Soberanía Digital en América Latina

La Construcción de Ecosistemas Digitales Seguros, Abiertos y Resilientes

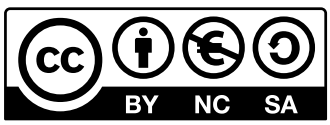
DIGI AMERICAS

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple AppGate Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluidattacks

Google kriptos LUMU netskope paloalto NETWORKS Schneider Electric SISAP Sistemas Aplicativos SOPHOS

TANIUM tenable Trellix TrendAI whalemate zscaler



Resumen ejecutivo

La soberanía digital se ha convertido en un tema central de los debates sobre política digital en todo el mundo. A medida que los gobiernos buscan fortalecer la ciberseguridad, modernizar los servicios públicos, ampliar las capacidades de inteligencia artificial y proteger la infraestructura crítica, muchos analizan cómo mantener la autoridad sobre su futuro digital sin dejar de estar conectados a la economía digital global.

En América Latina, estas conversaciones se dan en medio de una rápida transformación digital, de amenazas cibernéticas crecientes, de una demanda cada vez mayor de servicios de nube e inteligencia artificial, y de esfuerzos continuos por fortalecer los marcos de gobernanza digital. Si bien la soberanía digital a veces se asocia con la localización de datos, la autosuficiencia tecnológica o las restricciones a los proveedores extranjeros de tecnología, dichos enfoques no necesariamente mejoran la seguridad, la resiliencia ni el control. En un ecosistema digital interconectado, la soberanía no puede lograrse únicamente mediante el aislamiento físico.

Este documento sostiene que la soberanía digital debe entenderse como la capacidad de los gobiernos, las empresas y los ciudadanos de gobernar de manera segura sus datos, su infraestructura y sus servicios digitales, conservando al mismo tiempo la flexibilidad para elegir, adaptarse e innovar dentro de un ecosistema digital conectado a nivel global. Por lo tanto, la soberanía se mide mejor por la capacidad, la resiliencia y la confianza que por la ubicación física o la propiedad de los activos tecnológicos. Un ecosistema digital soberano es aquel que puede seguir operando durante incidentes cibernéticos, desastres naturales, disrupciones geopolíticas o choques en la cadena de suministro.

El documento examina los componentes clave de la soberanía digital, entre ellos la infraestructura, la computación en la nube, la gobernanza de datos, la ciberseguridad y la inteligencia artificial. En cada uno de estos ámbitos, las estrategias exitosas de soberanía enfatizan cada vez más principios comunes: seguridad, interoperabilidad, resiliencia, transparencia y capacidad de elección. La portabilidad de los datos, las arquitecturas multinube, las alianzas digitales confiables y los marcos de gobernanza eficaces pueden fortalecer la soberanía al reducir los puntos únicos de falla y aumentar la flexibilidad operativa.

Para América Latina, la soberanía digital representa una oportunidad significativa. La región puede aprovechar las inversiones en curso en infraestructura digital, servicios de nube, capacidades de ciberseguridad e inteligencia artificial, al tiempo que continúa fortaleciendo los ecosistemas locales de innovación y el desarrollo del talento. Dado que muchos países aún están construyendo la próxima generación de infraestructura digital, están bien posicionados para adoptar enfoques modernos que integren la seguridad, la resiliencia y la innovación desde el inicio.

El documento concluye que América Latina tiene la oportunidad de desarrollar un modelo de soberanía digital equilibrado y con visión de futuro: uno que proteja los intereses nacionales y a la vez preserve los beneficios de la apertura, la inversión y la conectividad global. Alcanzar esta visión requerirá una colaboración continua entre gobiernos, industria, academia y sociedad civil para construir ecosistemas digitales seguros, resilientes, interoperables y confiables. Al centrarse en la capacidad y no en el aislamiento, la región puede fortalecer su futuro digital y seguir siendo un participante activo en la economía digital global.

Índice

Introducción

La soberanía digital ha surgido como uno de los conceptos más importantes y debatidos en las discusiones sobre política digital en todo el mundo. Cada vez más, los gobiernos analizan cómo garantizar que la infraestructura digital crítica, los datos, los servicios de nube, los sistemas de inteligencia artificial y las capacidades de ciberseguridad se mantengan seguros, confiables y alineados con los intereses nacionales. En América Latina, estas conversaciones se están acelerando a medida que los países impulsan la transformación digital, amplían los servicios públicos digitales, fortalecen la ciberseguridad y buscan participar de manera más plena en la economía digital global.

Sin embargo, la soberanía digital suele malinterpretarse. En algunos debates se la equipara con la autosuficiencia tecnológica, con requisitos estrictos de localización de datos o con la reducción de la dependencia de proveedores extranjeros de tecnología. La confusión en torno a estos conceptos puede afectar negativamente la resiliencia digital.[1] Aunque pueden dar la ilusión de un mayor control, también pueden generar consecuencias no deseadas, entre ellas costos más altos, menor acceso a la innovación, una disminución de la visibilidad y las protecciones de ciberseguridad, y barreras al crecimiento económico. En un ecosistema digital interconectado, la soberanía no se logra simplemente trazando fronteras digitales.

En cambio, la soberanía digital debe entenderse como la capacidad de un país de ejercer un control significativo sobre su futuro digital. Esto incluye la capacidad de gobernar y proteger los datos, garantizar la continuidad de los servicios críticos, gestionar los riesgos digitales, mantener la visibilidad de las operaciones digitales y tomar decisiones de política de manera independiente sin dejar de estar conectado a los ecosistemas tecnológicos globales. Un ecosistema digital soberano es aquel que puede seguir operando durante incidentes cibernéticos, desastres naturales, disrupciones geopolíticas o choques en la cadena de suministro. Por lo tanto, la soberanía se mide mejor no por el aislamiento, sino por la capacidad, la resiliencia y la capacidad de elección.

Para América Latina, esta distinción es particularmente importante. La región enfrenta un panorama de amenazas en rápida evolución, una demanda creciente de capacidades de nube e inteligencia artificial, una dependencia cada vez mayor de la infraestructura digital y desafíos persistentes relacionados con

[1] https://trust.crowdstrike.com/?itemUid=27fd659c-2d6c-4f70-8f7e-abee777efb91&source=click

la inversión, la conectividad y la capacidad de ciberseguridad. Al mismo tiempo, los gobiernos buscan garantías de que los servicios digitales críticos seguirán estando disponibles, de que se respetarán las leyes y regulaciones nacionales, y de que los países conservarán la flexibilidad para determinar cómo se desarrollan sus economías digitales. Estos son objetivos legítimos que merecen respuestas de política bien fundamentadas.

Alcanzar estos objetivos requiere generar confianza en todo el ecosistema digital. Los gobiernos deben tener la certeza de que los proveedores de tecnología pueden ofrecer servicios seguros, resilientes y transparentes que operen conforme a las leyes locales y las prioridades de política pública. La industria, a su vez, debe demostrar que la infraestructura digital puede respaldar los intereses nacionales y a la vez brindar los beneficios de escala, innovación y seguridad que se derivan de la participación en redes globales. La confianza se fortalece mediante marcos de gobernanza claros, salvaguardas técnicas, mecanismos de transparencia e inversión a largo plazo en la capacidad digital local.

La resiliencia es igualmente central para la soberanía digital moderna. A medida que los gobiernos, las empresas y los ciudadanos dependen cada vez más de los servicios digitales, garantizar la continuidad durante incidentes cibernéticos, desastres naturales, tensiones geopolíticas o disrupciones en la cadena de suministro se convierte en una prioridad nacional. Esto implica reducir los puntos únicos de falla, diversificar las dependencias tecnológicas, habilitar la portabilidad de los datos y promover la interoperabilidad entre plataformas y proveedores. La soberanía se fortalece cuando las organizaciones pueden mover cargas de trabajo, datos y servicios entre entornos confiables sin sacrificar la seguridad ni la funcionalidad. En la práctica, la capacidad de elegir entre múltiples proveedores confiables puede brindar mayor resiliencia que la dependencia de una sola pila tecnológica, sin importar si esta es nacional o extranjera.

Esta perspectiva también reconoce el papel importante tanto de los actores nacionales como de los internacionales. Los países latinoamericanos deben seguir invirtiendo en ecosistemas locales de innovación, infraestructura digital, talento en ciberseguridad y tecnologías emergentes. Al mismo tiempo, los proveedores globales de tecnología confiables aportan una experiencia, una inversión, unas capacidades de seguridad y una experiencia operativa significativas que pueden ayudar a acelerar los objetivos digitales nacionales. El reto no consiste en elegir entre soluciones locales y globales, sino en crear marcos que les permitan trabajar juntas de manera eficaz.

Este documento sostiene que América Latina tiene la oportunidad de desarrollar un modelo de soberanía digital equilibrado y con visión de futuro, fundamentado en la seguridad, la resiliencia, la interoperabilidad y la innovación. En lugar de impulsar políticas que fragmenten los ecosistemas digitales, la región puede fortalecer la soberanía ampliando la infraestructura digital confiable, promoviendo una gobernanza de datos basada en riesgos, fomentando la competencia y la capacidad de elección, e impulsando la colaboración entre los gobiernos y la industria. Un enfoque de este tipo puede ayudar a asegurar que los países latinoamericanos mantengan el control sobre su futuro digital y sigan beneficiándose de las oportunidades que crea una economía digital conectada a nivel global.

El futuro de la soberanía digital en América Latina no se definirá por el aislamiento. Se definirá por la capacidad de la región de construir alianzas confiables, fortalecer la resiliencia digital, diversificar las opciones tecnológicas y crear marcos de gobernanza que habiliten tanto la seguridad como la innovación. Al enfocarse en estos objetivos, los países pueden desarrollar ecosistemas digitales que no solo sean soberanos, sino también competitivos, seguros y preparados para los desafíos de la era digital.

Definición de la soberanía digital

Del control a la capacidad

Los debates sobre la soberanía digital suelen comenzar con el concepto de control. Los gobiernos buscan un mayor control sobre los datos, la infraestructura crítica y los servicios digitales que sustentan la actividad económica, la administración pública y la seguridad nacional. Estos objetivos son razonables y cada vez más importantes a medida que las sociedades dependen más de las tecnologías digitales. Sin embargo, definir la soberanía principalmente a partir del control puede dar lugar a políticas que, de manera involuntaria, socaven los resultados que buscan alcanzar. Medidas como los requisitos amplios de localización de datos o las restricciones a los flujos transfronterizos de datos pueden aumentar los costos, limitar el acceso a la innovación, reducir la competencia y generar ineficiencias operativas. Los desafíos de soberanía de datos suelen abordarse mejor mediante la gobernanza, los controles de seguridad y los mecanismos de transparencia que únicamente a través de la localización.[2]

[2] https://www.cloudflare.com/the-net/building-cyber-resilience/challenges-data-sovereignty/

Algunas investigaciones sugieren que los marcos de gobernanza confiables, la interoperabilidad y las prácticas sólidas de seguridad se consideran cada vez más herramientas más eficaces para gestionar el riesgo digital que las restricciones geográficas rígidas.[3]

Para evitar confusiones, resulta útil distinguir varios conceptos relacionados pero diferentes. La soberanía digital se refiere a la capacidad de un país de gobernar y ejercer control sobre su ecosistema digital en sentido amplio, incluidas la infraestructura, los datos, la ciberseguridad y los servicios digitales. La soberanía de datos se refiere al marco jurídico y de gobernanza que se aplica a los datos. La residencia de datos alude a la ubicación física donde los datos se almacenan o procesan, mientras que la localización de datos es el enfoque de política más restrictivo, ya que exige que ciertas categorías de datos permanezcan dentro de las fronteras nacionales y, en algunos casos, limita las transferencias transfronterizas. Como se analiza en el documento de Digi Americas The Challenges of Government Data Centers in Building Resilient Digital Infrastructure, estos conceptos están relacionados, pero no deben utilizarse indistintamente, ya que cada uno tiene implicaciones de política diferentes.[4] Comprender esta jerarquía ayuda a aclarar que la localización de datos es una posible herramienta de política, y no la definición misma de la soberanía digital.

La soberanía digital no requiere autosuficiencia tecnológica. Más bien, requiere la capacidad de tomar decisiones independientes sobre cómo se implementa, se gobierna y se protege la tecnología. A medida que los ecosistemas digitales se vuelven más interconectados, la soberanía se redefine cada vez más en torno a la capacidad y no al control. La pregunta crítica ya no es simplemente dónde residen los datos o quién es dueño de una tecnología determinada. Se trata, más bien, de si los gobiernos, las empresas y los ciudadanos cuentan con las capacidades necesarias para gobernar, proteger y operar de manera segura sus activos digitales, garantizando al mismo tiempo el cumplimiento de las leyes locales y de los objetivos de política pública. Esta perspectiva se refleja en los marcos de soberanía digital desarrollados por los principales proveedores de tecnología, que enfatizan el control operativo,

[3] https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html
[4] https://digiamericas.org/wp-content/uploads/2025/09/DIPF_EN.pdf

la transparencia, la seguridad y la capacidad de elección del cliente en lugar del aislamiento respecto de los ecosistemas tecnológicos globales.[5] [6]

Un enfoque basado en capacidades también coloca la resiliencia y la diversificación en el centro de la soberanía. La importancia de la resiliencia ha quedado demostrada en la práctica. Por ejemplo, las restricciones que Ucrania mantenía antes de la guerra sobre el uso gubernamental de la nube pública dejaron sistemas gubernamentales críticos vulnerables a ataques físicos. Las reformas legales de emergencia que permitieron migrar los datos del gobierno a infraestructura de nube a hiperescala ayudaron a preservar la continuidad de los servicios públicos esenciales tras la invasión rusa, lo que ilustra que la resiliencia operativa —y no la ubicación física por sí sola— puede fortalecer la soberanía digital.[7]

En una era de amenazas cibernéticas crecientes, incertidumbre geopolítica y disrupciones en la cadena de suministro, los países deben garantizar que los servicios críticos puedan seguir operando en condiciones adversas. La soberanía se fortalece cuando las organizaciones pueden recuperarse de las disrupciones, migrar cargas de trabajo cuando sea necesario y evitar la dependencia de un solo proveedor, pila tecnológica o modelo de infraestructura. Por lo tanto, la portabilidad de los datos, la interoperabilidad y las arquitecturas multinube no son amenazas para la soberanía, sino habilitadores importantes de esta. Las investigaciones de empresas tecnológicas líderes de distintos eslabones de la cadena de suministro digital apuntan cada vez más a la flexibilidad, la redundancia y la capacidad de elegir entre proveedores confiables como componentes esenciales de la resiliencia digital moderna.[8] [9] [10]

Para América Latina, esta distinción es particularmente importante. La región tiene la oportunidad de fortalecer la soberanía digital sin sacrificar los beneficios de la conectividad, la inversión y la innovación globales. En lugar de centrarse únicamente en restricciones y en la localización, los responsables de política pueden impulsar un modelo centrado en la seguridad, la resiliencia, la gobernanza y la capacidad de elección. Un enfoque de este tipo permite a los países mantener la autoridad sobre

---

5 https://workspace.google.com/security/digital-sovereignty/
6 https://aws.amazon.com/compliance/digital-sovereignty/
7 https://digiamericas.org/wp-content/uploads/2025/09/DIPF_EN.pdf
8 https://cloud.google.com/resources/content/digital-sovereignty-infographic
9 https://www.cisco.com/site/us/en/learn/topics/computing/what-is-sovereign-cloud.html
10 https://blogs.nvidia.com/blog/what-is-sovereign-ai/

sus activos digitales críticos y seguir beneficiándose de alianzas confiables, tecnologías avanzadas y ecosistemas digitales integrados a nivel global. En última instancia, la soberanía digital no debe medirse por la eficacia con la que un país se aísla de la economía digital, sino por su capacidad de gobernar, proteger y sostener con confianza las capacidades digitales de las que depende su futuro.

Las capas y los principios de la soberanía digital

La soberanía digital no es una única política, tecnología o marco regulatorio. Es, más bien, el producto de capacidades que abarcan múltiples capas del ecosistema digital. En la base se encuentra la infraestructura física y digital, que incluye los centros de datos, las redes de conectividad, las plataformas de nube y los recursos de cómputo.[11] Por encima de esa capa se sitúa la gobernanza de datos, que comprende la protección de datos, la privacidad, el cifrado, los controles de residencia y los mecanismos de cumplimiento. Las capacidades de ciberseguridad aportan las funciones de visibilidad, detección de amenazas y respuesta a incidentes necesarias para proteger los activos digitales, mientras que la irrupción de la inteligencia artificial suma nuevas consideraciones relacionadas con el acceso al cómputo, la gobernanza de modelos, la gestión de datos y la capacidad de innovación.[12] [13] [14]

Si bien las tecnologías específicas pueden variar, las estrategias exitosas de soberanía se guían cada vez más por varios principios comunes. En primer lugar, la soberanía debe preservar la capacidad de elección y la flexibilidad, permitiendo que los gobiernos y las organizaciones seleccionen las tecnologías y los proveedores que mejor respondan a sus necesidades, en lugar de generar dependencia de una sola plataforma o ecosistema.[15] [16] En segundo lugar, la soberanía debe estar impulsada por la seguridad, reconociendo que las prácticas sólidas de ciberseguridad, la inteligencia de amenazas, el cifrado y la infraestructura resiliente suelen brindar una mayor protección que las restricciones geográficas por sí solas.[17] [18]

---

[11] https://www.trendmicro.com/en/what-is/data-sovereignty/digital-sovereignty.html
[12] https://aws.amazon.com/blogs/security/aws-digital-sovereignty-pledge-control-without-compromise/
[13] https://cloud.google.com/blog/products/identity-security/delivering-a-secure-open-sovereign-digital-world
[14] https://blogs.nvidia.com/blog/what-is-sovereign-ai/
[15] https://blog.cloudflare.com/sovereign-ai-and-choice/
[16] https://cloud.google.com/transform/digital-sovereignty-101-your-questions-answered/
[17] https://blog.checkpoint.com/security/securing-latin-america-in-2025-how-ai-and-cyber-threat-intelligence-are-reshaping-the-cyber-security-landscape/
[18] https://www.crowdstrike.com/en-us/resources/reports/latam-threat-landscape-report/

Este enfoque se alinea con marcos emergentes del sector que definen la confianza a partir de criterios objetivos y basados en evidencia, en lugar de la ubicación geográfica por sí sola. Estos marcos enfatizan la gobernanza, la gestión de riesgos y la transparencia como pilares centrales para evaluar a socios tecnológicos de confianza.[19] Esta perspectiva refuerza la idea de que la interconexión global entre socios confiables puede fortalecer la resiliencia, la seguridad y la competitividad, siempre que esas relaciones estén respaldadas por mecanismos claros de rendición de cuentas, controles de seguridad y prácticas transparentes de gestión de riesgos.

Igualmente importante es el principio de interoperabilidad.[20] La resiliencia digital moderna depende de la capacidad de mover datos, aplicaciones y cargas de trabajo entre entornos confiables cuando las circunstancias lo requieran. La portabilidad de los datos, los estándares abiertos y las arquitecturas interoperables reducen los puntos únicos de falla y fortalecen la continuidad operativa, lo que los convierte en componentes esenciales de un ecosistema digital soberano.[21] Por último, una soberanía eficaz combina proveedores globales de tecnología confiables con la gobernanza y el control locales, lo que permite a los países beneficiarse de la innovación, la inversión y la experiencia en seguridad a nivel global, manteniendo al mismo tiempo la autoridad sobre cómo se gobiernan y utilizan los activos digitales críticos.[22] [23]

En conjunto, estas capas y principios ilustran que la soberanía digital no se logra mediante el aislamiento. Se construye a partir de una infraestructura segura, una gobernanza eficaz, una ciberseguridad resiliente, el acceso a la innovación y la flexibilidad para operar dentro de un ecosistema digital global confiable e interconectado.

El contexto de América Latina

Impulsores regionales

Varias tendencias convergentes están convirtiendo a la soberanía digital en una consideración política cada vez más importante en América Latina. En primer lugar, los gobiernos de toda la

[19] https://www.itic.org/news-events/news-releases/iti-launches-framework-to-promote-secure-resilient-technology-ecosystems
[20] https://id4d.worldbank.org/guide/interoperability-frameworks
[21] https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2025.pdf
[22] https://www.mastercard.com/gb/en/news-and-trends/perspectives/2025/championing-trust-and-innovation-in-europe-s-digital-economy.html
[23] https://blog.google/intl/en-ca/products/supporting-businesses/advancing-sovereignty-choice-and-security-in-the-cloud-for-our-customers-in-canada/

región están modernizando sus marcos de protección de datos, privacidad, ciberseguridad y gobernanza digital a medida que los servicios digitales se integran más profundamente en el desarrollo económico y social.[24] Estos esfuerzos reflejan un reconocimiento creciente de que los ecosistemas digitales confiables son esenciales para atraer inversión, habilitar la innovación y respaldar la transformación digital.[25]

Al mismo tiempo, América Latina enfrenta un panorama de amenazas cibernéticas cada vez más sofisticado.[26] Los gobiernos, las instituciones financieras, los operadores de infraestructura crítica y las organizaciones del sector privado experimentan un volumen creciente de ataques de ransomware, filtraciones de datos, campañas de fraude y actividad patrocinada por Estados. Evaluaciones recientes de los principales proveedores de ciberseguridad indican que las amenazas cibernéticas dirigidas a la región siguen aumentando tanto en frecuencia como en complejidad, lo que genera una mayor demanda de infraestructura resiliente, capacidades de seguridad avanzadas y alianzas digitales confiables.[27] [28]

La magnitud del desafío es significativa. Investigaciones previas de Digi Americas encontraron que América Latina sufre más de 18.5 millones de ciberataques al año, mientras que solo siete de los 32 países de la región cuentan con marcos regulatorios para proteger la infraestructura crítica y solo 20 han establecido Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés).[29] Incidentes recientes — entre ellos el ataque de ransomware sufrido por Costa Rica en 2022, que derivó en la primera declaratoria de emergencia nacional del mundo a causa de un ciberataque, y el ataque de 2023 contra IFX Networks, que afectó a 78 entidades públicas y a más de 760 empresas privadas en la región— ponen de relieve la creciente importancia de contar con infraestructura digital resiliente y capacidades de ciberseguridad coordinadas.

La rápida adopción de la inteligencia artificial está generando presiones adicionales. Los gobiernos y las empresas buscan cada vez más acceso a la computación en la nube, a modelos avanzados de IA, al análisis de datos y a la infraestructura digital que puedan respaldar el crecimiento económico y

---

[24] https://desarrollodigital.cepal.org/en/indicators
[25] https://www.worldbank.org/en/programs/lac-digital
[26] https://www.crowdstrike.com/en-us/resources/reports/latam-threat-landscape-report/
[27] https://www.crowdstrike.com/en-us/resources/reports/latam-threat-landscape-report/
[28] https://www.mastercard.com/us/en/news-and-trends/stories/2025/ai-human-intelligence-cybersecurity.html
[29] https://digiamericas.org/wp-content/uploads/2025/09/DIPF_EN.pdf

la modernización del sector público.[30] Al mismo tiempo, los responsables de política evalúan cómo garantizar que estas tecnologías se implementen de maneras que se alineen con las prioridades nacionales, protejan la información sensible y promuevan los ecosistemas locales de innovación.[31] [32]

Estas dinámicas se desarrollan en un contexto de creciente competencia geopolítica y de mayor conciencia sobre las dependencias tecnológicas. Sin embargo, a diferencia de algunas regiones que han optado por enfoques más proteccionistas, América Latina ha favorecido en general la apertura, la inversión internacional y la integración digital global. Esto crea una oportunidad para que los países de la región desarrollen estrategias de soberanía que fortalezcan la seguridad, la resiliencia y las capacidades nacionales sin sacrificar los beneficios de participar en la economía digital global.

Construir sobre los cimientos estructurales existentes

La búsqueda de la soberanía digital en América Latina tiene lugar dentro de un panorama digital diverso y en evolución. Los niveles de desarrollo de la infraestructura digital, la adopción de la nube, la conectividad y la madurez en ciberseguridad varían de manera significativa entre los países y dentro de ellos. Si bien varios mercados se han consolidado como polos tecnológicos regionales, otros siguen enfrentando desafíos relacionados con el acceso a banda ancha, la capacidad de los centros de datos, el desarrollo de competencias digitales y el acceso a tecnologías avanzadas. Los enfoques regulatorios también evolucionan a distintas velocidades, lo que genera un entorno complejo para las organizaciones que operan en múltiples jurisdicciones.

Sin embargo, estos desafíos también deben verse como oportunidades. Dado que buena parte de la infraestructura digital de la región aún se encuentra en desarrollo, muchos países no están limitados por sistemas heredados y pueden adoptar enfoques modernos, habilitados por la nube y centrados en la seguridad desde el inicio. La creciente inversión en infraestructura de nube a hiperescala, servicios de ciberseguridad y capacidades de inteligencia artificial está ampliando el acceso a tecnologías que antes solo estaban disponibles en un número limitado de mercados. Al mismo tiempo, los gobiernos, las universidades y los socios del sector privado intensifican sus esfuerzos por fortalecer las competencias digitales

[30] https://www.oecd.org/en/publications/digital-government-outlook_0496b2bc-en/full-report/adopting-and-governing-ai-in-government_7ef312a9.html
[31] https://blogs.nvidia.com/blog/what-is-sovereign-ai/
[32] https://cloud.google.com/resources/content/strategic-importance-of-digital-sovereignty

y de ciberseguridad, lo que contribuye a formar la base de talento necesaria para sostener la transformación digital a largo plazo.

En lugar de ver las brechas de infraestructura, de fuerza laboral y regulatorias como barreras para la soberanía, los responsables de política pueden considerarlas áreas de inversión estratégica. Al enfocarse en la infraestructura digital, la capacidad de ciberseguridad, el desarrollo del talento y la modernización regulatoria, los países pueden fortalecer tanto sus capacidades digitales nacionales como su atractivo como destinos para la inversión tecnológica. El resultado puede ser un ecosistema digital más resiliente y competitivo que impulse el crecimiento económico y, a la vez, avance en los objetivos de soberanía.

La ventana de oportunidad

América Latina está en una posición singular para definir un enfoque moderno de la soberanía digital. A diferencia de las regiones que intentan adaptar requisitos de soberanía a ecosistemas digitales con décadas de antigüedad, muchos países de América Latina están construyendo la próxima generación de infraestructura digital justo cuando la soberanía, la ciberseguridad, la computación en la nube y la inteligencia artificial se convierten en prioridades estratégicas.[33] Esto crea la oportunidad de diseñar políticas que promuevan la seguridad, la resiliencia y la innovación de manera simultánea, en lugar de tratarlas como objetivos en competencia.

Un número creciente de proveedores globales de tecnología está invirtiendo en infraestructura de nube regional, capacidades de ciberseguridad, recursos de IA y programas de competencias digitales en toda América Latina. Combinadas con los crecientes esfuerzos de digitalización del sector público, estas inversiones crean condiciones favorables para que los países fortalezcan sus capacidades soberanas y mantengan al mismo tiempo el acceso a los ecosistemas globales de innovación.[34] [35] En lugar de perseguir modelos costosos y potencialmente restrictivos de autosuficiencia tecnológica, los países pueden aprovechar alianzas confiables para acelerar el desarrollo de una infraestructura digital segura y resiliente.

La cooperación regional también representa una oportunidad significativa. Muchos de los desafíos

[33] https://privatebank.jpmorgan.com/latam/en/insights/markets-and-investing/ideas-and-insights/wired-for-growth-latin-americas-digital-infrastructure-crossroads
[34] https://aws.amazon.com/blogs/security/aws-digital-sovereignty-pledge-control-without-compromise/
[35] https://cloud.google.com/resources/content/forrester-digital-sovereignty-trends

asociados con la ciberseguridad, la gobernanza de datos, la infraestructura digital y la adopción de la IA trascienden las fronteras nacionales. Una mayor alineación en los enfoques regulatorios, los flujos transfronterizos de datos, la cooperación en ciberseguridad y el fortalecimiento de capacidades digitales puede ayudar a los países a alcanzar sus objetivos de soberanía preservando al mismo tiempo los beneficios de la integración regional y global. Al anclar las estrategias de soberanía digital en la seguridad, la inversión, la interoperabilidad y la colaboración, América Latina tiene la oportunidad de convertirse en un modelo global de un enfoque abierto, resiliente e impulsado por la innovación.

La soberanía en la práctica

Ciberseguridad

La ciberseguridad ofrece quizá la ilustración más clara de que la soberanía no puede separarse de la resiliencia. América Latina sufre más de 18.5 millones de ciberataques al año y, sin embargo, solo siete de los 32 países de la región han establecido marcos regulatorios para proteger la infraestructura crítica y solo 20 mantienen CSIRT nacionales. Estas brechas de capacidad refuerzan la importancia de construir ecosistemas de ciberseguridad resilientes y colaborativos.[36]

Los ecosistemas modernos de ciberseguridad se apoyan en una combinación de experiencia local, inteligencia de amenazas global, tecnologías avanzadas y modelos de defensa colaborativa. Los actores de amenazas operan habitualmente a través de las fronteras, lo que hace que el intercambio de información, los mecanismos de respuesta coordinada y el acceso a la inteligencia de amenazas global sean componentes cada vez más importantes de la resiliencia cibernética nacional.[37] [38]

Investigaciones recientes también han destacado las posibles implicaciones para la ciberseguridad de las políticas restrictivas de localización de datos. La defensa cibernética eficaz depende cada vez más del intercambio oportuno de inteligencia de amenazas, telemetría de seguridad e información sobre respuesta a incidentes entre socios y jurisdicciones de confianza. Las políticas que restringen innecesariamente estos flujos de datos pueden reducir la capacidad de las organizaciones de identificar, proteger, detectar, responder y recuperarse ante ciberataques, al limitar la visibilidad sobre las amenazas emergentes y retrasar las respuestas coordinadas.[39]

---

[36] https://digiamericas.org/wp-content/uploads/2025/09/DIPF_EN.pdf
[37] https://www.crowdstrike.com/en-us/resources/reports/latam-threat-landscape-report/
[38] https://blog.checkpoint.com/research/latin-america-2025-mid-year-cyber-snapshot-reveals-39-surge-in-attacks-as-ai-threats-escalate-regional-risk/
[39] https://www.tandfonline.com/doi/full/10.1080/23738871.2024.2384724

De manera similar, concentrar datos sensibles o sistemas críticos en una sola ubicación geográfica puede crear, sin quererlo, blancos atractivos tanto para ataques cibernéticos como físicos, lo que aumenta la vulnerabilidad al espionaje, el sabotaje y la interrupción de los servicios. Las restricciones a los flujos transfronterizos de datos también pueden dificultar la investigación y la mitigación rápidas de incidentes cibernéticos que requieren cooperación internacional. Como lo demuestran los ataques recientes contra infraestructura gubernamental en América Latina y en otras regiones, la ubicación física por sí sola no garantiza la seguridad. Lejos de fortalecer la resiliencia, una localización excesiva puede reducir la redundancia, limitar el acceso a la experiencia global en ciberseguridad y generar puntos ciegos operativos.

Estas consideraciones también tienen implicaciones estratégicas más amplias. Los marcos fragmentados de gobernanza de datos y las restricciones innecesarias a los flujos transfronterizos de datos confiables pueden complicar el comercio internacional, limitar el acceso a servicios digitales avanzados y a capacidades de inteligencia artificial, y aumentar los costos de cumplimiento tanto para los gobiernos como para las empresas. En una región donde la ciberseguridad depende en gran medida de la cooperación internacional, preservar el intercambio confiable de información con aliados, proveedores de tecnología y socios regionales sigue siendo un componente importante de la resiliencia cibernética nacional.

Estas dinámicas subrayan la importancia de las políticas que enfatizan protecciones técnicas sólidas —incluidos el cifrado, la gestión de identidades y accesos, las arquitecturas seguras por diseño y la gobernanza de datos— con independencia de dónde se encuentren físicamente los datos. Del mismo modo, la cooperación internacional, las transferencias transfronterizas seguras de datos y la inversión continua en infraestructura de ciberseguridad ayudan a fortalecer la resiliencia y a la vez preservan los beneficios de un ecosistema digital interconectado.

Al mismo tiempo, los avances en inteligencia artificial están transformando tanto las operaciones cibernéticas ofensivas como las defensivas. La detección habilitada por IA, las capacidades de respuesta automatizada y el análisis de amenazas en tiempo real se están convirtiendo en herramientas importantes para proteger la infraestructura crítica y los servicios digitales.[40][41] Como

[40] https://www.sophos.com/en-us/content/security-threat-report
[41] https://cloud.google.com/security/resources/m-trends

resultado, la soberanía en materia de ciberseguridad se define cada vez más no simplemente por la propiedad de las herramientas de seguridad, sino por la capacidad de mantener la visibilidad, la conciencia situacional y un control eficaz en un entorno de amenazas que evoluciona con rapidez.

Inteligencia artificial

La inteligencia artificial se está convirtiendo rápidamente en un componente importante de los debates sobre soberanía digital en todo el mundo. A medida que los sistemas de IA se integran en la actividad económica, los servicios gubernamentales, la investigación científica y la infraestructura crítica, surgen preguntas sobre el acceso a los recursos de cómputo, la gobernanza de los datos de entrenamiento y de los modelos, la transparencia, la seguridad y la competitividad tecnológica a largo plazo.

En América Latina, varios países ya han adoptado o están desarrollando estrategias nacionales de IA. A medida que los gobiernos buscan implementar capacidades de IA cada vez más sofisticadas, el acceso a infraestructura de cómputo escalable, a ciberseguridad avanzada, a talento calificado y a ecosistemas tecnológicos confiables se convertirá en un componente central de la soberanía en IA.

Algunos países exploran cómo fortalecer sus capacidades nacionales de IA mediante inversiones en infraestructura, talento, investigación y ecosistemas de innovación. Otros se centran en asegurar que las organizaciones conserven un control significativo sobre cómo se implementan, gobiernan e integran los sistemas de IA en funciones críticas. Estos debates reconocen cada vez más que la soberanía en IA va más allá del acceso a los modelos en sí y abarca el ecosistema más amplio de cómputo, datos, ciberseguridad, gobernanza y capital humano que sustenta el desarrollo y la adopción de la IA.[42] [43]

Para América Latina, la IA representa una oportunidad de ampliar las capacidades digitales y, al mismo tiempo, evitar nuevas formas de dependencia. A medida que la tecnología continúa evolucionando,

[42] https://blogs.nvidia.com/blog/what-is-sovereign-ai/
[43] https://cloud.google.com/resources/content/strategic-importance-of-digital-sovereignty

mantener la flexibilidad, promover la interoperabilidad, apoyar la innovación local y garantizar el acceso a ecosistemas tecnológicos diversos puede resultar tan importante como cualquier plataforma o proveedor de IA en particular. En ese sentido, los mismos principios que sustentan la soberanía digital moderna —la capacidad de elección, la resiliencia, la seguridad y las alianzas confiables— también están dando forma cada vez más a los debates sobre el futuro de la soberanía en IA.[44] [45]

La intersección entre la IA y la ciberseguridad

A medida que las organizaciones implementan sistemas de IA cada vez más sofisticados, la ciberseguridad y la gobernanza de la IA se vuelven componentes inseparables de la resiliencia digital.[46] El uso de la IA para detectar amenazas cibernéticas representa una ventaja enorme. Los equipos de seguridad requieren conciencia contextual y visibilidad de la totalidad de sus entornos, incluidos los entornos de nube y los efímeros, y la IA puede ayudar a los defensores a procesar estos datos y a hacer que las detecciones sean más accionables. La IA es la mejor herramienta con la que cuentan los defensores para identificar y prevenir ataques de día cero y ataques sin malware, porque puede vencer amenazas novedosas a partir de indicios de comportamiento en lugar de firmas conocidas.

Por otro lado, la IA también está acelerando muchas cosas que tradicionalmente requerían conocimiento, recursos o tiempo, o los tres a la vez. Las herramientas de IA están reduciendo la barrera de entrada para los adversarios cibernéticos que buscan ataques lucrativos y destructivos. Los adversarios aprovechan la IA para la ingeniería social, las operaciones técnicas y las operaciones de información. Por ejemplo, en el caso de la ingeniería social, las herramientas de IA generativa resultan particularmente útiles para elaborar mejores señuelos de phishing —correos electrónicos que suenan más realistas—, crear identidades falsas en línea, especialmente personas ficticias, y comunicarse de manera más verosímil con las víctimas. La IA generativa también puede utilizarse para rastrear grandes conjuntos de datos, como los provenientes de filtraciones previas, o código en busca de vulnerabilidades. Los adversarios también están usando IA para generar grandes volúmenes de desinformación e incluso para desplegar campañas de ataque multilingües.

---

[44] https://www.paladincapgroup.com/wp-content/uploads/2025/06/AI-Tech-Stack-Report.pdf
[45] https://blogs.nvidia.com/blog/what-is-sovereign-ai/
[46] https://www.crowdstrike.com/content/dam/crowdstrike/marketing/en-us/documents/pdfs/public-policy/AI-Action-Plan-Comments.pdf

Los actores de amenazas están viendo las herramientas de IA como infraestructura integrada, y no como aplicaciones periféricas, y las convierten en vectores de ataque primarios. A medida que las organizaciones continúen adoptando herramientas de IA, la superficie de ataque seguirá expandiéndose y las herramientas de IA confiables surgirán como la próxima amenaza interna.

Ya estamos viendo herramientas que permiten descubrir vulnerabilidades a velocidad de máquina.[47] La IA permite a los equipos de seguridad estar a la altura del ritmo acelerado de los ataques. Por ejemplo, los agentes de IA pueden analizar volúmenes masivos de datos, detectar patrones y responder a las amenazas a velocidad de máquina, mientras los analistas humanos se concentran en la estrategia y la supervisión. Por ello, es urgente que la seguridad se incorpore a los sistemas de IA y que las organizaciones se adapten a las amenazas impulsadas por IA y modernicen sus políticas y operaciones de ciberseguridad.[48] Esto hace aún más oportuno que los conceptos relacionados con la soberanía digital no se malinterpreten de una manera que conduzca a peores resultados en materia de ciberseguridad.

Infraestructura y nube

En su base, la soberanía digital depende del acceso a una infraestructura digital segura, resiliente y confiable. Esto incluye los centros de datos, las redes de telecomunicaciones, los recursos de computación en la nube, la infraestructura de borde y los sistemas físicos que sustentan los servicios digitales. A medida que los gobiernos y las empresas dependen cada vez más de las tecnologías digitales, la disponibilidad y la resiliencia de esta infraestructura se convierten en una consideración estratégica para el crecimiento económico, los servicios públicos y la seguridad nacional.

En América Latina, la inversión en infraestructura de nube y en capacidad regional de centros de datos se ha acelerado en los últimos años, lo que amplía el acceso a recursos de cómputo avanzados y a la vez ayuda a atender preocupaciones relacionadas con la latencia, la resiliencia y el cumplimiento regulatorio.[49]

---

47 https://www.crowdstrike.com/en-us/blog/three-principles-to-safely-scale-agentic-ai/
48 https://www.crowdstrike.com/en-us/blog/shadow-ai-hidden-risk-expanding-across-the-enterprise/
49 https://www.undp.org/latin-america/blog/data-clouds-centers-ground-role-data-centers-lacs-digital-future

Al mismo tiempo, la creciente demanda de inteligencia artificial, servicios digitales y protección de infraestructura crítica está impulsando debates más amplios sobre cómo debe desarrollarse, gobernarse y sostenerse esa infraestructura a largo plazo.[50] [51]

Los enfoques regionales ya demuestran que no existe un modelo único para alcanzar la soberanía digital. Países como Argentina, Brasil, Chile, Colombia, Costa Rica, México, Paraguay y Uruguay han adoptado distintas combinaciones de estrategias de nube pública, nube privada y nube híbrida, al tiempo que fortalecen su legislación de privacidad y sus marcos de gobernanza digital. Esta diversidad ilustra que los objetivos de soberanía pueden perseguirse mediante múltiples modelos de infraestructura, según las prioridades nacionales, los entornos regulatorios y los niveles de madurez digital.[52]

La soberanía digital no exige necesariamente que cada componente de la infraestructura digital se desarrolle a nivel nacional. La pregunta central es, más bien, si los países tienen acceso a una infraestructura confiable y resiliente que respalde los objetivos nacionales y a la vez brinde flexibilidad, seguridad y continuidad del servicio. Las alianzas público-privadas, las estrategias regionales de inversión y los ecosistemas de infraestructura diversificados pueden contribuir a estas metas.

Muchos gobiernos también exploran enfoques híbridos que combinan infraestructura operada por el Estado con servicios de nube comerciales, lo que permite a las organizaciones alinear distintas cargas de trabajo con los requisitos operativos, de seguridad y regulatorios que correspondan. Los modelos híbridos ilustran que la soberanía se concibe cada vez más como una cuestión de gobernanza y de gestión de cargas de trabajo, y no como una decisión de infraestructura de "todo o nada".

Los gobiernos que consideren una mayor inversión en infraestructura digital nacional también deben tomar en cuenta consideraciones prácticas como los requerimientos de capital, los ciclos de renovación tecnológica, la dotación de personal de ciberseguridad, la escalabilidad y el rápido ritmo de la innovación. Estos factores influyen cada vez más en la resiliencia y la sostenibilidad a largo plazo, sin importar el modelo de infraestructura que se elija.[53]

---

[50] https://www.cisco.com/site/us/en/solutions/sovereign-critical-infrastructure/index.html
[51] https://www.se.com/ww/en/insights/sustainability/technology-and-innovation/reimagining-data-centers-ai-for-sustainable-impact/
[52] https://digiamericas.org/wp-content/uploads/2025/09/DIPF_EN.pdf
[53] https://digiamericas.org/wp-content/uploads/2025/09/DIPF_EN.pdf

Nube soberana

A medida que la computación en la nube se convierte en la base de la transformación digital, muchos gobiernos y organizaciones exploran cómo los servicios de nube pueden respaldar los objetivos de soberanía. El concepto de nube soberana ha surgido como uno de esos enfoques y, en general, se refiere a entornos de nube que ofrecen controles reforzados sobre los datos, las operaciones, el cumplimiento y la gobernanza, manteniendo al mismo tiempo el acceso a la escalabilidad y la innovación propias de las plataformas de nube modernas.[54]

Es importante señalar que la nube soberana no es una única tecnología ni un solo modelo de implementación. Según los requisitos nacionales, las capacidades de nube soberana pueden incluir entornos dedicados, despliegues de nube regionales, claves de cifrado gestionadas por el cliente, controles operativos y arquitecturas de nube híbrida que brinden mayor flexibilidad al tiempo que respaldan objetivos de cumplimiento, seguridad y resiliencia. Cada vez más, los proveedores de nube ofrecen una variedad de capacidades enfocadas en la soberanía, diseñadas para atender distintos requisitos legales, regulatorios y operativos, preservando a la vez la interoperabilidad y el acceso a los servicios globales.[55]

El creciente interés en los modelos de nube soberana refleja un cambio más amplio: pasar de concebir la soberanía como una cuestión de ubicación a entenderla como una cuestión de gobernanza, seguridad y control operativo. En lugar de centrarse únicamente en dónde se ubica la infraestructura, las organizaciones evalúan cada vez más cómo los entornos de nube pueden brindar seguridad, transparencia, resiliencia y un control operativo significativo sobre los activos digitales críticos.

Gobernanza de datos

La gobernanza de datos ocupa el centro de muchos debates sobre soberanía porque los datos funcionan cada vez más como un activo estratégico para los gobiernos, las empresas y las personas. A medida que los países desarrollan economías digitales y adoptan nuevas tecnologías, los responsables de política analizan cómo pueden protegerse, gobernarse y aprovecharse los datos de maneras que respalden tanto las prioridades nacionales como la innovación económica.

Estos debates suelen ir más allá de las cuestiones de ubicación de los

[54] https://www.cisco.com/site/us/en/learn/topics/computing/what-is-sovereign-cloud.html
[55] https://aws.amazon.com/compliance/europe-digital-sovereignty/

datos. La residencia de datos y la soberanía de datos son conceptos relacionados pero distintos. La residencia de datos se refiere a dónde se almacenan los datos, mientras que la soberanía de datos concierne a cómo se gobiernan, protegen y controlan. Una soberanía eficaz suele lograrse mediante mecanismos de gobernanza, cifrado y rendición de cuentas, con independencia de dónde se ubiquen físicamente los datos.[56]

Una gobernanza eficaz comienza también por comprender qué datos existen y cuán sensibles son. Desarrollar un marco de clasificación de datos basado en riesgos permite a los gobiernos determinar qué información requiere protección reforzada y qué datos pueden beneficiarse de una mayor interoperabilidad y de servicios habilitados por la nube. Los marcos de clasificación aportan una base práctica para aplicar requisitos de gobernanza, residencia y seguridad proporcionales a la sensibilidad de las distintas categorías de datos.[57]

Si bien algunas categorías de información sensible pueden justificar requisitos de manejo específicos, los marcos modernos de gobernanza de datos incorporan cada vez más un conjunto más amplio de herramientas, incluidos el cifrado, los controles de acceso, los mecanismos de auditoría, las protecciones de privacidad y los marcos de rendición de cuentas.[58] Estos enfoques reconocen que la soberanía puede alcanzarse mediante mecanismos de gobernanza y seguridad, además de los requisitos de residencia física.

Incidentes recientes también demuestran que la ubicación física por sí sola no garantiza la seguridad. El ataque de ransomware de 2024 contra el centro nacional de datos de Indonesia interrumpió más de 200 servicios públicos, lo que ilustra que concentrar sistemas críticos en un único entorno puede, en sí mismo, generar riesgo operativo.[59] Por lo tanto, una soberanía eficaz depende no solo de dónde residen los datos, sino también de la resiliencia, la redundancia, la gobernanza y las capacidades de ciberseguridad.[60]

---

[56] https://www.ibm.com/think/topics/data-sovereignty-vs-data-residency
[57] https://digiamericas.org/wp-content/uploads/2025/09/DIPF_EN.pdf
[58] https://www.cloudflare.com/the-net/building-cyber-resilience/ai-data-governance/
[59] https://www.reuters.com/technology/cybersecurity/cyber-attack-compromised-indonesia-data-centre-ransom-sought-reports-antara-2024-06-24/
[60] https://digiamericas.org/wp-content/uploads/2025/09/DIPF_EN.pdf

El reto para los responsables de política consiste en equilibrar la necesidad de proteger la información sensible con los beneficios de los flujos transfronterizos de datos que sustentan el comercio, la innovación, la ciberseguridad y las tecnologías emergentes. A medida que los ecosistemas digitales se vuelven más interconectados, los marcos de gobernanza eficaces desempeñarán un papel cada vez más importante para habilitar tanto la seguridad como el crecimiento económico.[61]

Construir un futuro digital soberano

La soberanía digital no puede lograrse con los gobiernos o la industria actuando por separado. Surge de una combinación de infraestructura confiable, gobernanza eficaz, ciberseguridad resiliente, innovación tecnológica y colaboración en todo el ecosistema digital. A medida que los países de América Latina continúan modernizando sus economías y sus servicios públicos, es probable que los enfoques más exitosos sean aquellos que equilibren las prioridades nacionales con los beneficios de la conectividad, la inversión y la innovación globales.

La diversificación se está convirtiendo cada vez más en un componente central de la soberanía digital, no solo entre proveedores de nube y ciberseguridad, sino también a lo largo de la cadena de suministro tecnológica más amplia que sostiene el hardware, el software, la conectividad, los centros de datos, la infraestructura de IA y los servicios digitales. Así como los países buscan diversificar sus fuentes de energía o sus cadenas de suministro, la resiliencia digital se fortalece cuando las organizaciones pueden apoyarse en múltiples proveedores, plataformas interoperables y cargas de trabajo portables. La diversificación reduce los puntos únicos de falla y brinda mayor flexibilidad para responder ante disrupciones técnicas, económicas o geopolíticas.

La industria desempeña un papel importante en este proceso al desarrollar tecnologías y servicios que permiten a las organizaciones ejercer un mayor control sobre sus entornos digitales. Cada vez más, los proveedores de nube, ciberseguridad y tecnología incorporan capacidades que refuerzan la soberanía directamente en sus ofertas, entre ellas opciones de residencia de datos, controles de cifrado, herramientas de gobernanza, mecanismos de

[61] https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2025.pdf

cumplimiento y arquitecturas seguras por diseño.[62] [63] [64] Estas capacidades permiten a los gobiernos y a las organizaciones perseguir objetivos de soberanía manteniendo al mismo tiempo el acceso a tecnologías avanzadas y a la experiencia global en seguridad.

Al mismo tiempo, la soberanía depende cada vez más de equilibrar las prioridades regionales con ecosistemas digitales conectados a nivel global. La infraestructura local y regional puede respaldar la resiliencia, el desempeño y los objetivos regulatorios, mientras que el acceso a la inteligencia de amenazas global, a los servicios de nube y a los ecosistemas de innovación fortalece la seguridad y la competitividad.[65] [66] La capacidad de operar entre entornos confiables e interoperables ayuda a reducir los puntos únicos de falla y respalda la continuidad durante períodos de disrupción.

La colaboración público-privada seguirá siendo igualmente importante. Los gobiernos, la industria, la academia y la sociedad civil aportan cada uno una experiencia única frente a desafíos como la ciberseguridad, el desarrollo de infraestructura digital, la identidad digital, la modernización de los pagos, la gobernanza de la inteligencia artificial y el desarrollo del talento. Los enfoques colaborativos pueden ayudar a asegurar que los marcos de política sean a la vez eficaces y adaptables, al tiempo que crean oportunidades para ampliar las capacidades digitales en toda la región.[67] [68]

---

[62] https://aws.amazon.com/blogs/security/aws-digital-sovereignty-pledge-control-without-compromise/

[63] https://www.cloudflare.com/the-net/building-cyber-resilience/ai-data-governance/

[64] https://www.sophos.com/en-us/content/security-threat-report

[65] https://www.crowdstrike.com/en-us/press-releases/crowdstrike-expands-cybersecurity-ecosystem-to-latin-america/

[66] https://www.sophos.com/en-us/press/press-releases/2025/11/sophos-accelerates-growth-and-leadership-latin-america-strong-regional

[67] https://www.mastercard.com/news/latin-america/en/newsroom/press-releases/pr-en/2025/december/innovation-forum-2025–five-key-takeaways-on-ai-cybersecurity-and-financial-inclusion/

[68] https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-057/19

A medida que los responsables de política evalúan estrategias de soberanía, varias consideraciones más amplias merecen atención. Los enfoques que preservan la interoperabilidad, respaldan los flujos transfronterizos de datos, fomentan la inversión y fortalecen las capacidades de ciberseguridad pueden ayudar a maximizar tanto la resiliencia como la innovación. Por el contrario, las políticas que de manera involuntaria fragmentan los ecosistemas digitales o limitan el acceso a los recursos globales de seguridad y tecnología pueden generar nuevos desafíos sin necesariamente mejorar los resultados en materia de soberanía.[69] [70] [71]

Un marco práctico para evaluar la soberanía digital confiable

Para traducir la soberanía digital de un objetivo de política pública a una capacidad operativa, los gobiernos y las organizaciones pueden aplicar un marco práctico de evaluación basado en tres preguntas: cómo se gobiernan los sistemas digitales, cómo se gestionan los riesgos y cómo se demuestra la transparencia. Este enfoque permite a los responsables de la formulación de políticas evaluar a los socios tecnológicos y la infraestructura digital con base en criterios objetivos, en lugar de depender principalmente de la geografía, la propiedad o la ubicación de la sede corporativa como sustitutos de la confianza.

Este marco no debería operar como un régimen rígido de certificación. Más bien, debería servir como una herramienta proporcional y basada en evidencia que pueda adaptarse a distintas cargas de trabajo, sectores y entornos de amenaza. Una base de datos de salud pública, una plataforma de administración tributaria, un entorno de entrenamiento de IA, un sistema de pagos y una carga de trabajo de defensa pueden requerir controles diferentes. Lo importante es determinar si el entorno tecnológico elegido puede demostrar niveles adecuados de gobernanza, resiliencia, seguridad, interoperabilidad y rendición de cuentas según el nivel de riesgo.

---

[69] https://www.cloudflare.com/the-net/building-cyber-resilience/challenges-data-sovereignty/
[70] https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html
[71] https://www.crowdstrike.com/en-us/resources/reports/latam-threat-landscape-report/

Marco de evaluación de la soberanía digital

Pilar	Pregunta central	Controles ilustrativos	Resultados medibles
Gobernanza	¿Los activos digitales están gobernados bajo marcos legales, institucionales y de rendición de cuentas claros?	Marco de clasificación de datos; autoridad responsable definida; base legal documentada para el procesamiento de datos; reglas de contratación basadas en criterios objetivos de seguridad y confianza; revisión de gobernanza del proveedor.	Cargas de trabajo críticas clasificadas; autoridad responsable identificada; obligaciones legales y de cumplimiento mapeadas; criterios de contratación aplicados de manera consistente entre proveedores.
Gestión de riesgos	¿Los riesgos se identifican, mitigan, monitorean y revisan durante todo el ciclo de vida tecnológico?	Evaluaciones de riesgo cibernético; gestión de riesgos de la cadena de suministro; gestión de vulnerabilidades; ciclo de vida de desarrollo seguro de software; planes de respuesta a incidentes; pruebas de continuidad del negocio y recuperación ante desastres; controles de cifrado e identidad.	Objetivos de tiempo de recuperación y punto de recuperación definidos para servicios críticos; planes de continuidad probados; incidentes de seguridad registrados y remediados; revisiones de riesgo de terceros completadas; sistemas críticos cubiertos por procedimientos de respuesta a incidentes.
Transparencia	¿Los gobiernos y usuarios pueden verificar cómo operan los sistemas, cómo se gestionan los riesgos y cómo se protegen los datos?	Documentación de seguridad; evaluaciones independientes; informes de auditoría; reportes de transparencia; divulgación de propiedad y contratación; registro de accesos; procedimientos de notificación de brechas.	Evidencia de auditoría disponible; registros de acceso mantenidos y revisables; periodicidad de reportes de transparencia establecida; certificaciones o evaluaciones independientes vigentes.
Interoperabilidad y portabilidad	¿Los datos, cargas de trabajo y servicios pueden trasladarse entre entornos confiables cuando sea necesario?	Estándares abiertos; requisitos de portabilidad de datos; planes de salida y transición; APIs; opciones de arquitectura híbrida o multinube; derechos contractuales de portabilidad.	Planes de salida probados; mecanismos de exportación de datos documentados; cargas de trabajo críticas portables o interoperables; riesgos de dependencia de un proveedor evaluados y mitigados.
Resiliencia y continuidad	¿Los servicios críticos pueden seguir operando durante una interrupción?	Procedimientos de respaldo y restauración; pruebas de conmutación por error; proveedores o modelos de infraestructura diversificados; intercambio de inteligencia de amenazas; protocolos de comunicación de crisis.	Respaldos probados para servicios críticos; ejercicios de conmutación por error completados; redundancia mapeada para sistemas esenciales; métricas de continuidad reportadas a la alta dirección.

Pilar	Pregunta central	Controles ilustrativos	Resultados medibles
Seguridad y protección de datos	¿Los controles técnicos son suficientes para proteger los datos independientemente de dónde se encuentren?	Cifrado en reposo y en tránsito; claves gestionadas por el cliente cuando corresponda; arquitectura de confianza cero; gestión de identidad y acceso; prevención de pérdida de datos; monitoreo y telemetría; arquitectura segura desde el diseño.	Cobertura de cifrada documentada; acceso privilegiado monitoreado; telemetría disponible para la detección de amenazas; controles de seguridad validados mediante pruebas o revisión independiente.

Un marco de este tipo ayudaría a los gobiernos de América Latina a evaluar los reclamos de soberanía de manera más consistente y basada en evidencia. En lugar de preguntar únicamente dónde tiene su sede un proveedor o dónde se encuentra físicamente la infraestructura, los responsables de la formulación de políticas podrían evaluar si el proveedor demuestra una gobernanza sólida, operaciones transparentes, manejo seguro de datos, controles de cadena de suministro, continuidad del negocio, interoperabilidad y mecanismos independientes de aseguramiento. Este enfoque apoya las alianzas confiables, al tiempo que preserva la flexibilidad para abordar cargas de trabajo de mayor riesgo mediante controles adicionales cuando sea necesario.

En última instancia, fortalecer la soberanía digital no se trata de elegir entre el control nacional y la integración global. Se trata de crear las condiciones que permitan a los gobiernos, las empresas y los ciudadanos gobernar de forma segura sus activos digitales, mantener la resiliencia frente a las disrupciones y beneficiarse de un ecosistema digital diverso y confiable. Al centrarse en la seguridad, la interoperabilidad, la inversión, la innovación y la colaboración, América Latina tiene la oportunidad de construir un modelo de soberanía digital que sea a la vez resiliente y abierto.

Conclusión

La soberanía digital moldea cada vez más los debates de política en todo el mundo, pero su significado continúa evolucionando. Si bien los primeros debates se centraban con frecuencia en el control, la propiedad y la localización, ha surgido una comprensión más práctica y con visión de futuro. La soberanía digital no se logra mediante el aislamiento respecto de los ecosistemas tecnológicos globales, sino a través de relaciones de confianza, infraestructura resiliente y la capacidad de gobernar con seguridad los activos digitales críticos. Se alcanza, más bien, mediante la capacidad de gobernar los datos de forma segura, proteger la infraestructura crítica, mantener la resiliencia operativa y ejercer una elección significativa sobre las tecnologías que sustentan el crecimiento económico, los servicios públicos y la seguridad nacional.

Para América Latina, esta distinción representa una oportunidad significativa. La región está ampliando su infraestructura digital, acelerando la adopción de la nube y de la inteligencia artificial, fortaleciendo sus capacidades de ciberseguridad y modernizando sus marcos de gobernanza digital. Al mismo tiempo, los responsables de política tienen la oportunidad de desarrollar un modelo de soberanía digital que refleje las prioridades y fortalezas particulares de la región y que equilibre la seguridad y la resiliencia con la apertura, la innovación y la competitividad económica.

Alcanzar esta visión requerirá una inversión sostenida en infraestructura digital, ciberseguridad, desarrollo del talento y tecnologías emergentes. También exigirá políticas que promuevan la interoperabilidad, respalden ecosistemas digitales confiables y permitan a las organizaciones beneficiarse tanto de las capacidades locales como de la innovación global. La soberanía se fortalece cuando los gobiernos, las empresas y los ciudadanos tienen la flexibilidad de elegir entre soluciones confiables, adaptarse a amenazas cambiantes y evitar dependencias que generen riesgos innecesarios.

En última instancia, la soberanía digital no debe verse como un destino, sino como un esfuerzo permanente por construir confianza, resiliencia y capacidad en todo el ecosistema digital. El éxito dependerá de una colaboración sostenida entre gobiernos, industria, academia y sociedad civil para garantizar que las tecnologías digitales sigan siendo seguras, accesibles y beneficiosas para todos. Por lo tanto, una ruta práctica hacia adelante debería

combinar principios de política pública con controles medibles: gobernanza clara, clasificación de datos basada en riesgos, salvaguardas técnicas seguras, gestión de riesgos de la cadena de suministro, mecanismos de transparencia, interoperabilidad y resiliencia probada. Al adoptar un enfoque equilibrado, fundamentado en la seguridad, la capacidad de elección, la interoperabilidad y la innovación, América Latina puede contribuir a dar forma a un modelo de soberanía digital resiliente, competitivo y confiable en un mundo cada vez más interconectado.


DIGI
AMERICAS