas horas.

3. Guerra multidominio en tiempo real: el caso de la Operación Resolución Absoluta en Venezuela

Si el nivel anterior describe la estructura, este segundo nivel ofrece evidencia empírica de su traducción operativa. La madrugada del 3 de enero de 2026, fuerzas estadounidenses ejecutaron en Caracas la Operación Resolución Absoluta, con el objetivo de capturar con vida a Nicolás Maduro y Cilia Flores. El análisis de esta operación, permite sostener un argumento disruptivo: no se trató de una operación militar convencional “apoyada” por tecnología, sino de una operación en la que la tecnología fue la operación misma, y donde la acción cinética final —el asalto físico— fue apenas el último eslabón de una cadena multidominio ya consumada.

La secuencia técnica es reveladora. Durante meses, la inteligencia estadounidense combinó inteligencia de señales (SIGINT), inteligencia de imágenes (IMINT) e inteligencia humana (HUMINT) para mapear en detalle la red de seguridad, rutinas y entorno inmediato del objetivo. En el momento de ejecución, el SPACECOM y el CYBER-

COM superpusieron efectos coordinados para abrir un corredor seguro de aproximación; los sistemas de defensa antiaérea de origen ruso y los radares de origen chino fueron neutralizados mediante guerra electrónica antes de que las aeronaves entraran en su alcance; y un corte cibernético selectivo de energía facilitó el desplazamiento terrestre de las fuerzas de extracción. Una flota de drones —inteligencia, vigilancia y reconocimiento (ISR), armados (Reaper) y furtivos— sostuvo monitoreo casi permanente sobre el objetivo durante semanas, mientras la guía satelital dirigía en tiempo real a las tropas en tierra durante el asalto final.

Este caso ilustra con precisión la tesis del artículo: los dominios espacial, cibernético, los elementos de inteligencia y cinéticos no actuaron de forma secuencial, sino simultánea e integrada, en una ventana operativa de apenas unas horas. La superioridad no residió en el número de tropas desplegadas, sino en el control absoluto de la información y de la infraestructura crítica del adversario antes de que este pudiera siquiera reaccionar. Es, en ese sentido, el ejemplo más nítido disponible hasta la fecha de cómo la carrera tecnológica descrita en la sección anterior se convierte en capacidad de intervención real.

4. El dominio cognitivo: lo antiguo con motor nuevo

El tercer nivel de análisis corresponde al dominio cognitivo, que conviene precisar no es una novedad conceptual: la guerra psicológica y la disputa por la percepción del adversario y de la propia población han existido desde la misma génesis de la guerra. Lo verdaderamente nuevo es la escala, la velocidad y la precisión de segmentación que la tecnología actual permite. Deppe y Schaal (2024) documentan cómo la OTAN, a través de su concepto exploratorio de guerra cognitiva (NATO ACT), define este dominio como el uso de tácticas, técnicas y herramientas habilitadas por tecnología para influir en la toma de decisiones humanas a nivel individual y social, alineando el comportamiento del adversario con los objetivos políticos, sociales, económicos o militares propios.

Miller (2023) profundiza en la dimensión ética del fenómeno, advirtiendo que la manipulación cognitiva mediada por tecnología plantea desafíos normativos distintos a los de la propaganda tradicional, precisamente por su capacidad de operar de forma personalizada y a gran escala mediante inteligencia artificial generativa y algoritmos de recomendación. En el caso venezolano, este dominio se activó en dos capas diferenciadas: una capa operativa, orientada a generar parálisis psicológica en las fuerzas de custodia antes y durante el asalto; y una capa narrativa posterior, en la que el aparato comunicacional oficialista caracterizó lo ocurrido como una "guerra cognitiva imperial" contra el pueblo venezolano, mientras la Ca-

sa Blanca amplificó testimonios virales de la propia operación como demostración de poder disuasivo hacia la región. Ambas narrativas, cabe subrayarlo, son actores interesados en la disputa, no fuentes neutrales, lo cual confirma que el dominio cognitivo permanece activo mucho después de que cesa la acción cinética.

5. Colombia y la periferia tecnológica

El cierre analítico exige una pregunta incómoda para naciones intermedias como Colombia: en este nuevo tablero, ¿somos actores o somos terreno? La evidencia sugiere que, sin una postura estratégica propia, países como el nuestro corren el riesgo de convertirse en espacio de disputa ajena antes que en sujetos activos de su propia seguridad. Esto exige incorporar explícitamente los espacios comunes de la seguridad —el marítimo, el espacial y el ciberespacio— como ámbitos de especial interés dentro de la arquitectura de seguridad nacional, con estrategias transversales que hoy, en buena medida, siguen pendientes de institucionalización plena.

La lección de la Operación Resolución Absoluta para una nación como Colombia no es únicamente táctica, sino conceptual: la superioridad ya no se mide en número de tropas o en plataformas convencionales, sino en la capacidad de un Estado para comprender, defender y eventualmente disputar el control de sus propios dominios espacial y cibernético. Ningún Sistema de Seguridad Nacional del siglo XXI puede considerarse completo si no integra lo ciber y lo espacial como ámbitos operativos propios, y no simplemente como anexos tecnológicos de los dominios tradicionales.

Conclusiones

La guerra contemporánea ya no se declara; ocurre porque todo el desequilibrio tecnológico entre las partes permite que suceda tan rápidamente que comienza mucho antes de que el mundo sepa que está en problemas. La hegemonía global ya no se trata simplemente de ocupación territorial, sino que se gestiona constantemente mediante el control de infraestructuras críticas (semiconductores, satélites, redes) y la capacidad de operar en dominios espaciales, cibernéticos y cognitivos simultáneamente, integrando en cada uno de ellos inteligencia de múltiples fuentes (SIGINT, IMINT, HUMINT) que hace posible la sincronización.

El caso de la Operación Resolución Absoluta confirma empíricamente esta tesis. La tecnología no acompañó la operación militar, la constituyó. Y el dominio cognitivo, lejos de ser una novedad, demuestra que la naturaleza de la guerra —disputar la voluntad del adversario— permanece intacta; lo que cambia es la velocidad, el alcance y la precisión con que hoy puede ejercerse.

Para países intermedios como Colombia, la conclusión es tanto una advertencia como una hoja de ruta.

La elección no es entre la paz y la guerra; se requiere que desarrollemos nuestra propia postura tecnológica y doctrinal, o que aceptemos que nuestro país está a punto de convertirse en un campo de batalla para disputas entre terceros. La geopolítica de las tecnologías de la información no es un asunto exclusivo de las grandes potencias, sino que es una condición de existencia para cualquier estado que quiera determinar su propio destino estratégico.

Referencias

Akram, S., Shahid, M., & Tunio, H. (2025). The Geopolitics of AI: Analyzing the Impact of Artificial Intelligence on Global Power Dynamics and International Relations. *Review Journal of Social Psychology & Social Works*, 282-300.

Deppe, C., & Schaal, G. (2024). Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. *Frontiers in Big Data*.

Miller, S. (2023). Cognitive warfare: an ethical analysis. *Ethics and Information Technology* , 1-10.

Ruck, J. (2026). A Geoeconomic Fix? European Industrial Policy on Semiconductors Amidst Global Competition. *JCMS: Journal of Common Market Studies*, 742-761.

Yılmaz, C. (2026). The Geopolitics of Artificial Intelligence Power, Regulation, and Global Governance. *Journal of Academic Social Studies*, 39-70.

Peters, M. (2023). Semiconductors, geopolitics and technological rivalry: The US CHIPS & Science Act, 2022. *Educational Philosophy and Theory*, 1642-1646.

Fabricio Cabrera Ortiz *es general de la reserva del Ejército Nacional de Colombia, doctor en Seguridad Internacional, consultor en seguridad y defensa, Presidente de la Junta Directiva del Consejo de Generales de la Reserva del Ejército Nacional (CGREN) y Asesor Estratégico del Centro de Pensamiento y Obsevación Estratégica (CEPOE).*

Conectar los marcos internacionales, coordinar la respuesta:

una hoja de ruta para el fortalecimiento de los CSIRT en América Latina

DOI: 10.29236/sistemas.n180a9

Resumen

La respuesta a incidentes cibernéticos requiere capacidades técnicas, responsabilidades institucionales claras y recursos que permitan sostener la operación. Para América Latina, uno de los desafíos consiste en traducir los marcos internacionales disponibles en decisiones acordes con las necesidades y condiciones de cada país. Este artículo examina, mediante una revisión documental, las aportaciones de la Unión Internacional de Telecomunicaciones, el Global Forum on Cyber Expertise, FIRST, NIST, la Open CSIRT Foundation, ENISA y la Organización de los Estados Americanos al establecimiento, la operación y la evaluación de los equipos de respuesta a incidentes de seguridad informática (CSIRT). El análisis distingue las funciones de estos instrumentos y propone una articulación que conecta mandato, comunidad atendida, servicios, gestión del riesgo, madurez y sostenibilidad. A partir de esta lectura, se plantea una hoja de ruta organizada en tres fases: mandato y diagnóstico; servicios y operación; y madurez, cooperación y aprendizaje. La propuesta constituye una orientación adaptable que requiere diagnóstico y validación en cada contexto. Se sostiene que la utilidad de los marcos debe comprobarse mediante procedimientos ejecutables, ejercicios, registros y seguimiento de mejoras. Su contribución reside en facilitar que el conocimiento técnico se convierta en una respuesta coordinada, verificable y sostenible.

Palabras claves

CSIRT; respuesta a incidentes; gobernanza; madurez; América Latina.

Introducción

La gestión de incidentes cibernéticos plantea una pregunta que resulta familiar para quienes diseñan, administran o protegen sistemas informáticos: ¿cómo convertir una recomendación general en una capacidad que funcione bajo presión? En el ámbito de la práctica un procedimiento adquiere valor cuando puede ejecutarse con los recursos disponibles y producir resultados verificables. En la respuesta a incidentes ocurre algo semejante. La existencia de una guía, una plataforma o un equipo formalmente constituido es un punto de partida, su éxito depende de cómo se articulan las personas, los procesos y las decisiones que permiten atender una afectación real (Killcrece et al., 2003).

Este artículo examina los principales marcos internacionales relacionados con el establecimiento, la operación y la evaluación de Equipos de Respuesta a Incidentes de Seguridad Informática, conocidos como CSIRT. El propósito es identificar sus aportaciones y discutir cómo pueden orientar el desarrollo de capacidades en América Latina. Para ello, se realiza una revisión documental de instrumentos publicados por la Unión Internacional de Telecomunicaciones (ITU), el Global Forum on Cyber Expertise (GFCE), FIRST, la Agencia de la Unión Europea para la Ciberseguridad (ENISA), la Open CSIRT Foundation, el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) y la Organización de los Estados Americanos (OEA).

La selección responde a la complementariedad de estos instrumentos. Algunos orientan la creación y el respaldo institucional de una capacidad nacional, otros permiten organizar servicios, integrar la respuesta a la gestión del riesgo o evaluar la madurez de un equipo (Ethembabaoglu,2026). Esta diversidad importa porque los problemas de implementación también son distintos: definir quién coordina un incidente no equivale a seleccionar una herramienta de monitoreo. Y disponer de especialistas no garantiza que existan procedimientos para compartir información o autorizar medidas de contención.

La revisión se organiza alrededor de cuatro preguntas: 1) ¿Qué problema busca resolver cada marco? 2) ¿A qué tipo de organización o equipo se dirige? 3) ¿Qué decisiones permite orientar? 4) ¿Qué ajustes requiere su aplicación en América Latina? Estas preguntas permiten examinar la utilidad de los instrumentos sin asumir que todos son equivalentes. Un catálogo de servicios, un modelo de madurez y una guía para establecer un CSIRT cumplen funciones relacionadas,

aunque diferentes. Su adopción conjunta exige comprender esas diferencias y definir una secuencia de aplicación.

También, es necesario precisar la unidad a la que se aplican las recomendaciones. Un CSIRT nacional puede ejercer funciones de coordinación entre instituciones, uno gubernamental puede concentrarse en entidades de la administración pública y uno sectorial puede atender necesidades compartidas por operadores de una industria. En cada caso cambia la comunidad atendida, esta delimitación determina qué reportes recibe el equipo, qué servicios ofrece y cuáles son los límites de su responsabilidad (Alghamdi, 2020).

Desde esta perspectiva, el artículo propone una lectura de los marcos orientada a decisiones institucionales y operativas. Para los profesionales esto implica relacionar cada recomendación con una necesidad concreta: establecer un canal de reporte, clasificar incidentes, documentar un procedimiento, verificar contactos o evaluar la capacidad de recuperación. Para los responsables de política pública, implica vincular esas tareas con atribuciones, presupuesto y mecanismos de coordinación.

El análisis no presenta una medición original de la madurez de los países latinoamericanos. Las recomendaciones que se desarrollan constituyen una propuesta de adaptación derivada de las fuentes examinadas. Su aplicación requiere un diagnóstico del contexto nacional o sectorial, así como validación mediante ejercicios y revisión de resultados. Y se destaca que la pertinencia de un marco debe juzgarse por su contribución a resolver problemas identificados, considerando los recursos y las responsabilidades de quienes lo utilizarán.

1. Por qué la respuesta es una cuestión de gobernanza

Cuando se identifica una intrusión, la atención suele concentrarse en las preguntas técnicas: cómo ingresó el atacante, qué sistemas comprometió y qué acciones permitirían contenerlo. Son preguntas indispensables. Sin embargo, conforme el incidente afecta servicios, proveedores o instituciones adicionales, aparecen otras decisiones igualmente relevantes: quién puede desconectar un sistema, quién informa a las entidades afectadas, qué información se comparte y qué autoridad determina cuándo debe escalarse la respuesta. La gobernanza se hace visible precisamente en estas decisiones (Kazeem, 2026).

Para comprender su importancia, pensemos en un escenario hipotético. Un proveedor de servicios digitales detecta actividad maliciosa en una plataforma utilizada por varias instituciones públicas. Su equipo técnico identifica indicios de compromiso, pero desconoce si puede comunicar detalles a todos los

clientes. Una entidad decide suspender conexiones, otra mantiene la operación porque el servicio resulta indispensable. Mientras tanto, el CSIRT nacional recibe información incompleta y carece de contactos actualizados para coordinar una evaluación conjunta. Aunque existen especialistas y herramientas, la respuesta encuentra obstáculos en las relaciones entre organizaciones.

Este escenario ilustra que la capacidad de respuesta incluye acuerdos sobre autoridad, responsabilidades y circulación de información. El GFCE (2017) sitúa la función nacional de respuesta dentro de la estructura institucional de ciberseguridad y destaca la necesidad de definir su mandato y su comunidad atendida. A su vez, NIST (2025) incorpora la respuesta a incidentes en la gestión del riesgo organizacional, vinculándola con decisiones que deben prepararse antes de que ocurra una afectación.

En este artículo la gobernanza de la respuesta se entiende como el conjunto de reglas, responsabilidades y mecanismos de coordinación que permite convertir información técnica en acciones institucionales.

Para los miembros de un CSIRT, esto tiene consecuencias muy concretas. Una recomendación de aislamiento necesita un responsable que pueda autorizarla, una alerta requiere un destinatario capaz de actuar y una recuperación demanda criterios para determinar si el servicio puede restablecerse con un riesgo aceptable. La eficacia técnica depende, en parte, de que estas decisiones estén previstas y puedan tomarse oportunamente (Boeke, 2018).

Una primera condición es la claridad del mandato. El CSIRT debe conocer a quién atiende, qué servicios presta y qué competencias corresponden a otras entidades. Coordinar la respuesta técnica no supone asumir automáticamente funciones de investigación penal, inteligencia o dirección de una crisis nacional. Esas actividades pueden relacionarse durante un incidente, pero requieren atribuciones y procedimientos específicos. Delimitar sus interfaces ayuda a reducir duplicidades y evita que las decisiones dependan exclusivamente de acuerdos informales entre personas (Kasim et al., 2023).

Una segunda condición es la confianza. Compartir información sobre un incidente puede revelar vulnerabilidades, datos sensibles o fallas de operación. Por ello, los actores necesitan saber quién tendrá acceso, para qué utilizará los datos y en qué condiciones podrá transmitirlos. Los canales de cooperación deben ofrecer protección y previsibilidad. Cuando estos acuerdos son claros, la información puede circular con mayor utilidad para el análisis y la coordinación (West-Brown et al., 2003).

Por último, la sostenibilidad constituye una tercera condición. Los contactos cambian, las herramientas requieren mantenimiento y los equipos necesitan formación continua. Un presupuesto que cubre únicamente la instalación inicial deja sin resolver la continuidad de la capacidad. La guía de la OEA (2023) sobre un modelo de negocio sustentable permite abordar esta dimensión mediante la planificación de servicios, recursos y respaldo institucional.

Para América Latina, estas consideraciones sugieren que la adaptación de los marcos internacionales debe comenzar por identificar quién decide, quién ejecuta y quién coordina en cada escenario relevante. Una matriz de responsabilidades, un directorio verificado y procedimientos de escalamiento pueden parecer entregables modestos frente a una plataforma avanzada, pero permiten utilizar mejor las capacidades existentes. Su valor debe comprobarse mediante ejercicios: si una alerta llega a la persona adecuada, si las autorizaciones se obtienen a tiempo y si las instituciones pueden actuar de manera coordinada. Así, la gobernanza se convierte en una condición operativa de la respuesta y en un criterio para evaluar su funcionamiento.

2. ITU y la construcción de la capacidad nacional

Establecer una capacidad nacional de respuesta a incidentes cibernéticos supone organizar una función que pueda operar de manera continua, atender a una comunidad definida y coordinarse con otras instituciones. La ITU ha promovido este proceso mediante orientaciones y mecanismos de cooperación, con especial atención a los países que necesitan desarrollar sus capacidades iniciales. Sus resoluciones reconocen la importancia de crear y mejorar equipos nacionales de respuesta, así como de facilitar la cooperación entre ellos (ITU, 2022a, 2022b).

La aportación de la ITU & World Bank (2025) puede comprenderse desde una pregunta práctica: ¿qué necesita un país para convertir la respuesta a incidentes en una capacidad institucional? La respuesta requiere relacionar la estrategia nacional de ciberseguridad con una estructura organizativa, personal preparado, procedimientos y recursos. Desde esta perspectiva, el equipo nacional forma parte de un sistema de gestión del riesgo en el que participan autoridades públicas, operadores de servicios, empresas y comunidades técnicas.

Esta orientación tiene una consecuencia inmediata: las decisiones sobre infraestructura deben derivarse de una definición previa de funciones. Antes de seleccionar plataformas de monitoreo, análisis o intercambio de información, conviene establecer qué servicios ofrecerá el equipo y qué problemas necesita resolver. Si su tarea princi-

pal es coordinar incidentes que afectan a diversas instituciones, necesitará mecanismos de comunicación y escalamiento diferentes de los que utiliza un equipo dedicado a proteger una sola red. La arquitectura técnica debe corresponder al alcance institucional de la operación.

El punto de partida es delimitar la comunidad atendida. Un CSIRT nacional puede asumir responsabilidades de coordinación para el país, aunque su capacidad de intervención directa se concentre inicialmente en determinadas entidades o servicios. Precisar esa diferencia permite comunicar expectativas realistas: qué incidentes recibe, a quién proporciona asistencia y en qué condiciones solicita apoyo de otros equipos. La amplitud del mandato debe guardar relación con los recursos disponibles y con la distribución de responsabilidades dentro del Estado (Dubois & Tatar, 2022).

En ese sentido, el enfoque de la ITU resulta valioso porque permite situar la creación del equipo dentro de una estrategia de desarrollo de capacidades. Cada país necesita identificar qué recursos ya existen y cuáles requieren articulación. Universidades, proveedores, entidades financieras y organismos públicos pueden disponer de conocimientos y equipos que contribuyan a la respuesta nacional. Reconocer esas capacidades ayuda a definir dónde conviene crear servicios y dónde resulta más útil establecer acuerdos de coordinación (Kamariotou & Kitsios).

La continuidad también debe formar parte del diseño. El equipo necesita mantener conocimientos, actualizar procedimientos y conservar relaciones de cooperación aun cuando cambien sus integrantes. Esto requiere presupuesto recurrente, formación y respaldo institucional. Una capacidad nacional adquiere mayor consistencia cuando sus funciones se documentan, sus servicios se prueban y sus resultados permiten justificar decisiones de mejora.

3. GFCE y el mandato de un CSIRT nacional

Una de las decisiones más importantes al establecer un CSIRT nacional es definir su mandato. Aunque puede parecer un asunto administrativo, determina aspectos esenciales de la operación: a quién atiende el equipo, qué servicios presta, qué autoridad tiene para coordinar y cómo se relaciona con otras instituciones. Las buenas prácticas del GFCE (2017) sitúan esta definición dentro de la estrategia y la estructura nacional de ciberseguridad, vinculándola con las necesidades y los riesgos del país.

El mandato puede entenderse como un acuerdo institucional sobre la función del equipo. Para que sea útil, debe responder preguntas que cualquier operador encontrará du-

rante un incidente: ¿quién puede solicitar asistencia?, ¿qué información debe proporcionar?, ¿qué acciones puede realizar el CSIRT?, ¿cuándo debe escalar el caso? y ¿qué decisiones corresponden a otras autoridades? La precisión de estas respuestas reduce incertidumbre y facilita que los especialistas actúen dentro de responsabilidades reconocidas (Hidalgo-Guijarro, 2023).

En ese sentido, el mandato funciona como una definición del alcance del servicio. Permite relacionar solicitudes con capacidades y establecer límites que protegen la operación. Un equipo responsable de coordinar alertas nacionales no necesariamente administra los sistemas afectados ni puede ordenar su desconexión. Por ello, necesita procedimientos que conecten sus recomendaciones con las personas que tienen autoridad sobre esos sistemas. La claridad institucional permite que el análisis técnico se convierta en una decisión ejecutable.

Las buenas prácticas del GFCE (2017) también destacan la importancia de fundamentar la capacidad nacional en una evaluación de riesgos. Este principio ayuda a evitar que el diseño responda únicamente a modelos disponibles o a oportunidades de financiamiento. Si el diagnóstico identifica dificultades de coordinación entre sectores, la prioridad puede ser establecer contactos y procedimientos compartidos. Si revela una comunidad con escasa capacidad para analizar incidentes, podría ser necesario desarrollar servicios de asistencia técnica, las decisiones deben guardar relación con problemas identificados.

Otro componente del mandato es su relación con funciones cercanas, como la investigación de delitos, la inteligencia, la regulación y la gestión de crisis. Un incidente puede activar varias de ellas, pero cada una responde a atribuciones y objetivos propios. El CSIRT necesita saber cuándo coordinarse con esas autoridades y en qué condiciones compartir información. Definir estas interfaces favorece una respuesta coherente y ayuda a evitar solicitudes que excedan sus competencias (Nowikowska, 2021).

Esta delimitación es especialmente relevante para construir confianza. Una organización que reporta un incidente necesita comprender cómo se utilizará la información y quién podrá acceder a ella. Si las reglas son ambiguas, puede retrasar la notificación o proporcionar datos insuficientes.

En cambio, condiciones claras de confidencialidad, protección y uso permiten establecer relaciones de cooperación más previsibles. El mandato debe acompañarse de procedimientos que hagan operativas esas condiciones (GFCE, 2017).

En América Latina, la adaptación requiere considerar la estructura institucional de cada país. En un sistema federal, caso de países como México, Argentina y Brasil, puede ser necesario acordar responsabilidades entre autoridades nacionales y subnacionales. Cuando los servicios esenciales dependen de operadores privados, la coordinación exige mecanismos que faciliten su participación. Estos ejemplos muestran que una función nacional debe diseñarse a partir de relaciones concretas, sin suponer que una misma ubicación administrativa resolverá todas las necesidades (Scholta et al., 2025).

El respaldo institucional debe, además, permitir que el equipo mantenga su capacidad a lo largo del tiempo. Un mandato amplio sin personal, presupuesto o acuerdos de cooperación genera expectativas difíciles de cumplir.

Por ello, resulta conveniente vincular cada responsabilidad con servicios definidos y recursos disponibles. La revisión periódica permite ajustar el alcance conforme cambian los riesgos y se desarrollan nuevas capacidades.

4. FIRST y el catálogo de servicios

Una vez definidos el mandato y la comunidad atendida, surge una pregunta operativa: ¿qué servicios puede ofrecer el equipo y qué necesitan sus usuarios? El *CSIRT Services Framework* de FIRST (2020) permite organizar esta discusión mediante un lenguaje común para describir servicios, funciones y actividades. Su utilidad consiste en ayudar a los equipos a definir su trabajo y comunicarlo de manera comprensible a otras organizaciones.

El marco agrupa los servicios en cinco áreas: 1) gestión de eventos de seguridad de la información, 2) gestión de incidentes, 3) gestión de vulnerabilidades, 4) conciencia situacional y 5) transferencia de conocimientos. Estas áreas permiten relacionar la observación de actividad potencialmente maliciosa con el análisis, la coordinación y el aprendizaje. No constituyen una obligación de implementar todos los servicios: cada equipo debe seleccionar los que correspondan a su mandato, a los riesgos de su comunidad y a sus recursos (Núñez-Agurto, 2022).

Esta estructura ayuda a distinguir actividades que suelen confundirse, un evento es una observación que requiere interpretación; un incidente supone una afectación o amenaza que demanda atención. Recibir registros, correlacionar alertas y coordinar la contención son tareas relacionadas, pero requieren procesos y responsabilidades diferentes. Separarlas permite identificar dónde se interrumpe el flujo de trabajo: en la detección, en el análisis o en la capacidad de convertir un hallazgo en una acción (Tanczer et al., 2018).

Figura 1. Áreas de servicios de un CSIRT según FIRST.



Fuente: Elaboración propia con base en FIRST (2020).

La gestión de vulnerabilidades introduce otra dimensión. El equipo puede identificar debilidades, analizar su relevancia, comunicar recomendaciones y colaborar en su tratamiento. Sin embargo, la responsabilidad de corregir una configuración o instalar una actualización puede corresponder al administrador del sistema, al proveedor o al fabricante. El catálogo debe aclarar qué apoyo proporciona el CSIRT y qué acciones espera de las organizaciones atendidas (FIRST, 2020).

La conciencia situacional permite integrar información para comprender el entorno de amenazas y apoyar decisiones. Su valor depende de seleccionar datos pertinentes y transformarlos en conocimiento utilizable. Una alerta sobre una vulnerabilidad, por ejemplo, resulta más útil cuando identifica los sistemas potencialmente afectados, explica las condiciones de explotación y ofrece recomendaciones acordes con la comunidad destinataria. El volumen de información distribuida no equivale, por sí mismo, a la calidad del servicio.

Por su parte, la transferencia de conocimientos reconoce que la respuesta también necesita formación, ejercicios y aprendizaje compartido. Los especialistas pueden utilizar los incidentes atendidos para mejorar procedimientos y desa-

rrollar capacidades en las instituciones de su comunidad. Esta función adquiere relevancia cuando los usuarios tienen diferentes niveles de preparación y requieren orientación para reportar, conservar información o aplicar medidas iniciales.

5. NIST y la integración de la respuesta al riesgo

Definir servicios permite ordenar el trabajo del equipo, pero la respuesta a incidentes necesita conectarse con las decisiones de la organización. En este punto son útiles herramientas como el *Cybersecurity Framework 2.0.* Su aportación consiste en vincular la preparación, la detección, la respuesta y la recuperación con actividades continuas de gobernanza y mejora (NIST, 2024).

Esta orientación amplía la mirada sobre el incidente, una intrusión puede comprometer información, interrumpir procesos o afectar servicios que dependen de proveedores externos. Para decidir cómo responder, los especialistas necesitan comprender la importancia de los activos afectados y las consecuencias de las medidas propuestas. La decisión de aislar un sistema, por ejemplo, debe considerar tanto la posibilidad de propagación como el efecto que su desconexión

Figura 2. Respuesta a incidentes y gestión del riesgo en NIST.



Fuente: Elaboración propia con base en NIST (2024).

tendría sobre la operación (Nelson et al., 2025).

NIST relaciona las funciones de gobernar, identificar y proteger con la preparación y la reducción del riesgo, mientras que detectar, responder y recuperar concentran actividades vinculadas con el manejo de incidentes. La mejora continua conecta estas funciones mediante aprendizajes que deben incorporarse a la gestión organizacional.

Ello permite comprender la respuesta como una capacidad que se prepara antes del incidente y se revisa después de su atención (Hajializadeh & Imani, 2021).

Este enfoque se traduce en preguntas concretas. ¿Existe un inventario suficientemente actualizado? ¿Se conocen las dependencias del servicio? ¿Los registros disponibles permiten investigar una afectación? ¿Está definido quién autoriza una medida de contención? ¿Las copias de respaldo pueden restaurarse en condiciones aceptables? Las respuestas condicionan el margen de actuación del equipo cuando ocurre un incidente y deben revisarse como parte de la preparación.

La relación con la continuidad operativa es especialmente importante. Recuperar un sistema requiere comprobar que puede volver a prestar su función y que las condiciones que permitieron el incidente han sido atendidas hasta un nivel de riesgo aceptado por la organización. Por ello, los especialistas deben coordinarse con responsables de procesos, administradores, proveedores y directivos. La recuperación combina verificación técnica con decisiones sobre prioridades y disponibilidad del servicio (Meçaj, 2026).

Esta arquitectura de gobernanza puede ilustrarse mediante un escenario hipotético de ransomware en una institución hospitalaria. El equipo técnico identifica equipos comprometidos y recomienda restringir conexiones. La decisión debe considerar qué sistemas sostienen la atención médica, cuáles pueden suspenderse y qué alternativas operativas existen. El análisis técnico necesita información sobre procesos críticos y autoridades para actuar. Este ejemplo muestra por qué la preparación debe involucrar a quienes administran el riesgo y la continuidad de la institución.

La comunicación forma parte también de la arquitectura de gobernanza. Durante un incidente, distintas personas necesitan información diferente: los operadores requieren instrucciones técnicas; los directivos, una valoración de impacto y opciones; y los usuarios afectados, orientación sobre la situación y las acciones que les corresponden. Definir responsables y canales ayuda a evitar mensajes contradictorios y permite actualizar la información conforme avanza la investigación (NIST, 2025).

El aprendizaje posterior también necesita traducirse en cambios. Identificar que una alerta se atendió tarde o que un contacto estaba desactualizado aporta valor cuando conduce a corregir el procedimiento, ajustar responsabilidades o capacitar al personal. La revisión debe examinar las condiciones que favorecieron el incidente y las dificultades encontradas durante su manejo. Así, los resultados de la respuesta retroalimentan la gestión del riesgo.

6. SIM3 y ENISA para medir madurez

Después de definir el mandato, organizar los servicios e integrar la respuesta a la gestión del riesgo, corresponde examinar qué tan consistente es el funcionamiento del equipo. La madurez permite abordar esta cuestión mediante criterios que relacionan las capacidades declaradas con su organización y ejecución. Por lo que esta dimensión representa una oportunidad de identificar qué procesos funcionan de manera previsible, cuáles dependen de esfuerzos individuales y dónde conviene concentrar las mejoras (Lee et al., 2024).

El *Security Incident Management Maturity Model*, conocido como SIM3 y promovido por la *Open CSIRT Foundation,* organiza la evaluación en cuatro dimensiones: 1) organización, 2) personas, 3) herramientas y 4) procesos. Estas dimensiones permiten examinar aspectos que van desde el mandato y las responsabilidades hasta la preparación del personal y la documentación de las actividades.

Su utilidad consiste en ofrecer una estructura para valorar el desarrollo del equipo y orientar decisiones de mejora (Open CSIRT Foundation, 2010)
.
La dimensión organizacional permite revisar si el equipo cuenta con una función reconocida y responsabilidades definidas. La relativa a las personas examina condiciones necesarias para desempeñar el trabajo, como conocimientos y formación. Las herramientas proporcionan soporte a la operación, mientras que los procesos permiten realizar actividades de manera consistente. La relación entre estas dimensiones explica por qué una capacidad técnica avanzada puede resultar insuficiente cuando existen dificultades de coordinación o procedimientos poco claros.

Por otra parte, ENISA desarrolló un modelo de evaluación de madurez para CSIRT nacionales y gubernamentales que incorpora SIM3 y otros referentes sobre capacidades. Su aportación consiste en relacionar los criterios de evaluación con una metodología que ayuda a examinar el desarrollo de los equipos. Estos instrumentos pueden utilizarse para establecer una línea de base y orientar revisiones posteriores, considerando el contexto y las funciones de la organización evaluada (ENISA, 2019).

Figura 3. Dimensiones de madurez de SIM3 y proceso de mejora.



Fuente: Elaboración propia con base en Open CSIRT Foundation (2010).

En este punto, es necesario distinguir entre autoevaluación, revisión externa y certificación. Una autoevaluación permite identificar brechas y organizar acciones; una revisión externa aporta una perspectiva adicional sobre los resultados; y una certificación responde a requisitos y procedimientos específicos.

Completar un diagnóstico interno no acredita automáticamente el cumplimiento de un esquema de certificación. Precisar estas diferencias evita atribuir a los resultados un alcance mayor del que poseen (Yesina & Holubnychyi).

La evaluación adquiere utilidad cuando se acompaña de evidencia. Un procedimiento escrito muestra que existe una instrucción, pero los registros de ejercicios y casos atendidos permiten examinar cómo se aplica. Del mismo modo, un directorio de contactos necesita pruebas de actualización y disponibilidad.

Para fines de mejora interna, conviene relacionar cada capacidad evaluada con documentos, registros o actividades que ayuden a comprender su funcionamiento. Esta es una recomendación de aplicación del modelo, cuyo detalle

debe ajustarse al propósito de la evaluación.

En América Latina, SIM3 y ENISA pueden ayudar a definir prioridades alcanzables sin exigir que todos los equipos recorran una trayectoria idéntica. Un CSIRT con recursos limitados podría comenzar por mejorar la documentación y la cobertura de sus servicios. Otros, con procedimientos establecidos, podrían concentrarse en ejercicios intersectoriales o revisión entre pares. La comparación resulta más útil cuando considera el mandato, la comunidad atendida y las condiciones de operación.

7. La OEA como puente de adaptación regional

Los marcos internacionales ofrecen criterios para diseñar y evaluar capacidades, pero su aplicación requiere comprender el entorno institucional donde operarán. La OEA aporta una perspectiva especialmente pertinente para América Latina y el Caribe mediante sus guías para CSIRT y sus iniciativas de cooperación. Su contribución permite relacionar las recomendaciones técnicas con preguntas sobre planificación, recursos y sostenibilidad.

La *Guía práctica para CSIRTs: Un modelo de negocio sustentable*, publicada en 2023, desarrolla esta dimensión. El término "modelo de negocio" debe entenderse aquí como una forma de organizar la propuesta de servicios, la comunidad atendida, los recursos y las relaciones que sostienen al equipo. Para un CSIRT público, la cuestión central es cómo mantener una función útil y viable a lo largo del tiempo (OEA, 2023).

Esta perspectiva permite abordar una dificultad frecuente en el diseño de capacidades: la diferencia entre financiar la instalación y sostener la operación. El establecimiento de un equipo puede requerir infraestructura, herramientas y contratación inicial, pero su continuidad implica formación, mantenimiento, actualización de procedimientos y disponibilidad de personal. La planificación necesita considerar estos compromisos desde el inicio y vincularlos con los servicios que se espera prestar.

La guía también ayuda a relacionar los servicios con las necesidades de la comunidad. Un equipo puede identificar numerosos problemas de ciberseguridad, pero necesita decidir cuáles puede atender directamente y cuáles requieren cooperación. Esta definición permite organizar prioridades y comunicar límites. Cuando el catálogo de servicios corresponde a la capacidad disponible, los usuarios tienen mayor claridad sobre la asistencia que pueden solicitar y las responsabilidades que conservarán durante el incidente (OEA, 2023).

La dimensión regional añade otra oportunidad, los incidentes pueden involucrar proveedores, infraestructura y organizaciones situados

en diferentes países. Las redes de cooperación facilitan el contacto entre equipos y crean espacios para intercambiar conocimientos y desarrollar capacidades. Sin embargo, su utilidad operativa depende de que los participantes sepan qué información compartir, por qué canales y en qué condiciones de protección. La cooperación necesita procedimientos que permitan utilizar oportunamente lo recibido (Aguilar Antonio, 2023).

La adaptación requiere reconocer diferencias entre países y sectores. Las prioridades de un equipo que coordina instituciones públicas pueden diferir de las de uno que atiende operadores financieros o universidades. Por ello, resulta conveniente utilizar las guías como instrumentos de planificación y revisión, incorporando el diagnóstico de necesidades y las condiciones locales. El objetivo es construir servicios que puedan prestarse de manera continua y mejorar mediante aprendizaje compartido.

Desde esta perspectiva, la cooperación regional puede apoyar ejercicios conjuntos, revisión de procedimientos y formación especializada. Sus resultados deberían traducirse en capacidades observables: contactos que funcionan, información que puede intercambiarse y

Figura 4. Modelo de sostenibilidad de un CSIRT según OEA (2023).



Fuente: elaboración propia con base en OEA (2023).

acciones correctivas que se completan. Esta propuesta permite evaluar el valor de los marcos por su contribución al funcionamiento de los equipos y a la coordinación de la respuesta en América Latina (Lima & Soares, 2021; Aguilar Antonio, 2021)

8. Una arquitectura complementaria de los marcos

Los instrumentos examinados permiten organizar la gestión de incidentes desde distintos niveles de decisión. Algunos orientan el establecimiento de una capacidad nacional; otros ayudan a definir servicios, integrar la respuesta al riesgo o evaluar el desarrollo de los equipos. Su complementariedad ofrece una base para construir una hoja de ruta en la que cada recomendación responda a una necesidad identificada y se traduzca en responsabilidades, recursos y procedimientos.

La tabla 1 sintetiza estas aportaciones. La última columna presenta propuestas de aplicación para América Latina, cuya pertinencia debe contrastarse con el diagnóstico de cada país o sector.

La articulación puede comenzar con las orientaciones de la ITU y el GFCE para definir el propósito de la capacidad nacional, su comunidad atendida y sus relaciones institucionales. Estas decisiones establecen el alcance dentro del cual se seleccionarán los servicios. Posteriormente, FIRST permite describir qué hará el equipo, mientras NIST ayuda a relacionar ese trabajo con la importancia de los activos y servicios que deben protegerse. Finalmente, SIM3 y ENISA aportan criterios para revisar el desarrollo de la capacidad y la OEA permite examinar cómo sostenerla mediante planificación y recursos.

Esta secuencia constituye una propuesta analítica en este artículo. Sin embargo, no se emite mencionar que no representa una metodología conjunta oficialmente adoptada por los organismos mencionados. Su utilidad consiste en ordenar preguntas que suelen abordarse por separado: quién coordina, qué servicios se prestan, cómo se toman decisiones y qué evidencia permite evaluar los avances.

La aplicación tampoco necesita seguir una trayectoria rígida. Un ejercicio puede mostrar que el catálogo de servicios excede los recursos disponibles o que el mandato deja dudas sobre quién autoriza una medida. En ese caso, la evaluación permite volver a las decisiones de diseño y corregirlas. La relación entre planificación, operación y aprendizaje hace posible que los marcos acompañen el desarrollo del equipo conforme cambian sus necesidades (NIST, 2025; ENISA, 2019).

Para América Latina, se propone organizar esta adaptación en tres fases: 1) Mandato y diagnóstico; 2) Servicios y operación; y 3) Madurez, cooperación y aprendizaje.

Tabla 1. Aportaciones de los marcos internacionales a la gestión de incidentes cibernéticos.

Organismo e instrumento	Función principal	Ámbito de aplicación	Aplicación propuesta para América Latina
ITU | Orientaciones para capacidades nacionales	Orientar el establecimiento de capacidades de respuesta y su vinculación con la estrategia nacional.	Nacional.	Definir funciones iniciales, recursos y relaciones de coordinación.
GFCE | Buenas prácticas para CSIRT nacionales	Precisar mandato, comunidad atendida y respaldo institucional.	Nacional e interinstitucional.	Acordar responsabilidades y mecanismos de cooperación entre actores.
FIRST | CSIRT Services Framework	Organizar y describir los servicios del equipo.	Equipos nacionales, sectoriales e institucionales.	Seleccionar una cartera de servicios acorde con necesidades y recursos.
NIST | SP 800-61 Rev. 3	Integrar la respuesta a incidentes en la gestión del riesgo.	Organizacional.	Vincular la operación técnica con prioridades institucionales y recuperación de servicios.
Open CSIRT Foundation | SIM3	Evaluar madurez en organización, personas, herramientas y procesos.	Equipos de gestión de incidentes.	Identificar brechas y dar seguimiento a mejoras.
ENISA | Modelo de evaluación de madurez	Orientar la evaluación de capacidades de CSIRT nacionales y gubernamentales.	Nacional y gubernamental.	Adaptar criterios de diagnóstico y revisión al mandato de cada equipo.
OEA | Guía práctica para CSIRTs, volumen 2	Orientar la planificación y sostenibilidad de los equipos.	CSIRTs de América Latina y el Caribe.	Relacionar servicios, costos recurrentes y respaldo institucional.

Fuente: elaboración propia.

Cada fase debe producir resultados verificables y considerar la sostenibilidad desde el inicio. El criterio de avance será la capacidad de ejecutar las funciones acordadas, documentar dificultades y completar mejoras. Las siguientes secciones desarrollan esta propuesta.

8.1 Primera fase: mandato y diagnóstico

La primera fase busca establecer qué capacidad necesita desarrollarse, a quién atenderá y cómo se relacionará con las instituciones existentes. Su producto principal es una definición compartida del alcance de la respuesta, respaldada por un diagnóstico de riesgos y recursos.

Esta orientación retoma las buenas prácticas del GFCE (2017) sobre el mandato nacional y las recomendaciones de planificación de la ITU (2025) y la OEA (2023).

Figura 5. Articulación de marcos internacionales para definir, desarrollar y sostener una capacidad nacional de gestión de incidentes.



Fuente: elaboración propia.

El diagnóstico debe comenzar por identificar las funciones y los servicios cuya afectación tendría consecuencias relevantes. Para ello, conviene examinar qué procesos dependen de sistemas digitales, qué proveedores intervienen y quién administra los activos. La información permitirá reconocer necesidades de coordinación y asistencia técnica. El nivel de detalle debe corresponder al alcance del equipo: un CSIRT nacional necesita una visión de actores y dependencias estratégicas, mientras uno institucional requiere mayor precisión sobre su infraestructura.

También, es necesario mapear las capacidades disponibles. Pueden existir equipos gubernamentales, sectoriales, académicos o empresariales que reciben reportes, analizan amenazas o atienden incidentes. El diagnóstico debe identificar qué hacen, a qué comunidad sirven y cómo se comunican. Esta revisión permite reconocer oportunida-

des de cooperación y evita diseñar servicios que dupliquen funciones sin una justificación operativa.

A partir de esa información, el mandato debe precisar la comunidad atendida, los servicios iniciales y las responsabilidades de coordinación. Del mismo modo, necesita establecer cómo se relacionará el equipo con autoridades reguladoras, responsables de infraestructura, organismos de investigación y gestores de crisis. Cuando varias instituciones intervienen, resulta conveniente acordar criterios de escalamiento y reglas para compartir información sensible. Una matriz de responsabilidades puede ayudar a documentar estas relaciones, siempre que las instituciones involucradas reconozcan su contenido y lo mantengan actualizado.

Por último, la evaluación de recursos completa el diagnóstico. Es necesario revisar perfiles profesionales, disponibilidad, formación, herramientas y presupuesto recurrente. Esta información permite ajustar las expectativas y priorizar servicios que puedan sostenerse. La planificación debería considerar costos de mantenimiento y continuidad, además de los necesarios para iniciar la operación (OEA, 2023).

Como propuesta de implementación, esta fase puede cerrar con cuatro entregables: 1) Un mandato aprobado, 2.) Un mapa de actores y capacidades, 3) Un directorio verificado de contactos y responsabilidades y 4.) Un plan inicial de recursos vinculado con los servicios prioritarios. Estos productos se plantean como instrumentos de trabajo y deben adaptarse a los mecanismos administrativos de cada país.

8.2. Segunda fase: servicios y operación

Con el mandato definido y las capacidades identificadas, la siguiente fase consiste en convertir los acuerdos institucionales en servicios que puedan prestarse de manera consistente. El equipo debe establecer cómo recibirá reportes, qué información analizará, cuándo solicitará apoyo y cómo comunicará los resultados. El marco de FIRST (2020) proporciona una referencia para organizar esta cartera, mientras las recomendaciones de NIST (2025) permiten relacionar su ejecución con la gestión del riesgo y la continuidad de los servicios.

La selección inicial debe responder a las necesidades de la comunidad atendida. Un equipo puede comenzar con recepción y clasificación de reportes, análisis inicial, coordinación de respuesta y difusión de alertas. La combinación dependerá del diagnóstico previo y de los recursos disponibles. Lo relevante es que cada servicio tenga destinatarios, responsables y condiciones de prestación claramente establecidos (FIRST, 2020).

Es importante que estas condiciones deben expresarse en procedi-

mientos utilizables. El canal de reporte necesita indicar qué datos se solicitan, cómo se protege la información y qué respuesta puede esperar el remitente. La clasificación requiere criterios para valorar severidad, impacto y urgencia. El escalamiento debe identificar qué circunstancias activan la intervención de otros equipos o autoridades. Estas definiciones facilitan el trabajo cotidiano y permiten reconocer dónde aparecen demoras o decisiones ambiguas.

La operación también necesita distinguir entre asistencia técnica y responsabilidad sobre los sistemas. El CSIRT puede analizar un caso y recomendar medidas, mientras la entidad afectada conserva la autoridad para ejecutarlas sobre su infraestructura. Cuando el incidente involucra a varias organizaciones, los procedimientos deben conectar esas responsabilidades mediante contactos y mecanismos de coordinación previamente acordados (FIRST, 2020; NIST, 2025).

Antes de considerar concluida esta fase, conviene probar los servicios con ejercicios y revisar casos atendidos. La verificación debería mostrar que los reportes llegan al canal previsto, se clasifican mediante criterios compartidos y se asignan a responsables identificados. También, debe permitir comprobar que las recomendaciones se comunican a quienes pueden actuar y que las dificultades quedan documentadas.

Como resultado, esta fase debe producir una cartera de servicios publicada, procedimientos de atención probados y registros que permitan revisar su funcionamiento. La madurez posterior se apoyará en esta evidencia: un equipo puede evaluar y mejorar con mayor precisión cuando conoce cómo ejecuta sus servicios y dónde encuentra obstáculos.

8.3. Tercera fase: madurez, cooperación y aprendizaje

Cuando los servicios comienzan a operar, la prioridad es examinar su consistencia y convertir la experiencia en mejoras. La tercera fase articula evaluación de madurez, cooperación y aprendizaje. Su propósito es identificar qué capacidades funcionan, cuáles requieren ajustes y cómo puede sostenerse su desarrollo mediante revisión periódica y colaboración con otros equipos.

SIM3 y el modelo de ENISA ofrecen referencias para establecer una línea de base y examinar dimensiones organizacionales, humanas, tecnológicas y procedimentales. La evaluación debe considerar el mandato y la comunidad atendida, de modo que los resultados puedan interpretarse en relación con las responsabilidades reales del equipo.

Las brechas identificadas deben traducirse en acciones específicas y alcanzables (Open CSIRT Foundation, 2010.; ENISA, 2019).

Esto implica relacionar cada hallazgo con evidencia de operación. Si el diagnóstico señala dificultades de escalamiento, conviene revisar los registros de casos y ejercicios para identificar sus causas. Si muestra dependencia de determinadas personas, puede ser necesario documentar conocimientos y establecer sustituciones. La evaluación adquiere utilidad cuando permite decidir qué cambiar y cómo verificar que la modificación funciona.

La cooperación amplía las posibilidades de aprendizaje y asistencia. Los equipos pueden intercambiar conocimientos, contrastar procedimientos y participar en ejercicios conjuntos. Sin embargo, estos vínculos requieren contactos reconocidos, condiciones de protección de la información y claridad sobre la asistencia disponible. La pertenencia a una red debe acompañarse de relaciones operativas que puedan activarse cuando resulte necesario. En América Latina, los ejercicios intersectoriales y transfronterizos pueden ayudar a identificar dificultades que una institución no observaría por sí sola. Un escenario que afecte a un proveedor compartido, por ejemplo, permite revisar cómo circulan las alertas, cómo se concilian prioridades y qué información necesita cada participante.

Los resultados deberían conducir a correcciones documentadas y a una prueba posterior de los cambios.

El aprendizaje también procede de los incidentes reales. La revisión posterior debe examinar qué permitió detectar el problema, qué decisiones facilitaron la contención y qué condiciones retrasaron la recuperación. Su finalidad es mejorar capacidades y procedimientos mediante una comprensión compartida de lo ocurrido. Las acciones acordadas necesitan responsables y seguimiento para que los hallazgos se incorporen a la operación (NIST, 2025).

Los indicadores pueden apoyar este proceso si se interpretan con cautela. Es posible observar contactos verificados, servicios probados, tiempos de clasificación y acciones correctivas completadas. Sin embargo, una variación aislada no explica todo el desempeño. Un incremento de reportes puede reflejar mayor visibilidad o confianza en el equipo; una reducción del tiempo de atención puede depender de cambios en la complejidad de los casos. Conviene combinar mediciones con revisión cualitativa de los resultados.

Como propuesta de aplicación, esta fase debe generar una evaluación de madurez, un plan de mejora y evidencia de seguimiento. La periodicidad dependerá de los riesgos, los recursos y los cambios de la organización. También será necesario revisar el mandato o la cartera de servicios cuando los ejercicios y la experiencia revelen nuevas necesidades.

Esta tercera fase constituye un ciclo continuo. La evaluación puede mostrar que deben modificarse acuerdos institucionales de la primera fase o procedimientos de la segunda. La hoja de ruta permite así conectar diseño, ejecución y revisión. Su valor para América Latina reside en ofrecer una secuencia adaptable que convierta las orientaciones internacionales en capacidades comprobables y sostenibles.

Conclusiones

Los marcos internacionales examinados ofrecen aportaciones complementarias para desarrollar la gestión de incidentes cibernéticos en América Latina. Su utilidad depende de traducir las orientaciones en decisiones sobre mandato, servicios, recursos y evaluación. La articulación permite relacionar el diseño institucional con la operación técnica y revisar los resultados mediante evidencia de funcionamiento.

La hoja de ruta propuesta organiza estas contribuciones en tres fases: 1) Mandato y diagnóstico; 2) Servicios y operación; y 3) Madurez, cooperación y aprendizaje. La primera establece el alcance y reconoce las capacidades disponibles. La segunda convierte los acuerdos en procedimientos y servicios probados. La tercera evalúa su consistencia y utiliza la experiencia para corregirlos. La relación entre fases permite revisar decisiones anteriores conforme cambian los riesgos y las necesidades.

Para los profesionales técnicos la principal implicación es que la respuesta necesita conectar el conocimiento técnico con responsabilidades institucionales claras. Detectar una afectación, recomendar una medida y recuperar un servicio exige información sobre prioridades, dependencias y autoridades.

Los marcos ayudan a organizar estas relaciones cuando su aplicación se acompaña de ejercicios, registros y seguimiento de mejoras.

Para los responsables de política pública, la propuesta destaca la importancia de sostener las capacidades más allá de su establecimiento inicial. La continuidad requiere personal, formación, mantenimiento y acuerdos de cooperación. La amplitud de los servicios debe corresponder a recursos que permitan prestarlos de manera consistente y a un mandato reconocido por las instituciones participantes.

América Latina puede utilizar los marcos internacionales para ordenar prioridades y desarrollar capacidades sobre recursos existentes.

El avance será observable cuando los reportes lleguen a quienes pueden atenderlos, las decisiones se coordinen dentro de atribuciones reconocidas y las lecciones se conviertan en mejoras verificables. Esa relación entre orientación, ejecución y aprendizaje constituye el fundamento de la hoja de ruta propuesta.

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), pp. 169–197. https://doi.org/10.5354/0719-3769.2021.57067

Aguilar-Antonio, J.M. (2023), The Need for a Multistakeholder Approach in Cybersecurity for National Security. Available at SSRN: https://ssrn.com/abstract=4900235

Alghamdi, S. M., Win, K., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. Comput. Secur., 99, 102030. https://doi.org/10.1016/j.cose.2020.102030

Boeke, S. (2018). National cyber crisis management: Different European approaches. *Governance, 31*, 449-464. https://doi.org/10.1111/gove.12309

Dubois, E., & Tatar, U. (2022). Mitigating Global Cyber Risk Through Bridging the National Incident Response Capacity Gap. *International Conference on Cyber Warfare and Security.* https://doi.org/10.34190/iccws.17.1.66

Ethembabaoglu, A., Kadenko, N. I., Angelova, Y., Zhauniarovich, Y., Van Wegberg, R., Parkin, S., & Van Eeten, M. (2026). "Tell Them They Are a Responsible Entity, Not a Customer": Understanding Practitioner Challenges in Sector CSIRTs. *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems.* https://doi.org/10.1145/3772318.3790613

European Union Agency for Cybersecurity [ENISA] (2019). *ENISA CSIRT maturity assessment model.* https://www.enisa.europa.eu/publications/study-on-csirt-maturity

European Union Agency for Cybersecurity [ENISA] (2020). *Driving the global ecosystem of incident response capabilities: New studies now available.* https://www.enisa.europa.eu/news/enisa-news/driving-the-global-ecosystem-of-incident-response-capabilities-new-studies-now-available

Forum of Incident Response and Security Teams [FIRST] (2020). *CSIRT services framework* (Version 2.1). https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

Global Forum on Cyber Expertise [GFCE] (2017). *GFCE global good practices: National computer security incident response teams (CSIRTs).* https://thegfce.org/wp-content/uploads/2020/06/NationalComputerSecurityIncidentResponseTeamsCSIRTs-1.pdf

Hajializadeh, D., & Imani, M. (2021). RV-DSS: Towards a resilience and vulnerability- informed decision support system framework for interdependent infrastructure systems. *Comput. Ind. Eng.*, 156, 107276. https://doi.org/10.1016/j.cie.2021.107276

Hidalgo-Guijarro, J. (2023). Equipo de respuesta ante incidentes informáticos para la seguridad de la información (CSIRT-UPEC). *SATHIRI.* https://doi.org/10.32645/13906925.1200

International Telecommunication Union [ITU] & World Bank (2025). *Guide to developing a national cybersecurity strategy: Strategic engagement in cybersecurity* (3rd ed.). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.03-2025-PDF-E.pdf

International Telecommunication Union [ITU] (2022a). *Resolución 58 (Rev. Ginebra, 2022): Fomento de la creación de equipos nacionales de respuesta a incidentes informáticos, en particular en los países en desarrollo.* https://www.itu.int/pub/T-RES-T.58-2022/es

International Telecommunication Union [ITU] (2022b). *Resolución 69 (Rev. Kigali, 2022): Facilitación de la creación de equipos nacionales de respuesta a incidentes informáticos, en particular en los países en desarrollo, y de la cooperación entre ellos.* https://www.itu.int/pub/D-RES-D.69-2022

Kamariotou, M., & Kitsios, F. C. (2023). Information Systems Strategy and Security Policy: A Conceptual Framework. *Electronics.* https://doi.org/10.3390/electronics12020382

Kassim, S. R. M., Li, S., & Arief, B. (2023). Understanding How National CSIRTs Evaluate Cyber Incident Response Tools and Data: Findings from Focus Group Discussions. *Digital Threats: Research and Practice, 4,* 1 - 24. https://doi.org/10.1145/3609230

Kazeem, L. O., Adedayo-Ajayi, V., Ajakwe, S., & Fiyinfoluwa, O. (2026). Incident Response in Cybersecurity: A Systematic Review. *Asian Journal of Current Research.* https://doi.org/10.56557/ajocr/2026/v11i411074

Killcrece, G., Kossakowski, K., Ruefle, R., & Zajicek, M. T. (2003). Organizational Models for Computer Security Incident Response Teams (CSIRTs). https://doi.org/10.21236/ada421684

Lee, G.-S., Kim, S., Lee, I., Brown, S., & Carbajal, Y. A. (2024). Adapting cybersecurity maturity models for resource-constrained settings: A case study of Peru. *The Electronic Journal of Information Systems in Developing Countries, 91.* https://doi.org/10.1002/isd2.12350

Lima, A. G. M., & Soares, C. O. (2021). Análisis de las ciberacciones y la ciberorganización en la OEA. *Hemisferio Revista del Colegio Interamericano de Defensa.* https://doi.org/10.59848/21.1207.hv7n3

Meçaj, J. (2026). Enhancing Business Cybersecurity Through Integrated Defense and Incident Response: A Comparative Decision Framework. *International Journal of Advanced Computer Science and Applications.* https://doi.org/10.14569/ijacsa.2026.0170166

National Institute of Standards and Technology [NIST]. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST Special Publication 800-61 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

Nowikowska, M. (2021). The Main Tasks of the Network of Computer Security Incident Response Teams in the Light of the Act on the National Cybersecurity System in Poland. *Cybersecurity in Poland.* https://doi.org/10.1007/978-3-030-78551-2_15

Nuñez-Agurto, D., Ron, M., Carrera, E. V., Tapia, F., Cruz, H., Recalde, L., & Fuertes, W. (2022). Design of an Academic CSIRT – A Proposal Based on Strategic

Planning Principles. *Emerging Research in Intelligent Systems.* https://doi.org/10.1007/978-3-030-96043-8_23

Open CSIRT Foundation (2010). SIM3 model & references. Recuperado el 6 de octubre de 2026, de https://opencsirt.org/csirt-maturity/sim3-and-references/

Organización de los Estados Americanos [OEA]. (2023). *Guía práctica para CSIRTs: Un modelo de negocio sustentable* (Vol. 2). https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Guia-CSIRT%202023%20ESP%20Digital.pdf

Scholta, H., Halsbenning, S., & Niemann, M. (2025). A coordination perspective on digital public services in federal states. *Gov. Inf. Q., 42*, 101984. https://doi.org/10.1016/j.giq.2024.101984

Tanczer, L., Brass, I., & Carr, M. (2018). CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. *Global Policy*. https://doi.org/10.1111/1758-5899.12625

West-Brown, M., Stikvoort, D., Kossakowski, K., Killcrece, G., Ruefle, R., & Zajicek, M. T. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs). https://doi.org/10.1184/r1/6574055.v1

Yesina, M., & Holubnychyi, D. (2023). CERT-UA assessment based on the CSIRT ENISA Maturity Model. *Radiotekhnika.* https://doi.org/10.30837/rt.2023.2.213.04

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.

ACIS

ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

¡AFILIATE YA!

Y DISFRUTA DE ESTOS BENEFICIOS

- Actualización en formación profesional y académica de manera constante.
- Candidatura a participación profesional en proyectos de ACIS.
- Candidato a Director o CoDirector de Grupo de Interés (GI).
- Candidatura a participar en consultorías solicitadas a ACIS por el sector privado y público.
- Candidatura a participar en eventos nacionales o internacionales como delegado de ACIS.
- Candidato a Miembro de Consejo Editorial de la Revista Sistemas.
- Descuentos especiales en cursos y eventos exclusivos en el área de las TIC.
- Referencia profesional para vinculación como Perito en procesos de arbitraje.
- Referencia para participación en Juntas Directivas.
- Inclusión en el gremio de Ingenieros de Sistemas más importante del país.
- Recepción trimestral de la revista SISTEMAS en formato digital.
- Acceso diferido a la base de Webinars de ACIS.
- Acceso exclusivo a oportunidades laborales a través de nuestro portal de empleo.
- Participación como conferencista o participante en las charlas semanales.
- Correo personal con @acis.org.co
- Asista a las funciones del Teatro Nacional con un 20% de descuento. Consulte la Programación y solicite el descuento a cursos@acis.org.co.
- 30% de descuento en los libros de la Casa Editorial ALFAOMEGA, consulte el Catálogo

Afiliación General

Afiliación + Precio de estudio de formulario

$342.000 + $63.000

Afiliación para recién egresados

Descuento de 20% para recién egresados, (2 años) + Precio de estudio de formulario

$273.600 + $63.000

301 5530540 | suscripciones@acis.org.co | www.acis.org.co

ACIS

ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

ACIS Conecta

*Desde **ACIS** queremos invitarte a ser parte de ACIS Conecta, una nueva iniciativa creada especialmente para nuestros asociados.*

Actualiza tu perfil, destaca tus competencias y prepárate para conectarte con nuevas oportunidades profesionales. Gracias a nuestras alianzas con el Gobierno, el sector empresarial y organismos internacionales, podrás acceder a proyectos, vacantes especializadas y programas de formación que impulsarán tu crecimiento.

¡Aplica a nuestra encuesta!

acis.org.co/acis-conecta

301 5530540

administrador@acis.org.co

www.acis.org.co