Deloitte.

Soberanía digital como estrategia nacional

Un enfoque holístico

Septiembre 2025

Introducción

El concepto de soberanía digital surge como respuesta ante la creciente necesidad de que los países y las organizaciones tengan control sobre sus datos y sistemas tecnológicos, especialmente en un contexto de globalización y digitalización acelerada. Este control es crucial para proteger la privacidad, asegurar la infraestructura crítica y prevenir el uso indebido de información por parte de entidades extranjeras. Además, la soberanía digital permite a los países establecer políticas de ciberseguridad que resguarden la seguridad nacional y fomenten la autonomía tecnológica, reduciendo la dependencia de tecnologías y servicios externos.

Por otro lado, la soberanía digital es esencial para impulsar la economía digital local, ya que promueve la innovación y protege los mercados internos de monopolios extranjeros. Asimismo, permite a los países establecer regulaciones que reflejen sus valores y prioridades, como la protección de derechos digitales y la promoción de una competencia justa. Además, asegura la preservación y promoción de la cultura e identidad digital de cada país al promover un control más ajustado sobre el contenido y las plataformas digitales.

La soberanía digital marca el inicio de una etapa en la que la tecnología adquiere un rol estratégico fundamental, pues avanza más allá de su función meramente habilitadora. Para gobiernos y organizaciones, el desafío ya no consiste únicamente en adoptar soluciones digitales, sino en definir quién controla los activos críticos —aquellos recursos digitales, tecnológicos y de infraestructura que son esenciales para conservar el control y la autonomía sobre su entorno digital—, cómo se protegen los datos y qué grado de autonomía se tiene para innovar sin depender de infraestructuras tecnológicas ajenas.

Tradicionalmente, la soberanía digital ha sido un concepto reservado para los Estados. Sin embargo, hoy debería reinterpretarse y ser adoptada por las empresas como una estrategia para reducir riesgos, proteger su competitividad y garantizar la continuidad operativa. Uno de los principales desafíos es convertir la complejidad tecnológica en ventajas competitivas, mediante el diseño de estrategias que equilibren la seguridad, la innovación y el crecimiento sostenible. La verdadera oportunidad reside en transformar la soberanía digital en un motor de resiliencia organizacional y creación de valor, posicionando, tanto a los países como a las empresas, como artífices de su propio futuro tecnológico.

Soberanía digital *vs.* aislamiento digital

La soberanía digital permite a los países gestionar y regular su entorno digital en línea con sus intereses nacionales, lo cual les permite mantener al mismo tiempo su integración en el panorama tecnológico global. Por otro lado, el aislamiento digital representa una desconexión del internet global, ya sea por elección o imposición, a menudo acompañada de estrictas medidas de censura o restricciones al acceso a tecnologías externas. En términos simples, se trata de una autosuficiencia tecnológica extrema.

Equiparar soberanía con aislamiento sería un error, pues tener soberanía digital no significa cerrar las fronteras tecnológicas, sino establecer las condiciones bajo las cuales estas se abren. Esta lógica es comparable a una política comercial soberana: no se trata de evitar el comercio, sino de definir con quién se comercia, bajo qué términos y con qué reglas.

Cuando la soberanía digital es malinterpretada o implementada de manera incorrecta, puede convertirse en aislamiento. Esto ocurre cuando se prohíben de forma masiva servicios digitales extranjeros sin ofrecer alternativas viables, cuando el control del internet se centraliza en el Estado sin salvaguardas para los derechos digitales, o cuando un país se desconecta de los estándares internacionales, dificultando la interoperabilidad y la cooperación.

Hablar con precisión sobre soberanía digital requiere también distinguir claramente entre el papel del gobierno y el de la empresa. Aunque ambos actores comparten riesgos y necesidades tecnológicas, sus objetivos, capacidades y consecuencias estratégicas son distintas:

En el **ámbito gubernamental,** la soberanía digital busca resguardar el interés nacional, la seguridad del Estado y los derechos fundamentales de los ciudadanos. Esto implica regular el flujo de datos sensibles, proteger infraestructura crítica, desarrollar capacidades tecnológicas soberanas, establecer marcos legales robustos en ciberseguridad e Inteligencia Artificial (IA), y participar activamente en los foros de gobernanza digital global. No ejercer esta soberanía puede derivar en una alta dependencia tecnológica, exposición al ciberespionaje y pérdida de control sobre datos estratégicos.

Las **empresas**, por su parte, debieran ejercer soberanía digital para asegurar el control estratégico sobre sus datos y sistemas. Esto incluye tener control sobre activos digitales críticos, evitar dependencias tecnológicas con proveedores únicos, cumplir con normativas de protección de datos en múltiples jurisdicciones, adoptar arquitecturas multinube con cifrado propio y evaluar riesgos asociados a políticas tecnológicas extranjeras. La falta de soberanía digital empresarial puede llevar a interrupciones operativas, sanciones regulatorias o pérdida de competitividad.

Competencia global y dimensión geopolítica

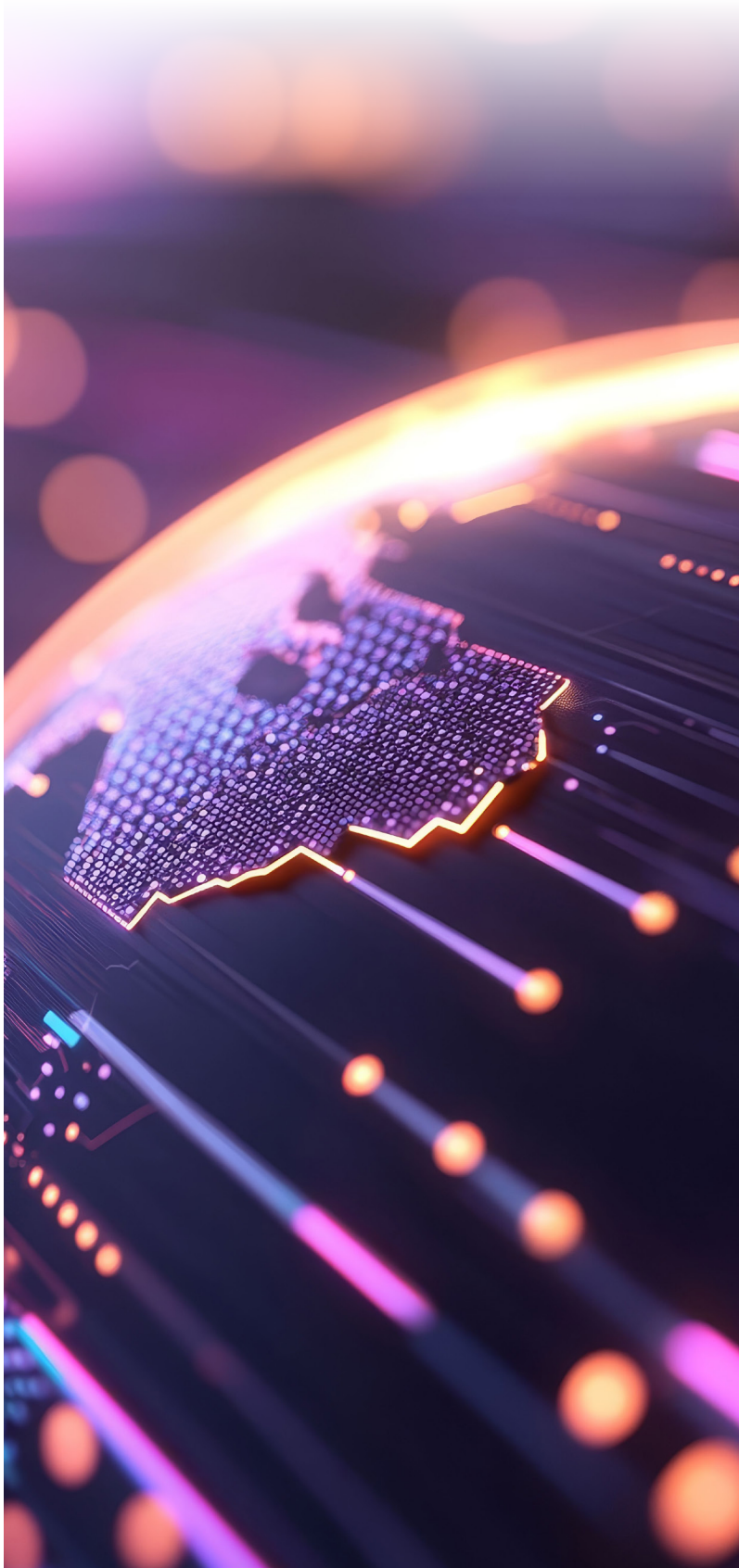
La soberanía digital ha trascendido de ser únicamente un tema técnico interno para convertirse en un asunto geopolítico de gran importancia en varios contextos, especialmente en la Unión Europea y en relación con las grandes empresas tecnológicas globales.

Ante una realidad marcada por la creciente digitalización y polarización, la infraestructura tecnológica es ya un activo estratégico que puede influir significativamente en el equilibrio de influencia y capacidades entre naciones. Esto sugiere que el control y desarrollo de tecnologías avanzadas pueden otorgar ventajas competitivas en términos económicos, de seguridad y políticos, lo que puede afectar la capacidad de un país para proteger sus intereses y proyectar su presencia en el escenario internacional. Por ello, muchos Estados están procurando reducir su dependencia de plataformas y proveedores tecnológicos extranjeros.

Esta preocupación ha sido evidente en debates sobre el despliegue de redes 5G, la adopción de servicios de Nube soberana, el acceso a semiconductores avanzados, o el control de plataformas de IA. Europa, por ejemplo, ha asumido la soberanía digital como uno de los pilares de su agenda estratégica en los últimos años. Un caso emblemático es la Unión Europea (UE), con iniciativas como GAIA-X,[1] un proyecto lanzado en 2020 que busca construir una infraestructura de datos europea segura, interoperable y federada, conforme a estándares de la UE, para dar a los Estados miembros mayor control sobre sus datos esenciales.

GAIA-X aspira a ser la base de un ecosistema de datos europeo que sirva de alternativa a los servicios en la Nube de los gigantes tecnológicos extranjeros, lo que fortalecería la autonomía estratégica del bloque. En palabras de sus impulsores, GAIA-X fue creado precisamente para que Europa "aumente el control sobre sus propios datos y cree mayor soberanía de datos"[2] y, de esta manera, reducir las dependencias no deseadas y el riesgo de *lock-in* tecnológico con proveedores dominantes.

Esta narrativa de búsqueda de "autonomía estratégica" repercute también en otros continentes. Gobiernos de diversos lugares están invirtiendo en desarrollar capacidades tecnológicas propias como medio para aislarse de palancas de poder externas. Por ejemplo, se promueven la fabricación nacional de equipos de telecomunicaciones, el desarrollo de Nubes locales, o marcos regulatorios que obliguen a los datos de ciudadanos a residir en servidores dentro del país *(data localization).*



El tema de la soberanía digital ha cobrado una relevancia fundamental en la agenda internacional, especialmente entre los países que integran el grupo BRICS (Brasil, Rusia, India, China y Sudáfrica). Este bloque —que aglutina a algunas de las economías emergentes más importantes del mundo—, ha colocado en el centro de sus prioridades la creación de condiciones tecnológicas, jurídicas y políticas que aseguren un mayor control sobre los datos, infraestructuras y sistemas digitales nacionales, con el objetivo de reducir la dependencia de plataformas y servicios occidentales y fortalecer su autonomía en la era de la información.

El grupo BRICS ha reconocido que la dependencia de infraestructuras y servicios digitales extranjeros representa un riesgo tanto para la seguridad nacional como para la autonomía económica y tecnológica. Por ello, los países miembros han emprendido acciones coordinadas, cada uno según sus capacidades y contextos, para promover la soberanía digital. Este esfuerzo incluye desde la inversión en infraestructura tecnológica propia, el desarrollo de normativas nacionales de protección de datos, la creación de plataformas alternativas a las grandes empresas tecnológicas occidentales, hasta la colaboración multilateral en innovación y ciberseguridad[3]:

Rusia ha sido uno de los actores más proactivos en este sentido, al impulsar el desarrollo de una "internet soberana" que permite el aislamiento de la red rusa (RuNet), en caso de amenazas externas, así como la creación de alternativas locales a sitios de redes sociales y otras plataformas extranjeras.

China ha construido un robusto ecosistema digital propio, desde motores de búsqueda hasta redes sociales y plataformas de comercio electrónico. Además, ha avanzado en la elaboración de leyes de ciberseguridad y protección de datos, así como en la promoción de estándares tecnológicos propios.

India ha apostado por la digitalización masiva de su economía, con propuestas como "Digital India", y ha promovido el desarrollo de aplicaciones y servicios nacionales, además del almacenamiento y procesamiento de datos dentro de sus fronteras.

Brasil y Sudáfrica también han mostrado interés en fortalecer su soberanía digital a través de la promoción de marcos regulatorios, inversión en infraestructura nacional y el impulso a industrias locales basadas en tecnología.

Al final, la competencia global por la soberanía digital refleja una realidad: quien controle los datos y la infraestructura tecnológica, va a controlar en gran medida su destino económico y de seguridad. Por ello, asegurar esa autonomía tecnológica se ha vuelto tan crucial, como lo fueron en épocas pasadas la soberanía territorial o energética.

Avances regionales: casos de Latinoamérica

En Latinoamérica, la soberanía digital está cobrando relevancia en la planificación estratégica de distintos países, aunque con grados de avance diversos. Existen ejemplos que ilustran iniciativas destacadas en la región y que se abordan a continuación:

Colombia es considerado un referente regional en gobierno digital, gracias a la continuidad de sus políticas de digitalización en la última década. Programas pioneros como Vive Digital,[4] la *Ley 1712* de 2014 sobre datos abiertos[5] y el CONPES de ciberseguridad[6] sentaron bases sólidas para la transformación digital del Estado. Como resultado, el país obtuvo, en 2023, uno de los mejores desempeños mundiales según el Índice de Gobierno Digital de la Organización para la Cooperación y el Desarrollo Económico (OCDE), ubicándose en el séptimo lugar entre los 38 países evaluados[7], por encima de Japón o naciones europeas como Luxemburgo. Este reconocimiento de la OCDE refleja un enfoque integral del país en materia digital, con mejoras equilibradas en todas las dimensiones, desde marcos institucionales hasta servicios centrados en el ciudadano. En pocas palabras, Colombia ha avanzado hacia la soberanía digital al fortalecer sus capacidades internas y adoptar estándares internacionales, sin dejar de mantener el timón de sus políticas tecnológicas.

Argentina ha orientado esfuerzos significativos para controlar su infraestructura crítica y fomentar la apertura tecnológica. La empresa nacional ARSAT[8] opera una Red Federal de Fibra Óptica (REFEFO) que interconecta a todo el país y un Centro Nacional de Datos propio, lo cual garantiza que gran parte del tráfico de internet y de los datos gubernamentales se manejen localmente[9]. Asimismo, Argentina lanzó sus satélites ARSAT-1 y ARSAT-2 geoestacionarios para telecomunicaciones, con lo cual se redujo la necesidad de arrendar capacidad a satélites extranjeros y aseguró cobertura sobre su territorio. En el plano del *software*, el gobierno impulsa el uso de *software* libre y la adopción de estándares abiertos, así como iniciativas de "ciencia abierta" para evitar dependencias onerosas de proveedores y favorecer la innovación local. Estas medidas, junto a la reciente puesta en marcha de centros de datos regionales de ARSAT y programas de conectividad en zonas remotas, apuntalan la soberanía tecnológica argentina y su resiliencia digital frente a eventos externos.

Uruguay, a pesar de su tamaño territorial, se destaca por la solidez de su infraestructura digital pública. Gracias a la labor de su operador estatal ANTEL, el país logró una cobertura nacional de fibra óptica[10], llegando con redes de alta velocidad a alrededor de 98% de los hogares —un hito inédito en la región[11]. Esto ha convertido a Uruguay en líder en conectividad de banda ancha, lo que ha habilitado a su vez el despliegue de servicios digitales avanzados en todo su territorio. Adicionalmente, ANTEL opera centros de datos públicos de primer nivel (incluyendo instalaciones certificadas *Tier-3*), y planea expandir esa capacidad local con nuevos *data centers* especializados. Asimismo, el país fue precursor con programas como Plan Ceibal[12] (que entregó *laptops* a estudiantes) y la digitalización casi total de trámites gubernamentales. Todo este ecosistema digital, mantenido mayormente por talento y recursos nacionales, ha dado a Uruguay una posición privilegiada para ejercer su soberanía digital, a la par de asegurar que sus comunicaciones y datos permanezcan bajo jurisdicción y normas propias.

México, si bien enfrenta retos en materia digital, recientemente dio un paso institucional importante creando la Agencia de Transformación Digital y Telecomunicaciones (ATDT), en 2024[13]. Esta nueva entidad federal fue concebida para unificar las capacidades tecnológicas del gobierno mexicano, generar mayor autonomía tecnológica y ahorrar costos. En la práctica, la ATDT va a concentrar funciones que antes estaban dispersas (como la estrategia digital nacional, la agenda de conectividad e, incluso, la Agencia Espacial Mexicana) con el objetivo de acelerar la digitalización gubernamental bajo estándares de soberanía tecnológica. Entre sus metas iniciales está desarrollar "Llave MX"[14], una plataforma de identidad digital única, así como coordinar el lanzamiento de un nuevo satélite de comunicaciones propio, hacia 2027. Aunque México tiene pendiente ampliar su infraestructura y mejorar indicadores de gobierno digital, la creación de la ATDT demuestra voluntad política para avanzar en esta agenda. De aprovecharse, podría detonar proyectos de gran impacto en conectividad rural, ciberseguridad nacional y modernización de servicios públicos, cimentando las bases para una mayor soberanía digital en todo el país.

En síntesis, en Latinoamérica existen ejemplos donde la persistencia en políticas digitales, la inversión en infraestructura propia y el desarrollo de talento local están dando resultados positivos. El progreso de países como los citados demuestra que, con una visión clara y dedicación, es factible disminuir la dependencia tecnológica y crear ecosistemas digitales más autosuficientes y alineados con las necesidades del país.

Autonomía impulsada por la soberanía digital y espacial

La concepción de soberanía digital describe el nivel de control sobre la infraestructura tecnológica, los datos, el *software* utilizado y, cada vez más, el acceso al espacio exterior. La libertad de elegir el propio destino digital implica tener la capacidad de tomar decisiones estratégicas y operativas de manera autónoma, aunque reconociendo que, en un mundo cada vez más interconectado, puede ser necesario colaborar y adoptar ciertas tecnologías o estándares globales.

Alcanzar dicha independencia digital permite alinear el ecosistema tecnológico con los valores, prioridades e intereses locales. Un país soberano digitalmente puede decidir, por ejemplo, adoptar IA para mejorar la educación pública o promover el desarrollo sostenible en sus propios términos, sin tener que aceptar criterios impuestos desde el exterior. De fondo, ejercer la soberanía digital se trata de generar mayor apalancamiento para la innovación, confianza tecnológica propia y desarrollo económico sostenido.

Tradicionalmente, la soberanía digital ha sido articulada en relación con tres pilares principales[15]:

1. **Soberanía de datos:** capacidad de un país u organización para controlar los datos que generan sus ciudadanos, empresas e instituciones públicas. Implica decidir cómo se recopilan, almacenan, procesan y transfieren esos datos dentro de su jurisdicción. Los datos —personales, de comportamiento o relativos a infraestructuras críticas— permanecen bajo normas locales, lo cual reduce el riesgo de accesos no autorizados o usos indebidos desde el extranjero.

2. **Soberanía física (infraestructura):** control sobre los dispositivos y equipos físicos que procesan, almacenan y transmiten la información. Incluye centros de datos propios, servidores, redes de telecomunicaciones, cableado y terminales (por ejemplo: antenas, *routers* o dispositivos móviles). Al poseer infraestructura nacional (o bajo administración local), se asegura que los sistemas críticos permanezcan operativos bajo las reglas propias y se mitigue la dependencia de proveedores foráneos para servicios esenciales.

3. **Soberanía de *software*:** facultad para decidir sobre los sistemas operativos, algoritmos, aplicaciones e interfaces digitales que se utilizan en la administración pública y la invdustria. Esto abarca desde el uso de *software* libre o desarrollado localmente hasta la autonomía en la gestión de plataformas de análisis de datos, IA y demás herramientas digitales para la toma de decisiones. Con este pilar, se evita la "discriminación algorítmica" o tener que operar bajo cajas negras tecnológicas impuestas externamente, lo cual permite adaptar la tecnología a la realidad y valores locales.

A estos tres pilares, se ha sumado un cuarto pilar emergente relacionado con la infraestructura orbital y espacial:

> **4. Soberanía espacial:** el derecho y capacidad de poseer, lanzar y controlar satélites propios. El espacio se ha convertido en una extensión del territorio digital soberano de un país, ya que a través de satélites independientes (o en asociaciones estratégicas) una nación puede expandir su conectividad hacia regiones remotas, proveer servicios esenciales de comunicación, mejorar la navegación y la observación terrestre e incluso reforzar su seguridad nacional desde el cielo. Contar con satélites propios reduce la dependencia tecnológica de servicios satelitales extranjeros y aumenta la resiliencia frente a amenazas o presiones externas.
>
> Distintos países en Latinoamérica han dado pasos en esta dirección, pues los programas satelitales nacionales ejemplifican cómo el control de infraestructura orbital otorga mayor autonomía. Por ejemplo, el histórico Sistema Satelital Morelos de México brindó independencia a los servicios de comunicación del Estado, en los años 80[16], mientras que el Venesat-1 o Simón Bolívar, fue el primer satélite artificial plenamente propiedad del Estado venezolano, lanzado en 2008[17]. Estas iniciativas demuestran que invertir en el espacio fortalece la soberanía digital al asegurar que las comunicaciones y datos críticos del país viajen por cielo propio.

Además de robustecer la autonomía, ejercer la soberanía digital en todos sus pilares conlleva proteger la privacidad de los ciudadanos (evitando actos de espionaje o vigilancia masiva), mantener la seguridad informática nacional, y garantizar que las decisiones sobre tecnología se tomen localmente. En definitiva, una estrategia holística de soberanía digital busca que la evolución digital ocurra bajo control doméstico, para fomentar la confianza en el ecosistema digital local y preservar el control democrático sobre recursos y servicios digitales.

El espacio y el sector privado: la nueva frontera de la soberanía digital

El lanzamiento del satélite Deloitte-1, en 2025, demostró cómo las empresas pueden expandir su presencia tecnológica al espacio en apoyo de la soberanía digital[18]. Tradicionalmente, la discusión sobre soberanía digital en el espacio se centraba en esfuerzos estatales (agencias gubernamentales lanzando satélites para comunicaciones, observación o navegación). No obstante, en años recientes el sector privado ha comenzado a desempeñar un rol dinámico en esta nueva frontera.

La presentación y puesta en órbita del satélite Deloitte-1, desarrollado en colaboración con SpaceX, marcó un punto de inflexión al mostrar que incluso empresas de servicios profesionales incursionan en la infraestructura espacial. Bajo un esquema de constelación de pequeños satélites, Deloitte-1 busca aprovechar datos y conectividad desde el espacio para brindar a sus clientes información en tiempo real y mejores capacidades de toma de decisiones. Este caso emblemático evidencia cómo la soberanía tecnológica también puede ser impulsada por actores privados al llevar su arquitectura digital más allá de la Tierra y, con ello, abrir la puerta para que otras organizaciones exploren iniciativas similares.

En los últimos años, hay empresas —fuera del sector aeroespacial tradicional— que también han puesto en órbita sus propios satélites o que han desarrollado misiones espaciales privadas para propósitos estratégicos, comerciales o tecnológicos. Por ejemplo, en 2023 Amazon lanzó satélites de prueba de su constelación Proyecto Kuiper. Según la organización, el objetivo de la misión fue proveer internet satelital de banda ancha a escala global, especialmente en regiones no conectadas[19].

El involucramiento de empresas privadas en el ámbito satelital complementa los esfuerzos gubernamentales y puede acelerar la innovación. Firmas tecnológicas, universidades y *startups* de la nueva economía espacial están lanzando satélites de bajo costo para diversos fines: monitoreo ambiental, Internet de las Cosas global, comunicaciones de banda ancha en zonas aisladas, etc. Esto contribuye a que las naciones tengan más opciones para lograr sus objetivos de conectividad y recolección de datos sin depender enteramente de infraestructura extranjera. Por ejemplo, consorcios público-privados podrían desplegar constelaciones de satélites para proveer internet satelital regional (reduciendo la brecha digital donde no llegan las redes terrestres), todo bajo control local o regional.

Empero, la inserción del espacio en la estrategia de soberanía digital también plantea nuevos desafíos. Se requieren marcos regulatorios claros sobre la propiedad y uso de satélites, protocolos de ciberseguridad espacial (para prevenir *hackeos* o interferencias a satélites), y estrategias de colaboración global que eviten una excesiva militarización o competencia insana en órbita. Pese a los retos, está claro que el espacio es la próxima frontera donde se va a dirimir parte de la autonomía tecnológica de las naciones.

Factores clave para progresar hacia la soberanía digital

La soberanía digital —como anteriormente se mencionó— no se limita al ámbito gubernamental, también las empresas están llamadas a construir su propia autonomía tecnológica. No obstante, los medios, responsabilidades y prioridades varían significativamente entre ambos actores. Lograr una soberanía digital efectiva requiere una estrategia integral a largo plazo y un conjunto de medidas concertadas en múltiples frentes. Entre los factores clave para avanzar en esta agenda, destacan los siguientes:

- **Infraestructura técnica nacional *vs.* infraestructura corporativa autónoma**

  Para los Estados, la soberanía digital comienza con el desarrollo de infraestructura crítica bajo control local: centros de datos nacionales, redes de fibra óptica, nodos de internet, Nubes públicas o comunitarias y sistemas de pagos digitales. Estas inversiones, además de garantizar el procesamiento y almacenamiento seguro de datos dentro del territorio nacional, fortalecen también la resiliencia frente a interferencias externas o interrupciones geopolíticas.

  En cambio, para las empresas, la construcción de soberanía digital implica evaluar la dependencia de proveedores extranjeros, alojar información sensible en Nubes privadas o híbridas bajo su control, y adoptar arquitecturas tecnológicas que aseguren continuidad operativa sin vulnerar normativas locales. Es clave contar con entornos digitales auditables y configurables para cumplir con exigencias regulatorias y preservar ventajas competitivas.

- **Formación de talento especializado: política pública *vs.* estrategia de recursos humanos**

  Desde la perspectiva estatal, lograr autonomía digital requiere una política pública activa para formar talento en ciberseguridad, IA, análisis de datos, *software*, redes y, en casos avanzados, operación satelital. La inversión en educación superior, academias tecnológicas, investigación e incentivos para evitar la "fuga de cerebros" resulta esencial para reducir la dependencia externa.

  Para las empresas, la prioridad está en atraer, retener y capacitar talento alineado con sus necesidades específicas. Esto incluye la formación continua en herramientas tecnológicas propias, la adopción de marcos de ciberseguridad, y la colaboración con instituciones educativas para crear perfiles profesionales relevantes. Sin una estrategia clara de capital humano, incluso las inversiones más avanzadas en tecnología pierden eficacia.

- **Regulación digital: marco legal nacional *vs.* cumplimiento y gobernanza interna**

  Los Estados tienen la responsabilidad de crear marcos legales que protejan los derechos digitales de los ciudadanos (como la privacidad, la no discriminación algorítmica o la seguridad de la información), promuevan el uso ético de nuevas tecnologías y faciliten la innovación. Una regulación eficaz debe ser robusta, pero también lo suficientemente flexible para adaptarse al dinamismo tecnológico. Leyes de protección de datos, estrategias nacionales de ciberseguridad y estándares abiertos son herramientas clave.

  Para las empresas, la soberanía digital implica no solo cumplir con las normas externas, sino desarrollar gobernanzas internas sólidas: políticas de tratamiento de datos, principios éticos en IA, mecanismos de auditoría algorítmica y estándares de interoperabilidad. La confianza del cliente, la integridad reputacional y la reducción de riesgos legales dependen de estas prácticas internas alineadas con los valores de soberanía y transparencia.

Implementar estas medidas de forma coordinada no es algo trivial, pero varios países han demostrado progresos en el camino hacia la soberanía digital. Un liderazgo institucional claro, presupuestos asignados a tecnología y la continuidad de políticas más allá de los gobiernos de turno, suelen marcar la diferencia. Hay que recordar que no se trata de aislarse tecnológicamente del mundo, sino de asegurarse de que la participación en la economía digital global se haga desde una posición de fortaleza y elección informada, en lugar de una dependencia pasiva.

La construcción de la soberanía digital exige un delicado equilibrio entre apertura a la innovación y salvaguarda de la seguridad, así como la protección de la privacidad, el fortalecimiento de infraestructuras críticas y el desarrollo de capacidades locales. Para avanzar en esta agenda, resulta indispensable diseñar marcos regulatorios propios pero compatibles con estándares internacionales, invertir en infraestructura digital resiliente y promover alianzas público-privadas que aseguren legitimidad y efectividad.

Conclusión

La soberanía digital ha dejado de ser un asunto de expertos en TI. Hoy, se ha convertido en una prioridad estratégica con amplias implicaciones económicas y geopolíticas. Desarrollarla de forma plena exige una visión a largo plazo, un compromiso financiero sostenido y un esfuerzo colaborativo que involucre al sector público, la industria privada, la academia y la sociedad civil. Cada país deberá encontrar su propio balance entre apertura e independencia, pero la tendencia es clara: gestionar el propio destino digital será uno de los principales diferenciadores de seguridad y autonomía nacional.

Para enfrentar la incertidumbre del futuro digital, un recurso viable para las naciones es invertir hoy en sus pilares de soberanía digital —desde cables submarinos y satélites hasta talentos locales y leyes modernas—. La autonomía tecnológica no implica aislarse, sino tener la capacidad de elección: poder cooperar globalmente desde la fortaleza interna, adoptar tecnologías extranjeras sin volverse rehén de ellas, y proteger a los ciudadanos en el ciberespacio con la misma determinación con que se protege el territorio físico.

La soberanía digital significa tener el control y la capacidad de decidir de manera independiente sobre los asuntos digitales en la actualidad. Equivale a tomar las riendas del progreso tecnológico para que este sirva al interés nacional y al bien común, en lugar de quedar a merced de intereses foráneos. Como demuestra la evolución reciente —desde Europa con GAIA-X hasta los países innovadores de Latinoamérica—, es posible reclamar ese destino digital propio y, sobre todo, necesario. Quienes lo logren, disfrutarán de una posición más segura y ventajosa en la economía del conocimiento; quienes se rezaguen, corren el riesgo de ver comprometida su soberanía de forma tan tangible como ocurría en el pasado con su soberanía política o económica.

En definitiva, la soberanía digital, concebida de manera holística, es el nuevo estandarte de la autonomía nacional en nuestros tiempos. Quienes la enarbolen con éxito, serán arquitectos de su futuro digital y garantes de su propio destino tecnológico.

Referencias

1. GAIA-X. *Together towards a federated and secure data infrastructure.* https://gaia-x.eu/
2. TNO. *"Gaia-X: a European initiative for greater digital sovereignty".* Organización Neerlandesa para la Investigación Científica Aplicada. https://www.tno.nl/en/digital/data-sharing/gaia-digital-sovereignty/
3. Belli, L. Et al. (2024). *Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries.* Computer Law & Security Review. https://www.sciencedirect.com/science/article/pii/S0267364924000839
4. Ministerio de Tecnologías de la Información y las Comunicaciones. *Live digital.* https://www.mintic.gov.co/portal/inicio/Micrositios/English-overview/Vive-Digital/
5. Función Pública. *Ley 1712.* Congreso de la República, Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882
6. Departamento Nacional de Planeación. Documentos CONPES. Gobierno de Colombia. https://www.dnp.gov.co/LaEntidad_/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-confianza-y-seguridad-digital.aspx
7. Organización para la Cooperación y el Desarrollo Económico (2023). *"OECD Digital government index".* OCDE. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/01/2023-oecd-digital-government-index_b11e8e8e/1a89ed5e-en.pdf
8. ARSAT. *Home.* https://www.arsat.com.ar
9. Jefatura de Gabinete de Ministros. Qué es la Red Federal de Fibra Óptica. Gobierno de Argentina. https://www.argentina.gob.ar/jefatura/innovacion-publica/telecomunicaciones-y-conectividad/conectar/que-es-la-red-federal-de
10. ANTEL. *Home.* https://www.antel.com.uy/
11. Larocca, N. (2025). "Antel Uruguay se defiende con fibra, 5G y *Data Centers*: los planes de su nuevo presidente". DPL News. https://dplnews.com/antel-uruguay-se-defiende-con-fibra-5g-y-data-centers/
12. Ceibal. *Home.* https://ceibal.edu.uy/
13. Agencia de Transformación Digital y Telecomunicaciones. *Home.* Gobierno de México. https://www.gob.mx/atdt
14. Llave MX. *Home.* Gobierno de México. https://www.llave.gob.mx/
15. Sánchez del Real, G. (2024). "La soberanía digital ¿qué es y cómo te afecta?". https://www.linkedin.com/pulse/la-soberan%C3%ADa-digital-qu%C3%A9-es-y-c%C3%B3mo-te-afecta-gracia-s%C3%A1nchez-del-real-unykf/
16. Secretaría de Infraestructura, Comunicaciones y Transportes. "Rumbo al espacio, sistema de satélites Morelos". Gobierno de México. https://elmirador.sct.gob.mx/cuando-el-futuro-nos-alcanza/rumbo-al-espacio-sistema-de-satelites-morelos
17. Parlamento Do Mercosul (2008). Reconocimiento por el lanzamiento del satélite Simón Bolívar. https://www.parlamentomercosur.org/innovaportal/v/876/2/parlasur/reconocimiento-por-el-lanzamiento-del-satelite-simon-bolivar.html
18. Consultancy (2025). *"Deloitte successfully launches its own satellite with the help of SpaceX".* https://www.consultancy.com.au/news/11054/deloitte-successfully-launches-its-own-satellite-with-the-help-of-spacex
19. Amazon (2023). *"Amazon shares an update on how Project Kuiper's test satellites are performing".* Amazon News. https://www.aboutamazon.com/news/innovation-at-amazon/amazon-project-kuiper-test-satellites-space-launch-october-2023-update

Contacto:

Brenda García Flores
Socia Líder de Política Pública para S-LATAM
Deloitte México
bgarciaflores@deloittemx.com

Germán Ortiz
Socio Líder de la Industria de Tecnología, Medios y Telecomunicaciones
Deloitte Spanish Latin America
gortiz@deloittemx.com

Deloitte.