Los desafíos de los centros de datos gubernamentales en la construcción de infraestructuras digitales resilientes

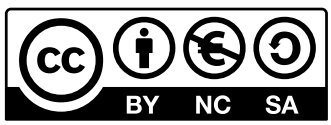
DIGI AMERICAS

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE Google

kriptos LUMU mastercard netskope paloalto NETWORKS fluid attacks we hack your software Resecurity

Schneider Electric SISAP Sistemas Aplicativos Strike Telefónica tenable Trellix TREND MICRO



Créditos

Digi Americas Alliance

Alain Karioty
Alexis Steffaro
Andy Kotz
Belisario Contreras
Brett DeWitt
Carlos Torales
Christian Torres
Cory Bullock
Fernando Quintero
Gene Yoo
Ghassan Dreibi
Hernan Armbruster
Jordana Siegel
Jorge Blanco
José Juan Haro
Mario de la Cruz Sarabia
Mauricio Benavides
Mauricio Nanne
Norberto (Bert) Milán
Patrick Ford
Rafael Alvarez
Ricardo Villadiego
Stephen Fallas

Editores

Belisario Contreras
Alexis Steffaro
Andy Kotz

DIGI AMERICAS **ALLIANCE MEMBERS**

aws Apple Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE Google
kriptos LUMU netskope paloalto NETWORKS fluid attacks we hack your software Resecurity
Schneider Electric SISAP Sistemas Aplicativos Strike Telefónica tenable Trellix TREND MICRO

Índice

Introducción

Los gobiernos operan en un entorno digital exigente y en evolución. Se enfrentan a varios desafíos apremiantes, desde el rápido ritmo del avance tecnológico y la adopción de tecnologías emergentes, como la inteligencia artificial, hasta el aumento de las expectativas de los ciudadanos de servicios sin interrupciones. En respuesta a estos desafíos, los gobiernos de todo el mundo están adoptando cada vez más soluciones de nube de hiperescala (también conocidas como nube pública). La nube de hiperescala ofrece una solución rentable para utilizar, mantener y actualizar la infraestructura de TI heredada local. Puede ayudar a las instituciones gubernamentales a proteger sus bases de datos e implementar mecanismos de ciberseguridad de vanguardia. Es eficiente, resiliente, confiable y escalable, ya que los recursos se pueden desplegar bajo demanda para satisfacer las necesidades cambiantes de las instituciones. La computación en la nube de hiperescala no solo tiene el potencial de reducir significativamente el consumo de energía y las emisiones de carbono en comparación con otras opciones de nube, sino que también desempeña un papel crucial en lograr un equilibrio entre sostenibilidad, innovación, rentabilidad y una ciberseguridad sólida. El Anexo B compara los beneficios y desafíos entre los centros de datos locales heredados y las diferentes opciones de nube.

Aunque los países reconocen los beneficios de los servicios en la nube para el sector público, su adopción generalizada, especialmente en los países en desarrollo, sigue siendo lenta. Las preocupaciones sobre aspectos como ciberseguridad, soberanía de los datos, la falta de conocimientos técnicos sobre la migración y operación en la nube, así como la privacidad[1], junto con la incertidumbre regulatoria, son algunos de los obstáculos para la integración más rápida de los servicios en la nube. A efectos de coherencia y claridad, el Anexo A explica los conceptos de soberanía digital, soberanía de datos, residencia de datos y localización de datos.

Además de las preocupaciones relacionadas con la seguridad y la privacidad, la adopción de servicios en la nube también requiere ajustes en los procesos administrativos y legales del gobierno para permitir la adquisición, contratación y gestión presupuestaria de servicios en la nube competitivos y transparentes (CAPEX vs. OPEX). En la mayoría de los casos, este tipo de cambios en los procesos administrativos gubernamentales se enfrentan a resistencias e incertidumbres.

En consecuencia, debido a los marcos de evaluación inadecuados para identificar y evaluar estas preocupaciones, los gobiernos de los países en desarrollo suelen elegir la configuración de una nube gubernamental que alberga un centro de datos gubernamental para ser compartido por todos los ministerios gubernamentales[2]. En la mayoría de los casos, esta decisión implica inversiones significativas en centros de datos administrados y de propiedad gubernamental

[1] Banco Mundial (2023) - Nota práctica de contratación institucional sobre computación en nube - Nota práctica institucional y de contratación sobre computación en nube : Marco de evaluación de la nube y metodología de evaluación (worldbank.org)
[2] Banco Mundial (2023) – Greening Public Administration with GovTech - Ecologizar la Administración Pública con GovTech: Hacia una transición digital ecológica (worldbank.org)

donde se deben abordar nuevas demandas, complejidades y desafíos para desarrollar la resiliencia en el panorama digital en rápida evolución.

Un centro de datos gubernamental a gran escala puede parecer una opción lógica para gestionar datos sensibles, pero esta estrategia conlleva varios desafíos y riesgos. Los gobiernos pueden enfrentar dificultades para mantenerse al día con la innovación tecnológica debido a procesos burocráticos, procedimientos de adquisición engorrosos, restricciones presupuestarias y la presencia de sistemas heredados (infraestructura, procesos, políticas y personal). Además, la actualización continua de sistemas y operaciones a gran escala representa un desafío constante.
Dado que los gobiernos suelen tardar en adoptar cambios disruptivos, su ritmo lento puede afectar la capacidad de los centros de datos gubernamentales para adaptarse a nuevas tecnologías, volviéndolos obsoletos en poco tiempo. Esto puede generar nuevos sistemas heredados y aumentar vulnerabilidades y riesgos, especialmente en el entorno de amenazas emergentes que enfrentamos hoy.

El propósito de este informe es abordar los siguientes aspectos: (i) proporcionar una herramienta que facilite el diálogo sobre los posibles beneficios, desafíos y riesgos vinculados al desarrollo de centros de datos gubernamentales en América Latina; (ii) analizar las tendencias y percepciones que están moldeando la arquitectura de estas infraestructuras; y (iii) explorar alternativas que permitan a los gobiernos desarrollar soluciones prácticas y efectivas, adaptadas a sus necesidades, mientras enfrentan los desafíos identificados.

El informe se estructura como se muestra a continuación:

1. **El surgimiento de los centros de datos gubernamentales:** proporciona una visión general de las fuerzas que están impulsando el desarrollo de los centros de datos gubernamentales, tanto en América Latina como a nivel mundial. Destaca factores clave, incluidas las iniciativas de transformación digital, la adopción de la nube, la inteligencia artificial, los marcos de políticas y las regulaciones.

2. **Ventajas y desafíos de los centros de datos gubernamentales actuales:** muestra el análisis de las ventajas y beneficios de desarrollar centros de datos gubernamentales. También aborda las principales preocupaciones, como la innovación, la disponibilidad de talento digital, la garantía de la seguridad y la privacidad, los ciberataques a los servicios digitales de los gobiernos, la gestión de costes y el logro de la eficiencia y la flexibilidad. Además, discute la importancia de la sostenibilidad (TI verde) y la necesidad de planificar para satisfacer las futuras demandas crecientes de digitalización. A través de estudios de casos relevantes, esta sección proporciona información práctica sobre cómo los diferentes gobiernos abordan estos aspectos.

3. **Adopción de la Colocación Híbrida para Habilitar una Infraestructura Digital Gubernamental Resiliente:** propone la Colocación Híbrida como una alternativa para que los gobiernos satisfagan las crecientes y exigentes necesidades de prestación de servicios eficientes, flexibles, escalables, seguros y resilientes; abordar los problemas de soberanía, residencia y privacidad; fomentar la innovación; y facilitar la evolución hacia el gobierno cognitivo a través de la habilitación de la inteligencia artificial y el creciente flujo de tecnologías emergentes e innovaciones digitales.

4. **Conclusiones y recomendaciones:** proporciona conclusiones y recomendaciones clave para los gobiernos que buscan avanzar en el desarrollo de una infraestructura de gobierno digital resiliente que aborde las crecientes necesidades actuales y futuras.

Se incluyen tres anexos, que ofrecen definiciones técnicas y precisiones sobre los siguientes conceptos clave: soberanía, infraestructura en la nube y clasificación de datos.

1 El auge de los centros de datos gubernamentales

Una de las principales fuerzas que impulsan el desarrollo de los centros de datos gubernamentales, tanto en América Latina como a nivel mundial, es el concepto de soberanía digital (véase el Anexo A para la definición de soberanía). Esta tendencia ha impactado significativamente las políticas públicas y los requisitos técnicos que algunos países están aplicando al sector del proveedor de servicios en la nube. En este capítulo, exploramos estos factores, sus implicaciones, beneficios y riesgos potenciales.

1.1 Fuerzas impulsoras detrás de los centros de datos gubernamentales

El desarrollo de centros de datos gubernamentales ha sido la respuesta de algunos gobiernos a la necesidad de ejercer la soberanía digital, especialmente sobre los datos y activos digitales del país. Esta estrategia ha sido impulsada por distintos modelos regulatorios, como la residencia de datos y las regulaciones de datos transfronterizas, entre otros.

La creciente demanda de soberanía digital ha reforzado el énfasis en el control gubernamental sobre el contenido y los procesos de información y comunicación digital, así como en la competencia justa dentro del mercado digital. También ha generado la necesidad de contar con opciones tecnológicas autónomas, el despliegue de capacidades digitales estratégicas y el desarrollo de una infraestructura resiliente. Este enfoque ha marcado la transición de una gobernanza reactiva a un modelo proactivo y basado en el riesgo, donde se establecen de manera explícita las acciones que los actores digitales deben llevar a cabo y las medidas que los gobiernos deben tomar para prevenir o mitigar riesgos[3].

Una de las implicaciones clave es la definición y el alcance de la soberanía digital, cuyo significado varía según el contexto y las prioridades de cada país o región. La complejidad se agrava debido a la ausencia de una guía unificada que especifique qué tipos de cargas de trabajo digitales, industrias y sectores deben cumplir con estos requisitos. A pesar de que las necesidades de soberanía dependen de múltiples factores, algunos de los temas fundamentales identificados incluyen la residencia de datos, la restricción del acceso del operador, la resiliencia y la transparencia[4]. Para más detalles, consulte el Anexo A, que presenta las definiciones de Soberanía Digital, Soberanía de Datos, Residencia de Datos y Localización de Datos utilizadas en este informe.

[3] Jelinek, Thorsten. The Digital Sovereignty Trap: Avoiding the Return of Silos and a Divided World (Springer Briefs in International Relations) (pp. 63-64). Springer Nature Singapore.
[4] Blog de seguridad de AWS (febrero de 2024) - https://aws.Amazon Web Services.com/blogs/security/how-aws-can-help-you-navigate-the-complexity-of-digital-sovereignty/

Como resultado, muchos gobiernos han determinado que exigir la residencia de datos como el requisito de que todo el contenido del cliente debe procesarse y almacenarse en un sistema de TI dentro de las fronteras del país específico proporciona una capa adicional de seguridad. La residencia de datos refleja una combinación de problemas asociados principalmente con los riesgos de seguridad percibidos en torno al acceso de terceros a los datos, incluidas las agencias policiales extranjeras. Los gobiernos quieren asegurarse de que sus datos estén protegidos contra el acceso no deseado no solo de los atacantes maliciosos generales, sino también de los actores de amenazas estatales y nacionales[5]. Una posición estricta sobre la residencia de datos a veces restringe el uso de proveedores globales de nube de hiperescala debido a la percepción errónea de que los datos corren un mayor riesgo porque los proveedores de nube de hiperescala pueden tener activos de infraestructura ubicados en un país que no sea donde se encuentra una entidad del sector público.

Esta percepción errónea ha llevado a algunos gobiernos a decidir que la mejor manera de proteger sus datos es tener control total sobre la infraestructura tecnológica, desde el suelo y las paredes del edificio hasta el software y el hardware. En otras palabras, optan por construir sus propios centros de datos locales, que hoy en día suelen ser nubes privadas gubernamentales.

La noción de que los datos en las instalaciones o en una nube privada del gobierno son más seguros debe evaluarse cuidadosamente, ya que lo contrario podría ser cierto: la nube de hiperescala puede ser más segura. La razón es simple: Los datos almacenados en las instalaciones en una sola ubicación centralizada pueden aumentar las vulnerabilidades de privacidad y seguridad debido a un solo punto de falla. Además, la estructura gubernamental rara vez proporciona el nivel de recursos y agilidad que requiere este sector dinámico. Por el contrario, una nube conectada globalmente se beneficia de las economías de escala, la evitación de riesgos y la resiliencia por diseño.

Además, los hiperescaladores como Amazon Web Services, Microsoft Azure, Google Cloud y otros crean, crecen y retienen profesionales altamente calificados y examinados que brindan garantías técnicas, operativas y de seguridad de primer nivel para salvaguardar la nube aprovechando los puntos de datos y las amenazas de todo el mundo. Además, esta categoría de proveedores de servicios en la nube se somete a amplios programas de cumplimiento con certificaciones de terceros, lo que garantiza el cumplimiento de estrictos estándares de seguridad y privacidad.
La industria de la ciberseguridad ofrece información sobre por qué la localización de datos y las restricciones de residencia pueden ser perjudiciales y costosas: Los problemas de seguridad de los datos pueden surgir al almacenar todos los datos en una ubicación geográfica, lo que es contrario al enfoque de diversificación comúnmente recomendado en la industria de la ciberseguridad y a menudo adoptado por grandes corporaciones internacionales para garantizar una seguridad sólida en una red geográficamente dispersa[6].

[5] Perspectivas de políticas de AWS: residencia de datos - https://d1.awsstatic.com/whitepapers/compliance/Data_Residency_Whitepaper.pdf
[6] Banco Mundial (2023) - Nota práctica de contratación institucional sobre computación en nube - Nota práctica institucional y de contratación sobre computación en nube : Marco de evaluación de la nube y metodología de evaluación (worldbank.org)

1.2 Panorama mundial

1.2.1 Soberanía

"A medida que el mundo se mueve en línea, es esencial facilitar los flujos de datos transfronterizos. No solo ha servido como base para la economía moderna, sino que también ha seguido desbloqueando beneficios sociales innovadores y prometedores. Sin embargo, en los últimos años, la fricción regulatoria en torno a los flujos de datos transfronterizos solo se ha profundizado, y los gobiernos de todo el mundo están lidiando con prioridades políticas en competencia para proteger la privacidad de los datos, la seguridad, la propiedad intelectual y el acceso de las fuerzas del orden"[7].

Al mismo tiempo, los gobiernos enfrentan desafíos para satisfacer las demandas y oportunidades aceleradas debido a los sistemas heredados, aislados y los almacenes de datos. Pasar a la nube pública o de hiperescala ha sido la respuesta de los principales gobiernos a nivel mundial.

"Para 2025, más del 75 % de los gobiernos operarán más de la mitad de las cargas de trabajo utilizando proveedores de servicios en la nube a hiperescala"[8].

Como resultado, los gobiernos y otros reguladores están publicando pautas y regulaciones cada vez más estrictas con respecto a la adopción de servicios en la nube para cargas de trabajo digitales críticas o sensibles. Los requisitos de soberanía estipulan que el uso de la nube de hiperescala por parte de los clientes debe ser inmune al impacto de las leyes y mandatos extranjeros.

"137 países y contando han promulgado algún tipo de leyes de protección de datos y soberanía"[9].

Como se mencionó anteriormente en este documento, las estrictas regulaciones de localización de datos han llevado a algunos gobiernos a decidir que la forma de mantener sus datos seguros es tener la propiedad completa de la "pila", en otras palabras, construir y operar sus propios centros de datos. Un ejemplo de la vulnerabilidad de un único punto de falla de este enfoque ha sido el caso de Ucrania:

[7] Foro Económico Mundial – Flujos de datos transfronterizos - https://www.weforum.org/projects/cross-border-data-flows/
[8] GARTNER (2023) – Principales tendencias tecnológicas del gobierno de 2023 - https://www.gartner.com/en/newsroom/press-releases/2023-04-17-gartner-announces-the-top-10-government-technology-trends-for-2023
[9] Accenture (2023) - Accenture-Sovereign-Cloud-PoV-Short-2023-24-May-FINAL.pdf

Cómo las preocupaciones por la ciberseguridad en Ucrania llevaron a la migración de datos gubernamentales a la nube pública

Antes de la guerra con Rusia, Ucrania tenía una Ley de Protección de Datos de larga data que prohibía a las autoridades gubernamentales procesar y almacenar datos en la nube pública. Esto significaba que la infraestructura digital del sector público del país se ejecutaba localmente en servidores ubicados físicamente dentro de las fronteras del país. Una semana antes de que comenzara la guerra en 2022, el gobierno ucraniano funcionaba completamente en servidores ubicados dentro de las ubicaciones de los edificios gubernamentales que eran vulnerables a los ataques.

El Ministro de Transformación Digital de Ucrania y sus colegas en el Parlamento reconocieron la necesidad de abordar esta vulnerabilidad. El 17 de febrero de 2022, días antes del inicio de la guerra, el Parlamento de Ucrania modificó su Ley de Protección de Datos para permitir que los datos gubernamentales se trasladen de los servidores locales existentes a la nube pública. Esto, en efecto, le permitió "evacuar" datos gubernamentales críticos fuera del país y hacia centros de datos en toda Europa. En 10 semanas, el Ministerio de Transformación Digital de Ucrania y más de 90 directores de transformación digital de todo el gobierno ucraniano trabajaron para transferir a la nube muchas de las operaciones y datos digitales más importantes del gobierno central [10].

[10] Banco Mundial (2023) - Nota práctica de contratación institucional sobre computación en nube - Nota práctica institucional y de contratación sobre computación en nube : Marco de evaluación de la nube y metodología de evaluación (worldbank.org)

Otro ejemplo reciente de la vulnerabilidad potencial de los centros de datos gubernamentales fue el ataque de ransomware al centro de datos nacional de Indonesia:

El centro de datos nacional de Indonesia encriptado con la variante de ransomware LockBit[11]

El centro de datos nacional de Indonesia se vio comprometido por un ataque de ransomware, que interrumpió los controles de inmigración en los aeropuertos y varios servicios públicos. El ataque se dirigió al Centro Nacional de Datos Temporales (PDNS) en Surabaya utilizando una variante del ransomware LockBit llamada Brain Cipher. Los piratas informáticos exigieron un rescate de 8 millones de dólares, que el gobierno se negó a pagar.

La violación afectó los servicios, como el procesamiento de visas y permisos de residencia, los servicios de pasaportes y los sistemas de gestión de documentos de inmigración, lo que provocó largas colas en los aeropuertos. Además, interrumpió la plataforma para la inscripción en línea de escuelas y universidades, lo que llevó a una extensión del período de inscripción. En total, al menos 210 servicios locales se vieron gravemente afectados. La violación puede exponer datos que pertenecen a instituciones estatales y gobiernos locales.

El ciberataque se vio facilitado por la desactivación del software Windows Defender, lo que permitió a los piratas informáticos infiltrarse en el sistema, desplegar malware, eliminar archivos y desactivar servicios. Las autoridades aislaron las áreas infectadas y **migraron datos críticos a la nube.**

Estos dos casos son claros ejemplos del nivel de vulnerabilidades que enfrenta la estrategia de centros de datos propiedad del gobierno y de cómo la alternativa más segura adoptada ha sido la nube de hiperescala. En los ejemplos, la nube de hiperescala fue la elección hecha por ambos países después de experimentar las vulnerabilidades del centro de datos propiedad y operado por el gobierno.

Desde una perspectiva diferente, la Unión Europea (UE) ha estado impulsando una sofisticada agenda de soberanía, elaborada a través de la colaboración entre gobiernos, empresas y reguladores, que se unen para desarrollar un marco regulatorio integral, que afectará a las economías globales. Este proceso participativo de múltiples partes interesadas implementado por la UE es sin duda un modelo a considerar a medida que más gobiernos entran en el diseño de sus propias políticas nacionales de infraestructura digital y estrategias de desarrollo.

Las medidas de localización de datos se están expandiendo a nivel mundial, lo que podría afectar la eficiencia y las oportunidades económicas de la economía digital. Los debates actuales sobre estas políticas a menudo no consideran el costo total que estas regulaciones imponen a la economía en su conjunto, ni exploran otras opciones que permitan mejorar la privacidad, seguridad y oportunidades digitales. Los servicios financieros internacionales, junto con muchas otras industrias, dependen de marcos bien diseñados para el manejo de datos, lo que les permite ofrecer servicios innovadores, eficientes y de alto valor a individuos, hogares y empresas. Por ello, es fundamental analizar con mayor profundidad los efectos de la localización de datos y visibilizar sus costos y oportunidades perdidas, especialmente a medida que la sociedad define nuevas reglas para la economía digital[12].

[11] The Record: Centro de datos nacional de Indonesia cifrado con la variante de ransomware LockBit (therecord.media)
[12] Institute of International Finance (2021) – Localización de datos: costos, compensaciones e impactos en toda la economía - https://stagingnew.iif.com/portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf

1.2.2 Industria de centros de datos

La creciente demanda de servicios en la nube, el uso cada vez mayor de dispositivos habilitados para la web, las crecientes regulaciones de soberanía y residencia de datos, la creciente cantidad de datos generados y la democratización de la inteligencia artificial (IA) están impulsando el crecimiento explosivo de la industria de los centros de datos.

Aunque diferentes fuentes de investigación ofrecen diferentes valoraciones de mercado y expectativas de crecimiento, todas coinciden en la certeza de un crecimiento explosivo a lo largo del futuro pronosticado. Por ejemplo, según Arizton (Data Center Market Research), el tamaño del mercado global de centros de datos se valoró en 215.730 millones de dólares en 2022 y se espera que alcance los 289.660 millones de dólares para 2028, lo que muestra una CAGR del 5,03 % durante el período de pronóstico. Según Statista (Data Center -Worldwide), se proyecta que el mercado global de centros de datos alcance los 340.200 millones de dólares para 2024 a una CAGR 2024-2028 del 6,56 %, lo que resultará en un volumen de mercado de 438.700 millones de dólares para 2028.

Los gobiernos que toman la decisión de desarrollar sus propios centros de datos como alternativa para cumplir con sus requisitos de soberanía digital deben ser conscientes de que se están convirtiendo en actores activos en la industria de centros de datos complejos y dinámicos. A continuación, las siguientes son ideas clave que los gobiernos deben considerar antes de ingresar a esta industria: [13]

- **Centros de datos de hiperescala:** para satisfacer la creciente demanda de potencia computacional, se prevé que los centros de datos de hiperescala aumenten su densidad de racks a una tasa de crecimiento anual compuesta (CAGR) del 7,8 %. Para 2027, la densidad promedio de racks alcanzará los 50 kW por rack, superando el promedio actual de 36 kW.
- **Eficiencia Energética y Objetivos Renovables:** la industria se enfrenta a una creciente presión para mejorar la eficiencia energética mientras cumple con los objetivos de energía renovable. Equilibrar las demandas de energía con la sostenibilidad es fundamental.
- **Desafíos y oportunidades:** los desarrolladores y operadores de centros de datos deben navegar por el profundo impacto del poder en la industria. El progreso exponencial de la IA y el aprendizaje automático impulsa cambios en el diseño, la selección de sitios y las estrategias de inversión.

[13] Data Center Frontier (2024) – 2024 Global Data Center Outlook - https://www.datacenterfrontier.com/white-papers/whitepaper/33036436/2024-global-data-center-outlook

1.3 Perspectivas de América Latina

La mayoría de los países de América Latina y el Caribe (más del 80 %) cubren en su legislación temas como la privacidad y la protección de datos, la transparencia y el acceso a la información del sector público, la firma digital, la adquisición electrónica, la ciberseguridad y el gobierno digital. Sin embargo, aproximadamente la mitad de los países de la región no han seguido completamente el ritmo de los problemas relacionados con las capacidades digitales avanzadas y los enfoques proactivos y anticipatorios dentro de sus marcos legales y regulatorios. Estos incluyen la identidad digital, el principio de una sola vez, el acceso a la información/datos del sector privado, el diseño digital, la computación en la nube, las cajas de arena legales y/o regulatorias, la inteligencia artificial, las tecnologías emergentes y el derecho a impugnar (es decir, la capacidad de solicitar exenciones de las reglas existentes o la capacidad de solicitar que se reconsideren las reglas), entre otros.[14]

Estas tendencias han llevado a las empresas y organizaciones de toda la región a reevaluar sus enfoques de gestión de datos, y algunas han optado por construir sus propios centros de datos para satisfacer sus necesidades.[15] Como se explicó anteriormente en este documento, con esta decisión, los gobiernos están entrando en una actividad altamente compleja y exigente.

El mercado de centros de datos de América Latina experimentó inversiones de 5.510 millones de dólares en 2022 y se espera que alcance los 8.810 millones de dólares para 2028.[16] Además de la aceleración de la transformación digital, la demanda de servicios de centros de datos se debe principalmente a la necesidad de cumplir con las leyes y regulaciones de soberanía de datos al tiempo que se garantiza la seguridad y la privacidad de los datos.

Durante la última década, la transformación digital ha sido una prioridad para los gobiernos latinoamericanos. Sin embargo, el nivel de desarrollo y madurez varía de un país a otro.[17] Una parte significativa de las estrategias de gobierno digital no están actualizadas, y muchas de ellas son anteriores a 2020, lo que indica la necesidad de una revisión continua para mantener el ritmo de los avances tecnológicos.

El panorama en la región se caracteriza por avances significativos y diversidad en los enfoques hacia la transformación digital. Los gobiernos de toda la región están invirtiendo activamente en el fortalecimiento de las infraestructuras digitales públicas de sus países, incluido el desarrollo de centros de datos nacionales e iniciativas en la nube, para mejorar la prestación de servicios públicos y la gobernanza. Por ejemplo, Argentina está invirtiendo 5,8 millones de dólares en el desarrollo de infraestructura en la nube (ARSAT) para consolidar los datos del sector público. Brasil ha invertido para fortalecer su capacidad en la nube y migrar los centros de datos existentes en los últimos años como

[14] OCDE (2023), Digital Government Review of Latin America and the Caribbean, https://www.oecd-ilibrary.org/governance/digital-government-review-of-latin-america-and-the-caribbean_29f32e64-en
[15] Forbes (2023) – Navegando por la seguridad y el cumplimiento de datos en América Latina - https://www.forbes.com/sites/forbestechcouncil/2023/04/26/edge-of-sovereignty-navigating-data-security-and-compliance-in-latin-americas-evolving-tech-landscape/?sh=52c5a20356bd
[16] Arizton (2023) – Mercado de Centros de Datos de América Latina - https://www.arizton.com/market-reports/latin-america-data-center-market-report-2025
[17] OCDE (2023), Digital Government Review of Latin America and the Caribbean, https://www.oecd-ilibrary.org/governance/digital-government-review-of-latin-america-and-the-caribbean_29f32e64-en

parte de la Estrategia de Gobierno Digital 2020-2022. República Dominicana está desarrollando una nube privada disponible para el sector público OGTICLOUD, que presta especial atención a las medidas de seguridad. En Panamá y Paraguay, las respectivas autoridades gubernamentales digitales están desarrollando una infraestructura de nube dedicada y esfuerzos informáticos. Uruguay se destaca dada la política integral de nube Nube Pública Estatal vigente desde 2019, que incluye soluciones IaaS, PaaS y SaaS en todo el sector público.[18]

Una tendencia notable dentro de los gobiernos es adoptar modelos de nube híbrida y combinar soluciones de nube locales e hiperescala para garantizar la soberanía de los datos y el uso eficiente de los recursos digitales. Uruguay es un ejemplo de esos gobiernos; la Agencia para el Gobierno Electrónico y la Sociedad de la Información y el Conocimiento (AGESIC) define la política de nube (pública) de hiperescala, conocida como la Nube de la Presidencia, que ofrece infraestructura de nube a las organizaciones del sector público.[19] Esta política admite una variedad de servicios en la nube adaptados a las necesidades de las organizaciones del sector público, promoviendo una infraestructura pública digital segura, escalable y rentable en todo el país. El modelo de Uruguay incluye varios servicios en la nube, lo que sugiere un enfoque flexible de la computación en la nube que podría involucrar elementos de nube híbrida para cumplir con diversos requisitos del sector público.

Los diferentes enfoques gubernamentales de la infraestructura digital se ilustran en la Tabla 1. (La información de esta tabla se basa en la normativa vigente a la fecha del informe).

[18] OCDE (2023), Digital Government Review of ¬Latin America and¬ the ¬Caribbean, https://www.oecd-ilibrary.org/governance/digital-government-review-of-latin-america-and-the-caribbean_29f32e64-en
[19] URUGUAY, Principios generales de la nube pública en el estado, https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/principios-generales-nube-publica-estado

Tabla 1 - Infraestructura Digital de los Gobiernos de América Latina[20]

País	Infraestructura en la Nube	Política Gubernamental de Centros de Datos/ Nube	Url de Regulación de la Nube	Protección de Datos/Leyes de Privacidad	Protección de Datos/ Leyes de Privacidad
ARGENTINA	Híbrido	ARSAT / Cloud First	https://rb.gy/6qvo5w	Ley de Protección de Datos Personales.	https://rb.gy/z3rqsq
BRASIL	Híbrido	SERPRO / DATAPREV	https://rb.gy/lok16c	Lei Geral de Proteção de Dados	https://rb.gy/2wth6s
CHILE	Híbrido	Cloud First/Smart	http://rb.gy/x2wkm6	Ley N ° 19.628 de Protección de la Vida Privada	http://rb.gy/jb6jue
COLOMBIA	Híbrido	Cloud First	https://rb.gy/oled0p	Ley de Protección de Datos Personales o Ley 1581 de 2012	https://rb.gy/gvbzyz
COSTA RICA	Híbrido	Cloud First	https://rb.gy/rwcr6c	Ley de Protección de la Persona frente al tratamiento de sus datos personales, Nº 8968	https://bit.ly/4bkLEC0
REP. DOMINICANA	Privado	OGTICLOUD	https://bit.ly/4eNtDiS	Ley de protección de datos personales	https://bit.ly/3zqkX1D
ECUADOR	Público	Nube pública preferida	https://bit.ly/4cn8j1l	Ley Orgánica de Protección de Datos Personales	https://bit.ly/45TSWLV
MÉXICO	Híbrido	INFOTEC /Soberanía tecnológica	https://bit.ly/4elie3E	Ley Federal de Protección de Datos Personales en Posesión de Particulares y sus Reglamentos	https://bit.ly/3zlLihb
PANAMÁ	Privado	Servicio de Nube Gubernamental	https://bit.ly/3xMjK40	Ley N° 81 de 2019 Sobre Protección de Datos Personales.	https://bit.ly/3xuDd9v
PARAGUAY	Híbrido	Nube-PY	https://bit.ly/3XGdQfx	Ley N ° 1682 Reglamento Información de Carácter Privado	https://bit.ly/3L5xNVr
PERÚ	Público	Servicios gubernamentales en la nube	https://bit.ly/3VOmZA8	Ley Nº 29733, Ley de Protección de Datos Personales	https://tinyurl.com/n6wawb4v
URUGUAY	Híbrido	Nube de la Presidencia de la Rep.	https://tinyurl.com/Avzza	Ley de Protección de Datos Personales y Hábeas Data	https://tinyurl.com/4yve48ha

La razón subyacente de dicha residencia establecida en las leyes de protección de datos y privacidad es la mayor preocupación por la ciberseguridad y la noción de que los datos en las instalaciones o en la nube privada serán más seguros. Por lo general, estas preocupaciones se relacionan con datos en temas como defensa, geopolítica, diplomacia, activos económicos estratégicos y ciudadanos. Los gobiernos podrían evaluar cuidadosamente estas preocupaciones de acuerdo con su contexto, pero lo contrario podría ser cierto: las nubes a hiperescala podrían ser más seguras. La lógica es simple. Los datos locales en una sola ubicación centralizada pueden aumentar las vulnerabilidades de privacidad y seguridad, ya que son más susceptibles a un solo punto de falla. Por el contrario, una nube conectada globalmente crea economías de escala. Los hiperescaladores como Amazon Web Services, Microsoft y otros tienen equipos de miles de expertos mundiales en ciberseguridad que trabajan para proteger la nube aprovechando los puntos de datos y las amenazas de datos de todo el mundo. "El mundo de la ciberseguridad ofrece lecciones sobre por qué la localización de datos y las restricciones de residencia pueden ser perjudiciales y costosas: los problemas de seguridad de los datos pueden surgir al almacenar todos los datos en un territorio geográfico, lo que es contrario al enfoque de diversificación más exigido en la industria de la ciberseguridad y a menudo adoptado por las empresas multinacionales para garantizar una seguridad sólida en una red geográficamente dispersa".[21]

Del mismo modo, la ciberseguridad surge como un desafío crítico en la región; solo siete de los treinta y dos países de América Latina y el Caribe tienen marcos regulatorios para proteger su infraestructura crítica de los ciberataques, y solo 20 países cuentan con Equipos de Respuesta a

[20] Elaboración propia a partir de portales de Gobiernos, y conjunto de datos GovTech del BANCO MUNDIAL 2023 , https://datacatalog.worldbank.org/search/dataset/0037889/govtech-dataset, y BID – Computación en la nube: Contribución al desarrollo de ecosistemas digitales en países del Cono Sur (iadb.org)
[21] Banco Mundial (2023) - Nota práctica de contratación institucional sobre computación en nube - Nota práctica institucional y de contratación sobre computación en nube : Marco de evaluación de la nube y metodología de evaluación (worldbank.org)

Incidentes de Seguridad Informática (CSIRT),[22] cuyas capacidades y recursos (por ejemplo, tecnológicos, financieros y humanos) varían de uno a otro, no siempre alcanzando un nivel plenamente operativo. Este nivel actual de preparación cibernética en la región sugiere que existe un déficit notable que debe abordarse, especialmente para aquellos países que están construyendo o planean construir sus propios centros de datos.

Uno de los parámetros para medir el déficit en el nivel de preparación para la ciberseguridad en la región es el impacto económico de los ciberataques. El costo anual de los ciberataques en América Latina y el Caribe podría superar los 90 millones de dólares estadounidenses para 2025, con un promedio de más de 18,5 millones de ataques por año. Los incidentes notables incluyen un ataque en Costa Rica en abril de 2022, que afectó a numerosas agencias gubernamentales y exigió un rescate de 10 millones de dólares estadounidenses. Otro ataque en mayo de 2022 tuvo como objetivo la Caja Costarricense de Seguro Social, causando interrupciones en los sistemas críticos, incluido el pago de la seguridad social. Estos ataques hicieron que el país declarara el estado de emergencia, convirtiéndose en el primer país en utilizar fondos de emergencia debido a un ciberataque. Del mismo modo, Colombia sufrió un importante ataque de ransomware de terceros a principios de septiembre de 2023, que interrumpió gravemente los servicios vitales en todo el país. Este ataque afectó directamente a 20 entidades públicas, mientras que otras 78 entidades públicas y 762 empresas privadas se vieron afectadas indirectamente en toda América Latina, así como en otros países como Argentina, Panamá y Chile.

[22] Informe LATAM Ciso (2024) – Cyber Readiness in Latin American Public Sectors - https://www.metabaseq.com/wp-content/uploads/2024/04/LATAM-CISO-Report-2024.pdf

2 Ventajas y desafíos de los centros de datos gubernamentales

La idea errónea de que los datos están en riesgo porque los proveedores de nube de hiperescala pueden tener activos de infraestructura ubicados en un país que no sea donde se encuentra una entidad del sector público, además de las regulaciones de privacidad y protección de datos, ha llevado a algunos gobiernos de América Latina (véase Tabla 1) a tomar o considerar la decisión de que la forma de mantener sus datos seguros es tener la propiedad completa de la "pila", desde el piso y las paredes del edificio hasta el software en los servidores, en otras palabras, para construir sus propios centros de datos (en las instalaciones) o nubes privadas del gobierno a pesar de que no tiene los mismos beneficios en escalabilidad, funcionalidad, seguridad, privacidad, rentabilidad o agilidad que las nubes de hiperescala.

La Tabla 2 aclara los conceptos erróneos sobre la nube, y específicamente sobre la "nube pública", donde a menudo hay más preocupación y confusión.

Tabla 2 - Conceptos erróneos comunes sobre el uso de la nube pública por parte de los gobiernos[23]

CONCEPCIÓN ERRÓNEA	REALIDAD
El uso de la nube pública es costoso.	La computación en la nube es rentable porque evita o reduce la necesidad de adquirir equipos costosos. Los ahorros pueden representar entre el 10 y el 20 por ciento del presupuesto operativo anual de TI.
Las soluciones locales siempre son más seguras que la nube pública.	Las soluciones locales no son intrínsecamente más seguras porque la seguridad más avanzada se puede implementar en tiempo real cuando se utiliza la infraestructura en la nube.
El ritmo de innovación es el mismo cuando se utilizan soluciones en la nube pública y local.	Los servicios en la nube son mejores para fomentar la innovación porque son fáciles de usar, se pueden escalar rápidamente y proporcionan nuevos servicios a medida que están disponibles, lo que reduce significativamente el tiempo que lleva pasar de la idea a una solución de trabajo.
Es posible que las soluciones de nube pública no garanticen la protección de datos.	Las entidades de nube pública son muy diferentes en naturaleza de los productos de nube personal, como Facebook. El modelo de negocio de la nube pública fomenta una fuerte protección de datos. Se pueden tomar medidas técnicas para elevar la protección de datos a un nivel muy alto.
El proveedor de servicios en la nube (CSP) puede ver los datos personales y compartirlos con un tercero.	Casi todos los CSP cifran los datos, lo que significa que los datos no son visibles para el proveedor sin descifrarlos. La mayoría de los CSP también admiten claves de cifrado de clientes, lo que significa que ni el CSP ni nadie más puede ver los datos sin la clave de cifrado administrada por el cliente.
Las soluciones en la nube son difíciles de escalar.	Los servicios en la nube tienen una escalabilidad casi ilimitada (la llamada elasticidad de la nube). Por lo tanto, permiten que los gobiernos y otras entidades públicas se amplíen en tiempos de alta demanda de los usuarios.
Las soluciones en la nube son menos sostenibles que los sistemas heredados.	El uso de la computación en la nube puede reducir el consumo de energía y las emisiones de carbono hasta en un 30 por ciento debido a las economías de escala.
Todos los tipos de nubes son iguales.	Para necesidades de migración de datos más extensas, una nube pública de hiperescala suele ser el camino óptimo para lograr todos los beneficios de la nube debido a la profundidad y amplitud de los servicios ofrecidos.
La infraestructura local debe desarrollarse antes de pasar a la nube.	No se necesita infraestructura local para comenzar a usar servicios en la nube, lo que ilustra una de las propuestas de valor más críticas de los servicios en la nube, particularmente en entornos de baja capacidad de TI.
Las soluciones en la nube requieren conectividad avanzada y de alta velocidad.	Los desarrollos en tecnología y dispositivos de Internet de las cosas (IoT) de baja potencia, así como la contenerización, permiten a las agencias públicas implementar soluciones incluso cuando la conectividad es baja. Algunos proveedores de nube de hiperescala ofrecen servicios especializados para clientes de baja conectividad.
Comenzar requiere una inversión significativa.	La nube pública permite a las organizaciones comenzar con casos de uso pequeños y directos y escalar más tarde si la solución funciona según lo previsto. No se necesita una inversión de capital inicial significativa.

[23] Banco Mundial (2022) - Ecosistema de migración gubernamental a la nube - https://www.worldbank.org/en/events/2022/06/12/government-migration-to-cloud-ecosystems-wbg

2.1 Ventajas y desafíos

La decisión potencial de que mantener los datos seguros es tener la propiedad completa de un centro de datos tiene algunos beneficios, pero también crea algunas preocupaciones con respecto a la capacidad de mantenerse al día con el rápido ritmo de las tecnologías emergentes como la inteligencia artificial, la seguridad, la innovación, la sostenibilidad y la rentabilidad.

Al considerar la opción de construir sus propios centros de datos para migrar desde la TI heredada, los gobiernos también deben considerar los beneficios y desafíos de otras alternativas disponibles que también sean viables y puedan cumplir con sus regulaciones de protección de datos y privacidad. A continuación se muestra una comparación de las principales ventajas y desventajas de las diferentes opciones para migrar datos heredados a la nube.[24]

Tabla 3 - Ventajas y desventajas de las opciones de migración a la nube

OPCIÓN	VENTAJAS	DESVENTAJAS
Migrar a un centro de datos del gobierno. Mantenimiento de sistemas de TI heredados (datos almacenados en las instalaciones).	• Control de datos que cumple con los requisitos de localización de datos.	• Los costos de capital para la inversión inicial y la capacitación de los empleados, las operaciones y el mantenimiento pueden ser extremadamente altos. • Las instalaciones a menudo están desactualizadas y subutilizadas. • El legado es inherentemente incapaz de escalar más allá de los requisitos definidos anteriormente sin inversiones de capital significativas. • La existencia continua de sistemas heredados incurrirá en costos cada vez mayores para las integraciones necesarias, mitigaciones, etc. • Inflexibilidad para satisfacer la demanda fluctuante. • Falta de confiabilidad debido a la falta de sistemas de respaldo extensos necesarios para proporcionar capacidades de recuperación ante desastres. • Ciberseguridad limitada y más costosa de proteger. • Rendimiento y capacidad limitados para integrar rápidamente aplicaciones de vanguardia e innovación. • La dificultad de construir centros de datos ecológicos a pequeña escala.
Migrar a la nube privada (datos almacenados en las instalaciones).	• El hardware, el almacenamiento de datos y la conexión se pueden personalizar con precisión a la tarea deseada para garantizar cierta seguridad con inversiones masivas. • El cumplimiento normativo puede ser difícil para los datos clasificados como "alto secreto".	• La flexibilidad para satisfacer la demanda fluctuante es limitada. • La falta de sistemas de respaldo extensos para la recuperación ante desastres puede conducir a una falta de confiabilidad. • Las capacidades de seguridad son limitadas; las soluciones de nube privada tendrán dificultades para mantenerse a la par con las funciones de seguridad basadas en la nube.

[24] Basado en Banco Mundial (2022) - Ecosistema de migración gubernamental a la nube https://www.worldbank.org/en/events/2022/06/12/government-migration-to-cloud-ecosystems-wbg

OPCIÓN	VENTAJAS	DESVENTAJAS
Migrar a un centro de datos de ubicación conjunta (datos almacenados externamente).	• Las nubes privadas externas a menudo ofrecen más escalabilidad que la infraestructura local. • Los costos de capacitación, operaciones y mantenimiento de los empleados son más bajos.	• La visibilidad y el control pueden verse reducidos debido a la falta de herramientas para monitorear las implementaciones de manera efectiva.
Aplique una nube híbrida (interconectando datos almacenados en las instalaciones o en nubes privadas con nubes públicas).	• Las organizaciones pueden mantener una infraestructura privada para activos confidenciales o cargas de trabajo que requieren baja latencia. • Se puede acceder a recursos adicionales en la nube pública cuando sea necesario. • La transición a la nube no tiene por qué ser abrumadora, ya que la migración puede llevarse a cabo gradualmente, con cargas de trabajo escalonadas en el tiempo.	• La interoperabilidad puede ser un desafío, ya que es difícil administrar múltiples sistemas dispares al mismo tiempo. • La infraestructura adicional aumenta la complejidad. • Se deben incurrir en costos para capacitar a los empleados, las operaciones y el mantenimiento.
Migrar a la nube pública (incluidos los proveedores de servicios de hiperescala).	• Los costos de capital son cero, ya que no hay necesidad de comprar hardware o software. • Las nuevas soluciones se pueden probar casi de inmediato. • El proveedor de servicios se encarga de todo el mantenimiento. • Las mejoras son prácticamente ilimitada; los recursos bajo demanda están disponibles para satisfacer las necesidades cambiantes. • La confiabilidad es alta, ya que una vasta red de servidores garantiza contra fallas. • Se proporcionan funciones avanzadas, como la seguridad habilitada por inteligencia artificial.	• El usuario pierde el control y la visibilidad sobre cómo y dónde se almacenan y gestionan los datos. • Se deben garantizar los requisitos de cumplimiento de la protección de datos de todas las industrias. En países con alta complejidad regulatoria, los requisitos de residencia de datos pueden exigir que ciertos tipos de datos se mantengan en las instalaciones, mientras que otras cargas de trabajo pueden residir en la nube pública. • La seguridad compartida significa que las amenazas a la seguridad también se comparten, donde los proveedores de la nube y los clientes trabajan juntos para proteger mejor los datos de los clientes. • Los usuarios pueden estar bloqueados en un proveedor. Este problema se puede mitigar a través de una solución multinube y una estrategia de salida clara. Sin embargo, una solución multinube aumentará los desafíos de interoperabilidad.

2.2 Preocupaciones clave en un mundo digital de rápida innovación

Los gobiernos que han decidido o están considerando desarrollar sus propios centros de datos enfrentan varios desafíos para mantener sus centros de datos a la vanguardia en un mundo que avanza rápida y exponencialmente en innovaciones tecnológicas. El ritmo sin precedentes del panorama digital introduce varias preocupaciones críticas, incluida la adopción de tecnologías emergentes como la inteligencia artificial, las amenazas a la ciberseguridad, el desarrollo y la retención del talento digital, la tecnología verde y la eficiencia de costos, entre otras. Algunas de las preocupaciones más apremiantes se describen en las siguientes subsecciones.

2.2.1 Innovación: Tecnologías nuevas y emergentes

La innovación juega un papel crucial en el gobierno al dar forma a las políticas, los servicios y el bienestar general de los ciudadanos. Sin embargo, solo una ligera mayoría de los líderes de gobiernos digitales en América Latina encuentran que el servicio público en su país es innovador. Los gobiernos latinoamericanos generalmente hacen principalmente énfasis en la innovación dentro de sus estrategias de gobierno digital. Algunos también han desarrollado estrategias digitales e inteligencia artificial específicamente para el sector público.[25]

Al igual que los gobiernos de otras partes, los gobiernos de la región buscan aprovechar el inmenso potencial de la IA de una manera estratégica y confiable. Ocho países han desarrollado o están desarrollando una estrategia nacional de IA (Argentina, Brasil, Chile, Colombia, México, Perú, República Dominicana y Uruguay), y siete se han adherido a los Principios de IA de la OCDE (Argentina, Brasil, Chile, Colombia, Costa Rica, México y Perú).[26]

La demanda de aceleradores de IA está superando la oferta, y las partes interesadas de la industria predicen un aumento significativo en la nueva capacidad del centro de datos para adaptarse a las mayores densidades de rack requeridas para impulsar las cargas de trabajo generativas de IA. Esto también podría imponer exigencias extenuantes a las infraestructuras de energía y refrigeración, así como aumentar el tamaño y el peso de los gabinetes de densidad extrema.[27]

El progreso de la región en IA también dependerá de la infraestructura informática implementada por los gobiernos. Los centros de datos gubernamentales tendrán el desafío de seguir el ritmo de la demanda de capacidad y espacio de centros de datos que requiere la inteligencia artificial, especialmente la IA generativa. Como resultado, esto se traduce en grandes y constantes inversiones de capital de fondos públicos para mantener sus centros de datos actualizados con el estado del arte para permitir la innovación basada en IA hacia un gobierno algorítmico.

[25] OCDE (2023), Digital Government Review of Latin America and the Caribbean, https://www.oecd-ilibrary.org/governance/digital-government-review-of-latin-america-and-the-caribbean_29f32e64-en
[26] OCDE (2022) -The Strategic and Responsible Use of AI in the Public Sector of LAC - https://www.oecd-ilibrary.org/sites/1f334543-en/index.html?itemId=/content/publication/1f334543-en#execsumm-d1e75
[27] Uptime Intelligence (2024) – Five Data Center Predictions for 2024 - https://intelligence.uptimeinstitute.com/sites/default/files/2024-01/Keynote%20report%20121_Five%20data%20center%20predictions%20for%202024.pdf

2.2.2 Talento y habilidades digitales

A medida que el mundo avanza a través de los avances tecnológicos y los cambios en la economía global, la competencia por el talento subraya la necesidad de que los países se adapten, innoven e inviertan en capital humano para garantizar la resiliencia económica y el crecimiento. Esta situación afecta directamente a la adquisición, el desarrollo y la retención de talento en los gobiernos, donde la adquisición, el desarrollo y la retención de talento es un desafío dado el limitado grupo de talento tecnológico con gran demanda a nivel mundial. [28]

"El gran desafío para los gobiernos latinoamericanos no es la tecnología. Es talento humano". [29]

Esta afirmación se ve respaldada por las bajas clasificaciones de los países de la región en el contexto global, según el IMD World Talent Ranking 2023. Brasil y Venezuela se encuentran en el extremo inferior del ranking, con Brasil en el puesto 63 y Venezuela en el puesto 62. Este posicionamiento sugiere desafíos en áreas críticas para la competitividad del talento, como la educación, las oportunidades económicas y la calidad de vida. Argentina aparece en una mejor posición en el puesto 54, lo que indica algunas fortalezas en el desarrollo, la atracción y la retención del talento en comparación con sus pares regionales. Chile y México también son notables, con Chile en el puesto 50 y México en el 59, lo que muestra el diverso panorama del desarrollo del talento en toda América Latina.

Dada la situación del talento en la región, los gobiernos enfrentan un gran desafío ya que deben competir por el talento técnico especializado con condiciones de trabajo que no son atractivas en comparación con las que ofrece el sector privado. Este aspecto fundamental debe ser considerado en los planes de los gobiernos para desarrollar sus infraestructuras digitales, especialmente aquellas que consideran la construcción de sus propios centros de datos, lo que requerirá habilidades especializadas que son escasas en la región.

2.2.3 Seguridad y privacidad

Los gobiernos están muy preocupados por el impacto económico y social de la seguridad digital y cómo los ciberataques, incluidos los delitos cibernéticos y el espionaje, afectarán la seguridad nacional y la confianza digital. Sin embargo, el nivel de preparación cibernética sigue siendo bajo. Por ejemplo, solo siete de los 32 países latinoamericanos tienen planes para proteger su infraestructura crítica de los ciberataques, y solo 20 países tienen Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT).[30]

Una de las amenazas más frecuentes, particularmente en América Latina, es el ransomware, que con frecuencia aprovecha las técnicas criptográficas para cifrar datos y exigir un rescate a las víctimas. La falta de políticas y regulaciones de ciberseguridad en América Latina aumenta el riesgo de ataques de ransomware, que pueden interrumpir gravemente las operaciones gubernamentales y comerciales. Estos ataques a infraestructuras críticas pueden tener efectos negativos generalizados en los ciudadanos de toda la región.

[28] Ranking Mundial de Talentos IMD (2023), https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-talent-ranking/
[29] Diego Molano Ministro de TIC de Colombia (2010-2015). Asesor - Transformación Digital de Gobiernos y Empresas. Inversor y mentor de startups.
[30] Informe LATAM Ciso (2024) – Cyber Readiness in Latin American Public Sectors - https://www.metabaseq.com/wp-content/uploads/2024/04/LATAM-CISO-Report-2024.pdf

A continuación se presentan ejemplos de ciberataques a infraestructuras y servicios digitales gubernamentales. (Es posible que hayan surgido nuevos casos desde la fecha de este informe).

Tabla 4 - Ciberataques en gobiernos latinoamericanos

PAÍS	CIBERATAQUE
ARGENTINA	**Registro Nacional de las Personas (RENAPER) (octubre 2021): Telecom Argentina (Julio 2020):** Sufrió un ataque exigiendo un rescate de 7,5 millones de dólares, afectando 18.000 estaciones de trabajo.
BRASIL	**Sistema Judicial Brasileño (2020-2022):** Sufrió 13 ataques cibernéticos consecutivos, interrumpiendo los servicios y arriesgando la destrucción de pruebas. **Secretario de Finanzas de Río de Janeiro (2022):** Experimentó una violación que afecta la recaudación de impuestos y los servicios ciudadanos. **Secretario de Estado de Finanzas de Río de Janeiro, Brasil (abril de 2022):** Dirigido por la pandilla de ransomware LockBit 2.0.
CHILE	**Ataque de ransomware de IFX Networks y Rhysida (Sep.2023)** impactando a entidades gubernamentales y al Ejército de Chile.
COLOMBIA	**Ataque de ransomware de IFX Networks (septiembre de 2023):** Más de 78 entidades estatales colombianas y 762 empresas privadas se vieron afectadas por un ataque de ransomware al proveedor de servicios de Internet IFX Networks.[31]
COSTA RICA	**Gobierno de Costa Rica (2022):** El ataque de ransomware Conti y el grupo Hive resultaron en la primera declaración de emergencia nacional del mundo debido al ransomware. **Todos los ataques exitosos fueron en centros locales o en la nube privada.** Costa Rica nunca pagó el rescate, pero ha gastado, hasta el 22 de junio, aproximadamente 24 millones de dólares.
REP. DOMINICANA	**Ministerio de Agricultura (agosto de 2022):** Ataque de ransomware cuántico, con más de 1 TB de archivos robados y una demanda de rescate.

[31] Elaboración propia Informe LATAM Ciso (2024) – Cyber Readiness in Latin American Public Sectors - https://www.metabaseq.com/wp-content/uploads/2024/04/LATAM-CISO-Report-2024.pdf y CONSENSUS (2023) A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America, https://consensus.app/papers/analysis-worst-cybersecurity-vulnerabilities-latin-florunda/d216a46058b358259944bd9bbb97f90d/?utm_source=chatgpt

ECUADOR	**Gobierno Municipal de Quito (abril 2022):** Enfrentó un ataque de ransomware, que derivó en la suspensión de servicios a la población.
MÉXICO	**Secretaría deDefensa de México (SEDENA) (2019-2021):** Ataques experimentados del software malicioso Pegasus de NSO Group contra periodistas y defensores de derechos humanos. PEMEX (2019): Ataque de ransomware, exigiendo 5 millones de dólares.
PANAMÁ	En 2023, Panamá obtuvo una puntuación alta en el Índice de Basilea contra el Lavado de Dinero (AML), lo que lo convierte en el país más susceptible a las amenazascibernéticas. **Ministerio de Desarrollo Social (2021):** Ataque de ransomware que afecta su infraestructura de red y sistemas de respaldo[32]
PERÚ	**Servicio de Inteligencia Peruano (2022):** Dirigido por Conti ransomware, con información limitada disponible sobre la violación. **Gobierno Peruano (2022)** Conti ransomware, que afecta a varias entidades gubernamentales.

La infraestructura gubernamental digital es un objetivo especialmente común para los ataques digitales, y los países en desarrollo están particularmente en riesgo debido a la menor capacidad y personal de ciberseguridad. Los centros de datos locales y las nubes privadas han sido atacados, como se muestra en el caso de Costa Rica mencionado anteriormente. [33]

Las crecientes amenazas a la seguridad están obligando a los centros de datos gubernamentales a mejorar y actualizar continuamente su tecnología y estándares de seguridad de TI para mantenerse al día con el cambiante panorama de amenazas. Aplicar tecnologías sofisticadas, como la gestión estricta del acceso a la identidad y el cifrado de autenticación multifactorial en reposo y en tránsito, sería muy costoso de adquirir de forma independiente. Además, las ciberamenazas avanzadas están superando a las herramientas de seguridad tradicionales. Los proveedores de la nube ahora utilizan redes globales de sensores y análisis basados en IA/ML para detectar y responder a las amenazas casi en tiempo real.

[32] Welivesecurity (2021) - https://www.welivesecurity.com/la-es/2021/01/12/ataque-ransomware-afecta-ministerio-desarrollo-social-panama/
[33] Banco Mundial (2022) - Ecosistema de migración gubernamental a la nube - https://www.worldbank.org/en/events/2022/06/12/government-migration-to-cloud-ecosystems-wbg

2.2.4 Eficiencia de costos

El panorama de la infraestructura digital en los gobiernos latinoamericanos es mixto, desde centros de datos locales, heredados o en construcción, nubes privadas locales o regionales, infraestructura híbrida y nube pública. Prácticamente todos los gobiernos de la región tienen un centro de datos, nuevo o heredado, para administrar. El costo de administrarlos, mantenerlos y actualizarlos es muy alto, con importantes desafíos para asegurar los presupuestos necesarios. El dilema que enfrentan estos gobiernos es la importante inversión heredada en servidores, almacenamiento y centros de datos que no son fáciles de desinvertir (especialmente para las adquisiciones más recientes), y las regulaciones sobre el posible uso indebido de fondos públicos si estas inversiones no se utilizan.

Una vez que los gobiernos deciden construir sus propios centros de datos, se convierten en parte de una industria dinámica, **intensiva en capital** y en crecimiento explosivo, la Industria de Centros de Datos (DCI). Es una industria que está experimentando cambios transformadores impulsados por la inteligencia artificial (IA) y la transición hacia la energía verde. El equipo altamente especializado necesario para soportar densidades de IA, en particular la refrigeración líquida, transformará el diseño tradicional de las instalaciones.[34]

Hay cuatro (4) actores especializados en la industria de centros de datos: bienes raíces (encontrar ubicaciones y negociar el terreno), inversores (financiar la construcción), desarrolladores (construir el centro de datos) y operadores (administrar el centro de datos). Dependiendo del enfoque del gobierno para desarrollar su propio centro de datos, desempeñará los cuatro roles o puede subcontratar algunos de ellos, como desarrollador/constructor de centros de datos, operador y potencialmente bienes raíces, cada uno trae sus propios desafíos de seguridad.

Independientemente del uso, los centros de datos locales requieren importantes inversiones de capital iniciales y costos de mantenimiento continuos. Para los centros de datos gubernamentales, estas inversiones iniciales y costos fijos pueden ser particularmente desafiantes, especialmente para los proyectos de IA que requieren recursos computacionales significativos. Además, las grandes inversiones requeridas para construir, operar y mantener la tecnología actualizada enfrentan el desafío adicional de las asignaciones y aprobaciones de capital y presupuesto operativo, que a menudo son procesos complejos, largos y burocráticos.

- **Altos costos de capital y operativos:** la construcción y el mantenimiento de un centro de datos requiere una inversión inicial significativa en infraestructura, hardware e instalaciones, así como costos continuos relacionados con el mantenimiento, las actualizaciones, los programas de cumplimiento y la dotación de personal. Para muchos gobiernos, estos costos pueden ser prohibitivos y pueden desviar fondos de otros servicios públicos críticos.

- **Rápida obsolescencia tecnológica:** el ritmo del cambio tecnológico puede dejar el hardware y el software del centro de datos obsoletos rápidamente, lo que requiere actualizaciones y reemplazos frecuentes. A los gobiernos les puede resultar difícil mantenerse al día con el ritmo del cambio, lo que conduce a ineficiencias y vulnerabilidades.

[34] Data Center Frontier (2024) – 2024 Global Data Center Outlook - https://www.datacenterfrontier.com/white-papers/whitepaper/33036436/2024-global-data-center-outlook

- **Preocupaciones de eficiencia energética y sostenibilidad:** los centros de datos implican un consumo significativo de electricidad, lo que contribuye a altos costos operativos e impactos ambientales. Alcanzar los objetivos de eficiencia energética y sostenibilidad puede ser un desafío, especialmente para las organizaciones del sector público con experiencia potencialmente limitada en estas áreas.

- **Complejidad de la gestión y la seguridad:** operar un centro de datos requiere conocimientos especializados en gestión de TI, ciberseguridad y cumplimiento. Los gobiernos deben invertir en personal calificado y medidas de seguridad avanzadas para proteger los datos confidenciales, que pueden ser costosos y complejos.

- **Desafíos de escalabilidad y flexibilidad:** a medida que crece la demanda de servicios digitales y surgen tecnologías como la Inteligencia Artificial, los gobiernos pueden tener dificultades para escalar la infraestructura de su centro de datos de manera rápida y rentable.

2.2.5 Eficiencia y flexibilidad

La eficiencia y flexibilidad de los gobiernos está directamente relacionada con la infraestructura digital a la que se prestan los servicios. Cada una de las infraestructuras digitales (locales, nube privada/pública y nube híbrida) tiene un impacto directo en la prestación de servicios. Este impacto está relacionado con la capacidad de la infraestructura para escalar, mantenerse actualizada y responder a los cambios tecnológicos y los requisitos de las diferentes agencias gubernamentales y servicios para ciudadanos y empresas.

Los centros de datos locales proporcionan control gubernamental sobre su infraestructura, lo que, en teoría, puede mejorar la eficiencia y la flexibilidad en la prestación de servicios, pero los desafíos prácticos de este modelo de infraestructura a menudo comprometen estos beneficios. Las restricciones presupuestarias, los problemas de escalabilidad y el ritmo del cambio tecnológico pueden obstaculizar la capacidad del gobierno para servir a sus ciudadanos de manera efectiva. Además, las complejidades operativas y las preocupaciones ambientales afectan aún más la flexibilidad del gobierno para adaptar y mejorar los servicios a los ciudadanos de manera oportuna. Los siguientes son los desafíos para la eficiencia y flexibilidad de los centros de datos locales:

- **Respuesta más rápida a los nuevos servicios:** la importante inversión requerida para establecer y mantener centros de datos locales puede limitar la capacidad del gobierno para responder rápidamente a las nuevas demandas de servicios o invertir en otras áreas que podrían beneficiar a los ciudadanos, como la educación o la atención médica.

- **Respuesta rápida a los cambios tecnológicos:** los rápidos cambios tecnológicos pueden hacer que las infraestructuras locales sean obsoletas, comprometiendo la eficiencia de la prestación de servicios. Las tecnologías emergentes como la inteligencia artificial (IA), la cadena de bloques y los gemelos digitales, entre otras (que pueden crear nuevos productos y servicios innovadores), requieren grandes inversiones para actualizar las infraestructuras existentes que pueden no considerarse dentro de los presupuestos aprobados para operar el centro de datos.

- **Complejidad en la gestión:** la complejidad operativa de la gestión de centros de datos locales requiere personal especializado y formación continua. Esta complejidad puede ralentizar la implementación de nuevos servicios o mejoras, retrasando los beneficios destinados a los ciudadanos.

- **Escalabilidad:** los centros de datos locales tienen un espacio finito, lo que puede limitar la capacidad del gobierno para ampliar los servicios en respuesta a las crecientes demandas de los ciudadanos/transacciones, las temporadas altas o las emergencias. Esta limitación desafía la flexibilidad del gobierno para adaptar los servicios rápidamente para satisfacer las necesidades de los ciudadanos.

- **Riesgo de concentración de datos:** la concentración de datos en instalaciones locales aumenta el riesgo de interrupciones significativas del servicio en caso de desastres o ciberataques. Tales interrupciones pueden afectar críticamente la capacidad del gobierno para proporcionar servicios oportunos y confiables a los ciudadanos, socavando la confianza pública.

2.2.6 Sostenibilidad

La sostenibilidad y la eficiencia energética son las principales prioridades para los centros de datos; una regulación más estricta y los requisitos de informes obligarán a los centros de datos a ofrecer un mejor rendimiento en eficiencia energética. Cumplir objetivos públicos más estrictos no será fácil para quienes operan infraestructura crítica. El mayor uso de software y procesadores que consumen más energía, la falta de disponibilidad de energía renovable en la red eléctrica y los crecientes requisitos de resiliencia frente al cambio climático, por ejemplo, harán que sea más difícil reducir las emisiones de carbono[35].

Es posible que el impacto ambiental de operar centros de datos locales que consumen mucha energía no se alinee con las crecientes expectativas del público y las estrictas regulaciones para operaciones gubernamentales sostenibles y ecológicas. Para garantizar una transformación digital sostenible, se necesitan esfuerzos para una infraestructura digital ecológica, lo que incluye la gestión de los riesgos climáticos y la reducción de la huella climática y ambiental de los centros de datos.

Los centros de datos ecológicos apoyan los esfuerzos de mitigación y adaptación al cambio climático al contribuir a la descarbonización de la economía de un país y ayudar a cumplir objetivos de sostenibilidad más amplios. Abordar la huella climática de los centros de datos requiere un enfoque circular del ciclo de vida, que abarque el diseño, la fabricación, las adquisiciones, las operaciones, la reutilización, el reciclaje y la eliminación de desechos electrónicos.[36]

Los desafíos de los centros de datos gubernamentales para cumplir con las expectativas de sostenibilidad son multifacéticos e involucran el uso de energía, la eficiencia, la escalabilidad y más:

- **Alto consumo de energía:** Los centros de datos locales consumen una gran cantidad de energía para las operaciones informáticas y los sistemas de refrigeración para mantener temperaturas óptimas para el hardware. Este alto consumo de energía es un desafío importante para la sostenibilidad, ya que a menudo se basa en fuentes de energía no renovables. Teniendo en cuenta que el suministro de energía es inestable en algunas regiones, particularmente en América Latina y el Caribe. Una continua escasez de energía en todo el mundo inhibe significativamente el crecimiento del mercado global de centros de datos, y el abastecimiento de energía es una prioridad para los operadores de todas las regiones, incluida América Latina. Por ejemplo, Querétaro, México, tiene solo 0,6 MW disponibles para arrendamiento, lo que indica una escasa disponibilidad de energía. Aunque la disponibilidad de centros de datos de América Latina aumentó modestamente en 2024, principalmente debido a más espacio en São Paulo, Brasil, que vio aumentar su disponibilidad a 62,1 MW desde 52,3 MW en el primer trimestre de 2024, este crecimiento sigue siendo leve. Esto indica que la demanda aún supera la nueva oferta en muchos mercados latinoamericanos.[37]

[35] UPTIME Intelligence (2024) Cinco predicciones de centros de datos para 2024, https://uptimeinstitute.com/resources/research-and-reports/five-data-center-predictions-for-2024
[36] UIT, Banco Mundial (2023) – Centros de datos ecológicos - https://www.itu.int/hub/publication/d-them-32-2023-01/
[37] Tendencias globales del centro de datos 2024 (CBRE) - Tendencias globales del centro de datos 2024 | CBRE

- **Requisitos de enfriamiento:** Los centros de datos requieren un enfriamiento extenso para evitar el sobrecalentamiento. Los métodos de enfriamiento tradicionales consumen mucha energía, lo que contribuye a altas emisiones de carbono y costos operativos.

- **Escalabilidad limitada:** Los centros de datos locales tienen capacidades físicas fijas. Ampliarlos o actualizarlos para incorporar tecnologías más ecológicas o mejorar la eficiencia energética puede ser un desafío logístico y costoso.

- **Capital inicial y costos de mantenimiento:** Invertir en tecnologías energéticamente eficientes o fuentes de energía renovables requiere un capital inicial significativo. Además, el mantenimiento continuo de estos sistemas aumenta el costo, lo que dificulta que algunas organizaciones justifiquen la inversión financieramente.

- **Dependencia de fuentes de energía no renovables:** La sostenibilidad de un centro de datos también se ve afectada por su fuente de energía. Muchos centros de datos locales todavía dependen de la electricidad generada a partir de fuentes no renovables, lo que tiene una mayor huella de carbono.

- **Gestión de desechos electrónicos:** Los centros de datos locales generan cantidades significativas de desechos electrónicos (desechos electrónicos) a partir de hardware obsoleto o roto. Reciclar o eliminar adecuadamente los desechos electrónicos es un desafío, y un manejo inadecuado puede conducir a la contaminación ambiental.

- **Uso del agua:** Algunas tecnologías de enfriamiento requieren grandes cantidades de agua, lo que contribuye a la escasez de agua en algunas regiones y afecta la sostenibilidad general del centro de datos.

2.2.7 Hiperescalabilidad

Un centro de datos de hiperescala es un centro de datos masivo que proporciona capacidades de escalabilidad extremas y está diseñado para cargas de trabajo a gran escala con una infraestructura de red optimizada, conectividad de red optimizada y latencia minimizada.

Los gobiernos requieren hiperescalabilidad para admitir datos masivos, transacciones de gran volumen y la adopción de tecnologías emergentes. Las siguientes son algunas razones a considerar:

- **Manejo de volúmenes masivos de datos:** con el crecimiento exponencial de los datos de diversas fuentes, incluidos los servicios públicos como la seguridad social, las agencias tributarias, la vigilancia y las operaciones administrativas, los centros de datos de hiperescala ofrecen la infraestructura necesaria para almacenar, procesar y analizar grandes conjuntos de datos de manera eficiente.

- **Mejora de la seguridad nacional y los servicios públicos:** los centros de datos de hiperescala pueden admitir las capacidades informáticas avanzadas necesarias para las operaciones de seguridad nacional, incluido el análisis de datos para la detección de amenazas y la prestación de servicios públicos a escala.

- **Adopción de nuevas tecnologías que exigen un alto poder de cómputo, como la inteligencia artificial (IA), especialmente la IA generativa:** los centros de datos a hiperescala proporcionan recursos informáticos y almacenamiento masivos, lo que permite que la inteligencia artificial generativa procese inmensos conjuntos de datos para capacitación e inferencia. Al alojar hardware especializado, como GPU (unidades de procesamiento de gráficos)

y TPU (unidades de procesamiento de tensores), los centros de datos aceleran los cálculos complejos y admiten aplicaciones y cargas de trabajo de IA.

La transición de los centros de datos locales a los centros de datos de hiperescala implica superar importantes desafíos relacionados con el consumo de energía, las redes, la escalabilidad y la eficiencia operativa, así como adoptar tecnologías y diseños que admitan una arquitectura y operaciones masivas y escalables para los gobiernos. Estas importantes inversiones superan los presupuestos iniciales, y alcanzar estos niveles de inversión es una tarea compleja, así como navegar por el proceso de asignación y aprobación del presupuesto.

Los gobiernos de la región que están en proceso de construcción o ya han construido centros de datos deben considerar las necesidades de hiperescalabilidad de diferentes agencias gubernamentales, especialmente aquellas que manejan grandes volúmenes de datos, como las agencias de seguridad social y tributarias.

2.2.7.1 Gestión y gobernanza de la exposición al riesgo cibernético

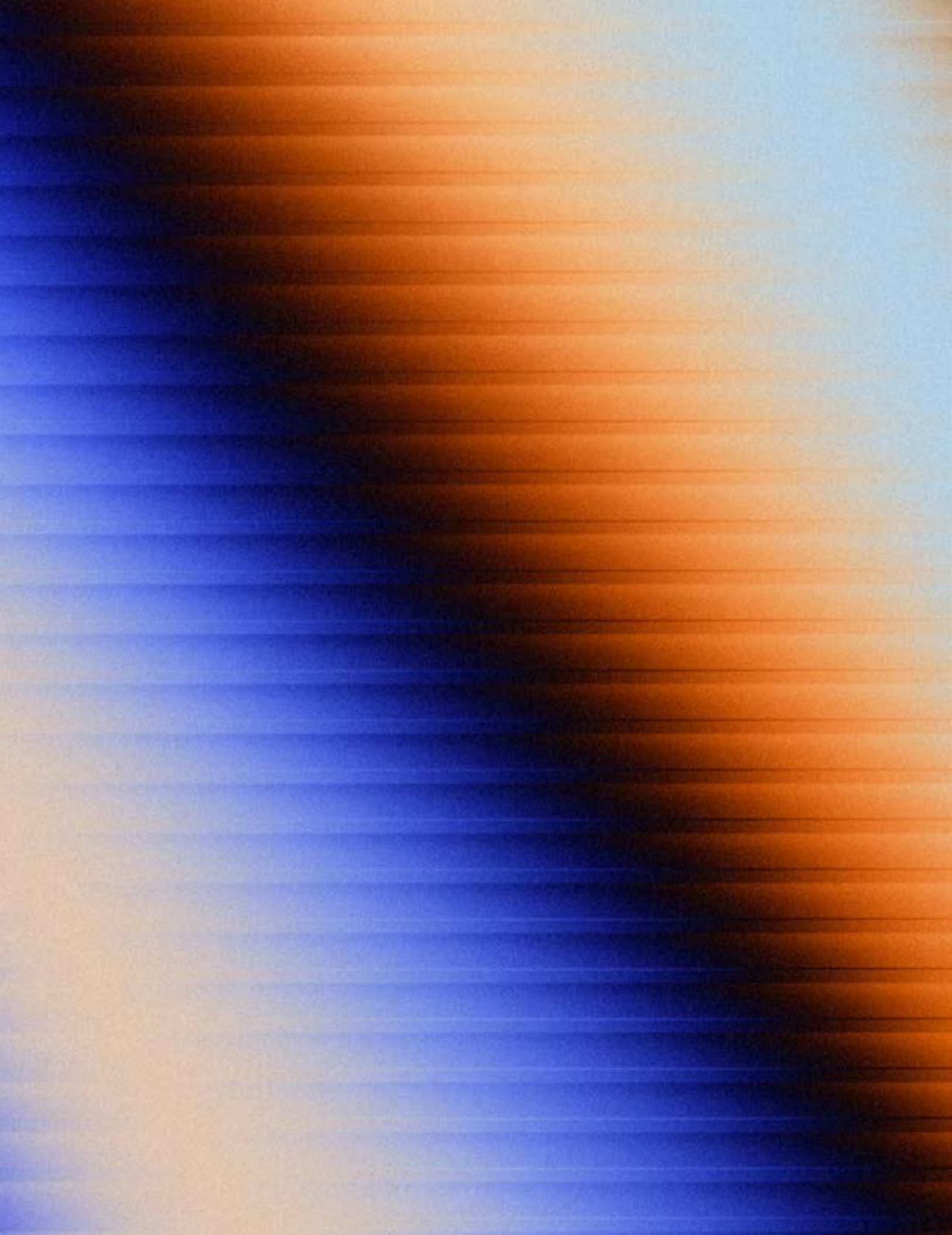
Los programas gubernamentales tradicionales de ciberseguridad, centrados en listas de verificación de cumplimiento, auditorías anuales y monitoreo de amenazas aisladas, se han vuelto insuficientes en una era de amenazas en rápida evolución por parte de actores estatales, sindicatos de ransomware y vulnerabilidades de la cadena de suministro.

En respuesta, los gobiernos deben adoptar una gestión proactiva y continua de la exposición al riesgo cibernético, alineando las operaciones de ciberseguridad con objetivos más amplios de gobernanza digital.

Las agencias pueden basarse en las mejores prácticas establecidas para:

- Agregar y analizar datos de herramientas de detección de endpoints, telemetría de red, sistemas en la nube, plataformas de identidad e inteligencia de amenazas.
- Cuantificar el riesgo continuamente y priorizar la remediación en función de la información sobre amenazas en tiempo real.
- Coordinar los esfuerzos de respuesta a incidentes entre ministerios y agencias.
- Informar las métricas procesables a los líderes ejecutivos para la toma de decisiones estratégicas.

Al poner en práctica la gestión de riesgos de esta manera, basándose en estándares reconocidos y marcos sólidos, los gobiernos pueden adaptarse dinámicamente a las amenazas emergentes, enfocar los recursos en las áreas de mayor exposición y reforzar la resiliencia en un panorama digital que cambia rápidamente.



3 Habilitación de una infraestructura digital gubernamental resiliente a través de la colocación híbrida

Los gobiernos de todo el mundo se enfrentan cada vez más a las demandas de un panorama digital en rápida innovación. Mantener los centros de datos tradicionales en las instalaciones o desarrollar nuevos centros de datos presenta desafíos importantes, incluidos altos costos de capital y operativos, rápida obsolescencia tecnológica, problemas de eficiencia energética y la complejidad de administrar y asegurar infraestructuras digitales a gran escala. Estos desafíos se ven agravados por la necesidad de seguir el ritmo de los avances tecnológicos, satisfacer las crecientes expectativas de los ciudadanos en materia de servicios digitales, adoptar tecnologías nuevas y emergentes y garantizar el cumplimiento de los requisitos normativos nacionales e internacionales.

Al desarrollar nuevos centros de datos, los gobiernos se convierten en partes interesadas en la industria de los centros de datos, lo que implica navegar por una industria compleja, altamente especializada e intensiva en capital. Se proyecta que el mercado de centros de datos alcance los 340.200 millones de dólares en 2024, esperando una tasa de crecimiento anual (CAGR 2024-2028) del 6,56 %, lo que resultará en un volumen de mercado de 438.700 millones de dólares para 2028.[38][39] En América Latina, el mercado se valoró en 5.510 millones de dólares en 2022 y se espera que alcance los 8.810 millones de dólares para 2028, creciendo a una TCAC del 8,14 %.[40]

Los gobiernos deben decidir si abordan todas o delegan algunas de las funciones en la cadena de valor de este sector, que consta de cuatro tipos principales de actores:

1. Desarrolladores (por ejemplo, Goodman, Mitsui Fudosan, Maple Tree, etc.),
2. Pperadores de centros de datos (por ejemplo, Equinix, Realidad Digital, etc.),
3. Empresas inmobiliarias (por ejemplo, JLL, Colliers, Cusham, etc.) y;
4. Inversores (capital privado, fondos de infraestructura, multilaterales, etc.).[41]

Los gobiernos deben ser conscientes de los desafíos y los requisitos importantes de la industria de los centros de datos antes de decidir construir los suyos propios y formar parte de esta industria. Estos desafíos y requisitos incluyen principalmente lo siguiente:

- **Altos costos de capital y operativos:** la construcción y el mantenimiento de un centro de datos exige una inversión inicial sustancial en infraestructura, hardware e instalaciones. Hay costos continuos relacionados con el mantenimiento, las actualizaciones y la dotación de personal. Estos costos pueden ser excesivamente altos, lo que puede llevar a desviar fondos de otros servicios públicos críticos.

[38] Statista – Centro de datos en todo el mundo - https://www.statista.com/outlook/tmo/data-center/worldwide
[39] Grand View Research - https://www.grandviewresearch.com/industry-analysis/data-center-market-report
[40] Arizton – Mercado de centros de datos – Pronóstico 2023-2028 - https://www.arizton.com/market-reports/global-data-center-market-report-2025
[41] Estructura de Investigación 2023 – Mercado Global de Centros de Datos - https://www.structureresearch.net/product/2023-global-data-centre-colocation-interconnection-report/

- **Rápida obsolescencia tecnológica:** el rápido ritmo del cambio tecnológico puede hacer que el hardware y el software del centro de datos se vuelvan obsoletos rápidamente, lo que requiere actualizaciones y reemplazos frecuentes. Esto crea ineficiencias y vulnerabilidades, ya que los gobiernos pueden tener dificultades para mantenerse al día con los últimos avances.

- **Problemas de eficiencia energética y sostenibilidad:** los requisitos de energía para los centros de datos están creciendo exponencialmente, lo que genera altos costos operativos e impactos ambientales. Lograr la eficiencia energética y la sostenibilidad es un desafío, particularmente para las organizaciones del sector público que pueden carecer de experiencia en estas áreas.

- **La complejidad de la gestión y la seguridad:** operar un centro de datos requiere conocimientos especializados en gestión de TI, ciberseguridad y cumplimiento. Los gobiernos deben invertir en personal calificado y medidas de seguridad avanzadas para proteger los datos confidenciales, lo que aumenta la complejidad y el costo.

- **Desafíos de escalabilidad y flexibilidad:** a medida que crece la demanda de servicios digitales y surgen nuevas tecnologías, los gobiernos pueden tener dificultades para escalar la infraestructura de su centro de datos de manera rápida y rentable. Los centros de datos locales tienen un espacio y una capacidad finitos, lo que puede limitar la capacidad de responder a las crecientes demandas o emergencias.

- **Desafíos de innovación:** los centros de datos gubernamentales podrían aislar e inhibir la innovación si se desconectan de ecosistemas tecnológicos más amplios o carecen de la escalabilidad para integrar tecnologías nuevas y emergentes, como la inteligencia artificial (IA). La incapacidad de adoptar e implementar rápidamente tecnologías de vanguardia puede obstaculizar el desarrollo de servicios públicos innovadores y limitar la capacidad del gobierno para responder a las necesidades cambiantes de los ciudadanos.

Los gobiernos se enfrentan a un dilema importante a la hora de decidir cómo asegurar la soberanía digital mientras gestionan las complejidades y los desafíos de diseñar, construir y operar sus propios centros de datos.

Para abordar este dilema, los gobiernos deben aprovechar la experiencia y la infraestructura de la industria de centros de datos existente para desarrollar alternativas al tomar la decisión de construir sus propios centros de datos. Al asociarse con líderes de la industria, los gobiernos pueden beneficiarse de tecnologías avanzadas, mejores prácticas y eficiencias operativas. Este enfoque no solo apoya a la industria local de centros de datos, sino que también garantiza que los centros de datos gubernamentales se construyan y mantengan con los más altos estándares. Al aprovechar la experiencia de los proveedores de centros de datos establecidos, los gobiernos pueden evitar las trampas comunes y acelerar el despliegue de una infraestructura digital robusta, segura y escalable.

El gobierno federal de los Estados Unidos es un buen ejemplo, donde el Congreso ha ordenado a las agencias federales que aprovechen todas las soluciones de centros de datos comerciales para satisfacer sus necesidades de misión (Ley Federal de Mejora de Centros de Datos de 2023, parte de la Ley de Autorización de Defensa Nacional (NDAA) para el año fiscal 2024). La Ley requiere acciones para que las agencias cubiertas operen sus centros de datos existentes. Estas pautas deben requerir que el jefe de una agencia (1) evalúe y actualice regularmente su cartera de aplicaciones para utilizar adecuadamente las tecnologías modernas, y (2) aproveche las soluciones comerciales de centros de datos, como la nube híbrida, la nube múltiple, la ubicación conjunta, la interconexión o la computación en la nube.

3.1 Colocación híbrida

Una de las alternativas para resolver el dilema es aprovechar la industria de los centros de datos, específicamente **los proveedores de Colocación Híbrida**. La colocación a menudo se percibe como un mero centro de datos donde se alquila espacio, energía y conectividad a Internet, pero puede ofrecer mucho más. Los centros de datos de colocación actuales proporcionan una variedad de servicios, como soluciones de TI administradas y de nube híbrida. Ofrecen una mayor densidad de potencia, que es esencial para escalar y admitir rápidamente nuevas tecnologías, sistemas de refrigeración eficientes, medidas de seguridad sólidas y conectividad a Internet de alta velocidad. Además, **algunos proveedores de colocación ofrecen acceso directo a los hiperescaladores de nube más populares, lo que mejora la flexibilidad y la escalabilidad (Colocación híbrida).**[42]

Al explorar el mundo de la colocación, es esencial comprender los diversos tipos de servicios de colocación disponibles. Los proveedores ofrecen diferentes opciones para adaptarse a las diversas necesidades y preferencias de las organizaciones. Estos son los seis tipos más comunes[43]:

- **Espacio en rack:** esta es la forma más básica de colocación, donde las organizaciones alquilan una cierta cantidad de racks o gabinetes dentro de un centro de datos. Cada rack proporciona espacio para servidores, switches y otros equipos de red. La colocación de espacios en rack es adecuada para organizaciones con requisitos moderados de infraestructura de TI.

- **Jaula:** en este tipo, un proveedor de centro de datos asigna una jaula dedicada dentro de las instalaciones de su centro de datos a un cliente específico. La jaula está rodeada por una valla o malla de seguridad, lo que proporciona una capa adicional de protección física. La colocación en jaulas ofrece más privacidad y seguridad que el espacio en rack, lo que la hace adecuada para organizaciones con mayores necesidades de seguridad.

- **Suite privada:** una suite privada es un espacio exclusivo y autónomo dentro de un centro de datos, que prioriza la privacidad y la seguridad. Ofrece amplias opciones de personalización para satisfacer necesidades específicas.

[42] AKCP – Cloud vs Colocation - https://www.akcp.com/blog/cloud-vs-colocation-which-is-best-for-you/
[43] Banco de datos – ¿Qué es la colocación? Guía definitiva de los beneficios de Colocation 2024 - https://www.databank.com/resources/blogs/everything-you-need-to-know-about-colocation/

Esto permite el alojamiento de un número más significativo de bastidores, equipos adicionales e incluso salas de reuniones dedicadas. Este tipo de colocación es particularmente adecuado para empresas u organizaciones más grandes que buscan un entorno adaptado y personalizado que se alinee con precisión con sus requisitos únicos.

- **Venta al por mayor:** este tipo de colocación está dirigido a organizaciones con amplias necesidades de infraestructura. Los proveedores mayoristas ofrecen un espacio dedicado a gran escala dentro de sus centros de datos, generalmente un piso o edificio entero. Esta opción permite a las organizaciones tener un control completo sobre su entorno, incluida la energía, la refrigeración y la infraestructura, y proporciona la flexibilidad para escalar rápidamente.

- **Híbrida:** la creciente demanda de cloud computing ha llevado a algunos proveedores a ofrecer servicios de Colocación Híbrida. Esto permite a las empresas colocar sus equipos informáticos en un centro de datos y, al mismo tiempo, conectarse a proveedores de servicios en la nube hiperescaladores para obtener recursos adicionales o configuraciones de nube híbrida. La Colocación Híbrida ofrece las ventajas tanto de la colocación como de la computación en la nube, lo que permite a las organizaciones optimizar su infraestructura y cargas de trabajo.

- **Perimetral:** a medida que crece la demanda de aplicaciones de baja latencia y computación perimetral, la colocación perimetral se ha convertido en una forma especializada de colocación. Los centros de datos perimetrales están ubicados estratégicamente más cerca de los usuarios finales o de ubicaciones geográficas específicas. Esto ayuda a minimizar la latencia y mejorar el rendimiento de las aplicaciones sensibles a la latencia y los dispositivos IoT.

3.2 Soberanía y privacidad[44]

La Colocación Híbrida, con los altos niveles de protección y seguridad de la nube de hiperescala, resuelve inquietudes y dudas sobre soberanía y privacidad. Para proteger y asegurar sus datos en la Colocación Híbrida, los gobiernos deben establecer un sistema claro para la clasificación de datos (véase el Anexo C para la definición de clasificación de datos). Este sistema es esencial para saber qué datos tienen y dónde se encuentran esos datos; qué tipos o clases de datos están expuestos, cómo están expuestos y cuáles son los riesgos potenciales; y a qué aplicaciones se accede, por quién y con qué fines. Los proveedores de Colocación Híbrida pueden y deben proporcionar esta información en función de sus mejores prácticas de soberanía.

[44] Databank – 2024 – Navigating The Challenge of Data Sovereignty and Colocation - https://www.databank.com/resources/blogs/navigating-the-challenges-of-data-sovereignty-and-colocation/

Superar los desafíos de la soberanía y la colocación de datos generalmente se reduce a implementar las mejores prácticas de gobernanza de datos sólidas. Las siguientes son las mejores prácticas clave en la soberanía de datos que siempre deben estar presentes para tener una Colocación Híbrida para la soberanía:

- **Llevar a cabo una diligencia debida exhaustiva:** antes de seleccionar una instalación de colocación, se debe llevar a cabo una diligencia debida integral para garantizar la alineación con las regulaciones de datos relevantes y los requisitos jurisdiccionales. Los contratos y los acuerdos de nivel de servicio (SLA) deben revisarse para aclarar la propiedad de los datos, la soberanía y las responsabilidades de cumplimiento.

- **Implementar un cifrado de datos sólido:** se deben utilizar mecanismos de cifrado sólidos para proteger los datos, tanto en tránsito como en reposo, dentro del entorno de colocación. Se deben implementar estándares de cifrado, como AES-256 para el cifrado de datos y TLS/SSL para canales de comunicación seguros, para garantizar la confidencialidad e integridad de los datos.

- **Establecimiento de controles de acceso granulares:** se deben implementar controles de acceso basados en roles (RBAC) y principios de privilegios mínimos para restringir el acceso a datos confidenciales dentro de la instalación de colocación. Los permisos de acceso deben configurarse en función de las funciones y responsabilidades del trabajo, y se deben aplicar medidas de autenticación estrictas, como la autenticación multifactor (MFA), para mejorar la seguridad.

- **Implementación de soluciones de residencia de datos:** las soluciones de residencia de datos deben implementarse para garantizar el cumplimiento de los requisitos de localización de datos. Se deben utilizar mecanismos de geofencing y etiquetado de datos para hacer cumplir las políticas de residencia de datos, restringiendo el almacenamiento de datos y el procesamiento a ubicaciones geográficas específicas según lo exijan las regulaciones.

- **Auditoría periódica de los registros de acceso:** se deben realizar auditorías periódicas de los registros de acceso y las rutas de actividad dentro del entorno de colocación para monitorear los intentos de acceso no autorizados o la actividad sospechosa y anómala. Se deben implementar mecanismos de registro sólidos y soluciones SIEM para rastrear las interacciones del usuario con los datos y los componentes de la infraestructura.

- **Implementación de medidas de prevención de pérdida de datos (DLP):** las soluciones de prevención de pérdida de datos (DLP) deben implementarse para monitorear y prevenir la exfiltración o fuga de datos no autorizados dentro del entorno de colocación. Las políticas de DLP deben configurarse para detectar y bloquear las transferencias de datos confidenciales fuera de los canales aprobados, mitigando el riesgo de violaciones de datos.

- **Garantizar copias de seguridad de datos redundantes:** se deben implementar soluciones de copia de seguridad de datos redundantes y de recuperación de desastres para protegerse contra la pérdida o corrupción de datos en la instalación de colocación. Las ubicaciones de

respaldo geográficamente dispersas y las tecnologías de replicación deben utilizarse para mantener la disponibilidad de datos y la resiliencia en caso de fallas de infraestructura o desastres.

- **Actualización periódica de parches de seguridad:** se deben realizar actualizaciones de seguridad y de software regulares para todos los sistemas y aplicaciones implementados dentro del entorno de colocación. Se debe implementar un proceso sólido de gestión de parches para remediar las vulnerabilidades conocidas y mitigar el riesgo de brechas o vulnerabilidades de seguridad.

- **Llevar a cabo una capacitación de concientización sobre la soberanía de los datos:** se deben proporcionar programas continuos de capacitación y concientización para el personal que trabaja dentro de la instalación de colocación para garantizar el cumplimiento de los principios de soberanía de los datos y los requisitos reglamentarios. Los empleados deben ser educados en las mejores prácticas de manejo de datos, las regulaciones de privacidad y la importancia de mantener la soberanía de los datos.

- **Contratar auditores externos para la verificación del cumplimiento:** se deben contratar auditores externos o expertos en cumplimiento para realizar evaluaciones y auditorías periódicas de la adhesión de la instalación de colocación a las regulaciones y mejores prácticas de soberanía de datos. Se debe obtener una verificación independiente de los esfuerzos de cumplimiento y se deben identificar áreas de mejora para fortalecer las medidas de soberanía de datos.

La Colocación Híbrida con las mejores prácticas para la soberanía es la alternativa que permite cumplir con todos los requisitos de sostenibilidad y escalabilidad y resuelve todas las inquietudes, dudas y temores con respecto a la ciberseguridad, la privacidad, la soberanía y la residencia de datos. Los gobiernos con una carga de trabajo altamente sensible, como los sistemas de defensa, inteligencia y electoral, también pueden requerir soluciones de seguridad soberana. Estos sistemas funcionan sin dependencia de Internet o uso compartido de telemetría y se detallan en la sección 3.3.1.

Este modelo de centro de datos proporciona una plataforma ágil, escalable y flexible que fomenta la innovación y la adopción de nuevas tecnologías, como la inteligencia artificial y otras tecnologías emergentes.

La colocación híbrida con una sólida gobernanza de datos y mejores prácticas de soberanía es un camino para cumplir con los requisitos de sostenibilidad, escalabilidad y seguridad para cargas de trabajo gubernamentales sensibles. Sin embargo, los gobiernos deben evaluar cuidadosamente todo el espectro de opciones, desde la nube pública hasta la híbrida y local, para garantizar que cada carga de trabajo esté alineada con la estrategia de infraestructura correcta. En muchos casos, las plataformas modernas en la nube ya ofrecen controles avanzados de soberanía, privacidad y residencia de datos, lo que las hace adecuadas incluso para casos de uso gubernamental delicados o de alta seguridad.

En situaciones en las que se necesita un aislamiento extraordinario o interoperabilidad heredada, un modelo híbrido o local puede seguir siendo apropiado, como se detalla en la sección 3.3.1. En general, las agencias gubernamentales deben adoptar un enfoque basado en el riesgo para decidir qué modelo

de infraestructura (colocación híbrida, nube pública o local) se adapta mejor a los requisitos específicos de cada carga de trabajo y a las regulaciones nacionales. Este enfoque equilibrado minimiza las implementaciones locales innecesarias al tiempo que garantiza protecciones sólidas para cargas de trabajo verdaderamente sensibles.

3.3 Seguridad

La Colocación Híbrida puede ayudar a las instituciones gubernamentales a aumentar la ciberseguridad mediante el despliegue de mecanismos de defensa de vanguardia. Esto es fundamental porque la sofisticación cada vez mayor de las herramientas maliciosas ha hecho que sea más fácil que nunca dañar la infraestructura digital de un gobierno. Los ataques criptográficos (comúnmente conocidos como ransomware) se han vuelto cada vez más comunes en América Latina.

La infraestructura gubernamental digital es un objetivo particularmente común para los ataques, y los países en desarrollo corren un riesgo particular debido a la menor capacidad y talento en materia de ciberseguridad. Para cargas de trabajo altamente sensibles, los gobiernos pueden adoptar implementaciones de seguridad soberana que operen en entornos con brechas de aire sin ninguna transmisión de telemetría a los sistemas de nube pública.

Aprovechar los proveedores de Colocación Híbrida permite a los gobiernos implementar tecnologías sofisticadas, como una sólida gestión de acceso a la identidad, autenticación multifactor y cifrado en reposo y en tránsito, que sería muy costoso adquirir por su cuenta. También invierten mucho en mantener actualizadas las funciones de seguridad para que coincidan con las capacidades de los adversarios y desarrollan constantemente nuevas funciones de seguridad, como la detección de amenazas de aprendizaje automático. Los proveedores de colocación respetan los estándares y regulaciones de la industria, lo que demuestra su dedicación a la seguridad y el cumplimiento. Adquieren certificaciones como ISO 27001 (Gestión de la Seguridad de la Información) o SOC 2 (Control de la Organización de Servicios) como prueba de su compromiso con el mantenimiento de prácticas de seguridad sólidas y el cumplimiento de estrictos requisitos de cumplimiento.

3.3.1 Opciones de seguridad soberana para cargas de trabajo gubernamentales de alta sensibilidad

A medida que los gobiernos de América Latina expanden los servicios digitales en áreas relacionadas con la defensa, la identidad ciudadana y las infraestructuras críticas, la necesidad de una seguridad sólida y un control integral se vuelve primordial. Si bien algunas cargas de trabajo delicadas pueden requerir instalaciones especializadas, las plataformas modernas en la nube también pueden ofrecer capacidades de seguridad avanzadas e implementaciones totalmente soberanas adaptadas a los requisitos nacionales.

Estos enfoques ofrecen modelos de seguridad, un cifrado sólido y el cumplimiento de regulaciones estrictas, garantizando que los datos y la telemetría gubernamental permanezcan bajo supervisión soberana. En jurisdicciones con mandatos estrictos de privacidad o preocupaciones geopolíticas, los gobiernos pueden optar por:

- Modelos de datos locales o de nube privada sin transmisión de datos externos para los activos más críticos.

- Implementaciones de Sovereign Cloud ofrecidas por proveedores líderes que permiten la residencia de datos en el país, con herramientas avanzadas para la detección de amenazas, sandboxing e integración con inteligencia nacional de amenazas.

Muchos proveedores de la nube cumplen o superan los marcos de seguridad y cumplimiento reconocidos, como FedRAMP, ISO 27001, SOC 2 y los estándares locales de residencia de datos. Para las cargas de trabajo de mayor sensibilidad, se pueden adoptar modelos fuera de línea, pero estos deben abordarse caso por caso.

3.4 Sostenibilidad

En este modelo, los proveedores de servicios de colocación deben cumplir con todos los requisitos y estándares de sostenibilidad provenientes de las agencias reguladoras, y los gobiernos tienen la responsabilidad de imponer sus requisitos de sostenibilidad en los centros de datos de los proveedores a través de la adquisición.

Los gobiernos deben utilizar estratégicamente su poder adquisitivo para fomentar prácticas ambientalmente sostenibles entre los proveedores de colocación. Esto implica seleccionar proveedores que prioricen la eficiencia energética, el uso de materiales respetuosos con el medio ambiente y la gestión responsable de los residuos. Al integrar criterios ecológicos en los procesos de adquisición, las organizaciones influyen en los proveedores para que adopten prácticas sostenibles y contribuyan a objetivos ambientales más amplios, promoviendo un cambio positivo en las cadenas de suministro y las industrias a través de decisiones de compra centradas en la sostenibilidad.

Las estrategias de ecologización en la adquisición de centros de datos requieren enfoques personalizados basados en el modelo de servicio que emplea la colocación o cualquier cosa como servicio. Los gobiernos a menudo se encuentran con situaciones en la adquisición ecológica de servicios de datos en las que consideraciones específicas están fuera de su control, particularmente en modelos subcontratados como los servicios en la nube, mientras que los grandes proveedores a menudo pueden aprovechar las economías de escala y la experiencia entre sitios con esfuerzos de sostenibilidad al realizar inversiones en eficiencia y tecnología ecológica.[45]

Los centros de datos gubernamentales tienen un tamaño y una capacidad instalados limitados, lo que les impide escalar para satisfacer las nuevas demandas de procesamiento masivo de datos y transacciones y adoptar tecnologías emergentes como la inteligencia artificial (IA) y la IA generativa.

Los proveedores de colocación híbrida complementan sus centros de datos con una infraestructura de nube de hiperescala, creando una escalabilidad casi ilimitada que permite:

- Agregar y eliminar servicios según sea necesario. Esta "elasticidad de la nube" puede ser automática y sin interrupciones.

- Construir un sistema con componentes adicionales (por ejemplo, conectar un servidor a otros para agregar potencia de procesamiento o almacenamiento). Este "escalado horizontal" puede aumentar la redundancia y garantizar que los

[45] UIT, Banco Mundial (2023) – Centros de datos ecológicos - https://www.itu.int/hub/publication/d-them-32-2023-01/

servicios sigan estando disponibles y sean confiables.

- Gestionar automáticamente diferentes tipos de escalado (autoescalado). Esta capacidad de escalar sin problemas es útil para gestionar las cargas máximas normales (como la matrícula escolar) y reaccionar ante emergencias (como desastres naturales o pandemias).

- Implementar tecnologías emergentes que requieran una alta potencia de cálculo, como la inteligencia artificial y los gemelos digitales.

3.5 Innovación – Gobierno cognitivo/algorítmico

La Colocación Híbrida proporciona vastos recursos informáticos y almacenamiento, lo que permite que la inteligencia artificial procese conjuntos de datos masivos para capacitación e inferencia.
Esta capacidad permite un cambio fundamental en la forma en que los gobiernos abordan sus misiones, un gobierno cognitivo[46]. Aprovecha los datos, las tecnologías de la información, la inteligencia artificial (IA) y el análisis de datos para mejorar la toma de decisiones, la rendición de cuentas y la transparencia.

El enfoque de sistemas cognitivos mejora significativamente con respecto al ciclo tradicional de "predecir-prevenir-evaluar". Los gobiernos ahora pueden diseñar programas con una arquitectura inteligente que modela o cambia los resultados futuros mediante la incorporación de información escalable y en tiempo real. Esto permite que los modelos predictivos se actualicen continuamente en función del rendimiento pasado.

Los siguientes son algunos aspectos clave del gobierno cognitivo:

Toma de decisiones basada en datos:
los gobiernos confían cada vez más en la evidencia pasada, los datos en tiempo real y las predicciones futuras para informar las políticas. Pueden tomar decisiones tácticas más informadas mediante el análisis de datos históricos y el monitoreo de información en tiempo real.

- **Retrospectiva:** los gobiernos utilizan análisis avanzados y aprendizaje automático para aprender del pasado: qué ha funcionado y qué no.

- **En tiempo real:** monitorean los eventos y datos actuales para informar las decisiones inmediatas.

- **Previsión:** el análisis predictivo y los ejercicios de simulación ayudan a anticipar eventos futuros e implementar medidas preventivas.

El gobierno cognitivo faculta a los funcionarios para tomar mejores decisiones, beneficiando a los ciudadanos, la atención médica y las poblaciones vulnerables. Es una solución dinámica que combina las mejores nubes públicas y privadas, mejorando la escalabilidad, la agilidad y la flexibilidad al tiempo que garantiza la seguridad y el cumplimiento de los datos.

[46] Deloitte Insights, El gobierno como sistema cognitivo, https://www2.deloitte.com/us/en/insights/industry/public-sector/government-trends/2021/government-as-a-cognitive-system.html

3.6 Infraestructura Pública Digital (DPI por sus siglas en inglés)

Con el rápido ritmo de la digitalización en los países, es fundamental que la transformación digital inclusiva y basada en los derechos esté integrada en la tecnología, la gobernanza y los ecosistemas digitales locales. En este contexto, junto con la infraestructura de Colocación Híbrida, es imprescindible implementar una infraestructura pública digital (DPI) responsable y centrada en las personas.

Infraestructura Pública Digital, o DPI, es un término al que ahora se refieren regularmente funcionarios gubernamentales, grupos de expertos, instituciones de desarrollo, organizaciones sin fines de lucro e incluso directores ejecutivos globales como un enfoque transformador para superar el progreso a escala. Países como Brasil[47], India, Singapur, Australia y Tailandia han construido y escalado DPI.[48]

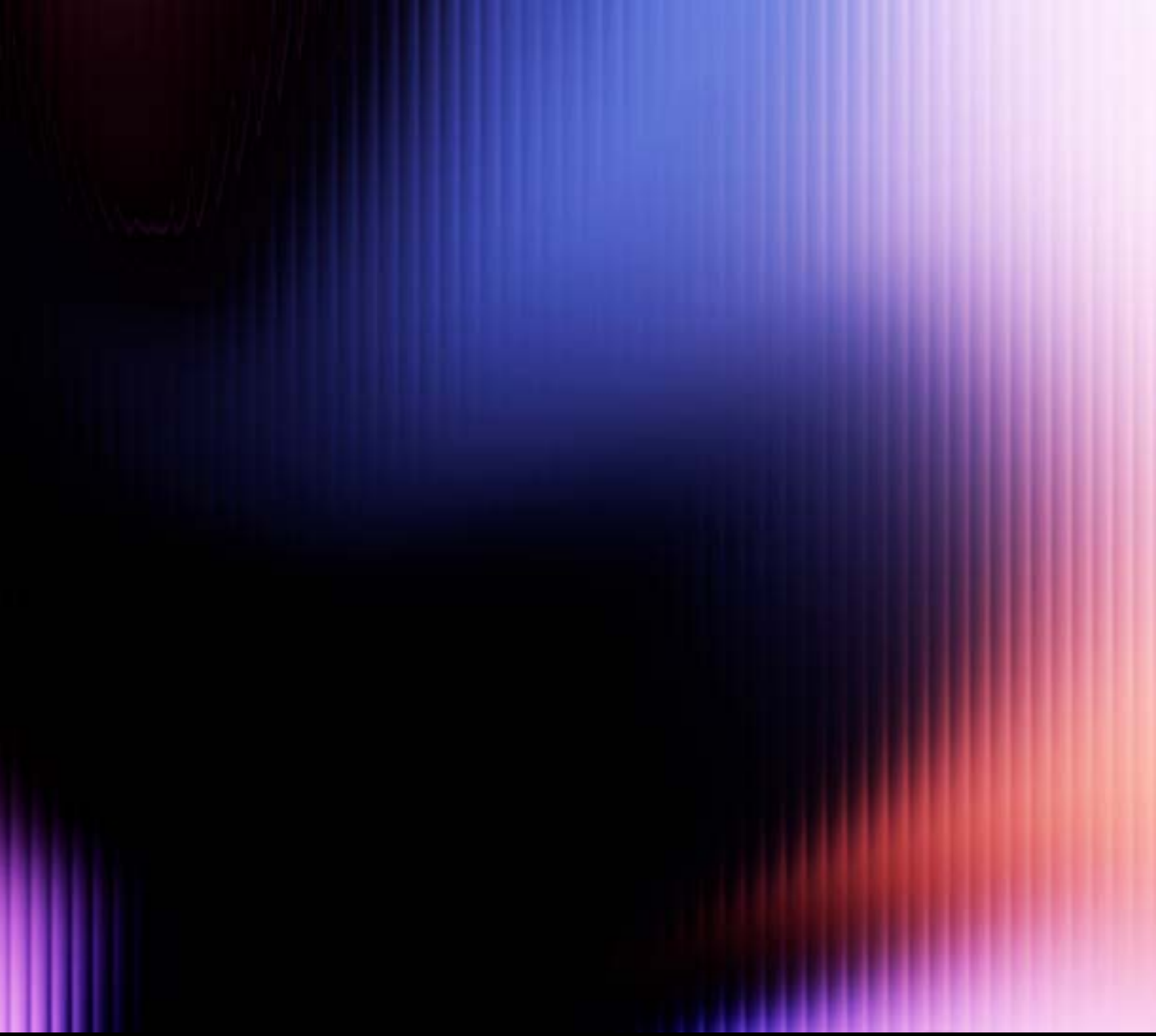
EL DIP representa un cambio radical para cualquier país, especialmente para los países de ingresos medios y bajos, donde se estima que puede acelerar el desarrollo económico entre un 20 % y un 33 %[49]. Es la base de la digitalización y el sistema que permite la prestación de servicios digitales a los ciudadanos y al sector privado. El DPI tiene diferentes definiciones, pero todos comparten principios básicos de confianza, seguridad, interoperabilidad, inclusión y accesibilidad[50].

El DPI tiene diferentes formas, y existe consenso en clasificarlo en tres tipos, según sus funciones:

- Identidad digital: la capacidad de las personas y las empresas para verificar de forma segura su identidad, así como servicios de confianza complementarios como firmas electrónicas y credenciales verificables.
- Pagos digitales: transferencia de dinero fácil e instantánea entre personas, empresas y gobiernos.
- Intercambio de datos basado en el consentimiento: flujo continuo de datos personales en los sectores público y privado, con salvaguardas para la protección de datos personales según los marcos de gobernanza de datos aplicables relevantes.
- Otros emergentes: puede haber otras funciones de tecnología DPI centrales emergentes, como descubrimiento y cumplimiento, credenciales verificables, DPI geoespacial, modelos de IA, infraestructura de clave pública (PKI) y confianza, firmas electrónicas y agregación de datos y contenido.

Los países latinoamericanos están avanzando en el desarrollo de infraestructuras públicas digitales (DPI) como la nube, la identidad digital, la interoperabilidad de datos, los pagos digitales y la notificación digital; sin embargo, los resultados son mixtos y se centran principalmente en la identidad digital/firma digital. Cubrir a toda la población y satisfacer el alto volumen de transacciones para una implementación completa de DPI requiere una infraestructura escalable que sería difícil de satisfacer solo con centros de datos locales.

[47] PNUD – El impacto humano y económico del DPI - https://www.undp.org/publications/human-and-economic-impact-digital-public-infrastructure
[48] Centro de Infraestructura Pública Digital - https://cdpi.dev/
[49] UNDP (2022) -Bold Investment for DPI - https://digitalpublicgoods.net/Bold-Investments-Executive-Summary.pdf.
[50] PNUD (2023) Acelerando LOS ODS a través de la infraestructura pública digital https://www.undp.org/publications/accelerating-sdgs-through-digital-public-infrastructure-compendium-potential-digital-public-infrastructure



4 Conclusiones y recomendaciones

Los centros de datos propiedad y operados por el gobierno se enfrentan a varios desafíos, incluida la necesidad de una alta inversión de capital, las dificultades para escalar rápidamente las operaciones, mantener altos niveles de seguridad de los datos y cumplir con las regulaciones nacionales e internacionales. Además, al construir y operar sus propios centros de datos, los gobiernos se convierten en actores de la industria de centros de datos altamente especializados, intensivos en capital y dinámicos. Esta participación requiere que los gobiernos asuman roles que van desde la adquisición de bienes raíces y la construcción de instalaciones hasta el desarrollo de infraestructura y la gestión de operaciones, áreas que requieren una sólida experiencia en la industria de centros de datos. Esto puede desviar la atención de su misión de gobernanza y prestación de servicios públicos.

La Colocación Híbrida surge como una solución prometedora a estos retos. Permite a los gobiernos aprovechar la infraestructura de vanguardia sin los altos costos iniciales asociados y los riesgos de sostenibilidad operativa. Esta proporciona escalabilidad y flexibilidad, lo que permite una gestión eficiente de los recursos que puede adaptarse a un mundo digital en rápida innovación. Ofrece características de seguridad mejoradas y cumplimiento con la soberanía de los datos a través de asociaciones estratégicas con proveedores experimentados. Al adoptar la Colocación Híbrida, los gobiernos pueden abordar eficazmente estos desafíos operativos y centrarse más en la innovación y la prestación de servicios públicos mejorados, evitando al mismo tiempo las complejidades de gestionar todos los aspectos de las operaciones del centro de datos. Este cambio estratégico aborda los desafíos operativos inmediatos y posiciona los servicios de infraestructura digital del gobierno para el crecimiento, la innovación y la resiliencia futuros.

A continuación se presenta un conjunto de recomendaciones para los gobiernos que consideran la estrategia de Colocación Híbrida:

1. **Evaluar las oportunidades de asociación:** los gobiernos deben evaluar posibles asociaciones con proveedores de colocación híbrida establecidos que tengan un historial comprobado de gestión de entornos sofisticados de centros de datos. Este enfoque aprovecha la experiencia del proveedor en bienes raíces, construcción y gestión de centros de datos, liberando recursos gubernamentales para centrarse en las funciones básicas del servicio público. Al participar en este modelo de servicios, el gobierno también está contribuyendo a fortalecer el desarrollo de la industria de los centros de datos, generando nuevos empleos, aumentando los ingresos fiscales y agregando capacidades de competitividad digital a sus propias economías.

2. **Enfoque en la escalabilidad y la flexibilidad:** los servicios de Colocación Híbrida seleccionados ofrecen escalabilidad y flexibilidad en la utilización de los recursos. Esto garantiza que los gobiernos puedan gestionar de manera eficiente y dinámica los servicios digitales en respuesta a las demandas fluctuantes sin la carga de las inversiones de infraestructura intensivas en capital.

3. **Mejorar las medidas de seguridad:** priorizar las instalaciones de Colocación Híbrida que proporcionan medidas de seguridad avanzadas que cumplen con los estándares gubernamentales. Esto incluye la seguridad física, el cifrado de datos, las defensas de ciberseguridad y el cumplimiento de la normativa nacional e internacional de protección de datos.

4. **Incorporar Prácticas de Sostenibilidad:** elegir proveedores de Colocación Híbrida que demuestren un compromiso con la sostenibilidad. Esto incluye el uso de fuentes de energía renovables, tecnologías de refrigeración energéticamente eficientes y diseños que minimicen el impacto ambiental de las operaciones del centro de datos.

5. **Fortalecer el Cumplimiento de la Soberanía de Datos:** asegurar que los acuerdos de Colocación Híbrida cumplan con las leyes de soberanía de datos para mantener el control sobre la ubicación y gestión de los datos. Esto es fundamental para abordar los requisitos legales y reglamentarios relacionados con la privacidad y la seguridad de los datos.

6. **Desarrollar Estrategias de Salida y Transición:** establecer términos contractuales claros con respecto a la transición de servicios y datos, tanto al inicio como a la posible terminación de los acuerdos de Colocación Híbrida. Esto incluye comprender los pasos logísticos y técnicos involucrados en trasladar los servicios de vuelta a la empresa o a otro proveedor si es necesario.

7. **Monitoreo continuo del desempeño y el cumplimiento:** implementar mecanismos de monitoreo para evaluar regularmente el desempeño de los proveedores de Colocación Híbrida y su cumplimiento con los estándares y SLA acordados. Esto ayudará a garantizar que los servicios de Colocación Híbrida permanezcan alineados con los objetivos del gobierno y las expectativas de prestación de servicios.

8. **Desarrollo de capacidades y transferencia de conocimientos:** invertir en programas de capacitación y desarrollo de capacidades para el personal de gestión de infraestructura digital del gobierno para garantizar que puedan administrar y supervisar de manera efectiva los servicios de Colocación Híbrida. Esto incluye comprender los aspectos técnicos de la colocación híbrida, así como las habilidades de gestión de proveedores.

9. **Apalancamiento Económico de Escala:** aplicar las economías de escala ofrecidas por los proveedores de Colocación Híbrida para reducir costos y mejorar la eficiencia del servicio, capitalizando los recursos compartidos y la infraestructura sin comprometer la calidad o seguridad del servicio.

10. **Invertir en talento digital:** abordar la brecha de habilidades digitales invirtiendo en programas de desarrollo de talento. Enfoque en la creación de capacidades en Colocación Híbrida, nube de hiperescala, infraestructura digital y gestión de servicios, ciberseguridad y tecnologías emergentes.

11. **Innovar con tecnologías cognitivas:** explorar el uso de la inteligencia artificial y el análisis de big data para transformar las operaciones gubernamentales en un sistema de gobierno cognitivo. Este enfoque puede mejorar la toma de decisiones, mejorar la prestación de servicios públicos y aumentar la transparencia y la rendición de cuentas.

12. **Realizar evaluaciones de la cadena de suministro:** realizar evaluaciones de seguridad exhaustivas de los proveedores de hardware, software y servicios involucrados en las operaciones del centro de datos. Esto debe incluir la evaluación de las relaciones entre las entidades en un entorno de colocación para identificar posibles vulnerabilidades.

13. **Desarrollar un marco claro para la clasificación de datos:** establecer un marco de clasificación de datos es crucial porque dicta cómo se manejan los datos en diferentes plataformas, ya sea que se almacenen en las instalaciones en un centro de datos de colocación o en la nube de hiperescala. Una clasificación adecuada garantiza que los datos confidenciales estén protegidos adecuadamente sin importar dónde residan, y ayuda a los gobiernos a cumplir con diversas regulaciones de protección de datos.

La implementación de estas recomendaciones requiere una planificación cuidadosa, inversiones, adquisiciones ecológicas y consideraciones políticas. Sin embargo, los beneficios de la transición a una plataforma de Colocación Híbrida (mejor prestación de servicios, mayor seguridad, mayor adaptabilidad, eficiencia y apoyo a la innovación) la convierten en una estrategia atractiva para los gobiernos latinoamericanos a medida que entran en el viaje de construir infraestructuras y servicios digitales resilientes al tiempo que cumplen con las regulaciones nacionales e internacionales.

Anexo A - Soberanía

Para mayor claridad y para cumplir con los propósitos de este informe, se utilizarán las siguientes definiciones:

- **Soberanía digital:** este es el término más amplio entre los siguientes tres conceptos, que abarca el control general que una nación o región ejerce sobre su entorno e infraestructura digital. La soberanía digital abarca las políticas, regulaciones y acciones que definen y defienden la capacidad de un estado para controlar su economía y ecosistema digital.[51]
- **Soberanía de datos:** la soberanía de datos se refiere específicamente al aspecto legal de los datos cuando los datos están sujetos a las leyes del país en el que se almacenan. Este concepto se centra en la idea de que la información digital está sujeta a las leyes y estructuras de gobernanza dentro del territorio nacional donde se recopilan o procesan los datos. Esto significa que los datos deben manejarse de acuerdo con las leyes locales, lo que puede afectar todo, desde las políticas de privacidad hasta la forma en que se manejan los datos en situaciones legales.[52]
- **Residencia de datos:** la residencia de datos se refiere a los requisitos para que los datos se almacenen en una jurisdicción específica. A menudo, impulsadas por requisitos legales, normativos o reglamentarios, las estipulaciones de residencia de datos dictan que los datos deben permanecer dentro de un país o un área geográfica específica. Las empresas deben asegurarse de que los sistemas de almacenamiento y procesamiento de datos cumplan con las regulaciones locales que dictan la residencia de los datos.
- **Localización de datos:** este es un subconjunto de la residencia de datos en el que no solo se requiere que los datos se almacenen dentro de ciertas fronteras, sino también restricciones a la transferencia de datos a otros países. Las leyes de localización de datos a menudo se implementan para proteger la información personal de la vigilancia extranjera, mejorar la seguridad de los datos de los ciudadanos o estimular el crecimiento económico local al exigir que los datos se almacenen y procesen a nivel nacional.

[51] Foro Económico Mundial – Geoeconomía y Política - https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/
[52] Forbes (2023) – El futuro de la seguridad de los datos - https://www.forbes.com/sites/forbestechcouncil/2023/07/19/the-future-of-data-security-data-residency-sovereignty-and-localization-are-all-here-to-stay/?sh=d7953a9a1a5d

Anexo B – Beneficios y desafíos de los centros de datos y las alternativas en la nube

Comparación de beneficios y desafíos a considerar entre los centros de datos locales y las diferentes opciones de nube.[53]

	BENEFICIOS	DESAFÍOS
CENTRO DE DATOS GUBERNAMENTAL	• Fuerte control de datos que cumple con los requisitos de localización de datos	• Costo de mantenimiento y actualización de los sistemas • Rendimiento y capacidad limitados para integrar rápidamente aplicaciones de vanguardia e innovación. • Ciberseguridad limitada y sistemas más caros de proteger • La dificultad de construir centros de datos ecológicos a pequeña escala • Se necesita un alto grado de experiencia técnica interna, incluidos los costos regulares de capacitación
NUBE PRIVADA		
Local	• Algunos ahorros de costos si se comparten en todo el gobierno. • Control de datos sólido que cumple con los requisitos de localización de datos	• Costo de mantenimiento y actualización de los sistemas • Ciberseguridad limitada y sistemas más caros de proteger • Dificultad para construir centros de datos ecológicos a pequeña escala • Se necesita un alto grado de experiencia técnica interna, incluidos los costos regulares de capacitación

[53] BANCO MUNDIAL (2022) - Ecosistema de migración gubernamental a la nube - https://www.worldbank.org/en/events/2022/06/12/government-migration-to-cloud-ecosystems-wbg

No local (hospedado por un proveedor de servicios en la nube)	• Mayor rentabilidad • Posibles beneficios de ciberseguridad y rendimiento y rentabilidad si los proporciona el proveedor de servicios en la nube • Cumplimiento de los requisitos de localización de datos	• Costo de mantenimiento y actualización de los sistemas • La sostenibilidad depende del proveedor de servicios en la nube. • Se requiere un alto grado de experiencia técnica
NUBE PÚBLICA		
Proveedor de nube pública nacional/ regional	• Rendimiento y escalabilidad mejorados • Mayor rentabilidad • Funciones de ciberseguridad mejoradas • Cumplimiento de los requisitos de localización de datos	• A menudo compromisos poco claros o menores con la sostenibilidad • Menos control sobre los datos • Las adquisiciones requerirán una gran atención a los acuerdos de nivel de servicio • Proveedor de lock-in
Proveedor de nube de hiperescala	• Máximo nivel de rendimiento y escalabilidad • Máximo nivel de rentabilidad • Máximo nivel de ciberseguridad • Capacidad de innovar rápidamente gracias al acceso a las herramientas más avanzadas, que se pueden actualizar con mayor regularidad • Fuerte compromiso con la sostenibilidad a través de centros de datos ecológicos, el uso de energía renovable y una gestión de datos más eficiente	• Las adquisiciones requerirán una gran atención a los acuerdos de nivel de servicio • Posibles problemas de bloqueo de proveedores (aunque se pueden mitigar a través de soluciones de múltiples nubes y una estrategia de salida clara) • Los problemas de localización y gobernanza de datos pueden limitar esta opción

Anexo C – Clasificación de datos

La clasificación de datos es un paso fundamental en la gestión de riesgos de ciberseguridad y un instrumento clave para respaldar la política de privacidad de datos y el cumplimiento de las regulaciones. Implica identificar los tipos de datos que se procesan y almacenan en un sistema de información propiedad u operado por una organización. También implica decidir sobre la sensibilidad de los datos y el posible impacto en caso de que los datos sean comprometidos, se pierdan o se utilicen de manera incorrecta.[54]

Para garantizar una gestión de riesgos efectiva, las organizaciones deben considerar clasificar los datos trabajando hacia atrás desde el uso contextual de los datos y creando un esquema de categorización que considere si un caso de uso dado tiene un impacto significativo en las operaciones de una organización (por ejemplo, si los datos son confidenciales, deben tener integridad y/o estar disponibles).

Aspectos clave de la clasificación de datos

- **Identificación:** determinar qué datos deben clasificarse, como correos electrónicos, documentos y bases de datos.
- **Categorización:** agrupar los datos en función de su tipo y sensibilidad. Las categorías comunes incluyen público, interno, confidencial/secreto y altamente confidencial/alto secreto.
- **Etiquetado:** asignar etiquetas a los datos para su rápida identificación. Las etiquetas ayudan a los usuarios y sistemas a reconocer el nivel de clasificación de los datos al instante.
- **Medidas de protección:** implementación de medidas de seguridad basadas en el nivel de clasificación. Por ejemplo, los datos altamente confidenciales pueden requerir cifrado y acceso restringido, mientras que los datos públicos pueden necesitar una protección mínima.

[54] Descripción general de la clasificación de datos de AWS - Descripción general de la clasificación de datos - Clasificación de datos (amazon.com)

Un caso de referencia útil de clasificación de datos es el marco desarrollado por el Reino Unido:

La estrategia de clasificación de datos del gobierno del Reino Unido está diseñada para proteger los activos de información clasificándolos en niveles apropiados de seguridad. Esta estrategia se describe en la Política de Clasificaciones de Seguridad del Gobierno (GSCP).

El GSCP emplea tres niveles de clasificación:

1. **OFICIAL:** este nivel cubre la mayoría de la información que debe gestionarse con cuidado debido a su sensibilidad o valor. Incluye operaciones, servicios y comunicaciones gubernamentales de rutina.

2. **SECRETO:** este nivel se utiliza para información que, de divulgarse, podría causar daños graves a la seguridad nacional, la defensa u otros intereses vitales del Reino Unido.

3. **ALTO SECRETO:** este nivel se aplica a la información que, si se ve comprometida, podría causar un daño excepcionalmente grave a la nación.

La política proporciona un enfoque estructurado para garantizar que los datos estén protegidos adecuadamente contra las amenazas prevalentes. También incluye orientación para trabajar de forma remota y consideraciones para los asesores de seguridad.

Además, la Estrategia Nacional de Datos (NDS) tiene como objetivo impulsar al Reino Unido a construir una economía de datos líder en el mundo al tiempo que garantiza la confianza pública en el uso de los datos. Se centra en desbloquear el valor de los datos en toda la economía y crear una comprensión compartida de cómo se utilizan los datos.[55]

[55] Política de clasificaciones de seguridad del gobierno del Reino Unido (GSCP) - Clasificaciones de seguridad del gobierno - GOV.UK (www.gov.uk)


DIGI
AMERICAS