

Ley que establece el marco de nube del Estado, la consolidación de centros de datos públicos y la soberanía y portabilidad de los datos públicos

Eleva a rango legal la nube preferente del Estado con clasificación previa de la información; exige alojamiento en territorio nacional solo para la información crítica y la secreta o reservada, y cifrado con claves bajo control del Estado para la confidencial; fija cláusulas obligatorias de portabilidad, salida y seguridad en los contratos, y ordena la consolidación de los centros de datos públicos con redundancia.

Comisión (Cámara de Diputados): Ciencia, Innovación Tecnológica y Sociedad Digital (+ Modernización de la Gestión del Estado y Contraloría) · **Revisora (Senado):** En asuntos de Salud, Educación, Cultura, Mujer y Desarrollo Social y Digital · **Prioridad:** media · **Costo fiscal:** bajo · **Plazo:** mediano

Plan Perú 2050: Transformación Digital, Perú en La Era Digital, Reforma Del Estado

I. Exposición de motivos

El Reglamento de la Ley de Gobierno Digital (DS 029-2021-PCM) establece que las entidades usan de forma preferente infraestructuras o plataformas provistas por proveedores de servicios en la nube y crea la infraestructura y plataforma como servicio Nube Perú. Sin embargo, este marco reglamentario no resuelve con rango de ley cuestiones que hoy condicionan la adopción segura y eficiente de la nube: no existe una obligación general de clasificar la información pública según su criticidad antes de decidir dónde alojarla; los contratos tecnológicos no siempre aseguran la portabilidad de los datos, el acceso a ellos ante el término del contrato o la insolvencia del proveedor, ni la jurisdicción aplicable; y numerosas entidades mantienen centros de datos propios subutilizados, con costos de energía, personal y renovación tecnológica que se duplican en todo el Estado. Tampoco hay criterios legales sobre la localización de la información crítica, ni se reconoce que la localización física no basta: un proveedor sujeto a una jurisdicción extranjera puede ser obligado a entregar datos que controla aunque estén alojados en el Perú, por lo que la confidencialidad depende del control de las claves criptográficas por el Estado. Los contratos tampoco exigen de forma uniforme certificaciones de seguridad, notificación de incidentes ni borrado verificable, y la consolidación sin redundancia puede crear puntos únicos de falla. El Reino Unido (política Cloud First), Estonia (embajada de datos para respaldo soberano) y Chile (Ley 21.180) ofrecen referencias de cómo combinar adopción de nube, continuidad y control público sobre los datos.

II. Fórmula legal

EL CONGRESO DE LA REPÚBLICA ha dado la Ley siguiente:

LEY QUE ESTABLECE EL MARCO DE NUBE DEL ESTADO, LA CONSOLIDACIÓN DE CENTROS DE DATOS PÚBLICOS Y LA SOBERANÍA Y PORTABILIDAD DE LOS DATOS PÚBLICOS

Artículo 1. Objeto y articulación

1.1. La presente ley tiene por objeto establecer el marco para el uso de servicios de computación en la nube por las entidades públicas, la consolidación de sus centros de datos públicos y la garantía de control, portabilidad, seguridad y continuidad de los datos públicos.

1.2. La presente ley se aplica sin perjuicio de las normas de seguridad digital, ciberseguridad y protección de datos personales, incluidas las del Reglamento de la Ley 31814, que prevalecen en sus respectivas materias. La información de los sistemas de defensa, inteligencia y orden interno se rige por su normativa especial y por la Ley 30999, Ley de Ciberdefensa.

1.3. Las leyes especiales que regulen el alojamiento de datos públicos se aplican conforme a la clasificación y a las reglas de localización de la presente ley.

Artículo 2. Definiciones y ámbito

2.1. Para efectos de la presente ley se entiende por: a) servicio de computación en la nube: modelo de provisión de recursos informáticos configurables, accesibles por red y bajo demanda; b) centro de datos público: instalación de una entidad pública destinada a alojar equipos de procesamiento y almacenamiento de

información; c) Nube Perú: infraestructura y servicios compartidos de computación administrados por la Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno y Transformación Digital.

2.2. Los artículos 3 a 6 son aplicables a las entidades del Poder Ejecutivo y a los gobiernos regionales y locales. Los organismos constitucionalmente autónomos, el Poder Judicial y el Congreso de la República los aplican en el marco de su autonomía y pueden adherirse a los acuerdos marco del artículo 8.

Artículo 3. Nube preferente con clasificación previa

3.1. Las entidades utilizan preferentemente servicios de computación en la nube para nuevos sistemas y renovaciones tecnológicas.

3.2. Antes de contratar o migrar, la entidad clasifica la información a alojar conforme a las categorías de excepción de los artículos 15, 16 y 17 del Texto Único Ordenado de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública, y, adicionalmente, según su criticidad para la continuidad operativa, conforme a los criterios que aprueba la Secretaría de Gobierno y Transformación Digital en el marco del sistema de gestión de seguridad de la información.

Artículo 4. Localización por clasificación y control de claves

4.1. Es información crítica para la continuidad del Estado aquella cuya indisponibilidad, alteración o divulgación afecta la seguridad nacional, el funcionamiento de los sistemas administrativos del Estado, los registros de identidad y de propiedad, o la prestación de servicios esenciales. El reglamento desarrolla estos criterios.

4.2. Solo la información crítica y la clasificada como secreta o reservada se aloja en infraestructura ubicada en territorio nacional. La demás información puede alojarse fuera del país conforme a las reglas de flujo transfronterizo de la Ley 29733, Ley de Protección de Datos Personales, cuando contenga datos personales.

4.3. La información confidencial y la crítica alojadas en servicios de terceros se cifran en reposo y en tránsito con claves generadas y custodiadas por la entidad o por Nube Perú en módulos criptográficos bajo control del Estado, sin acceso del proveedor a la información en claro.

4.4. El presente artículo se aplica exclusivamente a la información de titularidad de las entidades públicas o tratada por cuenta de ellas.

Artículo 5. Cláusulas obligatorias

Los contratos de servicios de nube y de alojamiento incluyen obligatoriamente:

- a) La titularidad exclusiva de la entidad sobre sus datos.
- b) La entrega íntegra de los datos y metadatos en formatos abiertos o estándar al término del contrato o a solicitud de la entidad.
- c) Un plan de salida y transición.
- d) La prohibición de usar los datos para fines distintos de la prestación del servicio.
- e) La aplicación de la legislación peruana y la solución de controversias conforme a la Ley 32069, Ley General de Contrataciones Públicas.
- f) La obligación del proveedor de notificar a la entidad, en la medida permitida por la ley aplicable, cualquier requerimiento de autoridad extranjera de acceso a los datos.
- g) Certificaciones vigentes de seguridad de la información y de servicios en la nube reconocidas internacionalmente.
- h) La notificación a la entidad de incidentes que afecten sus datos dentro de las veinticuatro horas de detectados.
- i) El acceso de la entidad a los registros de actividad de sus recursos y el derecho de auditoría o de presentación de informes de auditoría independientes.
- j) La eliminación verificable de los datos al término del contrato, previa entrega.

Artículo 6. Consolidación de centros de datos públicos

6.1. La Secretaría de Gobierno y Transformación Digital elabora el inventario de centros de datos públicos de las entidades del Poder Ejecutivo, con indicadores de uso, costo y eficiencia energética, y publica un resumen agregado; el detalle de ubicación y características técnicas se mantiene reservado.

6.2. Las entidades del Poder Ejecutivo no construyen ni amplían centros de datos propios sin informe técnico favorable de la Secretaría de Gobierno y Transformación Digital que acredite que la nube o la infraestructura compartida del Estado no satisfacen su necesidad.

Artículo 7. Continuidad operativa y redundancia

7.1. Las entidades que alojan servicios digitales críticos mantienen planes de continuidad y recuperación ante desastres, con pruebas periódicas, y los comunican a la Secretaría de Gobierno y Transformación Digital.

7.2. Los servicios digitales críticos se diseñan con redundancia en al menos dos zonas o sedes independientes y con capacidad de recuperación en un proveedor o infraestructura alternativa, conforme al plan de continuidad.

Artículo 8. Infraestructura compartida y acuerdos marco

La Presidencia del Consejo de Ministros, a través de Nube Perú, puede ofrecer a las entidades servicios de infraestructura compartida, y la Central de Compras Públicas – PERÚ COMPRAS puede implementar acuerdos marco de servicios de nube conforme a la Ley 32069, para obtener economías de escala.

Artículo 9. Transparencia

La Secretaría de Gobierno y Transformación Digital publica anualmente, en formato abierto, el gasto del Poder Ejecutivo en servicios de nube y en centros de datos propios, y el avance de la consolidación.

Primera. Disposición Complementaria Final

Reglamentación. El Poder Ejecutivo, mediante decreto supremo refrendado por el presidente del Consejo de Ministros y el ministro de Economía y Finanzas, reglamenta la presente ley en un plazo de ciento veinte días hábiles contados a partir del día siguiente de su publicación, y adecúa el Decreto Supremo 029-2021-PCM y el Reglamento de la Ley 32069.

Segunda. Disposición Complementaria Final

Financiamiento. La implementación se financia con cargo al presupuesto institucional de los pliegos, sin demandar recursos adicionales al Tesoro Público. La gestión centralizada de claves en Nube Perú se programa como meta sujeta a disponibilidad presupuestal.

Única. Disposición Complementaria Transitoria

Contratos vigentes. Los contratos de nube y alojamiento vigentes se adecúan a las cláusulas del artículo 5 en su primera renovación o modificación.

III. Análisis costo-beneficio

La clasificación de información, los planes de salida y la gestión de claves criptográficas generan costos administrativos y técnicos iniciales; la gestión de claves es centralizable en Nube Perú y la redundancia multizona eleva el costo de los servicios críticos. Al limitar la localización obligatoria a la información crítica y reservada, se evita encarecer el resto de servicios. A cambio, la consolidación de centros de datos subutilizados y las compras agregadas permiten ahorros en energía, personal y renovación de equipos. Beneficios: control efectivo sobre la confidencialidad de los datos públicos, menor dependencia de un proveedor, continuidad del Estado ante fallas o controversias y transparencia del gasto tecnológico. El ahorro neto debe estimarse con el inventario que la ley ordena; no existe cifra oficial agregada. Costo fiscal estimado: bajo.

Normas que modifica

- Decreto Supremo 029-2021-PCM, Reglamento de la Ley de Gobierno Digital, nube preferente y Nube Perú — *eleva_rango*
- Ley 32069 y D.S. 009-2025-EF, cláusulas de contratos de nube y acuerdos marco — *complementa*
- Ley 29733, Ley de Protección de Datos Personales, arts. 15 y ss. (flujo transfronterizo) — *complementa*
- TUO de la Ley 27806, arts. 15-17 (clasificación) — *complementa*

Entidades implicadas (quién hace qué)

- **SGTD** (rectora): Criterios de clasificación (art. 3.2), custodia de claves (art. 4.3), inventario y autorización de centros de datos (art. 6), infraestructura compartida (art. 8) y transparencia (art. 9).
- **PERÚ COMPRAS** (ejecutora): Acuerdos marco de servicios de nube (art. 8).
- **CNSD** (consultiva): Requisitos de seguridad y continuidad (arts. 5 y 7).

- — (ejecutora): Clasifican, incluyen cláusulas, mantienen continuidad y redundancia (arts. 3, 5, 7).
- — (regulada): Cumplen las cláusulas obligatorias del art. 5.
- **MINDEF** (regulada): Sistemas de defensa e inteligencia se rigen por su normativa y la Ley 30999 (art. 1.2).

Sujetos obligados: Entidades del Poder Ejecutivo y gobiernos regionales y locales; organismos autónomos en el marco de su autonomía; proveedores de nube contratados por el Estado.

Beneficiarios: El Estado (control de datos y continuidad) y la ciudadanía cuyos datos custodia.

Impacto económico estimado (confianza baja; referencial, no oficial)

Tipo: mixto

Costo para el Estado: No cuantificable con información pública

Horizonte: 2027-2031

Financiamiento: Presupuesto institucional de los pliegos, sin demandar recursos adicionales al Tesoro; gestión centralizada de claves como meta sujeta a disponibilidad presupuestal. Requiere coordinación con el Poder Ejecutivo e informe previo de sostenibilidad fiscal del MEF antes del dictamen.

Supuestos: Gestión de claves (módulos criptográficos) centralizable en Nube Perú y redundancia de servicios críticos tienen costo moderado; no hay inventario público de centros de datos ni del gasto en nube que permita estimar costo ni ahorro neto. Sin creación de plazas.

Beneficio para el Estado: Ahorro por consolidación de centros de datos y compras agregadas, a estimar con el inventario de línea de base.

Beneficio para la sociedad: Mayor confidencialidad y continuidad de servicios públicos digitales.

Inversión privada: Posible inversión de proveedores de nube en infraestructura local para atender información crítica y reservada; no cuantificable.

Costo para privados: Proveedores asumen certificaciones, notificación de incidentes y auditoría.

Riesgos: Clasificación deficiente; capacidad limitada de gestión de claves; concentración en pocos proveedores; conflictos con compromisos comerciales si la localización se extendiera a privados (excluido por art. 4.4).

Revisión especializada (asistida por IA, sobre la versión anterior)

- **Constitucional** — Conforme: Las reglas sobre nube y consolidación de centros de datos son de organización interna del Ejecutivo y de contratación pública (art. 76); la adecuación de contratos vigentes solo en su renovación respeta el art. 62. Compatible con la Constitución.
- **Técnica legislativa** — Con observaciones: El marco de nube está bien delimitado: preferencia, clasificación, cláusulas de salida y consolidación. Además, la adecuación de contratos vigentes respeta el art. 62 de la Constitución. Las observaciones son de técnica: delega al reglamento la definición de información crítica sin criterios legales y no define las figuras institucionales que menciona.
- **Concordancia normativa** — Con observaciones: Normas citadas correctas (D.L. 1412; D.S. 029-2021-PCM, que prevé la preferencia por la nube y Nube Perú; Ley 32069). Sin duplicidad legal, pero fija una regla de localización distinta de IA-05 e IA-14, y su inventario de centros de datos públicos se superpone con el Registro Nacional de Centros de Datos de CON-10 (MTC). Debe concordarse además con el D.S. 115-2025-PCM (art. 19, nube para IA).
- **Seguridad** — Con observaciones: Buen marco de portabilidad, clasificación y continuidad. Desde seguridad faltan requisitos mínimos exigibles a los proveedores de nube (certificaciones, notificación de incidentes, registros, borrado), control estatal de las claves de cifrado para información confidencial y crítica frente a accesos de jurisdicciones extranjeras, y evitar que la consolidación cree un punto único de falla.
- **Derecho tecnológico** — Con observaciones: Sólida: eleva a ley la nube preferente y NUBE PERÚ del DS 029-2021-PCM y añade portabilidad, plan de salida y consolidación de centros de datos. Pero confunde soberanía con localización: alojar en territorio nacional no evita el acceso de autoridades extranjeras a proveedores sujetos a su jurisdicción; la medida eficaz es el cifrado con claves bajo control del Estado. Debe armonizar su clasificación con la del TUO de la Ley 27806 y explicitar que la localización solo alcanza datos del Estado, en concordancia con los capítulos de comercio electrónico de los tratados vigentes.

IV. Efecto de la vigencia de la norma

No modifica normas. Complementa el Decreto Legislativo 1412 y eleva a rango legal la preferencia por la nube y Nube Perú previstas en el Decreto Supremo 029-2021-PCM, que se adecúa. Complementa la Ley 32069 y su reglamento (cláusulas y acuerdos marco), la Ley 29733 (flujo transfronterizo), el TUO de la Ley 27806 (clasificación), el Decreto de Urgencia 007-2020, el Decreto Supremo 126-2025-PCM, el artículo 19 del Decreto Supremo 115-2025-PCM y la Ley 30999. Es la regla general de localización de datos públicos; las normas especiales remiten a ella. El inventario comprende solo centros de datos públicos.

V. Indicador de éxito al 2031

A 2031, el 100% de los contratos de nube del Poder Ejecutivo incluye las cláusulas de portabilidad, salida y seguridad, el 100% de la información confidencial y crítica alojada en terceros está cifrada con claves bajo control del Estado y el número de centros de datos propios del Poder Ejecutivo se reduce respecto de la línea de base.

Normas relacionadas

- Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital — <https://www.gob.pe/institucion/pcm/normas-legales/289706-1412>
- Decreto Supremo 029-2021-PCM, Reglamento del Decreto Legislativo 1412 (modificado, entre otros, por los DS 075-2023-PCM y 098-2025-PCM) — <https://www.gob.pe/institucion/pcm/normas-legales/1705101-029-2021-pcm>
- Ley 32069, Ley General de Contrataciones Públicas, y su Reglamento aprobado por DS 009-2025-EF — <https://www.gob.pe/institucion/oece/colecciones/45029-ley-n-32069-ley-general-de-contrataciones-publicas-y-su-reglamento>
- Ley 29158, Ley Orgánica del Poder Ejecutivo — <https://www.leyes.congreso.gob.pe/Documentos/Leyes/29158.pdf>
- Ley 29733, Ley de Protección de Datos Personales — <https://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf>
- Ley 27806, Ley de Transparencia y Acceso a la Información Pública (TUO aprobado por Decreto Supremo 021-2019-JUS) — <https://www.leyes.congreso.gob.pe/Documentos/Leyes/27806.pdf>

Antecedentes

Periodo 2021-2026: PL 13372/2025-CR, Ley marco de soberanía digital y protección ciudadana frente al crimen organizado (en comisión). No se identificaron proyectos sobre nube del Estado.

Referencias internacionales

- Reino Unido: Government Cloud First policy — <https://www.gov.uk/guidance/government-cloud-first-policy>
- Estonia: Data Embassy (respaldo soberano de datos críticos del Estado) — <https://e-estonia.com/solutions/e-governance/data-embassy/>
- Chile: Ley 21.180, de Transformación Digital del Estado — <https://www.bcn.cl/leychile/navegar?idNorma=1138479>
- Unión Europea: Interoperable Europe Act, Reglamento (UE) 2024/903 — <https://interoperable-europe.ec.europa.eu/interoperable-europe/interoperable-europe-act>

Fuentes

- PCM, Secretaría de Gobierno y Transformación Digital (portal) — <https://www.gob.pe/gobiernodigital>
- Plataforma Nacional de Datos Abiertos — <https://www.datosabiertos.gob.pe/>

Propuesta ciudadana de libre uso — no es un proyecto presentado. Versión web:
<https://unimauro.github.io/agenda-legislativa-tech/p/GOB-13.html>