

La transición hacia modelos de soberanía en gobiernos de todo el mundo

Una nueva forma de adaptarse y sobrevivir para los organismos del sector público

En los organismos del sector público fuera de Estados Unidos, la soberanía digital dejó de ser una lista de verificación normativa más para transformarse en una estrategia clave de supervivencia. Los gobiernos han comprendido que no basta con cumplir las normativas o garantizar la soberanía dentro de una jurisdicción. Hoy el foco está en la autonomía estratégica: la capacidad de operar, realizar innovaciones y asegurar la continuidad de servicios esenciales de manera independiente, incluso frente a la retirada de soporte externo o las interrupciones en las cadenas de suministro globales.

Según un informe reciente de la Organización de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), "el 79 % de los países con legislación en materia de privacidad y protección de datos manifiestan preocupación por la soberanía digital"¹. Los gobiernos ya no pueden permitirse pasar por alto las dependencias de los sistemas cerrados y propietarios. El avance hacia la autonomía estratégica está marcado por tres factores clave:

- ▶ **Riesgo geopolítico:** Bajo condiciones normales, apoyarse en hyperscalers globales funciona. Sin embargo, en contextos de conflicto, esa dependencia pasa a ser un punto vulnerable grave. Las interrupciones de conectividad o los daños en la infraestructura pueden dejar fuera de juego a las operaciones basadas en la nube. Por eso, los países deben estar preparados para operar de manera autónoma cuando la cooperación internacional falla o resulta poco confiable. Para lograrlo, se necesitan sistemas preparados para entornos DDIL (denegados, interrumpidos, intermitentes y limitados), capaces de garantizar la continuidad de las funciones críticas, desde el comando y control en defensa hasta los servicios de emergencia para los ciudadanos, aun cuando el país pierda conectividad con el Internet global.
- ▶ **Capacidad de recuperación cibernética:** Los ciberataques impulsados por estados son cada vez más sofisticados, frecuentes y determinantes. La soberanía es clave para que las infraestructuras fundamentales (como las redes eléctricas, los sistemas de salud y las plataformas de defensa) puedan resistir interferencias externas y ataques a la cadena de suministro. El riesgo no es solo el robo de datos, sino también la introducción de código malicioso en actualizaciones de software en tránsito. En este contexto, los gobiernos necesitan garantías de soberanía: la capacidad de comprobar de forma independiente la integridad de su cadena de suministro de software, evitar el espionaje externo y asegurar que sus sistemas permanezcan íntegros.
- ▶ **Competitividad económica:** Cada vez más, los gobiernos consideran que la soberanía digital es un pilar de la seguridad nacional. Al localizar el desarrollo de la inteligencia artificial y el control de los datos, los motores del crecimiento económico futuro permanecen bajo jurisdicción nacional, en lugar de depender de un control externo. Crece la preocupación de que apoyarse en modelos de inteligencia artificial externos tipo "caja negra" derive en pérdida de propiedad intelectual y relevancia cultural. La autonomía estratégica permite que los países desarrollen estas capacidades digitales, impulsen ecosistemas locales de innovación y garanticen que el valor económico generado por la transformación digital se mantenga dentro de la economía nacional.

1 ["Data protection and privacy legislation worldwide"](#). UNCTAD, 17 de febrero de 2026.

Demanda global, realidades regionales

Si bien la necesidad de control es un fenómeno global, las influencias y los obstáculos que afectan al sector público cambian según la región.

Europa, Oriente Medio y África (EMEA), y Canadá

En la región EMEA, el principal desafío surge de la tensión entre la necesidad de contar con tecnología avanzada y la dependencia de proveedores ajenos a la Unión Europea (UE), lo cual expone a los gobiernos a riesgos jurisdiccionales, en particular a leyes extraterritoriales como las promulgadas por Estados Unidos, incluidas la ley Clarifying Lawful Overseas Use of Data ([CLOUD](#)) o la Foreign Intelligence Surveillance Act de 1978 ([FISA](#)).

Los organismos europeos deben hacer frente a un complejo entramado de normativas estrictas, entre las que se incluyen la Directiva [NIS2](#) de la Unión Europea en materia de ciberseguridad y la Ley de Resiliencia Operativa Digital (DORA) en materia de capacidad de recuperación operativa, además de [normativas nacionales](#) como la francesa SecNumCloud. La infraestructura de defensa sigue estando fragmentada, ya que las fallas de interoperabilidad de la Organización del Tratado del Atlántico Norte (OTAN) retrasan el intercambio de datos. Además, los países enfrentan una grave escasez de personal con habilitación en materia de seguridad para operar los entornos soberanos. Aunque Canadá se ubica en Norteamérica, enfrenta desafíos similares a los de EMEA debido a su infraestructura obsoleta. El Departamento de Defensa Nacional de Canadá se encuentra con un mosaico fragmentado de la infraestructura de red secreta consolidada (CSNI) y trabas burocráticas que ralentizan la adopción de las funciones modernas. Frente a estos riesgos, los organismos gubernamentales protegen los datos confidenciales de las interferencias legales extranjeras y cierran la brecha de software mediante el desarrollo de capacidades internas.

Asia-Pacífico (APAC)

En APAC, las políticas están marcadas por fuertes medidas proteccionistas y un cumplimiento normativo exigente, orientados a lograr la independencia tecnológica.

- ▶ **Ubicación de los datos:** Algunos países, como China, India e Indonesia, imponen fuertes restricciones de localización de datos. Esto obliga a que la información más importante se almacene íntegramente dentro del territorio nacional, lo cual restringe el uso de nubes públicas internacionales.
- ▶ **Responsabilidad estricta:** Singapur aplica rigurosos estándares de seguridad integral, según los cuales los funcionarios públicos pueden enfrentar sanciones penales por el uso indebido o la pérdida de datos, lo que fomenta una cultura de adquisiciones muy conservadora.
- ▶ **Requisitos globales y locales:** Se priorizan los modelos globales y locales (glocal), en los que la tecnología global se distribuye a través de partners locales para garantizar el control soberano sobre los sistemas.

Un objetivo clave de los países de APAC es desarrollar capacidades propias para reducir la dependencia a largo plazo de potencias extranjeras, ya que consideran la soberanía digital como un escudo frente a la vulnerabilidad geopolítica.

América Latina (LATAM)

En LATAM, la modernización se orienta a mantener la continuidad operativa y suele verse limitada por problemas estructurales más que por decisiones políticas.

- ▶ **Inestabilidad y falta de continuidad:** Los cambios frecuentes en el liderazgo político y la volatilidad económica ponen en riesgo la planificación de TI a largo plazo y los contratos de adquisición plurianuales en un contexto geopolítico incierto.

- ▶ **Enfoque en la seguridad interna:** Los organismos de defensa en LATAM priorizan la seguridad interna (protección de fronteras, lucha contra el narcotráfico) y optan por herramientas de vigilancia ágiles en lugar de invertir en infraestructura estratégica pesada².
- ▶ **Riesgos en las adquisiciones:** La ineficiencia y los riesgos de corrupción en las adquisiciones públicas reducen el valor real de los presupuestos tecnológicos, lo que genera la necesidad de adoptar sistemas abiertos, flexibles y rentables que puedan resistir recortes presupuestarios y cambios políticos sin atar al país a proveedores propietarios costosos y rígidos.

El enfoque de Red Hat frente a la soberanía digital

Para prosperar, los organismos del sector público de todo el mundo deben abordar la soberanía en todos estos aspectos. Red Hat ofrece las herramientas y el ecosistema necesarios para comprender y gestionar cada uno de ellos.

Soberanía de los datos e inteligencia artificial

Red Hat conoce la importancia de lograr control y autonomía completos sobre los datos fundamentales y los modelos de inteligencia artificial, lo que garantiza que los datos permanezcan dentro del país y que el control cumpla con las leyes locales. Los organismos deben implementar estrategias de inteligencia artificial soberana que preserven la propiedad de sus modelos y datos de entrenamiento, los cuales se ejecutan en infraestructura local en lugar de depender del acceso de la interfaz de programación de aplicaciones (API) a los modelos controlados por terceros. Red Hat® OpenShift® AI permite implementar funciones de inteligencia artificial soberana allí donde residen los datos. Facilitamos el control sobre la ubicación de los datos y el acceso a ellos mediante informática confidencial para proteger la información en uso y asegurar el cumplimiento de regulaciones como la Ley de Inteligencia Artificial de la Unión Europea (EU AI Act).

Soberanía tecnológica

Contar con la posibilidad de ejecutar cargas de trabajo sin depender de la infraestructura o el software propietario de un proveedor determinado es fundamental para mantener la autonomía a largo plazo y permitir la movilidad de aplicaciones sin limitaciones. Se recomienda que los gobiernos adopten estándares abiertos y plataformas de contenedores portátiles para evitar la dependencia de un solo proveedor. En caso de cambios en las políticas de un proveedor de nube o de incrementos en las tensiones geopolíticas, las cargas de trabajo pueden trasladarse a otra infraestructura sin necesidad de rediseñarlas. Red Hat reduce la dependencia de un solo proveedor a través de estándares open source. Nuestra plataforma es compatible con diversas arquitecturas de hardware (x86, Advanced RISC Machine [ARM], RISC-V), lo que permite que los sistemas nacionales se actualicen y evolucionen de manera autónoma, sin depender de terceros.

Soberanía operativa

Para sobrevivir y operar aun sin conexión, los organismos del sector público deben conservar control total y autonomía sobre sus operaciones de TI más importantes. La defensa y la infraestructura esencial deben enfocarse en la capacidad de recuperación operativa. Esto incluye automatizar los planes de recuperación ante desastres que tienen en cuenta escenarios de guerra y garantizar que las operaciones y el soporte estén a cargo de ciudadanos locales con habilitación de seguridad. Por ejemplo, Red Hat ofrece soporte soberano confirmado, es decir, soporte técnico que brindan ciudadanos locales verificados (p. ej., dentro de la Unión Europea), lo cual garantiza que ningún dato al que acceda el equipo de soporte salga de la jurisdicción. Además, Red Hat Ansible® Automation Platform automatiza la capacidad de recuperación, lo cual agiliza la recuperación y la aplicación de parches, incluso en entornos sin conexión (DDIL).

Soberanía de seguridad

La verificación independiente de la integridad, la seguridad y la confiabilidad de los sistemas y los procesos digitales permite que los organismos garanticen el cumplimiento normativo. Las instituciones deben transitar de la confianza implícita a la confianza demostrable, lo que implica

2 ["New Pentagon strategy to focus on homeland, Western Hemisphere"](#). DefenseNews, 25 de septiembre de 2025.

auditar exhaustivamente la cadena de suministro de software y poder evidenciar el cumplimiento de estándares, como Common Criteria, los Estándares Federales de Procesamiento de la Información (FIPS) y NIS2. Red Hat ofrece una cadena de suministro de software confiable que ofrece software firmado criptográficamente con procedencia verificada y una lista de materiales de software (SBOM), lo cual permite que los organismos auditen cada elemento y se aseguren de que no se introdujo código malicioso. Estas medidas de seguridad contribuyen a que los organismos cumplan con las regulaciones recientes como la Ley de Ciberresiliencia de la Unión Europea.

Autonomía estratégica a través del open source

Red Hat se apoya en una base abierta y flexible para abordar los desafíos del sector público, lo cual brinda a los organismos mayor control y opciones frente al aislamiento tecnológico. Este enfoque entiende que ningún proveedor por sí solo puede garantizar la soberanía digital. Con Red Hat, es posible diseñar una nube soberana distribuida entre diversos proveedores de infraestructura y entornos de nube, lo cual evita las limitaciones de una sola solución.

Durante más de 30 años, Red Hat ha brindado soluciones open source empresariales y confiables a instituciones con los requisitos más estrictos de seguridad y cumplimiento. El open source empresarial no es solo una tecnología, sino una base de arquitectura esencial para que los organismos del sector público alcancen verdadera soberanía digital y autonomía estratégica. A diferencia de los proveedores propietarios, que dependen de sistemas cerrados y opacos y exigen confianza implícita, Red Hat ayuda a los organismos a mantener el control total sobre su futuro digital. Este enfoque abierto permite que el sector público internacional controle el ritmo de la innovación mundial, desde el extremo táctico de la red hasta la inteligencia artificial soberana, mientras garantiza que las cargas de trabajo sigan siendo portátiles y resistentes. La adopción de un enfoque open source salvaguarda las operaciones esenciales frente a los riesgos de dependencia de un solo proveedor y la obsolescencia tecnológica. Con esta tecnología, Red Hat sigue la doctrina de apertura que prevalece en regiones como la Unión Europea. Este modelo previene la dependencia de un solo proveedor y posibilita la revisión y modificación del código, lo cual es clave para la seguridad y la confianza nacional.

▶ **Confianza y transparencia**

El modelo open source de Red Hat brinda una transparencia total, lo cual permite que los organismos del sector público inspeccionen el código fuente, comprueben la seguridad y auditen las cadenas de suministro de software. Esta capacidad de auditoría es fundamental para cumplir con los requisitos de garantía en EMEA y APAC. Asimismo, Red Hat entrega software firmado criptográficamente con procedencia verificada para cumplir con las regulaciones recientes como la [Ley de Resistencia Cibernética de la Unión Europea](#).

▶ **Soberanía operativa y soporte local**

Con el fin de hacer frente a los riesgos relacionados con la jurisdicción, Red Hat permite controlar la gestión de la infraestructura y así garantizar la soberanía operativa.

- ▶ **Soporte conforme a los requisitos de soberanía:** Como se indicó anteriormente, Red Hat ofrece soporte soberano confirmado en la Unión Europea, lo que garantiza que solo ciudadanos verificados y ubicados dentro de la UE presten este servicio. Ello asegura que los datos a los que tiene acceso el personal de soporte permanezcan dentro de la región.
- ▶ **Ecosistemas locales:** Se dispone de un ecosistema de partners de Red Hat junto con proveedores de nube locales certificados para ofrecer funciones de nube soberana que respeten las estrictas normativas nacionales de residencia de datos.

▶ **Independencia tecnológica**

Una estrategia de nube híbrida abierta permite que las cargas de trabajo se ejecuten en diversos entornos, como en las instalaciones, en una nube privada, en el extremo táctico de la red o en un entorno aislado.

- ▶ **Portabilidad:** Constituye la base para evitar la dependencia de un solo proveedor, un tema crucial para los organismos del sector público, sobre todo en LATAM y APAC. La capacidad de estas regiones para migrar las cargas de trabajo y los datos de manera eficiente es esencial para mantener la continuidad del servicio y responder de forma efectiva a cambios geopolíticos, como transformaciones políticas o económicas que obliguen a cambiar de proveedor tecnológico.
- ▶ **Operaciones en entornos sin conexión:** En el caso de los organismos del sector de defensa, las soluciones de Red Hat, como Red Hat Device Edge y Red Hat OpenShift, habilitan a los sistemas para operar de forma independiente en entornos DDIL sin conexión, lo que garantiza la continuidad de la misión incluso si la nube central no está disponible.

Red Hat brinda a los organismos del sector público la base abierta necesaria para diseñar una nube soberana capaz de soportar la incertidumbre, garantizar la protección segura de los datos y asegurar la continuidad operativa de la nación.

▶ Inteligencia artificial soberana

Mientras los gobiernos investigan y amplían el uso de la inteligencia artificial, Red Hat proporciona la plataforma adecuada para desarrollar una inteligencia artificial soberana. De este modo, los países pueden conservar la propiedad de sus modelos y datos de entrenamiento, e implementarlos en infraestructuras locales para cumplir con normativas como la Ley de Inteligencia Artificial de la Unión Europea, sin tener que depender del acceso mediante API a modelos controlados desde otros países.

Red Hat: la opción ideal para el sector público

Red Hat se ha consolidado como un aliado confiable del sector público, presente en todos los departamentos ejecutivos de Estados Unidos³ y ampliamente adoptado por la OTAN y los ministerios de defensa de todo el mundo. Gracias a su modelo de licencias y su apuesta por estándares abiertos, los organismos nunca quedan atados a un proveedor de manera indefinida. Las instituciones conservan el derecho a utilizar y mantener el software por un tiempo indeterminado, lo cual garantiza que sus inversiones a largo plazo estén protegidas frente a cambios en los planes de los proveedores o restricciones geopolíticas.

Con el aumento de los gastos, particularmente en el sector de la defensa, la inversión en la cartera de soluciones y servicios de Red Hat puede mostrar un retorno tangible. Se espera que los compromisos de inversión de los países miembros de la [OTAN](#) se dupliquen y lleguen al 5 % del PIB nacional para 2035⁴. Al adoptar una plataforma unificada, los organismos pueden destinar recursos de la operación de sistemas convencionales fragmentados hacia la creación de nuevas funciones para la misión, lo cual disminuye de manera significativa los costos operativos y el costo total de propiedad.

Próximos pasos para comenzar

- ▶ Obtén más información sobre la labor de [Red Hat en el sector público internacional](#) y comunícate con uno de nuestros representantes.
- ▶ Si deseas evaluar tu nivel de preparación en materia de soberanía digital, [lee esta publicación del blog](#) para dar los primeros pasos.



Acerca de Red Hat

Red Hat es el proveedor líder mundial de soluciones de software open source para empresas, que ha adoptado un enfoque impulsado por la comunidad para ofrecer tecnologías confiables y de alto rendimiento de Linux, nube híbrida, contenedores y Kubernetes. Ayuda a que los clientes desarrollen aplicaciones en la nube, integren las aplicaciones de TI nuevas y actuales, y automatizen y gestionen los entornos complejos. Es [una asesora de confianza de las empresas de la lista Fortune 500](#) y brinda servicios [galardonados](#) de soporte, capacitación y consultoría para que obtengan los beneficios de la innovación abierta en todos los sectores. Red Hat es un centro de conexión en una red internacional de empresas, partners y comunidades, a quienes ayuda a crecer, transformarse y prepararse para el futuro digital.

f facebook.com/redhatinc
X @RedHatLA
@RedHatLberia
in linkedin.com/company/red-hat

es.redhat.com
#3613114_0326

3 Datos de clientes de Red Hat, septiembre de 2025.

4 "[Defence expenditures and NATO's 5% commitment](#)". OTAN, 18 de diciembre de 2025.

ARGENTINA
+54 11 4329 7300

CHILE
+562 2597 7000

COLOMBIA
+571 508 8631
+52 55 8851 6400

MÉXICO
+52 55 8851 6400

ESPAÑA
+34 914 148 800