Secretaría General Iberoamericana

Secretaria-Geral Ibero-Americana

ESTUDIO

MODELO DE GOBERNANZA DIGITAL EN IBEROAMÉRICA

ANA BASCO Y PAULA GARNERO

2026

CON EL APOYO DE

Cooperación Española

Estudio para un modelo de gobernanza digital en Iberoamérica*

*Ana Basco y Paula Garnero
Febrero 2026

Resúmen Ejecutivo

El presente estudio tiene como objetivo analizar de manera comparada los marcos de gobernanza digital de los 22 países que conforman Iberoamérica y, a partir de ese diagnóstico, formular un modelo integral que contribuya al fortalecimiento institucional y al desarrollo inclusivo de la región, en línea con los principios establecidos en la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales (2023)[1].

La investigación responde a la necesidad de contar con un diagnóstico estructurado que traduzca los avances y desafíos de la región en evidencia sistemática y comparable, superando lecturas fragmentarias y capturando la gobernanza digital como un fenómeno multidimensional que articula visión estratégica, capacidades habilitantes e implementación efectiva, con un enfoque centrado en las personas y en la protección de derechos.

Contexto iberoamericano: la oportunidad y urgencia de una gobernanza digital compartida

Iberoamérica enfrenta una transformación estructural impulsada por la digitalización. En las últimas dos décadas, los 22 países que conforman la región han avanzado significativamente en la construcción de los cimientos de un Estado digital: El 88% de los países de América Latina y el Caribe cuenta con organizaciones responsables del gobierno digital y el 94% ha adoptado Estrategias Nacionales de Gobierno Digital, lo que refleja un compromiso político sostenido con la agenda de transformación digital[2]. La conectividad se ha expandido, los servicios públicos han migrado a entornos digitales y la ciudadanía demanda cada vez más interacciones ágiles, transparentes y seguras con sus gobiernos[3][4].

Sin embargo, este progreso coexiste con desafíos profundos. La región presenta trayectorias heterogéneas y niveles desiguales de madurez institucional. Mientras países como España, Uruguay, Brasil o Chile han consolidado ecosistemas digitales avanzados, otros enfrentan brechas estructurales en conectividad, capacidades estatales y marcos normativos.[5] A ello se suman fenómenos que trascienden las fronteras nacionales: la concentración de

[1] Secretaría General Iberoamericana [SEGIB]. (2023). Carta Iberoamericana de Principios y Derechos en los Entornos Digitales. XXVIII Cumbre Iberoamericana.
[2] OECD/CAF. (2024). Revisión del Gobierno Digital en América Latina y el Caribe: Construyendo Servicios Públicos Inclusivos y Responsivos. OECD Publishing
[3] 023 OCDE/BID Índice de Gobierno Digital de América Latina y el Caribe. Disponible en https://www.oecd.org/es/publications/2024/11/2023-oecd-idb-digital-government-index-of-latin-america-and-the-caribbean_5a9af6c4.html
[4] OECD (2026). Digital Government Index and Open, Useful and Re-usable Data Index: 2025 Results and Key Findings. OECD Working Papers on Public Governance, No. 90. OECD Publishing.
[5] Idem

infraestructuras digitales críticas en actores extra-regionales, la dependencia tecnológica, la velocidad de adopción de la inteligencia artificial que supera la capacidad regulatoria de los Estados, y los riesgos emergentes para la integridad democrática como la desinformación, los deepfakes o la opacidad algorítmica[6].

La economía digital iberoamericana representa ya un componente creciente del PIB regional y un motor potencial para la inclusión, la innovación y la productividad[7]. Pero su desarrollo sostenible requiere algo más que inversión en tecnología: exige marcos de gobernanza sólidos que equilibren la promoción de la innovación con la protección de derechos, que cierren brechas en lugar de profundizarlas, y que fortalezcan la autonomía estratégica de la región frente a un entorno global cada vez más fragmentado y competitivo[8].

Es en este contexto que la Secretaría General Iberoamericana (SEGIB) asume el mandato de sus estados miembros para impulsar una reflexión colectiva sobre la gobernanza digital en la región. La XXVIII Cumbre Iberoamericana celebrada en Santo Domingo en 2023[9] marcó un hito con la adopción de la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales[10], que sitúa a las personas en el centro de la transformación tecnológica y establece un marco común basado en la transparencia, la rendición de cuentas y la participación multiactor.

Este estudio se inscribe en ese compromiso. No se trata únicamente de diagnosticar el estado de la digitalización, sino de ofrecer a los países iberoamericanos —con sus realidades diversas, sus asimetrías y sus capacidades desiguales— un modelo de gobernanza digital que sea a la vez ambicioso y realista, estratégico y adaptable, y que permita traducir los principios de la Carta en instituciones, políticas y resultados concretos.

La SEGIB no parte de cero. La región cuenta con activos valiosos: una comunidad de países con vínculos históricos, lingüísticos y culturales; instituciones como la CEPAL, la CAF, el CLAD y la propia SEGIB que han acumulado conocimiento y capacidad de convocatoria; y una red de responsables públicos, técnicos, académicos y organizaciones de la sociedad civil que vienen trabajando en la agenda digital. El desafío es articular estos activos en una visión compartida que fortalezca la capacidad colectiva de los países iberoamericanos para gobernar su transformación digital.

CAPÍTULO 1.

[6] Relatoria del Diálogo Regional “Los retos de la gobernanza digital en América Latina y el Caribe”.(CAF,2026). Disponible en: https://scioteca.caf.com/bitstream/handle/123456789/2586/Relator%C3%ADa%20del%20di%C3%A1logo%20regional.%20Los%20retos%20de%20la%20gobernanza%20digital%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf?sequence=1&isAllowed=y

[7] eLAC2007, eLAC2010, eLAC2015, eLAC2024.https://desarrollodigital.cepal.org/es/elac

[8] OECD/CAF. (2024). *Revisión del Gobierno Digital en América Latina y el Caribe: Construyendo servicios públicos inclusivos y responsivos*. OECD Publishing. https://doi.org/10.1787/7a127615-es

[9] https://www.exteriores.gob.es/es/PoliticaExterior/Documents/Declaracion-xxviii-cumbre-rd_Es.pdf

[10] Secretaría General Iberoamericana [SEGIB]. (2023). Carta Iberoamericana de Principios y Derechos en los Entornos Digitales. XXVIII Cumbre Iberoamericana.

Este capítulo presenta un mapeo sistemático de los modelos institucionales y marcos normativos de gobernanza digital en los 22 países de Iberoamérica. Más que describir iniciativas aisladas, busca caracterizar cómo cada país organiza la conducción estratégica, la rectoría normativa y la implementación de su agenda digital.

Para ello, se emplea una metodología documental y comparada, basada en una arquitectura analítica común que abarca gobernanza estratégica, capacidades habilitadoras e implementación. Si bien el enfoque es integral, el eje del análisis se centra principalmente en la presencia, alcance y coherencia de los marcos normativos e institucionales (leyes, estrategias, autoridades rectoras y mecanismos de coordinación) que estructuran la política digital.

En consecuencia, los hallazgos se orientan a evaluar la solidez y coherencia de la arquitectura normativa e institucional que estructura la transformación digital en cada país. La aplicación homogénea de estos criterios permite identificar patrones regionales, tipologías institucionales y niveles diferenciados de madurez en términos de capacidad de conducción estratégica y articulación sistémica, que constituyen la base para la propuesta desarrollada en el capítulo siguiente.

Metodología

El capítulo adoptó una metodología mixta y documental para caracterizar de manera rigurosa y comparable la gobernanza digital en los 22 países de Iberoamérica. En una primera etapa, se realizó una revisión bibliográfica internacional —incluyendo marcos de referencia de organismos como OCDE, CEPAL, Banco Mundial y Naciones Unidas— con el objetivo de delimitar el marco conceptual y construir una arquitectura analítica común. A partir de esta base, se definieron dimensiones recurrentes de madurez en gobernanza digital (liderazgo estratégico, coherencia institucional, infraestructura digital, gestión de datos, confianza, capacidades y evaluación), que se tradujeron en una estructura operativa organizada en bloques: gobernanza estratégica, capacidades habilitadoras e implementación efectiva.

Sobre esa arquitectura, se llevó a cabo un relevamiento exhaustivo de fuentes primarias oficiales por país —normativa vigente, estrategias nacionales, arreglos institucionales y mecanismos operativos— complementado con índices internacionales y métricas estandarizadas como referencia contextual. El proceso incluyó triangulación, validación y curaduría normativa (verificación de vigencia, control de actualización, identificación de instrumentos derogados y contraste entre políticas y base legal), con el fin de asegurar trazabilidad y consistencia. Esta metodología permitió identificar marcos integrales y desarrollos fragmentarios, así como comparar niveles relativos de formalización institucional y madurez normativa en la región.

Sistematización de los resultados

Sobre la base del relevamiento y la curaduría, se conformó un **repositorio normativo sistematizado** que reúne los principales instrumentos legales, regulatorios y de política pública vinculados con la gobernanza digital en cada país, acompañados por referencias y enlaces de acceso. Este repositorio constituye la base empírica del estudio y habilita la comparación estructurada.

A partir de dicho repositorio se elaboró una **matriz general y comparativa** que sintetiza los principales elementos de la gobernanza digital de los 22 países. La matriz organiza la información conforme a la arquitectura conceptual previamente desarrollada, estructurada en tres grandes bloques analíticos que permiten ordenar el relevamiento de manera jerárquica y funcional.

La matriz general permite así traducir una arquitectura conceptual compleja en una herramienta comparativa homogénea, garantizando consistencia entre países y evitando abordajes fragmentarios por dimensión aislada. Cada celda de la matriz se construyó a partir del repositorio normativo validado, incorporando referencias a la normativa principal vigente y una caracterización sintética del grado de desarrollo relativo en cada componente. Esta estructura constituye el insumo central del análisis comparado y asegura trazabilidad entre fuentes, clasificación analítica y narrativa posterior.

Asimismo, para asegurar una comprensión integral del fenómeno, el estudio incorporó además **dos instrumentos complementarios**:

1. una **matriz específica de Gobernanza de Internet**, concebida como módulo transversal para relevar de manera integrada componentes regulatorios, institucionales y multiactor del ecosistema Internet (telecomunicaciones, neutralidad de red, administración de recursos críticos, coordinación y protección de derechos en línea); y
2. un **anexo específico sobre mecanismos de acceso a la información pública**, que sistematiza los canales digitales disponibles en cada país para el ejercicio efectivo de este derecho, complementando el análisis normativo con una aproximación operativa a los dispositivos institucionales y tecnológicos existentes.

El capítulo incluye asimismo una sección de síntesis que caracteriza la gobernanza digital de cada país, aplicando de manera sistemática la arquitectura analítica definida.

Principales hallazgos

El análisis comparado revela una realidad compleja y heterogénea en la gobernanza digital iberoamericana:

1. Avances significativos en fundamentos digitales: el 88% de los países de América Latina y el Caribe cuenta con organizaciones responsables del gobierno digital y el 94% ha adoptado Estrategias Nacionales de Gobierno Digital, lo que refleja un compromiso político sostenido. Países como Brasil, Chile, Colombia, España, Portugal, Uruguay presentan modelos avanzados e integrales, con marcos estratégicos claros, alta institucionalización y fuerte capacidad de implementación.
2. Heterogeneidad y asimetrías: coexisten trayectorias diferenciadas de desarrollo institucional. Junto a modelos consolidados, se identifican países con modelos en consolidación avanzada (Argentina, Costa Rica, Perú), modelos intermedios o fragmentados (Andorra, México, Ecuador, Panamá, Paraguay, República Dominicana) y modelos incipientes o con brechas estructurales (Bolivia, Guatemala, Honduras, Nicaragua, Venezuela, Cuba, El Salvador).
3. Desacople entre digitalización de servicios y capacidades habilitantes: en numerosos países, la expansión de servicios públicos digitales no siempre se corresponde con un

desarrollo equivalente de capacidades estructurales como gobernanza de datos, interoperabilidad de sistemas o institucionalización de la ciberseguridad, lo que genera ecosistemas funcionales en el corto plazo pero potencialmente frágiles.

4. La institucionalización como factor explicativo clave: más allá del nivel de desarrollo económico o inversión tecnológica, la estabilidad y claridad de los arreglos institucionales —rectorías claras, mecanismos de coordinación transversal y responsabilidades bien definidas— emerge como un factor determinante para sostener avances en el tiempo y evitar abordajes fragmentados.
5. Gobernanza de la inteligencia artificial como proxy de madurez: los países que han avanzado en la definición de enfoques integrales de gobernanza de la IA (Chile, Brasil, Perú, España, Portugal, Uruguay) tienden a mostrar mayores capacidades de coordinación intersectorial y alineamiento con principios de derechos, sugiriendo un efecto catalizador sobre otras dimensiones de la gobernanza digital.
6. Persistencia de brechas estructurales: el análisis confirma brechas significativas en conectividad, capital humano y capacidades estatales que condicionan el desarrollo de modelos integrales, especialmente en países de América Latina y el Caribe, donde persisten desafíos de inclusión digital, fragmentación normativa y dependencia tecnológica.

Desafíos transversales identificados

El diagnóstico identifica nueve desafíos estructurales que enfrenta la región:

1. Fragmentación normativa y asimetrías regulatorias: la coexistencia de marcos legales dispares, niveles heterogéneos de madurez institucional y velocidades de adopción tecnológica dificulta la interoperabilidad regional, encarece el cumplimiento regulatorio y limita la construcción de un espacio digital iberoamericano coherente.
2. Capacidades estatales desiguales y brechas de implementación: persiste una brecha significativa entre el diseño normativo y su implementación efectiva, asociada a limitaciones técnicas, presupuestarias y de recursos humanos en el sector público.
3. Dependencia tecnológica y limitada autonomía estratégica digital: la fuerte concentración de infraestructuras críticas, plataformas digitales y servicios de nube en actores extra-regionales reduce los márgenes de decisión soberana, incrementa riesgos de lock-in tecnológico y debilita la capacidad de los Estados para incidir en estándares y reglas globales.
4. Déficits en gobernanza de datos y uso estratégico de la información pública: persisten problemas de calidad, interoperabilidad, reutilización y protección de datos, así como una adopción incipiente de enfoques de gobierno basado en evidencia, limitando el potencial transformador de la digitalización y la inteligencia artificial.
5. Brechas territoriales y sociales en el acceso y uso de servicios digitales: la digitalización puede profundizar desigualdades preexistentes en conectividad, alfabetización digital, acceso a servicios públicos digitales y protección de derechos en entornos digitales.
6. Gobernanza de la inteligencia artificial aún incipiente y reactiva: en muchos países, los marcos de gobernanza de la IA se encuentran en etapas tempranas, con enfoques fragmentados o sectoriales, escasa coordinación interinstitucional y capacidades limitadas para evaluar riesgos, impactos y oportunidades de manera integral.

7. Debilidad de los mecanismos de coordinación regional: a pesar de la existencia de múltiples foros y espacios de diálogo, la cooperación regional sigue siendo fragmentada, con dificultades para traducir consensos políticos en instrumentos operativos, estándares comunes o proyectos conjuntos de alto impacto.
8. Tensiones entre innovación, regulación y protección de derechos: los Estados enfrentan el desafío de diseñar marcos regulatorios que promuevan la innovación sin descuidar la protección de derechos fundamentales, la transparencia algorítmica, la no discriminación y la rendición de cuentas.
9. Limitada inserción estratégica en la gobernanza digital global: los países no europeos de Iberoamérica enfrentan dificultades para incidir de manera coordinada en los espacios globales donde se definen estándares, principios y reglas del ecosistema digital.

CAPÍTULO 2.

El Capítulo 2 se propone formular un modelo integral de gobernanza digital para Iberoamérica a partir de los hallazgos del análisis comparado desarrollado previamente. Dicho análisis evidenció una realidad compleja: si bien la región ha avanzado de manera significativa en la construcción de fundamentos digitales —marcos normativos, estrategias e infraestructura institucional—, persisten desafíos estructurales asociados a la heterogeneidad institucional, la fragmentación normativa, las brechas de capacidades estatales y la necesidad de vincular la transformación digital con objetivos más amplios de desarrollo sostenible, legitimidad democrática y autonomía estratégica.

Sobre esta base, el capítulo desarrolla una propuesta que parte explícitamente de estas brechas y desafíos concretos, evitando enfoques abstractos o meramente normativos. El modelo se construye como una arquitectura institucional orientada a articular capacidades existentes, corregir fragmentaciones y anticipar las transformaciones tecnológicas en curso.

Como punto de partida, se revisa críticamente el modelo institucional propuesto por la CEPAL para América Latina y el Caribe, analizando sus fundamentos conceptuales y su diseño institucional, con el objetivo de identificar sus aportes y límites. A partir de este examen —y en diálogo con la literatura internacional y las experiencias comparadas analizadas en el Capítulo 1— el capítulo formula una propuesta superadora que integra dimensiones estratégicas, multinivel, geopolíticas y de derechos digitales, orientada a fortalecer la capacidad de los Estados iberoamericanos para conducir la transformación digital de manera coherente, inclusiva y alineada con el desarrollo sostenible.

Metodología

Sobre los hallazgos del capítulo anterior e incorporando aportes de la literatura internacional y aprendizajes derivados de experiencias comparadas examinadas a nivel global, se caracterizan los desafíos que enfrenta Iberoamérica para consolidar sistemas robustos de gobernanza digital.

Luego se revisa críticamente el modelo institucional recientemente propuesto por la CEPAL para América Latina y el Caribe, dado su peso técnico y su influencia en la agenda Latinoamericana. Este análisis examina sus fundamentos conceptuales, su arquitectura institucional y sus supuestos normativos, con el objetivo de identificar tanto sus aportes como sus límites frente a los desafíos contemporáneos de la gobernanza digital en Iberoamérica. El propósito no es desestimar dicho modelo, sino situarlo en un diálogo crítico y constructivo.

Finalmente, sobre la base de este análisis crítico e integrado, se formula una **propuesta superadora de modelo integral de gobernanza digital**. El modelo propuesto no parte de cero: retoma avances conceptuales existentes, pero los rearticula en una arquitectura más amplia y coherente, orientada a fortalecer la conducción estratégica del proceso de transformación digital. Su énfasis está puesto en consolidar capacidades estatales, asegurar coherencia normativa, promover inclusión y equidad, proteger derechos en entornos digitales y posicionar a los países iberoamericanos con mayor autonomía y capacidad de incidencia en el escenario tecnológico global.

Propuesta de modelo integral de gobernanza digital para Iberoamérica

El modelo desarrollado en este estudio trasciende el enfoque tradicional de gobierno digital y se inscribe en una concepción de **gobernanza digital estratégica iberoamericana**. Esta perspectiva integra la transformación digital del Estado con la política productiva, la autonomía tecnológica, la protección de derechos digitales, la regulación de mercados digitales y la cooperación regional. Parte del reconocimiento de que la arquitectura institucional nacional debe articularse con dinámicas multilaterales, mecanismos de coordinación regional y estrategias de posicionamiento internacional.

Esta ampliación conceptual no sustituye la dimensión administrativa de la digitalización —que continúa siendo indispensable—, sino que la incorpora en un marco más amplio en el cual el Estado no solo digitaliza servicios, sino que gestiona datos como activos estratégicos, participa en la definición de estándares con proyección internacional, articula con el sector tecnológico privado y promueve bienes públicos digitales compartidos en el espacio iberoamericano.

La arquitectura institucional propuesta no se limita a ordenar competencias internas del aparato estatal, sino que integra mecanismos de articulación multiactoral, coordinación multinivel y proyección regional, con el objetivo de fortalecer la capacidad colectiva de los países iberoamericanos para gobernar su transformación digital en un entorno global altamente competitivo y tecnológicamente concentrado.

Objetivos del modelo

Los objetivos del modelo se alinean con los principios establecidos en la **Carta Iberoamericana de Principios y Derechos en los Entornos Digitales de la SEGIB**[11], adoptando de manera explícita un enfoque basado en derechos humanos que coloca en el

[11] Adoptada en la XXVIII Cumbre Iberoamericana de Jefas y Jefes de Estado y de Gobierno, en Santo Domingo, República Dominicana, el 25 de marzo de 2023.

centro la dignidad y la autonomía de las personas, así como la inclusión, la transparencia, la rendición de cuentas y la cooperación regional como pilares de la gobernanza digital.[12]

1. **Objetivo 1. Fortalecer la capacidad del Estado para gobernar la transformación digital y la IA.** Reducir la brecha entre la velocidad de adopción tecnológica y la capacidad estatal de diseñar, implementar, supervisar y sostener políticas digitales con valor público que garanticen la centralidad de las personas.
2. **Objetivo 2. Proteger derechos, confianza e integridad democrática en entornos digitales.** Garantizar que la digitalización y el uso de la IA refuercen la legitimidad democrática, la transparencia, la seguridad y el ejercicio efectivo de derechos, evitando riesgos asociados a la desinformación, la automatización opaca y la pérdida de confianza institucional.
3. **Objetivo 3. Asegurar inclusión digital universal y reducción de brechas estructurales.** Orientar la gobernanza digital a cerrar brechas de acceso, capacidades e infraestructura, evitando que lo digital amplifique desigualdades sociales, territoriales, etarias o de género preexistentes.
4. **Objetivo 4. Aumentar la autonomía estratégica y la capacidad de decisión de los países iberoamericanos para contribuir al desarrollo sostenible.** Fortalecer la capacidad de los Estados para tomar decisiones informadas y soberanas sobre datos, infraestructuras tecnológicas y usos de la inteligencia artificial, promoviendo bienes públicos digitales, reduciendo dependencias críticas y favoreciendo esquemas de cooperación regional para el desarrollo.
5. **Objetivo 5. Fortalecer una gobernanza digital participativa, multinivel y multiactor.** Construir arreglos institucionales estables que articulen a los distintos niveles de gobierno y a actores públicos, privados, académicos y de la sociedad civil, mediante mecanismos de coordinación y diálogo orientados a producir resultados concretos, sostenibles y verificables.

Ejes estratégicos

La propuesta define ocho ejes estratégicos que operacionalizan los objetivos del modelo y orientan su traducción en capacidades estatales, arreglos institucionales y mecanismos de intervención concretos. Estos ejes no suponen la creación de nuevas estructuras, sino que organizan la agenda sustantiva dentro de la arquitectura institucional propuesta. Cada eje contribuye de manera diferenciada a los objetivos definidos y puede implementarse de forma modular y progresiva, permitiendo su adaptación a las prioridades y capacidades de cada país, sin perder coherencia con una visión iberoamericana compartida. En cada uno, se identifican casos de referencia global que ejemplifican buenas prácticas.

1. Capacidades estatales e institucionalidad para la gobernanza digital: funciones de rectoría estratégica, coordinación transversal, gobernanza de datos e IA, implementación técnica y control democrático.

[12] SEGIB, 2023. Carta Iberoamericana de Principios y Derechos en los Entornos Digitales de la SEGIB. https://www.segib.org/wp-content/uploads/2025/09/Carta_iberoamericana_derechos_digitales_ESP_web.pdf?_gl=1*1op0w7o*_ga*MTA4MDk2NDgzLjE3NjI0NTk0OTQ.*_ga_MCLNSVDYMK*czE3NzE0Mzc2MDIkbzEwJGcwJHQxNzcxNDM3NjAyJGo2MCRsMCRoMA..

2. Infraestructura tecnológica, interoperabilidad y digitalización del Estado: arquitectura común de interoperabilidad, estándares compartidos y servicios públicos digitales integrados.
3. Gobernanza de datos como infraestructura estratégica: reglas claras sobre calidad, acceso, uso y protección de datos públicos, reconociéndolos como activo estratégico y base para la IA.
4. Transparencia, auditoría algorítmica y rendición de cuentas: mecanismos de transparencia algorítmica, auditoría de sistemas automatizados y responsabilidades claras por decisiones apoyadas por IA.
5. Ciberseguridad y resiliencia digital: protección de infraestructuras críticas, capacidades de prevención y respuesta, y resiliencia sistémica.
6. Infraestructura digital crítica, capacidad de cómputo y soberanía tecnológica: control efectivo sobre centros de datos, capacidad de cómputo y redes, con enfoque en soberanía tecnológica.
7. Ciudadanía digital, alfabetización y legitimidad democrática: desarrollo de capacidades ciudadanas, participación multiactor y estrategias territoriales de inclusión digital.
8. Cooperación regional, proyección internacional y autonomía estratégica digital: articulación iberoamericana para incidir en estándares globales, reducir dependencias y construir bienes públicos digitales compartidos.

Arquitectura institucional

Se estructura a partir de una distinción analítica fundamental entre funciones y arreglos institucionales. En primer lugar, se identifican las funciones esenciales que todo sistema robusto de gobernanza digital debe cumplir —con independencia de su diseño organizacional específico— tales como la conducción estratégica, la rectoría normativa, la implementación operativa y la supervisión con garantías democráticas. Estas funciones definen el “qué” de la gobernanza digital: los roles sustantivos que deben estar claramente asignados para asegurar coherencia, capacidad de ejecución, coordinación multinivel y legitimidad democrática.

- La **función de conducción estratégica** se ubica en el centro de gobierno y tiene por objeto definir la visión integral de gobernanza digital, establecer prioridades nacionales y asegurar coherencia intersectorial, multinivel y presupuestaria. Integra la política digital con desarrollo productivo, innovación, derechos y proyección internacional, pudiendo ejercerse mediante un consejo o mecanismo equivalente ya existente, sin requerir necesariamente nuevas estructuras.
- La **función de rectoría normativa y coherencia sistémica** garantiza estándares comunes, interoperabilidad y lineamientos homogéneos en materia de datos, inteligencia artificial y ciberseguridad. Cumple un rol habilitante, acompañando a los organismos públicos en la adecuación progresiva de procesos y sistemas, y puede asignarse a entidades existentes fortalecidas, sin sustituir competencias de autoridades sectoriales.
- La **función de implementación y capacidad operativa** traduce estándares y lineamientos en plataformas, infraestructura compartida y proyectos estratégicos concretos. Se orienta al desarrollo técnico, asistencia a organismos y transferencia de capacidades, sin emitir normas ni ejercer funciones de fiscalización.

- La **función de supervisión y garantías democráticas** asegura legitimidad y confianza pública mediante la protección de derechos digitales, evaluación de impactos tecnológicos y supervisión de transparencia algorítmica. Puede ejercerse a través de órganos independientes o instituciones existentes con autonomía funcional garantizada.

Finalmente, la arquitectura incorpora una **dimensión transversal de articulación multiactor y cooperación regional**, que integra mecanismos de consulta con sector privado, academia y sociedad civil, coordinación con reguladores económicos y participación activa en instancias iberoamericanas, promoviendo armonización de estándares y desarrollo de bienes públicos digitales compartidos.

Modelos institucionales posibles

Las funciones definidas constituyen los componentes mínimos de una gobernanza digital estratégica. Sin embargo, su materialización institucional puede variar según la tradición administrativa, el grado de centralización y las capacidades de cada país.

El modelo integral propuesto no impone una estructura única ni exige la creación de nuevos organismos, siempre que exista una asignación clara de responsabilidades y coherencia sistémica. En este marco, pueden identificarse al menos tres configuraciones institucionales posibles, adaptables a las distintas realidades iberoamericanas.

1. *Modelo de articulación sobre estructuras existentes*

Este modelo parte de la premisa de que el país ya dispone de un entramado institucional desarrollado, por lo que la prioridad no es crear nuevas entidades, sino clarificar mandatos, fortalecer capacidades y formalizar mecanismos de coordinación. Las cuatro funciones de la gobernanza digital se asignan dentro de las estructuras vigentes.

- La **conducción estratégica** se ejerce desde el centro de gobierno mediante un Consejo interministerial formalizado, encargado de integrar la agenda digital con desarrollo productivo, innovación, derechos e inserción internacional. Su efectividad depende del respaldo político, reglas claras de coordinación y capacidad de incidir en prioridades y presupuesto.
- La **rectoría normativa** se asigna a una unidad especializada ya existente, fortaleciendo su mandato transversal para definir estándares comunes, interoperabilidad y lineamientos de gobernanza de datos e IA, bajo el principio de no sustituir competencias sectoriales.
- La **implementación operativa** se organiza de manera distribuida entre agencias y áreas técnicas existentes, coordinadas mediante estándares comunes y mecanismos formales de articulación, evitando duplicaciones y fragmentación tecnológica.
- La **supervisión democrática** se apoya en organismos de control ya establecidos —como autoridades de protección de datos o defensorías— fortaleciendo su coordinación para garantizar derechos digitales y rendición de cuentas.

Este modelo es especialmente adecuado en contextos institucionales consolidados donde la creación de nuevas entidades podría generar fricciones. Sus principales **fortalezas** son la alta viabilidad política, el aprovechamiento de capacidades instaladas y el menor costo

institucional. Entre sus **desafíos** se encuentran el riesgo de fragmentación, ambigüedad en responsabilidades y dependencia del liderazgo político.

Su efectividad requiere condiciones mínimas: mandato formal de coordinación, claridad en roles, estándares obligatorios de interoperabilidad, capacidad técnica suficiente y mecanismos de seguimiento. Cuando estas condiciones se cumplen, el modelo permite una gobernanza digital funcional y progresiva, aunque con menor grado de consolidación institucional que alternativas más estructuradas.

2. Modelo de integración funcional especializada

En este modelo, las funciones de **rectoría normativa** e **implementación operativa** se concentran en una única entidad especializada con autonomía técnica reforzada, mientras que la **conducción estratégica** permanece en el centro de gobierno y la **supervisión** continúa en manos de órganos independientes. El objetivo es reducir la fragmentación, aumentar la coherencia técnica y acelerar la transformación digital sin debilitar los contrapesos institucionales.

- La **conducción estratégica** se ejerce a través de un Consejo Nacional ubicado en la Presidencia o Jefatura de Gabinete, que define prioridades, articula la agenda digital con política productiva y derechos, y supervisa políticamente a la entidad especializada. Esta última —ya sea secretaría de alto rango o agencia ejecutiva— concentra la definición de estándares (interoperabilidad, datos, IA, arquitectura digital) y la ejecución técnica (plataformas transversales, infraestructura compartida, integración de sistemas y asistencia técnica). Para evitar conflictos de interés, debe garantizar una separación funcional interna entre el área normativa y la operativa.
- Las funciones de **rectoría normativa e implementación operativa** se concentran en una entidad especializada dependiente del Poder Ejecutivo, con autonomía técnica reforzada y mandato transversal. Esta entidad —ya sea una secretaría de alto rango o una agencia ejecutiva— debe contar con rango suficiente, presupuesto propio y estabilidad técnica para definir estándares de interoperabilidad, gobernanza de datos e inteligencia artificial, y al mismo tiempo desarrollar plataformas transversales, integrar sistemas y gestionar infraestructura compartida.
- La **supervisión democrática** se mantiene independiente, reforzando la capacidad técnica y la transparencia de los órganos de control existentes.

Este modelo resulta eficiente en contextos que requieren mayor agilidad y coherencia, aunque implica riesgos como concentración de poder técnico o debilitamiento de contrapesos.

Su efectividad depende de una clara delimitación entre conducción política y autonomía técnica, profesionalización estable, coordinación formal con reguladores y mecanismos sólidos de rendición de cuentas. Modelo de articulación sobre estructuras existentes: fortalece mecanismos de coordinación sin crear nuevas entidades, asignando funciones dentro del entramado institucional vigente.

3. Modelo de institucionalización consolidada

Este modelo se orienta a contextos de mayor madurez institucional y consenso político, donde la gobernanza digital se consolida como política de Estado mediante una base legal clara,

estabilidad organizacional y autonomía técnica reforzada. Las funciones dejan de depender exclusivamente de mecanismos de coordinación flexible y se institucionalizan en estructuras con mandato explícito y reglas formales de rendición de cuentas.

- La **conducción estratégica** permanece en el centro de gobierno, pero se formaliza por ley, con competencias definidas, mandato plurianual y capacidad de incidir en la planificación presupuestaria y en la aprobación de planes nacionales.
- La **rectoría normativa** se ejerce desde una entidad especializada con autonomía técnica y base legal propia —agencia o autoridad administrativa— con competencias claras en interoperabilidad, estándares digitales, gobernanza de datos e inteligencia artificial, incluyendo facultades para emitir lineamientos obligatorios. Esta institucionalización busca garantizar previsibilidad, profesionalización técnica y coherencia sistémica, sin sustituir competencias sectoriales.
- La fu**nción de supervisión** se ejerce de manera diferenciada y multinivel: una instancia política asegura coherencia estratégica; una autoridad técnica transversal verifica el cumplimiento normativo y arquitectónico; y órganos independientes garantizan control externo, legalidad y rendición de cuentas

El modelo es especialmente adecuado en países que buscan consolidar la transformación digital con estabilidad de largo plazo.

Entre sus **fortalezas** se destacan la continuidad institucional, claridad competencial y mayor capacidad de planificación estratégica. Entre sus **desafíos**, la mayor complejidad jurídica, posibles rigideces y riesgos de concentración técnica. Su efectividad requiere base legal clara, autonomía con control democrático, presupuesto estable, profesionalización técnica y coordinación formalizada con reguladores y autoridades sectoriales.

Dimensión iberoamericana

El modelo incorpora una dimensión transversal de cooperación regional, con una arquitectura ligera de tres niveles: foro político-estratégico de coordinación entre órganos nacionales de conducción, red técnica permanente entre autoridades digitales y mecanismo de articulación entre órganos de supervisión en materia de derechos digitales. Esta estructura busca fortalecer la incidencia colectiva de Iberoamérica en la gobernanza digital global, promover la armonización progresiva de estándares y reducir asimetrías frente a actores tecnológicos globales.

Conclusión

El estudio evidencia que Iberoamérica ha consolidado una base institucional relevante para la gobernanza digital, pero enfrenta desafíos estructurales que requieren un salto cualitativo hacia modelos más integrales, estratégicos y cooperativos.

Recomendaciones principales:

1. Fortalecer la institucionalidad de la gobernanza digital como política de Estado, con rectorías claras, mecanismos de coordinación transversal y responsabilidades bien definidas, asegurando continuidad más allá de los ciclos políticos.

2. Avanzar hacia modelos integrados de interoperabilidad y datos, reconociendo los datos como infraestructura estratégica y condición para la soberanía digital y el uso responsable de la IA.
3. Incorporar mecanismos sistemáticos de transparencia, auditoría algorítmica y rendición de cuentas en el diseño institucional, como condición para la legitimidad democrática de la transformación digital.
4. Desarrollar estrategias explícitas de gestión de infraestructuras digitales críticas y capacidad de cómputo, articulando políticas digitales, energéticas, industriales y territoriales.
5. Invertir sostenidamente en alfabetización digital crítica y participación ciudadana, reconociendo que la legitimidad de la gobernanza digital depende de la capacidad de la ciudadanía para comprender, utilizar y cuestionar las tecnologías que median su relación con el Estado.
6. Profundizar la cooperación regional iberoamericana, no solo para compartir experiencias, sino para incidir colectivamente en la definición de estándares globales, reducir dependencias críticas y construir bienes públicos digitales compartidos.
7. Adoptar enfoques graduales y adaptables en la implementación del modelo, reconociendo la heterogeneidad de trayectorias institucionales y capacidades estatales en la región.

La propuesta presentada ofrece un marco flexible, anclado en principios de derechos humanos, inclusión y autonomía estratégica, con el objetivo de que la transformación digital contribuya efectivamente a la legitimidad democrática, el desarrollo sostenible y el fortalecimiento del espacio iberoamericano en el escenario digital global.

Introducción

En Iberoamérica la gobernanza digital ha adquirido un papel central en las estrategias de modernización estatal y en la cooperación regional, impulsada tanto por la expansión de la conectividad como por la necesidad de ofrecer servicios públicos más eficientes, transparentes e inclusivos. De acuerdo con la *Revisión del Gobierno Digital en América Latina y el Caribe (ALC)*[13], la región ha avanzado significativamente en la construcción de los llamados *fundamentos digitales*, como la conectividad básica, los portales de servicios y las estrategias nacionales de gobierno electrónico, pero muestra un progreso desigual en áreas más complejas como la interoperabilidad, el uso de datos abiertos y la innovación digital.

En términos generales, la región ha logrado consolidar una primera generación de reformas orientadas a la construcción de fundamentos digitales, tales como la conectividad básica, los portales de servicios y la formulación de estrategias nacionales de gobierno electrónico. No obstante, el tránsito hacia modelos más sofisticados, basados en interoperabilidad, datos abiertos e innovación digital, evidencia trayectorias heterogéneas y niveles desiguales de madurez institucional[14]. Este proceso se inscribe en una etapa de transición en la que la mayoría de los países ha establecido bases institucionales relevantes para avanzar hacia una transformación coherente y centrada en las personas[15].

En cuanto a los avances, la última década muestra un fortalecimiento institucional y estratégico significativo. El 88% de los países de América Latina y el Caribe cuenta con organizaciones responsables del gobierno digital y el 94% ha adoptado Estrategias Nacionales de Gobierno Digital, lo que refleja un compromiso político sostenido con la agenda de transformación digital[16]. Algunos países, como Colombia, Uruguay, Perú, Brasil y México, registran desempeños destacados en comparación con estándares internacionales, evidenciando mayores niveles de consolidación institucional y capacidades de implementación[17]. A nivel regional, la adopción de la Carta Iberoamericana de Principios y Derechos en Entornos Digitales constituye un hito normativo orientado a situar a las personas en el centro de la transformación tecnológica[18]. Asimismo, más de la mitad de los países cuenta con leyes de protección de datos personales y marcos regulatorios para los Sistemas de Identificación Digital, mientras que algunos países previamente rezagados muestran mejoras aceleradas en conectividad, talento y estrategias de inteligencia artificial[19].

---

[13] OECD/CAF. (2024). Revisión del Gobierno Digital en América Latina y el Caribe: Construyendo servicios públicos inclusivos y responsivos. OECD Publishing. https://doi.org/10.1787/7a127615-es

[14] Ídem.

[15] Organización para la Cooperación y el Desarrollo Económicos (OCDE) & Banco Interamericano de Desarrollo (BID). (2024). Índice de Gobierno Digital 2023: América Latina y el Caribe. OECD Public Governance Policy Papers.

[16] OECD/CAF. (2024). Revisión del Gobierno Digital en América Latina y el Caribe: Construyendo Servicios Públicos Inclusivos y Responsivos. OECD Publishing

[17] Organización para la Cooperación y el Desarrollo Económicos (OCDE) & Banco Interamericano de Desarrollo (BID). (2024). Índice de Gobierno Digital 2023: América Latina y el Caribe. OECD Public Governance Policy Papers.

[18] Secretaría General Iberoamericana [SEGIB]. (2023). Carta Iberoamericana de Principios y Derechos en los Entornos Digitales. XXVIII Cumbre Iberoamericana.

[19] Palma, I., & Rojas, A. (2024). Estudio Prácticas de identificación digital para el acceso a servicios de gobierno en Iberoamérica. CLAD/SEGIB

Sin embargo, estos progresos conviven con desafíos estructurales que limitan el impacto sistémico de las políticas digitales. La región presenta dificultades para consolidar organizaciones públicas basadas en datos, lo que restringe la capacidad de diseñar, monitorear y evaluar políticas sustentadas en evidencia[20]. La gestión fragmentada de la información en silos institucionales, la débil interoperabilidad y la ausencia de estándares comunes profundizan estas limitaciones[21] [22]. Persisten además brechas de inclusión digital y bajos niveles de uso efectivo de servicios en línea, lo que evidencia una distancia entre la oferta digital y su apropiación ciudadana[23]. A ello se suman déficits críticos en ciberseguridad y escasez de talento especializado, así como debilidades en el monitoreo y evaluación del ciclo de políticas digitales[24] [25] [26] [27]. En materia de inteligencia artificial, si bien proliferan los planes nacionales, la implementación efectiva y la asignación de recursos continúan siendo insuficientes, configurando un escenario caracterizado por avances programáticos sin correlato pleno en la ejecución[28].

La gobernanza digital en Iberoamérica combina una base institucional crecientemente consolidada con brechas significativas en capacidades, coordinación y resultados. El desafío estratégico radica en transitar desde una digitalización predominantemente instrumental hacia un modelo integral, basado en datos, interoperable, éticamente orientado y articulado regionalmente, capaz de traducir los compromisos normativos y estratégicos en mejoras tangibles para la ciudadanía [29] [30].

En este contexto, y frente a la necesidad de contar con un diagnóstico estructurado que traduzca los avances y desafíos en evidencia sistemática y comparable, el presente estudio persigue dos objetivos centrales. Primero, analizar de manera comparada los marcos de gobernanza digital de los 22 países de Iberoamérica. Segundo, formular una propuesta de

[20] Banco Mundial. (2023). Datos para una mejor gobernanza: Construyendo ecosistemas analíticos gubernamentales en América Latina y el Caribe.
[21] Naser, A. (Coord.). (2021). Gobernanza digital e interoperabilidad gubernamental: una guía para su implementación (LC/TS.2021/80). CEPAL
[22] Santini, J. F., Sacco Capurro, F., Rogger, D., Lundy, T., Kim, G., de León Miranda, J., Cocciolo, S., & Casanova, C. (2024). Data for Better Governance: Building Government Analytics Ecosystems in Latin America and the Caribbean. World Bank.
[23] Roseth, B., Reyes, A., & Santiso, C. (Eds.). (2018). El fin del trámite eterno: Ciudadanos, burocracia y gobierno digital. Banco Interamericano de Desarrollo [BID].
[24] Organización de los Estados Americanos [OEA] & CISCO. (2022). Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades.
[25] Leonardo, C., Solano, E., Cruz, A., Peguero, C., & Lizardo, R. (2024). Ciberseguridad en América Latina: Estrategias nacionales. LAC4 / EU CyberNet.
[26] Santini, J. F., Sacco Capurro, F., Rogger, D., Lundy, T., Kim, G., de León Miranda, J., Cocciolo, S., & Casanova, C. (2024). Data for Better Governance: Building Government Analytics Ecosystems in Latin America and the Caribbean. World Bank.
[27] Organización para la Cooperación y el Desarrollo Económicos (OCDE) & Banco Interamericano de Desarrollo (BID). (2024). Índice de Gobierno Digital 2023: América Latina y el Caribe. OECD Public Governance Policy Papers.
[28] Durán, R., Moreno, A., Adasme, S., Rovira, S., Jordán, V., y Poveda, L. (Coords.). (2025). Índice Latinoamericano de Inteligencia Artificial (ILIA) 2025. Documentos de Proyectos (LC/TS.2025/68). Comisión Económica para América Latina y el Caribe (CEPAL) y Centro Nacional de Inteligencia Artificial (CENIA).
[29] Palma, I., & Rojas, A. (2024). Estudio Prácticas de identificación digital para el acceso a servicios de gobierno en Iberoamérica. CLAD/SEGIB.
[30] Comisión Económica para América Latina y el Caribe [CEPAL]. (2023). Análisis de los modelos de gobernanza de datos en las ciudades de América Latina.

modelo integral que contribuya al fortalecimiento institucional y al desarrollo inclusivo de la región, en línea con los principios y objetivos de la SEGIB.

El informe se organiza en dos partes articuladas. La primera presenta el análisis comparado de los marcos de gobernanza digital de Andorra, Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, España, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Portugal, República Dominicana, Uruguay y Venezuela. Este relevamiento se estructura en torno a ejes que reflejan los principales componentes de la gobernanza digital contemporánea: estrategias nacionales de digitalización, economía digital, ciberseguridad, conectividad, datos y privacidad, identidad digital, infraestructuras críticas, interoperabilidad, gobierno digital, inteligencia artificial y gobernanza de Internet. La utilización de estos ejes permite un abordaje homogéneo y facilita la comparación de arreglos institucionales, marcos normativos y mecanismos de coordinación.

La segunda parte, de carácter propositivo, se apoya en la evidencia recogida para identificar brechas, asimetrías y áreas de convergencia regional, y a partir de allí delinear un modelo de gobernanza digital orientado a mejorar la coherencia estratégica, la capacidad de implementación y la articulación regional. De este modo, el análisis comparado constituye la base empírica sobre la cual se construye la propuesta conceptual del estudio.

Marco conceptual del estudio y alcances de la gobernanza digital

Se entiende por gobernanza digital de Iberoamérica al conjunto de instituciones, normas, procesos y relaciones intersectoriales que orientan la transformación digital de los países, garantizando la protección de derechos, la inclusión y el desarrollo sostenible en el entorno digital. A diferencia de enfoques centrados exclusivamente en el Estado, esta visión incorpora la interacción entre los poderes públicos, el sector privado, la academia, la sociedad civil y los organismos internacionales, en un entramado de gobernanza colaborativa y multinivel.

Desde esta perspectiva, la gobernanza digital implica tanto la gestión pública digital (infraestructura, interoperabilidad, servicios electrónicos) como la gestión del ecosistema digital nacional, que abarca ámbitos como la ciberseguridad, la protección de datos personales, la identidad digital, la gobernanza de Internet y el uso ético de tecnologías emergentes como la inteligencia artificial. Este enfoque integral responde al mandato de la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales (CIPDED), que promueve un desarrollo tecnológico centrado en las personas, basado en la transparencia, la rendición de cuentas y la participación de múltiples actores.

La gobernanza digital se ha configurado como un ámbito conceptual e institucional en evolución, atravesado por diferencias en capacidades estatales, arreglos regulatorios y contextos socioeconómicos. Si bien no existe un modelo único, universalmente adoptado o normativamente ejemplar que funcione como referencia estándar para los diversos países, algunos organismos internacionales han desarrollado marcos conceptuales que orientan la formulación de políticas digitales. Entre ellos, destacan los aportes de la **CEPAL**, la **OCDE** y el sistema de **Naciones Unidas** que, aunque no proponen “modelos” cerrados, ofrecen enfoques analíticos consistentes, con énfasis y supuestos diferentes.

El aporte de Comisión Económica para América Latina y el Caribe (CEPAL)

Sobre la definición propuesta por Whittingham Munévar[31], la CEPAL avanza hacia la noción de **gobernanza digital,** definida como: "la articulación y concreción de políticas de interés público con los diversos actores involucrados (Estado, Sociedad Civil y Sector Privado), con la finalidad de alcanzar competencias y cooperación para crear valor público y la optimización de los recursos de los involucrados, mediante el uso de tecnologías digitales" [32]. **La gobernanza digital, por tanto, implica establecer estructuras y procesos que aseguren la alineación entre la estrategia de gobierno digital y los objetivos estratégicos del gobierno; la articulación de políticas de interés público entre actores; una administración adecuada de riesgos y oportunidades; y la optimización de los recursos mediante el uso racional de tecnologías digitales**[33].

La CEPAL también propone diferenciar el plano estratégico y normativo del plano organizacional y operativo. En este sentido, distingue entre los conceptos de **Gobernanza digital y de institucionalidad del Gobierno Digital;** mientras que la gobernanza define los alcances, contenidos, política pública, marco normativo, liderazgo, infraestructura y soluciones comunes, **la institucionalidad, se refiere al esquema organizacional (incluyendo sus normas y procedimientos) encargado de implementar los servicios y soluciones digitales del Estado[34].**

En su Agenda Digital para América Latina y el Caribe (eLAC2024), la CEPAL enfatiza sobre la necesidad de alcanzar una transformación digital para un desarrollo productivo, inclusivo y sostenible para América Latina y el Caribe. En este marco, la gobernanza digital se presenta como una herramienta para cerrar la brecha de productividad y la desigualdad en la economía digital: "La gobernanza digital debe promoverse mediante un marco institucional que facilite la coordinación de políticas públicas, fomente la inversión en infraestructura y garantice la inclusión social para evitar que la digitalización profundice las brechas existentes"[35]. Luego, la eLAC2026, propone un marco conceptual organizado en tres pilares temático y tres ejes habilitadores:

Infografía: Marco conceptual de eLAC2026. Pilares temáticos y ejes habilitadores

---

[31] Whittingham Munévar, M. V. (2010). ¿Qué es la gobernanza y para qué sirve? *Revista Análisis Internacional*, (2), 219–235. https://revistas.utadeo.edu.co/index.php/RAI/article/view/24/26

[32] Naser, A. (Coord.). (2021). *Gobernanza digital e interoperabilida d gubernamental: una guía para su implementación* (Documentos de Proyectos, LC/TS.2021/80). Comisión Económica para América Latina y el Caribe (CEPAL). https://www.cepal.org/es/publicaciones/47018-gobernanza-digital-interoperabilidad-gubernamental-guia-su-implementacion

[33] Comisión Económica para América Latina y el Caribe (CEPAL). (s. f.). ¿Qué es la gobernanza? Definición desde la CEPAL. Biblioguías de la CEPAL. Recuperado de https://biblioguias.cepal.org/gobierno-digital/concepto-gobernanza

[34] Ídem.

[35] Comisión Económica para América Latina y el Caribe (CEPAL). (2022). Agenda Digital para América Latina y el Caribe (eLAC2024) (LC/CMSI.8/5). CEPAL. https://www.cepal.org/es/proyectos/agenda-digital-america-latina-caribe-elac2026/agenda-digital-2024

Fuente: Observatorio de Desarrollo Digital de las Naciones Unidas[36].

El aporte de Organización para la Cooperación y Desarrollo Económico (OCDE)

A diferencia de CEPAL y ONU que han abordado la digitalización desde perspectivas más amplias de desarrollo o cooperación multilateral, la **OCDE** ha concentrado de manera sistemática sus esfuerzos en el desarrollo conceptual y normativo del concepto de **Gobierno Digital**. En términos generales, la OCDE orienta el diseño y la implementación de estrategias de gobierno digital mediante un conjunto de principios, pero no prescribe una estructura institucional específica ni un esquema organizativo uniforme para los Estados. Entre los **principios fundamentales se destacan la apertura, transparencia e inclusión en los procesos gubernamentales, fomentando la participación de actores públicos, privados y de la sociedad civil para fortalecer la confianza pública y reducir brechas digitales** [37].

Un hito central en esta trayectoria fue la adopción, el 15 de julio de 2014, de la *Recommendation of the Council on Digital Government Strategies*, aprobada por el Consejo de la OCDE a propuesta del Comité de Gobernanza Pública[38]. Esta Recomendación

[36] Comisión Económica para América Latina y el Caribe (CEPAL). (s. f.). eLAC: Agenda digital para América Latina y el Caribe. Observatorio de Desarrollo Digital. Recuperado de https://desarrollodigital.cepal.org/es/elac#:~:text=La%20agenda%20actualmente%20vigente%2C%20eLAC2026%2C%20fue%20aprobada,Caribe%2C%20mediante%20la%20integraci%C3%B3n%20y%20cooperaci%C3%B3n%20regional

[37] Organisation for Economic Co-operation and Development (OCDE). (2014). Recommendation of the Council on Digital Government Strategies (OECD/LEGAL/0406). Recuperado de https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406

[38] En 2012, la Red de Gobierno Electrónico de la OCDE del Comité de Gobernanza Pública (actualmente denominado Grupo de Trabajo de Altos Funcionarios de Gobierno Digital (E-Leaders)) estableció un grupo de trabajo informal de 13 miembros de la OCDE para desarrollar un instrumento

constituye el primer instrumento jurídico internacional específicamente dedicado al gobierno digital y proporciona orientación a los países adherentes sobre cómo adaptarse a los cambios tecnológicos y aprovechar de manera estratégica las oportunidades que ofrecen las tecnologías digitales [39] [40]. Un punto de inflexión fue reconocer una nueva etapa de madurez en el uso de tecnologías digitales por parte de los gobiernos y **el tránsito desde el gobierno electrónico hacia el gobierno digital**, entendido como la integración de tecnologías digitales dentro de las estrategias de modernización del Estado con el objetivo de crear valor público[41]. Este cambio implicó pasar de la digitalización de procesos administrativos a la integración de tecnologías digitales como parte estructural de las estrategias de modernización del Estado, con un enfoque integral (*whole-of-government*), liderazgo político claro y marcos organizacionales capaces de coordinar la implementación dentro y entre niveles de gobierno.

El primer informe de implementación presentado al Consejo en 2017 concluyó que los adherentes habían avanzado en la alineación de marcos estratégicos y en la adopción de prácticas innovadoras basadas en la Recomendación, pero identificó la necesidad de **fortalecer los marcos de política, consolidar capacidades institucionales y ampliar la difusión e implementación a nivel subnacional**[42]. El segundo informe presentado en 2024 confirmó progresos adicionales en la alineación de estrategias nacionales con los principios de la Recomendación, aunque subrayó que se requieren mayores esfuerzos e inversiones para aprovechar plenamente el potencial de las tecnologías digitales en el sector público[43]. En particular, destacó la importancia de **fortalecer la gobernanza y la coordinación del gobierno digital, así como de reforzar las capacidades institucionales asociadas a su implementación.**

El **Digital Government Index (DGI) de la OCDE** (ver Anexo 3)[44], con tres ediciones (2019, 2023 y 2025)[45] constituye otro insumo estratégico para este estudio. Sus resultados permiten

---

legal sobre gobierno digital. El primer borrador fue debatido por los E-Leaders en Berna, Suiza, los días 29 y 30 de octubre de 2013 [GOV/PGC/EGOV(2013)1] y posteriormente se basó en consultas con las comunidades políticas de la OCDE, en particular con el Comité de Política de la Economía Digital (actualmente denominado Comité de Política Digital) y una consulta pública celebrada entre noviembre de 2013 y enero de 2014. Fuente:OECD, Recommendation of the Council on Digital Government Strategies, OECD/LEGAL/0406. Recuperado de https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406

[39] OECD/CAF. (2024). Revisión del Gobierno Digital en América Latina y el Caribe: Construyendo Servicios Públicos Inclusivos y Responsivos. OECD Publishing

[40] Organisation for Economic Co-operation and Development (OCDE). (2014). Recommendation of the Council on Digital Government Strategies (OECD/LEGAL/0406). Recuperado de https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406

[41] Ídem.

[42] Ídem.

[43] Ídem.

[44] En el Anexo III se ofrece una caracterización metodológica del índice y los resultados de la edición 2025 del DGI de OECD, basada en el documento *Digital Government Index and Open, Useful and Re-usable Data Index: 2025 results and key findings* (OECD Working Papers on Public Governance No. 90). OECD, 2026. Disponible en https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/02/digital-government-index-and-open-useful-and-re-usable-data-index_dbe102ed/6347ec74-en.pdf

[45] Hasta la fecha (febrero de 2026), el índice ha tenido tres iteraciones principales: i) Edición 2019 (Publicada en 2020): El piloto y línea base; ii) Edición 2023 (Publicada en 2024): Refinó la metodología para incluir temas como identidad digital e IA; iii) Edición 2025 (Publicada el 16 de febrero de 2026): donde Chile ascendió al Top 10 global. Cabe señalar que, a partir de la encuesta de 2023, se desarrolló además una versión específica para América Latina y el Caribe, el *2023*

caracterizar de manera sistemática los principales desafíos que enfrentan los países miembros y en proceso de adhesión de la OCDE en materia de gobierno digital. Si bien, a los fines de este trabajo, el alcance geográfico de este índice es limitado (sólo a 9 de los 22 países iberoamericanos en su tercera edición), en el año 2023, la OCDE junto al Banco Interamericano de Desarrollo (BID), realizaron una medición especial extendiendo la evaluación al conjunto de países de América Latina y el Caribe[46].

El DGI proporciona evidencia comparada y referencias concretas de buenas prácticas que enriquecen y orientan la discusión sobre posibles modelos de gobernanza digital. En particular, permite identificar casos de desempeño destacado (países ubicados entre las primeras diez posiciones del ranking) cuyas trayectorias ofrecen aprendizajes significativos en términos de coordinación institucional, desarrollo de infraestructura digital pública y uso estratégico de datos e inteligencia artificial. Finalmente, el índice ofrece un marco metodológico sólido que estructura el análisis en seis dimensiones —Digital by design, Data-driven public sector, Government as a platform, Open by default, User-driven y Proactiveness— articulando de manera coherente estrategia, capacidades institucionales, infraestructura tecnológica, apertura, enfoque centrado en las personas y uso anticipatorio de datos e inteligencia artificial . Esto constituye un punto de partida robusto para repensar y proponer un modelo de gobernanza digital alineado con las oportunidades y desafíos que enfrentan los países de Iberoamérica.

El aporte de la Organización de las Naciones Unidas (ONU)

La perspectiva de la Organización de las Naciones Unidas en materia de gobernanza digital se inscribe en una concepción profundamente política y ética del orden internacional contemporáneo. La gobernanza digital es entendida como parte integral del mandato multilateral orientado a la paz, el desarrollo sostenible y la protección universal de los derechos humanos. El Global Digital Compact de 2024 afirma explícitamente que el futuro digital debe construirse sobre la base de la Carta de las Naciones Unidas, el derecho internacional y la Declaración Universal de Derechos Humanos, consolidando un marco normativo común que garantice que la transformación tecnológica permanezca subordinada a la dignidad humana y al interés público global[47]. En este sentido, la cooperación digital se convierte en un instrumento estructural para evitar que la innovación tecnológica avance sin supervisión democrática o genere nuevas asimetrías de poder a escala global.

El Pacto Digital Mundial organiza esta visión en torno a objetivos estratégicos que incluyen el cierre de brechas digitales, la promoción de un entorno digital abierto, seguro y protegido, la gobernanza equitativa de los datos y la regulación de tecnologías emergentes, incluida la inteligencia artificial, en beneficio de la humanidad[48]. Este enfoque se sustenta en principios

OECD/IDB Digital Government Index of Latin America and the Caribbean, lo que permitió ampliar el alcance del análisis más allá de los países miembros de la organización.

[46] Organización para la Cooperación y el Desarrollo Económicos (OCDE) & Banco Interamericano de Desarrollo (BID). (2024). Índice de Gobierno Digital OCDE-BID 2023: América Latina y el Caribe (OECD Public Governance Policy Papers). OCDE y BID. https://www.oecd.org/en/publications/government-at-a-glance-2025_0efd0bcd-en.html

[47] United Nations. (2024). *Global Digital Compact (Zero draft)*. United Nations. https://www.un.org/digital-emerging-technologies/sites/www.un.org.techenvoy/files/Global_Digital_Compact_Zero_Draft.pdf

[48] Ídem.

transversales tales como la centralidad de los derechos humanos, la rendición de cuentas, la transparencia, la interoperabilidad y la participación multiactor, reconociendo que la arquitectura digital global no puede ser gobernada exclusivamente por Estados o por actores tecnológicos privados. De este modo, la ONU promueve un modelo de gobernanza cooperativa que busca articular responsabilidades compartidas y consolidar estándares éticos universales mínimos para el ecosistema digital[49].

Esta agenda adquiere mayor densidad política con la adopción del Pacto para el Futuro en 2024, que integra formalmente el Pacto Digital Mundial como uno de sus componentes estratégicos y reafirma la necesidad de fortalecer la cooperación internacional para gestionar los riesgos y oportunidades derivados de las tecnologías digitales y emergentes[50]. La transformación digital es presentada no solo como una cuestión de modernización tecnológica, sino como un desafío sistémico que exige renovar el multilateralismo, ampliar la confianza entre Estados y consolidar mecanismos de coordinación global frente a riesgos transfronterizos.

Capítulo 1. Análisis comparativo de los modelos de gobernanza digital Iberoamérica

El presente capítulo desarrolla un mapeo sistemático de los modelos institucionales de gobernanza digital y de sus marcos normativos en los 22 países de Iberoamérica. El objetivo no es únicamente describir iniciativas o políticas aisladas, sino caracterizar de manera estructurada cómo cada país organiza la conducción estratégica, la rectoría normativa y la implementación operativa de su agenda digital, así como los instrumentos legales que la sustentan.

Para ello, se adoptó una metodología de carácter documental y comparado, orientada a asegurar consistencia conceptual y comparabilidad entre países. A partir de una arquitectura analítica común —organizada en bloques y dimensiones que abarcan gobernanza estratégica, capacidades habilitadoras e implementación— se relevaron y sistematizaron normas, estrategias, arreglos institucionales y políticas públicas vinculadas con la transformación digital del Estado. Este enfoque permitió evitar lecturas fragmentarias y capturar la gobernanza digital como un fenómeno multidimensional, donde interactúan liderazgo político, marcos regulatorios, capacidades técnicas y mecanismos de coordinación.

No obstante, es importante precisar el encuadre específico de este ejercicio. Si bien el análisis adopta una mirada integral sobre la gobernanza digital, el eje estructurante del relevamiento en este capítulo se centra principalmente en la **presencia, alcance y coherencia de los marcos normativos e institucionales** que ordenan la agenda digital en cada país. En consecuencia, el foco analítico se sitúa prioritariamente en la existencia —o ausencia— de leyes, estrategias formales, decretos, autoridades rectoras y dispositivos de coordinación que dotan de estabilidad, jerarquía y previsibilidad a la política digital. Por ello, los hallazgos y tipologías que emergen del análisis comparativo deben ser leídos en ese código: no constituyen una medición directa del nivel de digitalización efectiva ni del desempeño

[49] Ídem.
[50] United Nations. (2024). *Pact for the Future* (A/79/L.2). United Nations General Assembly.

operativo de los servicios públicos digitales, sino una evaluación cualitativa de la arquitectura normativa e institucional que sustenta —o condiciona— dichos desarrollos.

Los hallazgos que se presentan a lo largo del capítulo son el resultado directo de este ejercicio metodológico. No se trata de valoraciones ad hoc, sino de conclusiones derivadas de la aplicación homogénea de los mismos criterios analíticos a todos los países considerados. Este procedimiento permite identificar patrones regionales, tipologías institucionales, niveles diferenciados de madurez normativa e institucional y brechas estructurales, constituyendo la base empírica sobre la cual se construye la propuesta desarrollada en el capítulo siguiente.

Metodología

Para caracterizar de manera rigurosa, homogénea y comparable de la gobernanza digital en los 22 países de Iberoamérica el presente capítulo adoptó un enfoque metodológico de carácter **mixto** y **documental**, basado en un proceso sistemático de **relevamiento**, **triangulación**, **curaduría** y **sistematización** de fuentes normativas, institucionales y técnicas. La metodología se diseñó para asegurar consistencia conceptual y comparabilidad entre países, evitando lecturas fragmentarias y permitiendo capturar la gobernanza digital como un fenómeno **multidimensional** que articula visión estratégica, capacidades habilitadoras e implementación efectiva.

En una primera etapa se realizó una **revisión bibliográfica internacional** orientada a delimitar el marco conceptual y construir una arquitectura analítica común. Esta revisión incluyó publicaciones de organismos multilaterales y redes especializadas (por ejemplo, OCDE, CEPAL, Banco Mundial, ONU y otros marcos de referencia utilizados en el informe), así como literatura técnica sobre gobierno digital, gobernanza de datos, ciberseguridad, identidad digital, interoperabilidad y regulación de tecnologías emergentes. Esta instancia permitió identificar dimensiones recurrentes de madurez en gobernanza digital —liderazgo político, coherencia institucional, infraestructura digital, gestión de datos, confianza, capacidades humanas y evaluación— y traducirlas en una estructura operativa de análisis comparable entre países.

Con base en la arquitectura conceptual, se desarrolló un relevamiento exhaustivo de fuentes primarias por país, priorizando **documentación oficial** y normativa vigente. El relevamiento incluyó, entre otros:

- **Leyes, decretos, reglamentos, resoluciones y directrices** vinculadas con las dimensiones del estudio (protección de datos personales, ciberseguridad, identidad digital, interoperabilidad, acceso a la información, etc.).
- **Estrategias nacionales, agendas digitales, planes de modernización y programas de gobierno** asociados a la transformación digital del Estado, la economía digital y la innovación pública.
- **Instrumentos e institucionalidad sectorial** (autoridades regulatorias de telecomunicaciones, agencias digitales, organismos de protección de datos, unidades de ciberseguridad y CERT/CSIRT, entre otros).
- **Comunicados institucionales, hojas de ruta, documentos de implementación y portales oficiales**, utilizados para complementar la identificación de mecanismos

operativos (por ejemplo, plataformas de interoperabilidad, portales únicos de servicios, sistemas de identidad y firma digital).

Esta fase tuvo como resultado la identificación de marcos integrales y desarrollos parciales o fragmentarios, así como el registro del estado de actualización normativa y el grado de formalización institucional por dimensión.

Para contextualizar comparativamente algunos componentes del ecosistema digital —sin sustituir el relevamiento normativo e institucional— se integraron **índices internacionales** y métricas estandarizadas (por ejemplo, indicadores de gobierno digital, conectividad, datos abiertos e inteligencia artificial utilizados en el informe). Estos insumos se utilizaron como referencia complementaria para interpretar brechas, patrones regionales y niveles relativos de desempeño, y para enriquecer la lectura comparada de dimensiones específicas como conectividad, apertura de datos y gobernanza de IA.

De manera complementaria, se aplicó un proceso de **validación y curaduría normativa** que incluyó: verificación de fuentes oficiales, control de fechas de actualización, depuración de duplicados, identificación de instrumentos derogados o en revisión legislativa y contraste entre documentos de política y su base legal habilitante. Asimismo, se incorporaron observaciones cualitativas cuando un instrumento formaba parte de un ecosistema normativo más amplio (por ejemplo, la articulación entre estrategias de transformación digital y marcos de protección de datos o ciberseguridad). Este procedimiento buscó asegurar **trazabilidad**, **consistencia** y **calidad documental** del repositorio.

Sistematización en repositorio normativo y matrices comparativas

Sobre la base del relevamiento y la curaduría, se conformó un **repositorio normativo sistematizado** que reúne los principales instrumentos legales, regulatorios y de política pública vinculados con la gobernanza digital en cada país, acompañados por referencias y enlaces de acceso. Este repositorio constituye la base empírica del estudio y habilita la comparación estructurada.

A partir de dicho repositorio se elaboró una **matriz general y comparativa** que sintetiza los principales elementos de la gobernanza digital de los 22 países. La matriz organiza la información conforme a la arquitectura conceptual previamente desarrollada, estructurada en tres grandes bloques analíticos que permiten ordenar el relevamiento de manera jerárquica y funcional.

En esta instancia metodológica, los bloques no se abordan como categorías descriptivas —ya desarrolladas en el marco conceptual— sino como **unidades operativas de sistematización**, que orientan la clasificación de la evidencia normativa e institucional relevada. De este modo, como señalamos previamente, el Bloque 1 concentra los instrumentos estratégicos y marcos rectores que estructuran la visión país y la rectoría institucional; el Bloque 2 agrupa las capacidades habilitadoras que sostienen la viabilidad técnica, jurídica y organizacional del ecosistema digital; y el Bloque 3 releva la materialización operativa de dichas definiciones en términos de servicios, acceso y ejercicio efectivo de derechos.

La matriz general permite así traducir una arquitectura conceptual compleja en una herramienta comparativa homogénea, garantizando consistencia entre países y evitando abordajes fragmentarios por dimensión aislada. Cada celda de la matriz se construyó a partir del repositorio normativo validado, incorporando referencias a la normativa principal vigente y una caracterización sintética del grado de desarrollo relativo en cada componente. Esta estructura constituye el insumo central del análisis comparado y asegura trazabilidad entre fuentes, clasificación analítica y narrativa posterior.

Asimismo, para asegurar una comprensión integral del fenómeno, el estudio incorporó además **dos instrumentos complementarios**:

1. una **matriz específica de Gobernanza de Internet**, concebida como módulo transversal para relevar de manera integrada componentes regulatorios, institucionales y multiactor del ecosistema Internet (telecomunicaciones, neutralidad de red, administración de recursos críticos, coordinación y protección de derechos en línea); y
2. un **anexo específico sobre mecanismos de acceso a la información pública**, que sistematiza los canales digitales disponibles en cada país para el ejercicio efectivo de este derecho, complementando el análisis normativo con una aproximación operativa a los dispositivos institucionales y tecnológicos existentes.

Descripción de dimensiones analizadas

Bloque 1. Gobernanza Estratégica y Marcos Rectores.

Este bloque reúne los instrumentos que estructuran la visión estratégica del país en materia digital y definen la arquitectura superior de gobernanza del ecosistema tecnológico. Su inclusión responde a la necesidad de identificar si los Estados cuentan con una orientación explícita, coherente y de largo plazo para conducir la transformación digital, o si, por el contrario, esta se desarrolla de manera fragmentada y reactiva. En este nivel se observan las decisiones fundacionales: cómo se conceptualiza el desarrollo digital, qué prioridades se establecen, qué institucionalidad ejerce la rectoría y bajo qué principios se ordena la acción pública.

1. Estrategias/Agendas Digitales

Las Estrategias y/o Agendas Digitales constituyen el marco político y programático mediante el cual un país orienta el desarrollo, adopción y uso de las tecnologías digitales en toda la economía y la sociedad. Su propósito es articular una visión de largo plazo que abarque múltiples dimensiones: conectividad e infraestructura, economía digital, inclusión y habilidades, innovación, datos, inteligencia artificial, ciberseguridad y, entre ellas, también la digitalización del sector público.

En términos conceptuales, una estrategia digital nacional trasciende el gobierno digital, al definir cómo la digitalización contribuye al desarrollo socioeconómico del país en su conjunto. Estas estrategias integrales suelen establecer:

- principios rectores para el ecosistema digital,

- prioridades multisectoriales,
- metas nacionales en materia de infraestructura, talento, innovación y transformación productiva,
- lineamientos para la gobernanza del entorno digital, y
- mecanismos de articulación entre Estado, sector privado, academia y sociedad civil.

Su función principal es coordinar esfuerzos dispersos, ordenar inversiones, dar previsibilidad regulatoria y asegurar que los beneficios de la digitalización sean amplios e inclusivos. Estas estrategias cumplen un rol de política pública transversal, orientada no solo al funcionamiento del Estado, sino también al desarrollo económico, la competitividad, la inclusión social y la gobernanza de Internet.

2. Transformación Digital del Estado

La Transformación Digital del Estado (TDE) se presenta en Iberoamérica como un proceso estratégico esencial para modernizar la gestión pública y redefinir la relación entre el Estado y la ciudadanía. Esta categoría se refiere específicamente a los instrumentos políticos y normativos que orientan el uso estratégico de las tecnologías digitales para modernizar el Estado, mejorar la gestión pública y crear valor público con foco en las personas[51]. A diferencia de iniciativas aisladas de digitalización del gobierno o de los servicios públicos, la TDE implica una visión sistémica e integrada que busca transformar estructuras, prácticas y capacidades del sector público a largo plazo.

Desde esta perspectiva, la transformación digital del Estado no se limita a la informatización de procedimientos, sino que constituye un proceso estructural que involucra cambios en la cultura organizacional, en los métodos de trabajo y en los procesos administrativos, así como la adopción de infraestructuras y plataformas digitales que permitan ofrecer servicios más eficientes, seguros y centrados en las necesidades reales de la ciudadanía[52]. Es un marco de política pública transversal, cuya finalidad es transformar el funcionamiento del Estado en sentido amplio, incluyendo: i) visión estratégica; ii) gobernanza institucional; iii) arquitectura digital del Estado; iv) infraestructura habilitadora; competencias de los equipos públicos; v) innovación pública.

3. Gobernanza de Internet

La gobernanza de Internet constituye un componente estructural de la arquitectura digital de los Estados contemporáneos. Se refiere al conjunto de principios, normas, políticas, instituciones y procesos mediante los cuales se gobierna el funcionamiento, la evolución y el uso de Internet, asegurando que opere como una infraestructura estable, segura, abierta, interoperable y accesible, al tiempo que se protegen los derechos de las personas usuarias y se coordinan los intereses de los múltiples actores involucrados.

[51] Naser, A. (Coord.). (2021). Gobernanza digital e interoperabilidad gubernamental: una guía para su implementación (LC/TS.2021/80). CEPAL.
[52] Cubo, A., Hernández Carrión, J. L., Porrúa, M., & Roseth, B. (2022). Guía de transformación digital del gobierno. Banco Interamericano de Desarrollo.

Su alcance trasciende el accionar exclusivo del Estado y se organiza como un ecosistema multiactor, en el que participan organismos públicos, empresas privadas, la comunidad técnica, el sector académico y la sociedad civil, con roles y responsabilidades diferenciadas en ámbitos como la infraestructura de redes, la regulación económica, la protección de derechos, la seguridad digital y la gestión de recursos críticos.

En el contexto iberoamericano, la gobernanza de Internet comprende un conjunto amplio y heterogéneo de dimensiones, que incluyen, entre otras:

- la gestión y regulación del espectro radioeléctrico y de las infraestructuras de telecomunicaciones;
- los marcos de competencia y regulación de los operadores de servicios de conectividad;
- el reconocimiento y la implementación de principios como la neutralidad de la red y los estándares de calidad del servicio;
- la resiliencia, seguridad y continuidad operativa de las redes y servicios digitales;
- la administración de dominios y otros recursos críticos de Internet;
- la promoción del acceso a Internet como habilitador de derechos digitales;
- la existencia de mecanismos de participación y coordinación multiactor en los procesos de definición y toma de decisiones.

4. Gobernanza en Inteligencia Artificial (IA)

En este estudio, la gobernanza en inteligencia artificial (IA) se entiende como el conjunto de normas, regulaciones, políticas públicas y arreglos institucionales que orientan el desarrollo, despliegue y uso de la IA, con el objetivo de maximizar sus beneficios económicos y sociales, al tiempo que se gestionan sus riesgos, se protegen los derechos fundamentales y se promueve un uso ético, transparente y responsable de esta tecnología.

Bajo esta definición, la gobernanza en IA no se limita a la regulación estricta de los sistemas algorítmicos, sino que comprende un marco más amplio de dirección estratégica, coordinación institucional y alineamiento normativo, que permite integrar la IA en las agendas nacionales de desarrollo, innovación y transformación digital. Este enfoque reconoce que la gobernanza de la IA debe garantizar, de manera simultánea, la promoción de la innovación, la justicia y la no discriminación, la rendición de cuentas y el acceso equitativo a los beneficios derivados de su adopción

En coherencia con este enfoque, el presente análisis adopta como referencia los resultados del Índice Latinoamericano de Inteligencia Artificial (ILIA) 2025, elaborado por el Centro Nacional de Inteligencia Artificial (CENIA) de Chile. La elección de esta fuente responde a que su concepción de gobernanza en IA se encuentra alineada con una visión integral y multidimensional, en la que la orientación estratégica del Estado, la inserción internacional y los marcos regulatorios constituyen pilares centrales del ecosistema de IA.

En su versión 2025, la gobernanza en IA representa una de las tres grandes dimensiones que integran el ILIA[53], lo que refleja el reconocimiento de que la adopción de la IA no es un proceso

[53] Las tres grandes dimensiones que integran el índice son : i) Factores Habilitantes; ii). Investigación, Desarrollo y Adopción; iii) Gobernanza.

meramente tecnológico, sino un fenómeno profundamente institucional y político. Metodológicamente, la matriz registra para los países incluidos en el ILIA el puntaje de la subdimensión de Gobernanza expresado en un índice base 100 y que se integra en partes iguales por tres subdimensiones:

i. Visión y estrategia en inteligencia artificial. Evalúa la capacidad de los Estados para definir una orientación clara respecto del desarrollo y uso de la IA, articulando objetivos económicos, sociales y tecnológicos en una narrativa coherente de largo plazo.

ii. Vinculación internacional en inteligencia artificial. Se asocia con el carácter transnacional de la gobernanza en IA y con la necesidad de articular marcos normativos, principios éticos y estándares comunes más allá de las fronteras nacionales. Esta dimensión captura el grado en que los países participan en foros multilaterales, iniciativas regionales y espacios globales de discusión sobre IA, así como su adhesión a principios internacionales relacionados con la transparencia, la no discriminación, la protección de derechos y la responsabilidad algorítmica.

iii. Regulación de la inteligencia artificial. Analiza la existencia y el alcance de leyes, proyectos normativos y marcos regulatorios que inciden sobre el desarrollo y uso de sistemas de IA. El enfoque adoptado reconoce la diversidad de trayectorias regulatorias en la región y contempla tanto regulaciones específicas de IA como marcos transversales —por ejemplo, protección de datos personales, derechos digitales, transparencia y responsabilidad— que operan como salvaguardas frente a los riesgos asociados a la tecnología.

Bloque 2. Capacidades Habilitadoras

El segundo bloque se concentra en las capacidades estructurales que hacen posible la implementación efectiva de las estrategias definidas en el nivel superior. Mientras que el primer bloque define el rumbo, este bloque examina si existen las condiciones técnicas, regulatorias e institucionales necesarias para sostenerlo. Se trata de infraestructuras, estándares y mecanismos transversales que garantizan que el ecosistema digital funcione de manera segura, confiable e interoperable.

5. Gobernanza de datos, protección de datos personales, interoperabilidad y datos abiertos

Esta categoría integra un conjunto de dimensiones interdependientes del ecosistema de datos, que incluyen la gobernanza de datos, la protección de datos personales, la interoperabilidad de sistemas y la apertura de datos públicos. En los países iberoamericanos, estos componentes suelen encontrarse regulados de manera conjunta o articulada a través de marcos normativos y políticas complementarias, lo que justifica su análisis integrado dentro de una misma dimensión. Este enfoque permite ofrecer una visión sistémica de cómo los Estados conciben, gestionan y ponen en valor el dato como un activo estratégico y como un bien público digital.

Desde una perspectiva conceptual, la gobernanza de datos se refiere al conjunto de políticas, estándares, reglas y responsabilidades que regulan la gestión de los datos a lo largo de todo su ciclo de vida, garantizando su calidad, integridad, disponibilidad, seguridad y uso estratégico para la toma de decisiones públicas [54] [55] [56]. En este marco, la protección de datos personales constituye un componente central, al establecer salvaguardas para la privacidad, la seguridad de la información y la confianza ciudadana en el uso de servicios digitales y en el tratamiento de datos por parte del Estado[57] [58]. A su vez, la interoperabilidad se configura como una condición habilitante de la gobernanza de datos, en tanto permite el intercambio seguro y eficiente de información entre sistemas y organismos públicos, evitando silos de información y mejorando la calidad de los servicios digitales.

Por su parte, los datos abiertos representan una dimensión complementaria pero analíticamente diferenciable dentro del ecosistema de datos. Se entienden como un bien público digital orientado a promover la transparencia, la rendición de cuentas, la participación ciudadana y la innovación, a través de la publicación proactiva de información gubernamental en formatos abiertos y reutilizables [59]. Si bien la apertura de datos se apoya en capacidades de gobernanza, calidad e interoperabilidad, su lógica principal se vincula con el acceso público, la reutilización y el impacto externo de los datos, lo que justifica su tratamiento específico dentro de la matriz comparativa.

Desde el punto de vista metodológico, la matriz identifica para cada uno de los 22 países analizados el estado de desarrollo de los marcos normativos, estratégicos e institucionales asociados a estas dimensiones. En particular, se releva la existencia de:

- leyes de protección de datos personales o marcos de privacidad, ya sean generales, sectoriales o transversales;
- políticas, estrategias o lineamientos de gobernanza de datos e interoperabilidad, incluyendo modelos organizacionales y disposiciones para la gestión y el intercambio de datos en el sector público;
- leyes, políticas o estrategias de datos abiertos, así como la existencia de portales nacionales formalmente establecidos para su publicación y reutilización.

[54] DAMA International. (2017). DAMA International's Guide to the Data Management Body of Knowledge (DAMA-DMBOK2) (2nd ed.). Technics Publications.
[55] Ladley, J. (2019). Data Governance: How to Design, Deploy and Sustain an Effective Data Governance Program (2nd ed.). Elsevier Science – Academic Press.
[56] Cabello, (2022). El camino de desarrollo de las ciudades inteligentes: una evaluación de Bogotá, Buenos Aires, Ciudad de México y São Paulo (LC/TS.2022/86). CEPAL. https://www.cepal.org/es/publicaciones/48000-camino-desarrollo-ciudades-inteligentes-evaluacionbogota-buenos-aires-ciudad
[57] Cubo, A., Hernández Carrión, J. L., Porrúa, M., & Roseth, B. (2022). Guía de transformación digital del gobierno. Banco Interamericano de Desarrollo.
[58] OECD/CAF. (2024). Revisión del Gobierno Digital en América Latina y el Caribe: Construyendo servicios públicos inclusivos y responsivos. OECD Publishing. https://doi.org/10.1787/7a127615-es
[59] Cabello, (2022). El camino de desarrollo de las ciudades inteligentes: una evaluación de Bogotá, Buenos Aires, Ciudad de México y São Paulo (LC/TS.2022/86). CEPAL. https://www.cepal.org/es/publicaciones/48000-camino-desarrollo-ciudades-inteligentes-evaluacionbogota-buenos-aires-ciudad

Cuando no se identifican marcos integrales, se consignan iniciativas parciales, tales como decretos, lineamientos administrativos o documentos programáticos que avanzan de manera fragmentaria en la regulación, gestión o apertura de la información pública.

Adicionalmente, el análisis de la dimensión de datos abiertos se complementa con el Open Data Inventory (ODIN), elaborado por Open Data Watch[60]. Este índice internacional evalúa la disponibilidad, cobertura y nivel de apertura de los datos estadísticos oficiales que publican los países, a partir de un conjunto estandarizado de indicadores sociales, económicos y ambientales. ODIN mide tanto la existencia y desagregación de los datos (cobertura) como su accesibilidad y reutilización conforme a los principios de datos abiertos (apertura), permitiendo realizar comparaciones internacionales y dar seguimiento a los avances en materia de transparencia y uso de datos para el desarrollo.

6.Ciberseguridad / Seguridad Digital

La ciberseguridad constituye una dimensión fundamental de la gobernanza digital, en tanto se orienta a garantizar la confianza, la resiliencia y la continuidad del funcionamiento del entorno digital sobre el cual se apoyan los servicios públicos, la actividad económica y el ejercicio de derechos en la sociedad contemporánea. Desde una perspectiva conceptual, refiere al conjunto de enfoques, principios y mecanismos destinados a prevenir, gestionar y mitigar riesgos y amenazas que afectan a los sistemas de información, las redes, los servicios digitales y los datos, tanto del Estado como de los distintos actores que interactúan en el ecosistema digital[61] [62].

En este sentido, la ciberseguridad abarca dimensiones técnicas, organizacionales y normativas orientadas a proteger los activos digitales frente a accesos no autorizados, usos indebidos, alteraciones, interrupciones o capturas de información. Su objetivo es salvaguardar atributos clave como la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de los sistemas y datos, así como reducir impactos potenciales sobre la prestación de servicios, la seguridad nacional y los derechos de las personas usuarias. Complementariamente, la seguridad de la información pone el acento en la protección de los datos y en la continuidad operativa de las organizaciones, reforzando la dimensión de derechos y confianza en el uso de tecnologías digitales[63] [64].

[60] El Open Data Inventory (ODIN) es un índice global que evalúa qué tan abiertos y utilizables son los datos estadísticos oficiales que publican los países. Fue desarrollado por Open Data Watch (ODW) y es ampliamente utilizado por organismos multilaterales (Banco Mundial, BID, ONU, etc.) como referencia para diagnosticar madurez en datos abiertos y capacidades estadísticas.
[61] Lara, J. C. (2024). Ciberseguridad en América Latina: Estrategias nacionales en 2024. Derechos Digitales.
[62] Cubo, A., Hernández Carrión, J. L., Porrúa, M., & Roseth, B. (2022). Guía de transformación digital del gobierno. Banco Interamericano de Desarrollo.
[63] LAC4 – Latin America and Caribbean Cyber Competence Centre. (2023). Evolution of cybersecurity in Latin America and the Caribbean: Secure horizons in the digital ecosystem.
[64] Cubo, A., Hernández Carrión, J. L., Porrúa, M., & Roseth, B. (2022). Guía de transformación digital del gobierno. Banco Interamericano de Desarrollo.

7. Infraestructuras Digitales Críticas (IDC)

Las Infraestructuras Digitales Críticas (IDC) comprenden el conjunto de sistemas, redes, plataformas, servicios y activos tecnológicos cuya operación resulta indispensable para asegurar la continuidad de las funciones esenciales del Estado, así como la seguridad, el bienestar social y el funcionamiento económico de un país. Estas infraestructuras sostienen servicios vitales —tales como salud, energía, transporte, telecomunicaciones, finanzas y servicios públicos digitales— y su interrupción, degradación o compromiso puede generar impactos significativos a nivel social, económico, institucional y democrático[65] [66].

Desde una perspectiva conceptual, la protección de las IDC se inscribe en un enfoque de resiliencia sistémica, orientado a garantizar la disponibilidad, confiabilidad y continuidad de servicios esenciales frente a amenazas de diversa naturaleza, tanto físicas como digitales. En este sentido, las IDC constituyen un ámbito especializado y estratégico dentro de la gobernanza de la ciberseguridad, pero trascienden el plano puramente técnico al involucrar decisiones de política pública vinculadas con la gestión del riesgo, la seguridad nacional, la continuidad del Estado y la protección de derechos fundamentales.

La gobernanza de las infraestructuras digitales críticas implica, por lo tanto, la identificación y clasificación de activos críticos, la definición de responsabilidades y obligaciones para los distintos actores involucrados —públicos y privados—, y la adopción de mecanismos de prevención, protección, monitoreo y respuesta ante incidentes. Este enfoque reconoce que una parte sustantiva de las infraestructuras críticas se encuentra en manos de operadores privados, lo que refuerza la necesidad de esquemas de coordinación público-privada, marcos regulatorios claros y capacidades institucionales especializadas.

8. Identidad Digital

La Identidad Digital (ID) se entiende, en el ámbito de la acción estatal, como la representación electrónica de la identidad legal de una persona, que permite su identificación y autenticación en entornos digitales con pleno reconocimiento de derechos y obligaciones. Se sustenta en un conjunto de atributos, datos y credenciales que posibilitan una identificación inequívoca, segura y confiable, habilitando la realización de trámites, transacciones y el acceso a servicios públicos digitales [67] [68] [69].

La implementación de la identidad digital se articula, en general, a través de un Sistema de Identificación Digital (SID), concebido como una infraestructura pública digital que integra

[65] Cubo, A., Hernández Carrión, J. L., Porrúa, M., & Roseth, B. (2022). Guía de transformación digital del gobierno. Banco Interamericano de Desarrollo.
[66] Lara, J. C. (2024). Ciberseguridad en América Latina: Estrategias nacionales en 2024. Derechos Digitales.
[67] World Bank. (2018). G20 Digital Identity Onboarding. https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf
[68] CFATF GAFIC. (2021). ¿Qué es la Identidad Digital (ID)? Mesa de Investigación de la Secretaría del GAFIC. https://www.cfatf-gafic.org/home-test/documentos-en-espanol/rinc%C3%B3n-de-investigaciones/17082-%C2%BFqu%C3%A9-es-la-identidad-digital-id-_nov_2021/file
[69] Palma, I., & Rojas, A. (2024). Prácticas de identificación digital para el acceso a servicios de gobierno en Iberoamérica. Secretaría General Iberoamericana (SEGIB) & Centro Latinoamericano de Administración para el Desarrollo (CLAD).

dimensiones tecnológicas, jurídicas y organizacionales. Este sistema organiza los procesos de registro, verificación y autenticación de identidades bajo estándares elevados de seguridad, privacidad e interoperabilidad, y opera a través de canales digitales regulados por políticas, lineamientos y marcos normativos oficiales[70]. En este sentido, la identidad digital no constituye únicamente una solución tecnológica, sino un arreglo institucional complejo que requiere gobernanza, reglas claras y capacidades estatales sostenidas.

Como infraestructura habilitante, un SID de carácter universal, único e inequívoco constituye un pilar central de la administración pública digital. Su existencia permite avanzar hacia servicios públicos digitales más accesibles, personalizados, interoperables y seguros, contribuyendo a la eficiencia del Estado, a la reducción de costos administrativos y al fortalecimiento de la confianza ciudadana en los entornos digitales[71] [72]. Al mismo tiempo, la identidad digital cumple un rol clave en la inclusión digital, en la medida en que facilita el acceso efectivo a derechos, prestaciones y servicios, siempre que su diseño contemple criterios de equidad, accesibilidad y protección de datos personales.

Desde una perspectiva de gobernanza digital, la identidad digital se vincula estrechamente con otras dimensiones del ecosistema, como la protección de datos personales, la interoperabilidad de sistemas, la ciberseguridad y la provisión de servicios públicos digitales. Su adecuada implementación requiere definir con claridad las responsabilidades institucionales, los mecanismos de control y supervisión, y los equilibrios entre eficiencia, seguridad y respeto por los derechos fundamentales, en particular la privacidad y la autodeterminación informativa.

En el plano comparado, los países presentan trayectorias heterogéneas en el desarrollo de sistemas de identidad digital, que van desde marcos jurídicos y plataformas consolidadas de alcance nacional, hasta iniciativas parciales o componentes aislados —como firmas electrónicas o mecanismos de autenticación específicos— integrados de manera incipiente en las estrategias de transformación digital del Estado. El análisis de esta dimensión permite, así, caracterizar los distintos niveles de madurez institucional y comprender el rol de la identidad digital como condición habilitante clave para la digitalización del Estado y el ejercicio efectivo de derechos en el entorno digital.

Bloque 3. Implementación, Servicios y Acceso

El tercer bloque analiza la dimensión más tangible de la gobernanza digital: aquella que se expresa en la interacción cotidiana entre el Estado y la ciudadanía. Aquí se observa cómo las definiciones estratégicas y las capacidades habilitadoras se traducen en resultados concretos en términos de servicios digitales, acceso efectivo, transparencia y garantía de derechos. Este nivel permite pasar del diseño institucional a la experiencia real de uso.

[70] Ídem.
[71] World Bank. (2018). G20 Digital Identity Onboarding. https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf
[72] Secretaría General Iberoamericana [SEGIB]. (2023). Carta Iberoamericana de Principios y Derechos en los Entornos Digitales. XXVIII Cumbre Iberoamericana.

9. Gobierno digital (servicios públicos digitales y Interoperabilidad de sistemas)

El Gobierno Digital (GD) se concibe como el uso estratégico e integral de las tecnologías digitales para transformar las estructuras, procesos y modos de acción del Estado, con el objetivo de crear valor público, mejorar la eficiencia institucional, fortalecer la transparencia y promover una relación más abierta y participativa con la ciudadanía[73] [74]. Este enfoque trasciende la mera digitalización de trámites y supone un cambio estructural en la gestión pública, que redefine la forma en que el Estado diseña políticas, organiza sus servicios y responde a las demandas sociales.

En este marco, los Servicios Públicos Digitales (SPD) representan la expresión operativa y visible del gobierno digital, al materializarse en las prestaciones, trámites y gestiones que la ciudadanía puede realizar a través de plataformas digitales. Su desarrollo permite avanzar hacia servicios más accesibles, inclusivos y centrados en las personas, mejorando la experiencia de uso, reduciendo cargas administrativas y optimizando los tiempos y costos de interacción entre el Estado y la sociedad [75] [76]. Asimismo, los servicios públicos digitales constituyen un canal clave para el ejercicio efectivo de derechos y el acceso equitativo a políticas públicas en el entorno digital.

La interoperabilidad de sistemas, por su parte, se entiende como la capacidad de los sistemas, plataformas y procesos de información de intercambiar datos y compartir información de manera segura, estandarizada y continua, posibilitando la integración funcional entre organismos públicos y, en determinados casos, con actores externos relevantes [77] [78]. Lejos de ser un componente accesorio, la interoperabilidad constituye una condición habilitante esencial para la provisión de servicios públicos digitales integrados, la simplificación de trámites, la eliminación de silos de información y la coordinación interinstitucional.

Desde una perspectiva sistémica, el gobierno digital, los servicios públicos digitales y la interoperabilidad conforman un conjunto estrechamente interrelacionado. Mientras el gobierno digital define la visión y los principios de transformación del Estado, los servicios públicos digitales materializan esa visión en la experiencia cotidiana de la ciudadanía, y la interoperabilidad proporciona la infraestructura organizativa y técnica necesaria para que

---

[73] Organisation for Economic Co-operation and Development (OCDE). (2014). Recommendation of the Council on Digital Government Strategies (OECD/LEGAL/0406). Recuperado de https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406

[74] Cubo, A., Hernández Carrión, J. L., Porrúa, M., & Roseth, B. (2022). Guía de transformación digital del gobierno. Banco Interamericano de Desarrollo.

[75] Roseth, B., Reyes, A., & Santiso, C. (Eds.). (2018). El fin del trámite eterno: Ciudadanos, burocracia y gobierno digital. Banco Interamericano de Desarrollo [BID]

[76] Cont, W., Romero, C., Lleras, G., Unda, R., Celani, M., Gartner, A., Capelli, L., Zipitria, L., Besfamille, B., Figueroa, N., López Azurmendi, S., & Fisher, R. (2021). IDEAL 2021: El impacto de la digitalización para reducir brechas y mejorar los servicios de infraestructura. CAF. https://scioteca.caf.com/handle/123456789/1762

[77] Cubo, A., Hernández Carrión, J. L., Porrúa, M., & Roseth, B. (2022). Guía de transformación digital del gobierno. Banco Interamericano de Desarrollo.

[78] Palma, I., & Rojas, A. (2024). Prácticas de identificación digital para el acceso a servicios de gobierno en Iberoamérica. Secretaría General Iberoamericana (SEGIB) & Centro Latinoamericano de Administración para el Desarrollo (CLAD).

dicha experiencia sea coherente, eficiente y sostenible en el tiempo. El análisis conjunto de estas dimensiones permite comprender cómo los Estados avanzan en la digitalización de la gestión pública y en la construcción de administraciones más ágiles, integradas y orientadas al valor público.

Además, a fin de contextualizar comparativamente el grado de madurez del gobierno digital en los países analizados, el estudio tomó en consideración el Índice de Desarrollo del Gobierno Electrónico (EGDI)[79] elaborado por Naciones Unidas, reconocido como la principal métrica internacional en la materia. El EGDI ofrece una visión integral del ecosistema digital estatal al combinar información sobre la oferta de servicios públicos digitales, las condiciones de infraestructura de telecomunicaciones y las capacidades de la población para utilizarlos, permitiendo captar tanto los esfuerzos de digitalización del Estado como los factores estructurales que condicionan su adopción y sostenibilidad. En este marco, los resultados más recientes disponibles (EGDI 2024) fueron utilizados como insumo complementario de análisis, aportando una referencia comparativa regional que enriquece la lectura de las trayectorias nacionales sin sustituir el relevamiento normativo e institucional desarrollado en la matriz. El detalle del ranking de los 22 países de Iberoamérica, junto con su agrupamiento por niveles de desarrollo, se presenta en el Anexo 2, con el objetivo de facilitar la interpretación de brechas, patrones regionales y desafíos estructurales asociados a la transformación digital del Estado.

10. Conectividad y acceso a internet

Esta dimensión permite evaluar en qué medida los países garantizan el acceso efectivo de la ciudadanía al entorno digital. El análisis se focaliza, por un lado, en la identificación de disposiciones legales o normativas que reconocen explícitamente el acceso a Internet como un derecho de la ciudadanía o como una obligación del Estado y, por otro, en la utilización de indicadores internacionales de acceso a Internet y de conectividad, que permiten medir el grado de penetración, cobertura y disponibilidad de la infraestructura digital.

La distinción entre Conectividad y Acceso a Internet obedece a razones metodológicas claras. Mientras que Acceso a Internet —derivado de datos del Banco Mundial y la UIT— mide el porcentaje de personas que efectivamente utilizan Internet, Conectividad captura la calidad estructural y el desempeño técnico de la red. De este modo, Acceso refleja un nivel de adopción poblacional, mientras que Conectividad representa la capacidad del país para soportar servicios digitales de mayor complejidad, diferenciando entre países con infraestructura robusta y aquellos con limitaciones que afectan la provisión de servicios públicos digitales.

Este enfoque combinado posibilita vincular el reconocimiento normativo del acceso con su materialización efectiva en términos de conectividad y uso por parte de la población, sin relevar políticas ni instrumentos específicos de implementación.

[79] https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index

11. Indicador de acceso a internet

La categoría de **Acceso a Internet** se basa en el indicador internacional “Individuos que utilizan Internet (% de la población)”, elaborado por la UIT y difundido por el Banco Mundial. Este indicador mide el porcentaje de personas que han utilizado Internet en los últimos tres meses desde cualquier dispositivo, captando el acceso efectivo de la población al entorno digital. Su definición incluye el uso de computadoras, teléfonos móviles, consolas, televisores inteligentes y otros dispositivos conectados, ofreciendo una visión amplia y comparada del acceso individual a Internet.

La utilización de la base de datos de la UIT garantiza la comparabilidad internacional, ya que los datos se recopilan mediante cuestionarios estandarizados enviados anualmente a reguladores de telecomunicaciones, ministerios sectoriales y oficinas de estadística. Tras su armonización, la UIT publica series temporales ampliamente utilizadas para monitorear la brecha digital, evaluar el desarrollo de la sociedad de la información y orientar políticas de inclusión digital en todo el mundo.

En la matriz elaborada para este estudio, se registra para cada uno de los 22 países el dato más reciente disponible del porcentaje de individuos que utilizan Internet. Se incorporó exclusivamente este indicador debido a su solidez metodológica y su consistencia estadística, sin ajustes ni estimaciones adicionales. Cuando no existían datos recientes en la base del Banco Mundial, se consignó el último valor disponible, y en los casos con ausencia total de información, la matriz lo deja explícitamente identificado, garantizando transparencia y comparabilidad en la dimensión de acceso.

12. Indicador de Conectividad

El indicador de **Conectividad** se define en este mapeo según la metodología del Índice Latinoamericano de Inteligencia Artificial (ILIA) 2025, como parte de su subdimensión de Infraestructura. Este indicador evalúa las condiciones técnicas de acceso a Internet —incluyendo velocidad de descarga móvil, cobertura de redes móviles y suscripciones activas de banda ancha móvil— que actúan como proxies de la capacidad real de la población para utilizar servicios digitales avanzados, incluidos aquellos basados en inteligencia artificial. En conjunto, estos componentes permiten medir la calidad efectiva de la infraestructura digital disponible en cada país.

En la matriz elaborada para este estudio, la columna de Indicador de Conectividad registra el puntaje del ILIA 2025 para cada uno de los 22 países, expresado en una escala base 100. Para los países no incluidos en el ILIA —Andorra, España y Portugal— se recurrió a fuentes oficiales y públicas que permiten aproximar sus condiciones de conectividad siguiendo criterios equivalentes de medición. La matriz incorpora únicamente valores finales comparables, evitando estimaciones que pudieran afectar la consistencia metodológica, y asegurando así una lectura homogénea del desempeño regional en materia de infraestructura digital.

Caracterización de la gobernanza digital por país

En conjunto, el repositorio normativo y las tres herramientas de sistematización construidas —matriz general, matriz específica de Gobernanza de Internet y anexo de acceso a la información— constituyen la infraestructura analítica que permite elaborar perfiles nacionales consistentes, comparables y metodológicamente trazables. La arquitectura por bloques y dimensiones opera como criterio común de lectura, asegurando que cada país sea analizado bajo los mismos parámetros conceptuales y estructurales. Esta estandarización metodológica es la que habilita una caracterización sistemática de los modelos de gobernanza digital, evitando sesgos descriptivos o abordajes fragmentarios.

De este modo, la presente sección no introduce información adicional distinta de la contenida en las matrices, sino que traduce y articula esa evidencia en un formato narrativo que permite comprender de manera integrada la configuración institucional de cada país. La combinación entre repositorio normativo, matrices comparativas y síntesis nacional asegura trazabilidad, coherencia conceptual y comparabilidad regional, pilares fundamentales para el análisis posterior y la formulación de recomendaciones de política pública.

Andorra

El ecosistema de gobernanza digital de Andorra se caracteriza por un diseño institucional compacto, altamente centralizado y estratégicamente orientado, coherente con la escala territorial y administrativa del país. La arquitectura general muestra un patrón de planificación de largo plazo con fuerte alineación a estándares europeos, una implementación progresiva basada en programas plurianuales y una lógica de integración sistémica entre innovación, digitalización estatal y desarrollo económico. En conjunto, el modelo presenta altos niveles de coherencia vertical entre visión estratégica, instrumentos de ejecución y plataformas operativas, aunque con ciertas lagunas regulatorias específicas en áreas emergentes y en marcos normativos sectoriales que aún no se encuentran plenamente desarrollados.

En el nivel de marcos estratégicos, Andorra dispone de una Estrategia de Transformación Digital con horizonte 2030 implementada mediante ciclos trienales, actualmente el período 2024–2027, cuyo objetivo es consolidar un Estado digital avanzado mediante digitalización administrativa, transformación empresarial y fortalecimiento de capacidades ciudadanas, incorporando interoperabilidad, identidad digital y adopción tecnológica bajo un enfoque centrado en derechos y bienestar social. Esta visión se articula con la Estrategia Nacional de Innovación y Emprendimiento 2021–2030, que funciona como estrategia país de modernización, impulsa el uso de datos, servicios públicos digitales e infraestructura tecnológica e introduce instrumentos de innovación regulatoria y experimental como sandbox y living lab dentro de un modelo de gobernanza de cuádruple hélice. En gobernanza de Internet, el país presenta un esquema sectorial centralizado sin ley específica integral, en el cual la regulación se estructura a través de la legislación de telecomunicaciones y un modelo de operador único público que concentra infraestructura y provisión de servicios, configurando un sistema altamente integrado pero con limitada explicitación normativa de principios de gobernanza. En inteligencia artificial, el país carece de legislación específica, aunque adoptó en 2024 un Código Ético de IA que orienta el desarrollo responsable en sectores público y

privado mediante principios de derechos humanos, transparencia e inclusión, integrando la adopción tecnológica dentro de su estrategia general de transformación digital.

En materia de capacidades habilitadoras, Andorra cuenta con un marco robusto de protección de datos personales establecido por la Llei 29/2021, alineada con estándares internacionales, que regula derechos, obligaciones, seguridad, decisiones automatizadas y transferencias internacionales bajo supervisión de la autoridad nacional, complementado por lineamientos estratégicos que reconocen al dato como activo público e impulsan plataformas de interoperabilidad y economía del dato. En datos abiertos, el país no posee política nacional integral ni portal centralizado, aunque dispone de estadísticas oficiales de calidad técnica y un desempeño intermedio según ODIN con 59 sobre 100, evidenciando avances en formatos y metadatos pero debilidades en cobertura y licenciamiento, además de una inserción internacional limitada en iniciativas globales de datos abiertos. En ciberseguridad, la Estrategia Nacional 2024–2027 introduce medidas para fortalecer resiliencia, gobernanza y obligaciones de seguridad, promueve el uso de inteligencia artificial para detección de amenazas y proyecta un sistema de cumplimiento por niveles de madurez institucional hacia 2029, buscando consolidar capacidades nacionales especializadas. En infraestructuras digitales críticas, no existe aún un marco jurídico específico ni catálogo oficial, por lo que la protección se sustenta principalmente en orientaciones estratégicas y capacidades operativas de organismos técnicos, lo que revela un desarrollo institucional incipiente en esta dimensión.

En el plano de implementación y acceso, el país presenta avances tangibles que reflejan la traducción operativa de su estrategia digital. El gobierno digital se apoya en un modelo de interoperabilidad en consolidación centrado en el Interoperability Bus, plataforma nacional de intercambio seguro de datos presentada en 2025 que habilita comunicaciones trazables entre administraciones y sector privado bajo el principio de solo una vez, institucionalizado mediante acuerdos interadministrativos y respaldado por marcos jurídicos de protección de datos y validez documental. En identidad digital, Andorra dispone de un sistema sólido basado en firma electrónica regulada, credencial oficial integrada al registro civil y una cartera digital nacional en fase final de despliegue que permitirá autenticación robusta y gestión móvil de credenciales, consolidando un esquema unificado para ciudadanía y empresas. En conectividad, el país muestra un desempeño sobresaliente con cobertura casi total de fibra óptica, velocidades superiores a 180 Mbps y cobertura móvil prácticamente universal, resultado de una infraestructura moderna gestionada por un operador público único que garantiza acceso homogéneo incluso en condiciones geográficas complejas. En transparencia y acceso a la información pública, el derecho se ejerce mediante plataformas digitales centralizadas como el portal de transparencia, la plataforma de trámites y el boletín oficial digital, configurando un sistema formalizado y operativo. En conjunto, el modelo andorrano evidencia un alto grado de alineación entre estrategia, capacidades y resultados, sustentado en centralización institucional, infraestructura avanzada y planificación de largo plazo, aunque con desafíos pendientes en el desarrollo de marcos regulatorios específicos en áreas clave de la gobernanza digital.

Argentina

El esquema de gobernanza digital de Argentina se caracteriza por una arquitectura institucional y normativa de densidad media alta, estructurada en torno a instrumentos estratégicos, marcos regulatorios sectoriales y plataformas operativas que, en conjunto,

configuran un ecosistema funcional y relativamente consolidado, aunque con desafíos de actualización, integración normativa y homogeneización entre políticas. El país muestra un patrón consistente en la construcción de capacidades digitales desde el Estado, con avances relevantes en institucionalidad, interoperabilidad y provisión de servicios, coexistiendo con vacíos regulatorios específicos y discontinuidades estratégicas que inciden sobre la sostenibilidad de algunas iniciativas.

En el plano de los marcos estratégicos de alto nivel, Argentina cuenta con la Agenda Digital Argentina aprobada por el Decreto 996/2018 como principal instrumento rector, que define objetivos amplios en conectividad, infraestructura, inclusión, regulación, modernización estatal y desarrollo productivo digital, además de establecer un sistema de gobernanza con instancias de planificación, coordinación interministerial y monitoreo que ordena la transformación digital del sector público. La gobernanza de Internet se apoya en un enfoque normativo sectorial cuyo eje es la Ley 27.078, que reconoce a Internet como servicio público esencial y consagra principios como acceso universal, neutralidad de red, privacidad e interconexión justa, bajo rectoría regulatoria del ENACOM y con participación multiactor mediante espacios formales e informales de diálogo. En inteligencia artificial, el país presenta un nivel avanzado según ILIA 2025, con puntajes altos en visión institucional y coordinación interorganismos, sustentados en la existencia de lineamientos éticos de 2023, mecanismos de transparencia algorítmica y órganos especializados, aunque la falta de actualización del Plan Nacional de IA de 2019 introduce una limitación estructural para la continuidad estratégica.

En cuanto a las capacidades habilitadoras, el país dispone de un andamiaje normativo relativamente robusto en gobernanza de datos sustentado en la Ley 25.326 de Protección de Datos Personales, complementada por normativa de datos abiertos, lineamientos de interoperabilidad y políticas de gobierno digital que reconocen al dato como activo público, aun sin contar con una estrategia nacional integral específica. En datos abiertos, el desempeño es intermedio según ODIN 2024 2025 con 59 sobre 100, destacándose la cobertura por sobre la apertura y evidenciándose avances institucionales acompañados de debilidades en licenciamiento y reutilización. En ciberseguridad, la Segunda Estrategia Nacional de 2023 y el Plan Federal 2025 2027 establecen un marco integral de protección de infraestructuras críticas, coordinación federal y gestión de incidentes mediante institucionalidad especializada y CERT.ar. En infraestructuras digitales críticas no existe una ley integral ni un catálogo oficial unificado, pero sí un esquema operativo en consolidación basado en la estrategia de ciberseguridad y en obligaciones sectoriales en áreas estratégicas. En identidad digital, el país presenta un sistema sólido sustentado en el RENAPER, el DNI biométrico, la firma digital con validez jurídica y plataformas de autenticación como AutenticAR y Mi Argentina, que permiten interoperabilidad segura entre servicios públicos y privados.

En el nivel de implementación, servicios y acceso, Argentina evidencia un grado significativo de operacionalización de su agenda digital. El gobierno digital se apoya en estándares técnicos de interoperabilidad vigentes y en sistemas transversales como GDE, TAD y SADE que integran trámites y documentos digitales bajo principios de seguridad y minimización de datos. En conectividad, el país muestra indicadores sólidos, con cobertura de banda ancha fija del 70,4 por ciento, velocidades promedio de 93,4 Mbps y desempeño superior al promedio regional en infraestructura y cobertura móvil, en un marco regulatorio que reconoce

a Internet como servicio esencial y establece obligaciones estatales de acceso universal. En transparencia y acceso a la información pública, el derecho se ejerce mediante un ecosistema digital institucionalizado articulado alrededor del portal nacional gestionado por la AAIP, complementado por portales de transparencia activa y datos abiertos conforme a la Ley 27.275. En conjunto, estos elementos muestran que la estrategia y las capacidades habilitadoras se traducen en mecanismos concretos de prestación de servicios, acceso a información y ejercicio de derechos en el entorno digital, configurando un modelo con bases institucionales sólidas pero aún en proceso de integración normativa plena y actualización estratégica.

Bolivia

El sistema de gobernanza digital de Bolivia presenta una configuración en transición, caracterizada por la coexistencia de instrumentos estratégicos formales con capacidades institucionales y regulatorias aún en consolidación. El país dispone de lineamientos nacionales claros que establecen una dirección estratégica hacia la digitalización estatal y el desarrollo tecnológico, pero la arquitectura general revela asimetrías entre planificación, desarrollo normativo y despliegue operativo. Este patrón evidencia un modelo de construcción progresiva en el que la voluntad estratégica se encuentra más avanzada que la institucionalización integral de los marcos regulatorios y técnicos necesarios para sostener una gobernanza digital plenamente articulada.

En el plano estratégico, Bolivia cuenta con un marco explícito estructurado principalmente en la Agenda Digital 2030 y el Plan Estratégico de Gobierno Electrónico 2018–2025, que operan conjuntamente como estrategia nacional de transformación digital orientada a modernizar el Estado mediante el uso soberano de TIC, con ejes en conectividad, gobierno digital, economía digital y gobernanza digital. La transformación digital se concibe como política de Estado con metas medibles vinculadas a simplificación administrativa, interoperabilidad, masificación de identidad y firma digital, fortalecimiento de ciberseguridad y modernización de infraestructura tecnológica, además de impulsar adopción tecnológica en sectores públicos clave mediante plataformas integradas y automatización de procesos. En gobernanza de Internet, el país se apoya en la Ley 164 de telecomunicaciones y en la institucionalidad liderada por AGETIC y ATT, configurando un esquema sectorial sin normativa integral específica y con vacíos relevantes como la ausencia de neutralidad de red explícita, de ley de protección de datos personales y de régimen robusto de acceso a la información pública, junto con participación multiactor incipiente y no institucionalizada. En inteligencia artificial, Bolivia se ubica en una fase inicial según ILIA 2025, con puntajes bajos y clasificación de explorador, sin estrategia nacional, institucionalidad especializada ni mecanismos formales de gobernanza, aunque con iniciativas regulatorias en elaboración que indican un estadio embrionario de desarrollo.

En materia de capacidades habilitadoras, el país dispone de bases parciales que permiten cierto funcionamiento del ecosistema digital pero sin consolidar un marco sistémico integral. La gestión de datos se apoya en la Ley 164 y en principios constitucionales que respaldan el acceso a la información y el intercambio de datos entre entidades públicas, aunque Bolivia carece de ley de protección de datos personales y de una estrategia nacional de gobernanza de datos, lo que genera vacíos en estándares de calidad, arquitectura y ciclo de vida del dato; existe un anteproyecto legislativo pendiente que refleja un proceso de construcción normativa

aún inconcluso. En datos abiertos, el desempeño es intermedio según ODIN 2024 2025 con 59 sobre 100, destacándose la cobertura estadística por sobre la apertura, con fortalezas en estadísticas sectoriales y debilidades en licenciamiento, finanzas públicas y claridad de uso, además de una inserción internacional limitada en iniciativas globales. En ciberseguridad, el país presenta avances institucionales y se encuentra elaborando una estrategia nacional, pero el marco regulatorio sigue fragmentado y sin régimen integral que articule estándares, protección de infraestructuras críticas y legislación penal amplia, lo que reduce la resiliencia frente a amenazas digitales. En infraestructuras digitales críticas no existe un marco jurídico ni técnico específico, ni identificación formal de activos críticos, por lo que la protección se produce de manera implícita a través de funciones de organismos técnicos y regulaciones sectoriales, configurando un sistema operativo pero no institucionalizado.

En el nivel de implementación y acceso, Bolivia muestra avances normativos y programáticos acompañados de limitaciones estructurales en infraestructura y despliegue. El gobierno digital se sustenta en planes vigentes que establecen la obligación de interoperabilidad estatal mediante plataformas centralizadas administradas por AGETIC y basadas en estándares abiertos, integrando registros públicos, simplificación de trámites y planificación estatal dentro del modelo de gobierno soberano, aunque su implementación práctica aún se encuentra en consolidación. En identidad digital, el país dispone de una base sólida de identificación física y biométrica sustentada en el SEGIP y en normativa de firma digital, pero el desarrollo de una identidad digital nacional integral aún está en proceso y no cuenta con estrategia formal equivalente a la de países más avanzados. En conectividad, el acceso a Internet está reconocido legalmente como parte del principio de acceso universal a telecomunicaciones, pero los indicadores muestran infraestructura limitada y bajos niveles relativos de cobertura y calidad, evidenciando un ecosistema de conectividad incipiente con desafíos significativos. En transparencia y acceso a la información pública, el derecho está reconocido constitucionalmente y mediante decreto, pero el país carece de una ley integral operativa, existiendo solo proyectos legislativos en trámite, lo que restringe la institucionalización efectiva del acceso digital a la información. En conjunto, el modelo boliviano refleja una gobernanza digital en fase de consolidación estructural, con planificación estratégica definida y avances institucionales relevantes, pero aún condicionada por brechas regulatorias, tecnológicas y de capacidad que limitan la traducción plena de la estrategia en resultados operativos sostenidos.

Brasil

El modelo de gobernanza digital de Brasil se distingue por un alto grado de institucionalización normativa, densidad estratégica y capacidad operativa, configurando uno de los ecosistemas más consolidados y coherentes de la región. La arquitectura general presenta una articulación robusta entre planificación de largo plazo, marcos regulatorios integrales y plataformas tecnológicas funcionales, lo que evidencia un patrón de madurez sistémica en el que la estrategia, la institucionalidad y la implementación operan de manera coordinada. Este nivel de consolidación se refleja en la existencia de políticas digitales con jerarquía normativa, órganos formales de coordinación interministerial y mecanismos de gobernanza multiactor que aseguran continuidad estratégica y alineación entre niveles de gobierno.

En el plano de los marcos estratégicos, Brasil cuenta con una Estrategia Brasileña para la Transformación Digital institucionalizada por decreto que actúa como eje estructurante de la

política digital nacional, organizada en ejes habilitadores y de transformación orientados a expandir acceso tecnológico, innovación, confianza digital, capacitación y proyección internacional, así como a digitalizar la economía, el gobierno y la ciudadanía. La coordinación de alto nivel se canaliza mediante el Comité Interministerial para la Transformación Digital, que integra ministerios clave y la Casa Civil, consolidando una gobernanza estratégica centralizada pero articulada. La transformación digital del Estado se sustenta en la Ley 14.129 de 2021, que establece principios obligatorios para la digitalización del sector público, interoperabilidad, participación ciudadana y gobierno como plataforma, complementada por la Estrategia Nacional de Gobierno Digital 2024–2027 y por instrumentos operativos que orientan a los distintos niveles federativos a alinear sus políticas. En gobernanza de Internet, el país presenta uno de los marcos más avanzados de la región, estructurado en torno al Marco Civil da Internet que consagra principios como neutralidad de red, privacidad, libertad de expresión y responsabilidad de intermediarios, junto con el CGI.br como órgano multiactor institucionalizado que coordina el desarrollo del ecosistema. En inteligencia artificial, Brasil se posiciona como país pionero según ILIA 2025, con altos puntajes en institucionalidad, participación social y estrategia nacional, sustentados en estructuras interinstitucionales, sistemas de reporte estadístico avanzados y un plan público de fomento tecnológico de gran escala.

En cuanto a las capacidades habilitadoras, Brasil dispone de uno de los marcos más completos de la región en gobernanza de datos, basado en la LGPD y supervisado por la Autoridade Nacional de Proteção de Dados, que regula el tratamiento de información en sectores público y privado y establece obligaciones de responsabilidad proactiva. Este sistema se complementa con el Modelo Federal de Gobernanza y Compartición de Datos y con instancias rectoras que definen estándares de interoperabilidad, calidad y seguridad, integradas a la estrategia nacional de gobierno digital, lo que configura un esquema integral de gestión del dato. En datos abiertos, el país exhibe alto nivel de madurez con 69 sobre 100 en ODIN 2024 2025 y liderazgo regional, sustentado en un marco legal completo, portal nacional consolidado y amplia disponibilidad de datos reutilizables, aunque persisten desafíos en uniformidad de licencias. En ciberseguridad, la Estrategia Nacional E Ciber 2025 consolida un modelo avanzado con gobernanza centralizada, certificaciones, niveles de madurez, gestión de riesgos, protección de infraestructuras críticas y uso de tecnologías emergentes, articulado mediante un entramado normativo sectorial que cubre derechos digitales, seguridad de la información y regulación del entorno digital. En infraestructuras críticas, el país cuenta con una política nacional formal que establece definiciones, instrumentos y sistemas de gestión, complementada por medidas específicas dentro de la estrategia de ciberseguridad que incluyen monitoreo de riesgos, alertas, estándares mínimos y mecanismos de resiliencia, lo que configura un régimen integral y estructurado.

En el nivel de implementación, servicios y acceso, Brasil evidencia un alto grado de materialización de su estrategia digital. El gobierno digital se apoya en la arquitectura ePING, que fija estándares técnicos obligatorios para interoperabilidad en todos los organismos federales y define especificaciones en interconexión, seguridad, intercambio de información y accesibilidad, operando dentro de un modelo federado pero normativamente unificado. En identidad digital, el país posee uno de los sistemas más avanzados de la región basado en el CPF como identificador único, la Identificación Civil Nacional y la plataforma gov.br, que integran autenticación, biometría y verificación de datos en un punto único de acceso a servicios públicos digitales. En conectividad, Brasil presenta indicadores líderes regionales

con altos niveles de cobertura móvil, penetración de banda ancha y adopción de 5G, lo que refleja una infraestructura robusta y madura. En transparencia y acceso a la información pública, el derecho se ejerce principalmente mediante plataformas digitales centralizadas como Fala.BR y el Portal da Transparência, complementadas por portales institucionales y catálogos de datos abiertos, evidenciando un elevado grado de estandarización y digitalización de los mecanismos de acceso. En conjunto, el caso brasileño muestra un ecosistema de gobernanza digital consolidado, caracterizado por coherencia normativa, institucionalidad robusta, infraestructura avanzada y una capacidad sostenida de implementación que posiciona al país entre los referentes regionales en materia digital.

Chile

El sistema de gobernanza digital de Chile presenta un alto nivel de madurez institucional y coherencia estructural, caracterizado por la integración consistente entre planificación estratégica, marcos regulatorios vinculantes y plataformas operativas consolidadas. El país exhibe un modelo en el que la digitalización se concibe como política pública estructural y no únicamente como modernización administrativa, lo que se refleja en una arquitectura normativa densa, rectoría técnica especializada y mecanismos de implementación obligatorios que aseguran continuidad y alineación entre niveles institucionales. Este diseño produce un ecosistema digital con elevada estabilidad normativa, fuerte orientación a derechos y una capacidad sostenida de ejecución estatal.

En el plano de los marcos estratégicos, Chile cuenta con la Estrategia de Gobierno Digital 2030, que define la construcción de un Estado digital integrado, confiable y centrado en las personas mediante principios de digitalización por diseño, interoperabilidad, uso del dato como activo estratégico y enfoque de una sola vez, junto con un esquema institucional liderado por la Secretaría de Gobierno Digital que coordina capacidades, inversión y talento. La transformación digital estatal se encuentra jurídicamente respaldada por la Ley 21.180 de 2019, que establece la digitalización obligatoria de procedimientos administrativos, expediente electrónico, firma digital, interoperabilidad, archivo electrónico y neutralidad tecnológica, con implementación gradual hasta 2027. En gobernanza de Internet, el país presenta un modelo normativamente estructurado basado en legislación sectorial y capacidades regulatorias consolidadas, incluyendo la Ley General de Telecomunicaciones y la consagración explícita de la neutralidad de red, junto con rectoría técnica especializada que articula la relación digital entre Estado y ciudadanía. En inteligencia artificial, Chile se posiciona como país pionero según ILIA 2025, con altos puntajes en visión estratégica e institucionalidad sustentados en una Política Nacional de IA vigente y en proceso de actualización, mecanismos avanzados de transparencia algorítmica y un proyecto legislativo con enfoque de riesgo orientado a protección de derechos y seguridad.

En materia de capacidades habilitadoras, Chile dispone de un marco integral y articulado de gobernanza de datos sustentado en la Ley 21.180, que establece interoperabilidad obligatoria, estándares técnicos y requisitos de seguridad e integridad para plataformas estatales, complementado por normativa técnica y por una política nacional de datos abiertos que obliga a publicar información reutilizable. La protección de datos personales se rige por la Ley 19.628, que regula tratamiento y derechos en sectores público y privado, integrándose al ecosistema institucional de gobierno digital y ciberseguridad. En datos abiertos, el país

presenta alto nivel de madurez con 67 sobre 100 en ODIN 2024 2025, destacándose en cobertura estadística y disponibilidad de datos reutilizables, sustentado en un marco legal completo, portal nacional y adhesión a estándares internacionales, aunque persisten desafíos en cobertura subnacional y uniformidad de licencias. En ciberseguridad, la Política Nacional 2023–2028 y la Ley 21.663 de 2024 establecen un sistema integral obligatorio que define servicios esenciales, estándares mínimos, reportes de incidentes, certificaciones y fiscalización, creando además la Agencia Nacional de Ciberseguridad como autoridad especializada. En infraestructuras digitales críticas, esta misma ley establece definiciones formales, obligaciones estrictas para operadores críticos y mecanismos de supervisión coordinados con capacidades operativas del CSIRT y regulaciones sectoriales, configurando un régimen robusto y estructurado.

En el plano de implementación y acceso, Chile evidencia un alto grado de traducción operativa de su estrategia digital. El gobierno digital se sustenta en un marco jurídicamente vinculante que obliga a los organismos a intercambiar información mediante estándares abiertos y expedientes electrónicos interoperables, lo que asegura coherencia técnica y organizacional del ecosistema estatal. En identidad digital, el país cuenta con un sistema consolidado basado en ClaveÚnica, respaldado por normativa de firma electrónica y por la obligación legal de autenticación digital en trámites públicos, con el Registro Civil como autoridad de identidad y validaciones biométricas integradas. En conectividad, el acceso a Internet ha sido reconocido legalmente como servicio público de telecomunicaciones y el país presenta indicadores sobresalientes de infraestructura, velocidades y adopción tecnológica, posicionándose entre los líderes regionales y con expansión avanzada de redes 5G. En transparencia y acceso a la información pública, el ejercicio del derecho se realiza predominantemente mediante plataformas digitales centralizadas que integran solicitudes, publicación proactiva y mecanismos de reclamo en línea, complementadas por portales de datos abiertos que facilitan acceso directo y reutilizable a la información estatal. En conjunto, el caso chileno refleja un ecosistema de gobernanza digital altamente institucionalizado, con fuerte coherencia entre estrategia, regulación e implementación, y con capacidad sostenida para traducir sus políticas digitales en resultados operativos y en garantías efectivas para la ciudadanía en el entorno digital.

Colombia

El sistema de gobernanza digital de Colombia presenta un grado elevado de institucionalización estratégica y articulación intersectorial, sustentado en una arquitectura de políticas públicas integradas al sistema formal de planificación estatal. El modelo colombiano se distingue por su coherencia estructural, basada en la utilización de instrumentos de política nacional como los documentos CONPES y los planes de desarrollo para fijar prioridades digitales, lo que otorga estabilidad, continuidad y capacidad de coordinación a la agenda digital. Este diseño genera un ecosistema en el que la estrategia digital no opera como un programa aislado, sino como un componente transversal de la política pública nacional, con capacidad de incidir simultáneamente en competitividad, innovación, inclusión, servicios públicos y desarrollo económico.

En el plano de los marcos estratégicos, Colombia articula su estrategia digital a través de un conjunto integrado de instrumentos de planificación nacional que funcionan de manera equivalente a una estrategia digital formal, destacándose la Política Nacional para la

Transformación Digital e Inteligencia Artificial (CONPES 3975 de 2019), que establece lineamientos para interoperabilidad, infraestructura digital, arquitectura empresarial del Estado, apertura de datos y servicios digitales centrados en el ciudadano. La rectoría institucional recae en el Ministerio de Tecnologías de la Información y las Comunicaciones, respaldado por legislación sectorial que define su rol como autoridad de política TIC, mientras que la regulación del entorno de conectividad corresponde a la Comisión de Regulación de Comunicaciones, con reconocimiento explícito de la neutralidad de la red. En gobernanza de Internet, el país presenta un esquema relativamente consolidado basado en marcos normativos sectoriales coordinados y no en una ley única integral, pero con principios y capacidades regulatorias claramente establecidos. En inteligencia artificial, Colombia se ubica en un nivel avanzado según ILIA 2025, con altos puntajes en gobernanza derivados de una política nacional específica, un marco ético adoptado en 2021 y una hoja de ruta 2024 orientada a gobernanza, educación, investigación, innovación y protección de derechos, lo que evidencia una institucionalidad en expansión y con orientación estratégica definida.

En materia de capacidades habilitadoras, Colombia dispone de un sistema sólido y estructurado de gobernanza de datos sustentado en el CONPES 3975, que reconoce el dato como activo estratégico y establece lineamientos para su ciclo de vida, interoperabilidad, calidad y uso analítico, complementado por manuales técnicos y estándares operativos desarrollados por MinTIC. El régimen de protección de datos personales es completo y vigente, y se articula con el marco de acceso a la información pública que consolida la apertura de datos como obligación estatal. En datos abiertos, el país presenta alto nivel de desarrollo con 67 sobre 100 en ODIN 2024 2025 y liderazgo regional, sustentado en un marco legal completo, portal nacional, estrategia de datos e inserción activa en iniciativas internacionales, aunque con desafíos en licenciamiento uniforme y cobertura subnacional. En ciberseguridad, Colombia cuenta con una arquitectura institucional consolidada basada en documentos estratégicos y en la Estrategia Nacional 2024–2030, que prioriza protección de infraestructuras críticas, coordinación interinstitucional, cultura de seguridad y cooperación internacional, aunque carece de una ley integral única, lo que implica que el principal desafío reside en traducir la estrategia en capacidades operativas homogéneas. En infraestructuras digitales críticas, el país dispone de lineamientos estratégicos y bases conceptuales establecidas en documentos de política nacional que incorporan acciones específicas para fortalecer resiliencia y gestión de riesgos, configurando un marco relevante aunque todavía en proceso de consolidación normativa plena.

En el plano de implementación, servicios y acceso, Colombia muestra avances significativos en la materialización de su estrategia digital mediante instrumentos normativos y plataformas operativas que estructuran el funcionamiento del ecosistema estatal. El gobierno digital se apoya en uno de los marcos de interoperabilidad más desarrollados de la región, sustentado en normativa que define el intercambio seguro y estandarizado de información como obligación institucional, incorporando dimensiones técnicas, semánticas, organizacionales y de seguridad, junto con estándares, APIs, arquitecturas empresariales y catálogos de datos comunes. En identidad digital, el país ha desarrollado un sistema moderno basado en la cédula digital multibiométrica y en la política nacional de identidad digital, que habilita autenticación segura y acceso a servicios ciudadanos digitales, aunque su despliegue aún se encuentra en fase de expansión y con debates jurídicos sobre su regulación. En conectividad, el acceso a Internet está reconocido legalmente como servicio público esencial y universal, y el país presenta niveles adecuados de infraestructura con alta cobertura móvil y avances en

despliegue de 5G, aunque con velocidades fijas moderadas. En transparencia y acceso a la información pública, el derecho se ejerce dentro de un marco normativo robusto que integra apertura, protección de datos y mecanismos institucionales de supervisión, evidenciando una estructura formal consolidada para el acceso digital a la información estatal. En conjunto, el caso colombiano refleja un modelo de gobernanza digital estructuralmente sólido, con fuerte anclaje institucional, instrumentos estratégicos integrados y una capacidad significativa de implementación, aunque aún enfrenta retos en homogeneización regulatoria y consolidación operativa de algunos componentes críticos.

Cuba

El sistema de gobernanza digital de Cuba se caracteriza por un modelo altamente centralizado y de implementación gradual, estructurado en torno a la rectoría estatal directa sobre el desarrollo tecnológico y la informatización de la sociedad. La arquitectura institucional muestra una orientación programática más que normativa integral, en la que la digitalización se inserta dentro de la estrategia general de actualización del modelo económico y social, con avances progresivos en servicios digitales y modernización administrativa pero con limitaciones estructurales en apertura, conectividad y participación multiactor. Este diseño configura un ecosistema donde la dirección estratégica es clara y concentrada, aunque la consolidación de capacidades y resultados depende de procesos incrementales y de la disponibilidad de infraestructura tecnológica.

En el plano de los marcos estratégicos, la digitalización se articula a través de la Política Integral para el Perfeccionamiento de la Informatización de la Sociedad y del Programa Rector de la Informatización, liderados por el Ministerio de Comunicaciones, que funcionan como eje rector del gobierno digital sin adoptar la forma de una estrategia única con horizonte temporal definido. Este enfoque programático prioriza el desarrollo progresivo desde presencia digital hacia transacción y transformación, promoviendo portales unificados, servicios en línea, plataformas de pago y fortalecimiento de la cultura digital institucional y ciudadana. La transformación digital estatal se vincula además al Objetivo General 10 del programa gubernamental 2024–2026, que establece acciones para digitalizar procesos, ampliar servicios, mejorar interoperabilidad y desarrollar capacidades tecnológicas, complementado por la Agenda Digital de Cuba y la estrategia nacional de inteligencia artificial. En gobernanza de Internet, el modelo se sustenta en la Constitución de 2019, que reconoce el rol rector del Estado en el desarrollo tecnológico, y en normativa sectorial como el Decreto Ley 35 de 2021, que regula telecomunicaciones, redes y responsabilidades de usuarios y proveedores bajo supervisión centralizada del MINCOM. En inteligencia artificial, Cuba se ubica en un nivel intermedio según ILIA 2025, con una estrategia nacional formal adoptada pero no actualizada, institucionalidad concentrada en un solo organismo y ausencia de legislación específica, lo que evidencia avances iniciales combinados con limitaciones estructurales de gobernanza.

En materia de capacidades habilitadoras, el país cuenta con instrumentos relevantes aunque con un grado de desarrollo heterogéneo. La Ley 149 de 2022 establece un marco moderno de protección de datos personales que regula derechos, obligaciones y transferencias, y la política nacional de informatización integra lineamientos sobre interoperabilidad, estandarización, infraestructura y ciberseguridad, aunque no existe una estrategia nacional explícita de gobernanza de datos ni una política integral de datos abiertos. En esta última dimensión, Cuba presenta un nivel bajo de madurez con 45 sobre 100 en ODIN 2024 2025,

reflejando disponibilidad parcial de estadísticas pero escasa apertura y reutilización, ausencia de portal nacional y limitaciones institucionales para la publicación de datos, además de una inserción internacional reducida en iniciativas de datos abiertos. En ciberseguridad, el Decreto 360 de 2019 establece el marco para la protección del ciberespacio y de la infraestructura tecnológica nacional, mientras que en infraestructuras digitales críticas el marco jurídico reconoce la existencia de sistemas esenciales y establece obligaciones para su protección mediante normas de informatización y estrategias nacionales, aunque sin una ley integral específica ni un régimen detallado de obligaciones regulatorias.

En el plano de implementación y acceso, Cuba presenta avances operativos acotados y condicionados por restricciones estructurales. El gobierno digital se desarrolla dentro del proceso general de informatización estatal y del despliegue progresivo de infraestructuras digitales, sin un marco nacional formal de interoperabilidad comparable con otros países, lo que limita la integración sistémica de plataformas. En identidad digital, el país dispone de una base técnica sólida sustentada en el registro poblacional y en el carné de identidad modernizado con biometría y elementos de seguridad, complementada por normativa sobre firma digital y documentos electrónicos que habilita futuros sistemas de autenticación digital. En conectividad, el acceso a Internet se regula como servicio de telecomunicaciones bajo control estatal y el país presenta indicadores muy bajos de infraestructura, con limitada penetración, velocidades reducidas y cobertura inferior al promedio regional, lo que constituye uno de los principales condicionantes del ecosistema digital. En transparencia y acceso a la información pública, la ausencia de una ley general y de mecanismos institucionalizados de participación limita la formalización de este derecho, que se canaliza principalmente mediante portales oficiales definidos por la administración pública. En conjunto, el caso cubano refleja un modelo de gobernanza digital con dirección estratégica centralizada y marcos normativos relevantes en áreas específicas, pero con desarrollo operativo desigual y desafíos significativos en infraestructura, apertura informacional y consolidación institucional que condicionan la evolución del ecosistema digital.

Ecuador

El sistema de gobernanza digital de Ecuador presenta una arquitectura institucional y normativa en consolidación, caracterizada por un enfoque estructurado principalmente a través de instrumentos legales y políticas públicas antes que por una estrategia única integral. El modelo evidencia una base normativa relativamente robusta que articula derechos digitales, modernización estatal y desarrollo tecnológico, aunque con heterogeneidad en niveles de madurez entre dimensiones y con desafíos asociados a la coordinación estratégica y a la consolidación institucional. Este patrón configura un ecosistema donde el marco jurídico funciona como eje ordenador del proceso de digitalización, mientras la planificación estratégica evoluciona de forma progresiva mediante políticas sectoriales y planes nacionales.

En el plano de los marcos estratégicos, la gobernanza digital ecuatoriana se sustenta en un conjunto de leyes que constituyen el núcleo regulatorio del ecosistema, destacándose la Ley Orgánica de Gobierno Digital de 2023, la Ley Orgánica de Protección de Datos Personales de 2021 y la Ley Orgánica de Ciberseguridad de 2023, complementadas por planes de gobierno electrónico y políticas de gobierno abierto. La Política Pública para la Transformación Digital 2025–2030 define la hoja de ruta nacional para modernizar el Estado

mediante conectividad, talento digital, servicios públicos digitales, economía digital, innovación tecnológica y seguridad digital, incorporando interoperabilidad, identidad digital, simplificación administrativa y uso de inteligencia artificial. En gobernanza de Internet, el país presenta un modelo respaldado constitucionalmente que reconoce el acceso a las TIC y el derecho a la información, bajo rectoría del Ministerio de Telecomunicaciones y de la Sociedad de la Información, lo que otorga una base jurídica sólida para el ejercicio de derechos digitales. En inteligencia artificial, Ecuador se ubica en una fase incipiente según ILIA 2025, con avances regulatorios relevantes derivados de marcos legales existentes pero sin estrategia nacional ni institucionalidad específica, lo que refleja un desarrollo asimétrico donde el componente normativo progresa más rápido que la planificación estratégica.

En materia de capacidades habilitadoras, Ecuador dispone de un marco funcional de gobernanza de datos sustentado en la ley de protección de datos personales y en políticas de transformación digital que establecen lineamientos para interoperabilidad, seguridad de la información y gestión estratégica del dato, complementados por normas técnicas y estándares de intercambio de información. Aunque no existe una estrategia única dedicada exclusivamente a gobernanza de datos, el conjunto de instrumentos vigentes configura un sistema operativo relativamente completo. En datos abiertos, el país presenta un nivel medio alto con 65 sobre 100 en ODIN 2024 2025, destacándose en apertura más que en cobertura y respaldado por portal nacional, catálogo de datos y marco legal integral, además de participación en iniciativas internacionales, aunque con desafíos en cobertura subnacional y continuidad institucional. En ciberseguridad, Ecuador cuenta con legislación específica y con una estrategia nacional reciente que reconoce la alta vulnerabilidad del país y establece acciones para fortalecer gobernanza, gestión de riesgos, capacidades técnicas, cooperación internacional y protección de infraestructuras críticas, incorporando institucionalidad especializada y mecanismos de coordinación. En infraestructuras digitales críticas, el país dispone de lineamientos estratégicos que reconocen formalmente activos esenciales y asignan responsabilidades de protección, aunque aún carece de una ley específica y de un catálogo oficial, lo que sitúa el marco en una fase principalmente programática.

En el plano de implementación y acceso, Ecuador evidencia avances concretos que reflejan la traducción progresiva de su marco normativo en mecanismos operativos. El gobierno digital se sustenta en una política pública obligatoria de interoperabilidad establecida por decreto y desarrollada mediante normas técnicas que definen estándares, arquitectura de servicios, buses de integración y catálogos de intercambio de información, reforzada por políticas recientes de transformación digital y por la legislación de transparencia que habilita el intercambio institucional de datos. En identidad digital, el país avanza hacia un modelo unificado basado en la cédula electrónica biométrica y en infraestructura de firma electrónica, integradas progresivamente a servicios públicos digitales y respaldadas por bases de datos civiles centralizadas. En conectividad, el acceso a Internet se regula como servicio público de telecomunicaciones con principios de universalidad, continuidad y calidad, y el país presenta niveles moderados de infraestructura con mejoras aceleradas en velocidad móvil, despliegue de 5G y expansión de cobertura. En transparencia y acceso a la información pública, el derecho se ejerce mediante un esquema digital mixto que combina portales centralizados, plataformas institucionales descentralizadas y mecanismos en línea de solicitud, sustentado en obligaciones legales de publicación de información estatal. En conjunto, el caso ecuatoriano refleja un modelo de gobernanza digital en fase de consolidación institucional, con bases normativas sólidas, avances operativos visibles y una trayectoria de fortalecimiento

progresivo, aunque todavía condicionado por desafíos de coordinación estratégica y homogeneización de capacidades a nivel sistémico.

El Salvador

El ecosistema de gobernanza digital de El Salvador presenta un modelo de desarrollo institucional en expansión, caracterizado por una fuerte centralización estratégica y una rápida producción normativa reciente orientada a modernizar la administración pública mediante tecnologías digitales. El país muestra un patrón de consolidación acelerada en el nivel regulatorio y programático, impulsado desde el Poder Ejecutivo, que convive con brechas operativas y estructurales en infraestructura, datos y capacidades sistémicas. Esta configuración refleja un proceso de transición desde un esquema de digitalización inicial hacia un modelo más integral de gobernanza digital, en el que la arquitectura normativa avanza con mayor velocidad que la madurez del ecosistema tecnológico y administrativo.

En el plano de los marcos estratégicos, El Salvador cuenta con la Agenda Digital Nacional 2020–2030 como instrumento rector que define prioridades en interoperabilidad, servicios digitales, datos, innovación pública y modernización estatal, complementada por la Ley General para la Modernización Digital del Estado aprobada en 2023, que establece obligaciones legales para la digitalización administrativa, el uso de datos abiertos, la interoperabilidad institucional y la creación de plataformas digitales, otorgando al Ejecutivo facultades amplias de coordinación e implementación. La transformación digital se concibe como una política integral orientada a desmaterialización documental, firma electrónica, registros digitales y portales únicos de servicios con autenticación unificada, con el objetivo de mejorar la eficiencia, transparencia y calidad de servicios. En gobernanza de Internet, el modelo se estructura en torno a una rectoría centralizada liderada por la Secretaría de Innovación de la Presidencia y un marco sectorial de telecomunicaciones regulado por SIGET, sin una ley específica integral de gobernanza de Internet. En inteligencia artificial, el país se ubica en una etapa incipiente según ILIA 2025, aunque registra avances relevantes con la aprobación en 2025 de una ley específica que crea la Agencia Nacional de Inteligencia Artificial, estableciendo una base institucional formal para el desarrollo de políticas en esta materia.

En materia de capacidades habilitadoras, El Salvador dispone de un marco actualizado de protección de datos personales aprobado en 2024 que regula derechos, obligaciones y supervisión, complementado por la legislación de acceso a la información pública que establece principios de publicidad, calidad y disponibilidad de datos. El país cuenta con instrumentos de interoperabilidad y políticas digitales que incorporan lineamientos sobre gestión y uso del dato, aunque no posee una estrategia nacional autónoma de gobernanza de datos y el sistema depende en gran medida de la articulación institucional liderada por la Secretaría de Innovación. En datos abiertos, el desempeño es bajo con 32 sobre 100 en ODIN 2024 2025, reflejando cobertura limitada, escasa reutilización y fragmentación institucional, pese a la existencia de un marco legal completo y adhesión a estándares internacionales. En ciberseguridad, el país dispone de legislación penal especializada para delitos informáticos, pero carece de una estrategia nacional integral actualizada, lo que evidencia una brecha significativa en planificación estratégica de seguridad digital. En infraestructuras digitales críticas, no existe un régimen legal integral, aunque la normativa penal reconoce y protege sistemas tecnológicos esenciales vinculados a servicios públicos y sectores estratégicos,

configurando un esquema de protección parcial basado en tipificación de conductas más que en regulación preventiva.

En el plano de implementación y acceso, El Salvador evidencia avances iniciales con resultados heterogéneos. El gobierno digital se sustenta en lineamientos de interoperabilidad establecidos en la política nacional de transformación digital y en la legislación de acceso a la información pública que promueve estandarización y disponibilidad de datos, aunque la plataforma de interoperabilidad estatal se encuentra aún en fase incipiente y con baja integración sistémica. En identidad digital, el país ha desarrollado un ecosistema emergente basado en la plataforma del Registro Nacional de las Personas Naturales y en el Documento Único de Identidad electrónico, que permite autenticación segura para trámites en línea y se proyecta como base para una futura billetera ciudadana digital integrada. En conectividad, el acceso a Internet se regula dentro del régimen general de telecomunicaciones y el país presenta niveles de infraestructura intermedios bajos, con conectividad móvil adecuada pero banda ancha fija limitada y velocidades moderadas. En transparencia y acceso a la información pública, el derecho se ejerce mediante portales digitales centralizados y sistemas electrónicos de solicitud administrados bajo la ley correspondiente, permitiendo mecanismos de transparencia activa y acceso bajo demanda. En conjunto, el caso salvadoreño muestra un modelo de gobernanza digital en proceso de consolidación, con avances normativos significativos y liderazgo ejecutivo claro, pero aún condicionado por desafíos de infraestructura, integración tecnológica y fortalecimiento institucional necesarios para alcanzar una madurez sistémica plena.

España

El sistema de gobernanza digital de España se configura como uno de los más avanzados y consolidados del espacio iberoamericano y europeo, caracterizado por una arquitectura normativa densa, una institucionalidad especializada y una coordinación multinivel plenamente articulada con el marco regulatorio de la Unión Europea. El modelo español evidencia un alto grado de madurez sistémica en el que la estrategia, la regulación y la implementación se encuentran estrechamente integradas, generando un ecosistema digital estable, interoperable y orientado a derechos. Esta estructura se sustenta en una combinación de planificación estratégica nacional, legislación vinculante y mecanismos técnicos obligatorios que aseguran coherencia entre niveles de gobierno y continuidad de políticas públicas.

En el plano de los marcos estratégicos, España cuenta con una estrategia digital nacional de alcance país representada por las agendas España Digital 2025 y España Digital 2026, que operan como hoja de ruta estructurante de la transformación digital mediante ejes que abarcan conectividad, competencias digitales, ciberseguridad, digitalización pública y empresarial, economía del dato, inteligencia artificial y derechos digitales, integrando la política tecnológica con objetivos económicos y sociales. La transformación digital del Estado se encuentra respaldada por un marco jurídico vinculante basado en las Leyes 39/2015 y 40/2015, que establecen la tramitación electrónica como regla general y definen la arquitectura digital obligatoria del sector público, articulándose con la estrategia nacional para orientar la modernización administrativa. En gobernanza de Internet, el país presenta un esquema altamente institucionalizado y alineado con el marco europeo, bajo la rectoría del Ministerio para la Transformación Digital y de la Función Pública, que integra estrategia,

regulación sectorial y protección de derechos en el entorno digital. En inteligencia artificial, España dispone de un sistema avanzado con estrategia actualizada en 2024, un anteproyecto legislativo alineado con el AI Act europeo y la creación de la Agencia Española de Supervisión de Inteligencia Artificial, primera autoridad especializada de este tipo en Europa, encargada de supervisar cumplimiento normativo, transparencia, trazabilidad y protección de derechos.

En materia de capacidades habilitadoras, España cuenta con un sistema integral de gobernanza de datos basado en el RGPD y en la Ley Orgánica 3/2018, complementado por marcos obligatorios de interoperabilidad y seguridad como el ENI y el ENS, y reforzado por estrategias nacionales que promueven la economía del dato y la creación de espacios sectoriales, con una autoridad de control consolidada. En datos abiertos, el país presenta un nivel alto de madurez con 77 sobre 100 en ODIN 2024 2025 y posicionamiento global destacado, sustentado en un marco legal completo, estrategia nacional, adhesión a estándares internacionales y amplia disponibilidad de datos, aunque con retos en ciertos conjuntos subnacionales. En ciberseguridad, España dispone de un marco estratégico robusto que incluye planes nacionales, regulaciones específicas para redes 5G y centros operativos especializados, orientado a fortalecer capacidades de prevención, detección y respuesta, así como a consolidar un ecosistema empresarial e innovador en seguridad digital. En infraestructuras críticas, el país posee uno de los sistemas más completos de protección, con legislación específica, catálogo nacional de infraestructuras estratégicas, obligaciones de gestión de riesgos y notificación de incidentes, además de capacidades operativas consolidadas mediante CSIRT especializados y un sistema nacional de coordinación en torno al Consejo de Seguridad Nacional.

En el plano de implementación, servicios y acceso, España evidencia un alto grado de operacionalización de su estrategia digital. El gobierno digital se sustenta en uno de los marcos de interoperabilidad más avanzados de Europa, estructurado en el Esquema Nacional de Interoperabilidad y reforzado por legislación que obliga al intercambio automatizado de datos y al uso de plataformas comunes, complementado por planes de digitalización que impulsan servicios compartidos y modelos de identidad interoperable. En identidad digital, el país dispone de un sistema altamente robusto basado en el DNI electrónico y su versión digital, con autenticación criptográfica, biometría y certificación jurídica plena, alineado con estándares europeos y con integración progresiva hacia la identidad digital europea. En conectividad, España presenta una infraestructura muy desarrollada con cobertura masiva de fibra óptica, velocidades superiores a 250 Mbps y despliegue extendido de redes 4G y 5G, lo que configura uno de los ecosistemas de acceso más avanzados del continente. En transparencia y acceso a la información pública, el derecho se ejerce mediante un sistema digital multinivel que combina portales estatales, autonómicos y locales, plataformas de datos abiertos y mecanismos de reclamación en línea, garantizando altos niveles de acceso y reutilización de información pública. En conjunto, el caso español refleja un modelo de gobernanza digital plenamente institucionalizado, con coherencia normativa, capacidades técnicas consolidadas y una implementación operativa madura que lo posiciona como referencia internacional en desarrollo digital estatal.

Guatemala

El ecosistema de gobernanza digital de Guatemala presenta un nivel de desarrollo incipiente y fragmentado, caracterizado por avances puntuales en digitalización administrativa y

gobierno abierto, combinados con vacíos estructurales en institucionalidad, regulación y planificación estratégica. El país evidencia una arquitectura digital en transición, donde existen iniciativas relevantes pero no articuladas bajo un marco integral de política digital nacional, lo que limita la coherencia sistémica, la capacidad de coordinación interinstitucional y la consolidación de un modelo estatal digital plenamente estructurado. Este patrón configura un entorno en el que coexisten instrumentos operativos con debilidades en rectoría estratégica, formalización normativa y capacidad institucional.

En el nivel de marcos estratégicos, Guatemala carece de una estrategia digital nacional consolidada y opera mediante instrumentos dispersos, como el Plan de Gobierno Digital y la Comisión Presidencial de Gobierno Abierto y Electrónico, instancia de coordinación con alcance limitado y sin jerarquía ministerial. La transformación digital del Estado se organiza principalmente a través del Plan de Gobierno Digital 2020–2026, que define ejes de eficiencia administrativa, inclusión digital, transparencia y educación digital, impulsando interoperabilidad, simplificación de trámites, identidad digital e infraestructura tecnológica, aunque sin respaldo de una ley marco integral de gobierno digital. En gobernanza de Internet, el país se apoya en fundamentos constitucionales de acceso a la información y libertad de expresión, así como en normas sectoriales y el plan digital, pero carece de una estrategia específica y de mecanismos institucionalizados multiactor. En inteligencia artificial, Guatemala se encuentra en etapa temprana de desarrollo, con puntajes bajos en el ILIA 2025 y ausencia total de estrategia nacional, institucionalidad dedicada, participación social o regulación específica, lo que confirma un estadio exploratorio sin marcos formales de conducción.

En el plano de capacidades habilitadoras, el país presenta un desarrollo desigual. La gobernanza de datos carece de una ley de protección de datos personales y de una estrategia nacional formal, y aunque existen iniciativas de interoperabilidad y portales de datos abiertos, estos no cuentan con estándares homogéneos ni obligatoriedad transversal. En datos abiertos, Guatemala alcanza un nivel medio con 55 sobre 100 en ODIN 2024 2025, mostrando fortalezas en estadísticas económicas pero brechas en licenciamiento, cobertura subnacional y reutilización. En ciberseguridad, el país no dispone aún de una estrategia nacional vigente, aunque avanza en la aprobación de un proyecto legislativo integral que propone tipificar delitos informáticos, crear un CSIRT nacional y fortalecer capacidades institucionales, lo que representa un paso relevante pero aún no consolidado. En infraestructuras digitales críticas, no existe legislación específica ni identificación formal de activos críticos, y el país presenta alta vulnerabilidad estructural en sectores estratégicos, sin autoridad rectora ni catálogo oficial, lo que refleja una capacidad limitada de protección sistémica.

En términos de implementación, servicios y acceso, Guatemala mantiene un nivel operativo inicial. El gobierno digital se sustenta principalmente en la ley de firma electrónica de 2008, que reconoce la validez jurídica de comunicaciones y transacciones digitales y constituye la base legal para servicios electrónicos estatales, aunque sin un marco integral de interoperabilidad. En identidad digital, el país no posee un sistema nacional digital y se apoya en el Documento Personal de Identificación físico con biometría, sin credenciales electrónicas ni arquitectura estatal de autenticación digital integrada. En conectividad, el acceso a Internet se regula como servicio de telecomunicaciones bajo un modelo liberalizado y no como derecho, y los indicadores muestran una infraestructura limitada, baja penetración móvil y brechas significativas de acceso. En transparencia, Guatemala sí dispone de un marco legal

consolidado mediante la Ley de Acceso a la Información Pública, que establece principios de máxima publicidad, procedimientos y obligaciones institucionales, constituyendo uno de los componentes más desarrollados del ecosistema digital. En conjunto, el caso guatemalteco refleja un sistema de gobernanza digital en fase inicial de consolidación, con avances normativos sectoriales y herramientas operativas, pero aún sin la cohesión estratégica, la institucionalidad robusta ni las capacidades técnicas necesarias para sostener una transformación digital estatal plenamente integrada.

Honduras

El ecosistema de gobernanza digital de Honduras se caracteriza por un nivel de desarrollo intermedio con rasgos de transición institucional, donde coexisten instrumentos estratégicos recientes y esfuerzos de modernización con brechas estructurales en regulación, capacidades técnicas y coordinación sistémica. El país ha avanzado en la formulación de políticas nacionales que delinean una visión de transformación digital estatal, pero aún enfrenta limitaciones en institucionalidad especializada, marcos normativos integrales y consolidación operativa, lo que configura un modelo en proceso de estructuración más que plenamente consolidado.

En el plano de gobernanza estratégica, Honduras dispone de un esquema dual conformado por la Política Nacional de República Digital 2022–2025 y el Plan Nacional de Gobierno Digital 2023–2026, que funcionan de manera complementaria como visión país y hoja de ruta operativa respectivamente. Estos instrumentos priorizan la modernización del Estado, la transparencia, el uso estratégico de tecnologías, la interoperabilidad, la identidad digital y el fortalecimiento de capacidades públicas, con metas explícitas de mejora en indicadores internacionales. La transformación digital se concibe como rediseño institucional integral orientado a eficiencia, valor público y ciudadanía digital, incorporando simplificación de trámites, plataformas compartidas, estandarización de procesos y fortalecimiento de la rectoría tecnológica. Sin embargo, la gobernanza de Internet mantiene un carácter sectorial e incipiente, con avances regulatorios puntuales pero sin estrategia integral ni autoridad rectora especializada. En inteligencia artificial, Honduras se ubica en fase exploratoria según el ILIA 2025, sin estrategia nacional, institucionalidad ni regulación específica, aunque existen iniciativas aisladas de uso tecnológico, lo que evidencia un ecosistema emergente aún no estructurado.

Respecto de las capacidades habilitadoras, el país presenta avances parciales combinados con vacíos relevantes. El marco de acceso a la información pública es sólido y se sustenta en la Ley de Transparencia y Acceso a la Información Pública y en disposiciones constitucionales que reconocen el hábeas data, pero Honduras carece de una ley integral de protección de datos personales, cuyo proyecto permanece en trámite. En datos abiertos, el desempeño es medio-bajo, con 50 sobre 100 en ODIN 2024 2025, reflejando avances en estadísticas macroeconómicas pero debilidades en cobertura sectorial, licencias abiertas e interoperabilidad. En ciberseguridad, el país presenta un rezago significativo: no dispone de estrategia nacional ni de CSIRT, aunque el Plan de Gobierno Digital prevé su creación futura, lo que muestra un reconocimiento institucional del problema pero sin implementación aún. En infraestructuras digitales críticas, el vacío es más pronunciado, ya que no existe legislación, definiciones oficiales, autoridad competente ni mecanismos de protección, lo que evidencia un nivel bajo de preparación sistémica frente a riesgos digitales.

En el ámbito de implementación, servicios y acceso, Honduras muestra avances iniciales pero todavía fragmentados. La interoperabilidad estatal se encuentra en fase emergente y funciona más como prioridad estratégica que como sistema operativo consolidado, con diagnósticos oficiales que identifican intercambio de datos aislado y ausencia de estándares comunes. En identidad digital, el país dispone de bases sólidas gracias al Registro Nacional de las Personas y al DNI biométrico modernizado desde 2021, respaldado por normativa de firma electrónica, pero aún no cuenta con un sistema nacional integral ni credenciales digitales interoperables. En conectividad, el acceso a Internet está regulado sectorialmente aunque no reconocido como derecho, y los indicadores muestran infraestructura limitada, con banda ancha fija poco extendida pese a cobertura móvil relativamente adecuada. En transparencia, el país exhibe uno de sus componentes más desarrollados, con un esquema digital centralizado basado en portales oficiales y sistemas electrónicos de solicitudes bajo supervisión institucional. En conjunto, Honduras configura un sistema de gobernanza digital en etapa de consolidación inicial, con planificación estratégica reciente y bases institucionales en desarrollo, pero todavía condicionado por brechas regulatorias, técnicas y de coordinación que restringen su madurez estructural.

México

El ecosistema de gobernanza digital de México presenta un nivel de desarrollo relativamente avanzado con rasgos de heterogeneidad institucional, caracterizado por la coexistencia de marcos estratégicos tempranos, capacidades técnicas consolidadas en áreas específicas y brechas de actualización normativa y coordinación interinstitucional. El país dispone de bases estructurales sólidas en materia de regulación, conectividad y datos abiertos, pero su madurez sistémica se ve condicionada por la necesidad de actualización estratégica y de mayor articulación entre instrumentos existentes.

En el plano de gobernanza estratégica, México cuenta con la Estrategia Digital Nacional de 2013 como marco rector integral orientado a maximizar el impacto económico, social y político de la digitalización mediante objetivos vinculados a gobierno, economía, educación, salud y seguridad, apoyados en habilitadores como conectividad, inclusión, interoperabilidad y datos abiertos. La transformación digital del Estado se articula dentro de esta estrategia a través del eje de transformación gubernamental, que prioriza simplificación de trámites, ventanilla única, firma electrónica, interoperabilidad y uso intensivo de datos para mejorar políticas públicas y servicios. La gobernanza de Internet se sustenta en un entramado institucional robusto, con regulación sectorial avanzada y un regulador autónomo especializado, junto con reconocimiento legal explícito del principio de neutralidad de la red. En inteligencia artificial, el país presenta un escenario mixto: dispone de una estrategia nacional desde 2018 y de propuestas de agenda actualizadas, así como avances regulatorios relevantes, pero mantiene debilidades en institucionalidad y visión estratégica según indicadores comparativos regionales, lo que evidencia un campo aún en consolidación.

En materia de capacidades habilitadoras, México exhibe fortalezas significativas combinadas con vacíos estructurales. El país posee un marco legal vigente de protección de datos personales y estándares de gestión de información, aunque carece de una estrategia nacional integral de gobernanza de datos y de un modelo estatal plenamente articulado de interoperabilidad. En datos abiertos, el desempeño es muy alto a escala regional y global, con 76 sobre 100 en el ODIN 2024 2025, lo que refleja un ecosistema robusto de disponibilidad,

licenciamiento abierto, reutilización y estándares técnicos. En ciberseguridad, el país cuenta con una estrategia nacional publicada en 2017 que estableció principios de derechos humanos, gestión de riesgos y cooperación multiactor, pero su falta de actualización y la dispersión institucional han limitado su implementación efectiva. En infraestructuras digitales críticas, el país no dispone de una ley integral ni de un catálogo oficial, aunque existen iniciativas operativas recientes de fortalecimiento de capacidades mediante simulaciones y ejercicios coordinados, lo que indica avances técnicos sin consolidación normativa.

En el ámbito de implementación, servicios y acceso, México muestra un nivel de desarrollo intermedio con componentes institucionales consolidados. El país dispone de un marco formal de interoperabilidad para el sector público federal mediante el Esquema de Interoperabilidad y de Datos Abiertos, que define estándares técnicos y organizacionales para el intercambio seguro de información entre entidades gubernamentales. En identidad digital, el sistema se estructura alrededor de la CURP como identificador único nacional, complementado por la firma electrónica avanzada y desarrollos recientes de credenciales digitales, configurando una arquitectura funcional aunque aún no plenamente integrada. El acceso a Internet cuenta con reconocimiento constitucional explícito, lo que constituye uno de los niveles más altos de protección jurídica en la región, mientras que los indicadores de conectividad muestran infraestructura intermedia con alta cobertura móvil y banda ancha en expansión. En transparencia, México dispone de un ecosistema digital altamente institucionalizado basado en la Plataforma Nacional de Transparencia bajo supervisión autónoma, lo que evidencia un alto grado de formalización del acceso a la información pública. En conjunto, México presenta un sistema de gobernanza digital con capacidades técnicas y regulatorias relevantes, pero cuya consolidación plena depende de la actualización de sus marcos estratégicos, la integración institucional y la armonización de políticas digitales a escala nacional.

Nicaragua

El ecosistema de gobernanza digital de Nicaragua se caracteriza por un nivel bajo de institucionalización, con avances normativos puntuales pero sin un sistema estratégico integrado que articule de manera coherente visión, capacidades y resultados. La arquitectura digital nacional presenta rasgos fragmentarios, con iniciativas aisladas y marcos regulatorios parciales que configuran un entorno funcional limitado, con brechas significativas en coordinación institucional, desarrollo tecnológico y garantías operativas para el despliegue pleno de políticas digitales.

En el plano estratégico, el país no dispone de una estrategia nacional de gobierno digital formalizada ni de un documento integral que establezca prioridades, metas y mecanismos de implementación transversales. La transformación digital del Estado se desarrolla principalmente a partir de regulaciones sectoriales de telecomunicaciones y dispositivos de control administrativo, sin constituir un marco habilitante integral ni alineado con estándares internacionales. La gobernanza de Internet descansa en fundamentos constitucionales generales vinculados a libertad de expresión y acceso a la información, pero carece de institucionalidad especializada y de instrumentos regulatorios específicos que estructuren el ecosistema digital. En inteligencia artificial, el país no cuenta con legislación, estrategia ni institucionalidad dedicada, lo que lo sitúa en una etapa inicial sin marcos formales para orientar el desarrollo, adopción o supervisión de estas tecnologías.

En cuanto a capacidades habilitadoras, Nicaragua posee un desarrollo incipiente y asimétrico. El país dispone de una ley de protección de datos personales vigente desde 2012 que regula definiciones, tratamiento y seguridad de la información, pero su aplicación es limitada debido a la inexistencia de la autoridad de control prevista, lo que impide la supervisión efectiva del sistema y debilita la implementación de obligaciones legales. No existe estrategia nacional de gobernanza de datos ni marcos integrales de interoperabilidad o apertura, lo que mantiene al ecosistema en un estado fragmentado. En datos abiertos, el desempeño es bajo con 43 sobre 100 en el ODIN 2024 2025, reflejando disponibilidad parcial, baja reutilización y ausencia de estándares internacionales de apertura. En ciberseguridad, el país adoptó una estrategia nacional 2020 2025 orientada a soberanía digital, resiliencia y protección de infraestructuras, pero su implementación ha sido limitada y cuestionada, evidenciando debilidad institucional y capacidades técnicas restringidas. En infraestructuras digitales críticas no existe legislación específica ni un régimen nacional de protección, lo que deja la seguridad de sistemas esenciales sin obligaciones sectoriales ni autoridad especializada.

En el plano de implementación y acceso, la digitalización estatal avanza de manera gradual y no sistemática. Existen portales y herramientas digitales y participación en redes regionales, pero no se identifica un marco nacional publicado que defina estándares técnicos, interoperabilidad y gobernanza de datos para el sector público. El sistema de identidad digital es incipiente y se basa principalmente en la cédula física tradicional, complementada por un marco legal de firma electrónica que habilita autenticación digital pero sin integración a un ecosistema estatal interoperable. El acceso a Internet se encuentra regulado como servicio de telecomunicaciones sin reconocimiento constitucional como derecho, mientras que los indicadores de conectividad muestran limitaciones estructurales, con baja penetración de banda ancha fija y velocidades que permiten usos básicos. En materia de transparencia, el derecho de acceso a la información pública se ejerce mediante un esquema descentralizado basado en portales institucionales y unidades administrativas, sin plataforma nacional unificada, lo que restringe la trazabilidad y homogeneidad del ejercicio digital del derecho. En conjunto, Nicaragua presenta un modelo de gobernanza digital con bases legales aisladas pero sin integración sistémica, donde el principal desafío radica en construir una arquitectura institucional coordinada que permita transformar capacidades normativas dispersas en un ecosistema digital funcional, interoperable y sostenible.

Panamá

El ecosistema de gobernanza digital de Panamá muestra un grado intermedio de madurez caracterizado por una institucionalidad clara, avances operativos visibles y una arquitectura normativa funcional, aunque con rezagos en actualización estratégica y consolidación de marcos integrales. El país presenta una estructura relativamente coherente liderada por una autoridad rectora especializada, lo que le permite articular iniciativas digitales relevantes, pero mantiene desafíos en estandarización, integración sistémica y formalización de instrumentos estratégicos de nueva generación.

En el plano estratégico, Panamá organiza su gobernanza digital a partir de la Autoridad Nacional para la Innovación Gubernamental como órgano rector y de los Impulsores Estratégicos AIG 2024–2029, que definen una visión de transformación digital centrada en el ciudadano, orientada a servicios públicos totalmente digitales, interoperables y seguros, con énfasis en portal único, autenticación digital, pasarelas de pago, infraestructura tecnológica

común y adopción de tecnologías emergentes. La transformación digital del Estado se sustenta además en la Agenda Digital Panamá 2020 y en la Ley de Gobierno Electrónico 83/2012, que proporcionan un marco operativo estable aunque no actualizado, lo que evidencia continuidad institucional con cierta obsolescencia estratégica. La gobernanza de Internet se configura mediante un modelo institucionalizado pero sin ley específica, en el que la agenda digital nacional concibe la conectividad como infraestructura habilitante del desarrollo bajo rectoría de la AIG. En inteligencia artificial, el país se ubica en una fase incipiente de gobernanza según el ILIA 2025, con avances regulatorios y proyectos legislativos en preparación, pero con debilidades en visión estratégica e institucionalidad, reflejando un ecosistema en construcción.

En materia de capacidades habilitadoras, Panamá presenta un desarrollo desigual pero con bases normativas relevantes. El país dispone de un marco robusto de protección de datos personales sustentado en la Ley 81 de 2019 y su reglamentación, que establece derechos, obligaciones y notificación de incidentes, bajo supervisión de ANTAI, aunque no cuenta con una estrategia nacional integral de gobernanza de datos ni con un modelo plenamente articulado de interoperabilidad estatal. En datos abiertos, el desempeño es medio-alto con 62 sobre 100 en el ODIN 2024 2025, evidenciando avances en apertura y marcos legales completos, aunque persisten brechas en cobertura subnacional, licenciamiento y sostenibilidad institucional. En ciberseguridad, la Estrategia Nacional 2021–2024 constituye el principal instrumento, orientado a resiliencia, protección de infraestructuras críticas y fortalecimiento del CSIRT Panamá, con planes recientes para evolucionar hacia un modelo nacional unificado. En infraestructuras digitales críticas no existe ley específica ni catálogo oficial, pero la estrategia reconoce formalmente su relevancia y define acciones estratégicas para sectores esenciales, lo que configura un esquema de protección incipiente con base programática.

En el plano de implementación, servicios y acceso, el país evidencia progresos operativos significativos aunque aún en consolidación. Panamá ha desarrollado servicios públicos digitales centralizados y una arquitectura técnica basada en interoperabilidad progresiva coordinada por la AIG, lo que refleja un proceso de modernización estatal en marcha aunque sin estandarización plena. El sistema de identidad digital se apoya en una cédula biométrica moderna y un marco avanzado de firma electrónica, pero todavía no existe una identidad digital única nacional, por lo que la autenticación permanece fragmentada. El acceso a Internet no está reconocido como derecho, aunque se promueve mediante políticas de acceso universal, y los indicadores muestran infraestructura intermedia con buena cobertura móvil y banda ancha fija aceptable. En transparencia, el derecho de acceso a la información pública se ejerce mediante un sistema digital relativamente centralizado basado en portales y plataformas supervisadas por ANTAI, lo que permite transparencia activa y solicitudes electrónicas. En conjunto, Panamá presenta un modelo de gobernanza digital funcional y con liderazgo institucional claro, cuyo principal desafío radica en consolidar la integración normativa y técnica de sus componentes para evolucionar desde un sistema operativo en desarrollo hacia un ecosistema digital plenamente articulado, interoperable y estratégicamente actualizado.

Paraguay

El ecosistema de gobernanza digital de Paraguay presenta una estructura estratégica relativamente definida y orientada a largo plazo, aunque con brechas relevantes en institucionalidad especializada, marcos regulatorios integrales y despliegue operativo. El país muestra una planificación digital clara y coherente en el plano programático, pero enfrenta desafíos en consolidación normativa, articulación transversal y madurez de implementación, lo que configura un modelo en transición desde una etapa de diseño estratégico hacia una fase de consolidación institucional y técnica.

En el plano de gobernanza estratégica, Paraguay dispone de una hoja de ruta nacional explícita, el Plan Nacional TIC 2022–2030, aprobado por decreto y liderado por el MITIC, que establece un enfoque integral para construir un país conectado, seguro y competitivo mediante cuatro ejes: infraestructura digital, transformación del Estado, desarrollo del ecosistema TIC y ciberseguridad, alineados con el Plan Nacional de Desarrollo 2030 y los ODS. La transformación digital estatal se concibe como una modernización estructural orientada a interoperabilidad, simplificación de trámites, identidad digital, plataformas comunes, gestión estratégica de datos y fortalecimiento de capacidades institucionales, con el objetivo de migrar desde un Estado fragmentado hacia uno digital centrado en las personas. La gobernanza de Internet adopta un enfoque principalmente sectorial, donde la red es tratada como infraestructura habilitante dentro de políticas TIC más amplias, bajo rectoría del MITIC y con participación de actores como CONATEL, pero sin un marco transversal explícito ni principios normativos sobre neutralidad, derechos digitales o gobernanza del ecosistema. En inteligencia artificial, el país se ubica en una fase incipiente, sin estrategia nacional, institucionalidad responsable ni mecanismos de participación multiactor, lo que evidencia ausencia total de arquitectura de gobernanza en esta materia.

En términos de capacidades habilitadoras, el país presenta un desarrollo desigual y fragmentado. El marco de protección de datos es limitado, sustentado en disposiciones constitucionales y en la Ley 6534/2020 restringida a datos crediticios, sin normativa integral ni autoridad especializada, lo que genera vacíos regulatorios en gobernanza del dato. En datos abiertos, Paraguay cuenta con bases jurídicas claras como las leyes 5189/14 y 5282/14, un portal nacional centralizado y lineamientos emitidos por el MITIC, alineados con estándares internacionales de apertura y transparencia, lo que configura un esquema institucional funcional aunque acotado. En ciberseguridad, la institucionalidad se apoya en la Ley 6207/2018 que crea el MITIC y le otorga competencias para interoperabilidad y optimización de procesos, junto con instrumentos estratégicos como la Agenda Digital y el Plan Nacional TIC, que promueven digitalización y eficiencia institucional con niveles de madurez heterogéneos entre sectores. En infraestructuras digitales críticas no existe ley específica ni catálogo nacional, pero la Estrategia Nacional de Ciberseguridad 2025–2028 reconoce su importancia y plantea acciones de gestión de riesgos, fortalecimiento del CSIRT y estándares mínimos para sectores estratégicos, lo que configura un enfoque programático aún sin obligatoriedad regulatoria.

En el plano de implementación, servicios y acceso, Paraguay presenta avances institucionales con limitaciones operativas. El país dispone de un marco legal para gobierno digital mediante la Ley 6207/2018, que otorga al MITIC funciones rectoras para interoperabilidad y optimización de trámites, aunque todavía no existe un esquema nacional

formalizado de interoperabilidad, por lo que los servicios públicos digitales interoperables se mantienen en desarrollo intermedio. En identidad digital, el sistema se basa en cédula física y en la Ley 4017/2010 de firma electrónica, que provee una base jurídica sólida pero sin plataforma unificada ni credencial digital nacional, reflejando un modelo aún incipiente. El acceso a Internet no está reconocido como derecho, y la infraestructura presenta un nivel medio-bajo de desarrollo con 45,90 puntos, buena conectividad móvil pero penetración desigual y velocidades moderadas en banda ancha fija. En transparencia, el derecho de acceso a la información pública se ejerce mediante un esquema digital centralizado articulado en torno al Portal Unificado y al portal nacional de datos abiertos, conforme a la Ley 5282/2014. En conjunto, Paraguay muestra una gobernanza digital estratégicamente planificada pero institucionalmente incompleta, donde la principal brecha no radica en la ausencia de visión sino en la consolidación normativa, técnica y operativa necesaria para transformar sus lineamientos programáticos en un ecosistema digital plenamente integrado y funcional.

Perú

El ecosistema de gobernanza digital de Perú evidencia un nivel de desarrollo institucional relativamente avanzado, caracterizado por la existencia de marcos normativos robustos, instrumentos estratégicos de largo plazo y capacidades regulatorias especializadas, aunque con brechas de articulación estratégica y desafíos persistentes de implementación homogénea. El país presenta un modelo donde la arquitectura jurídica y programática se encuentra más consolidada que su ejecución operativa, lo que configura una gobernanza digital estructuralmente sólida pero con niveles desiguales de madurez entre sectores y niveles de gobierno.

En el plano estratégico, Perú dispone de un andamiaje normativo fuerte encabezado por la Ley de Gobierno Digital (Decreto Legislativo Nº 1412, 2018), que establece obligaciones para todo el Estado en materia de identidad digital, interoperabilidad, servicios digitales, seguridad digital y gobernanza de datos bajo rectoría de la Secretaría de Gobierno Digital. Sin embargo, el país no cuenta con una estrategia nacional integral actualizada que articule visión, metas y hoja de ruta común, lo que genera implementación fragmentada y avances heterogéneos. La Política Nacional de Transformación Digital al 2030 constituye el principal instrumento estratégico, orientado a construir un Estado centrado en las personas mediante servicios digitales interoperables, uso estratégico de datos, plataformas comunes y tecnologías emergentes, priorizando eficiencia, transparencia y participación ciudadana. La gobernanza de Internet se encuentra en consolidación institucional, con una visión estratégica explícita que reconoce a Internet como infraestructura habilitante del desarrollo bajo la rectoría de la Secretaría de Gobierno y Transformación Digital. En inteligencia artificial, Perú se posiciona como uno de los países más avanzados de la región, con 74,36 puntos en gobernanza según ILIA 2025, legislación específica vigente desde 2023 y una Estrategia Nacional de IA respaldada por la Ley Nº 31.814, que define ejes de entrenamiento, infraestructura, datos, ética y modelo económico, configurando un marco regulatorio e institucional altamente estructurado.

En el ámbito de capacidades habilitadoras, Perú muestra un ecosistema relativamente consolidado con estándares formales y autoridades especializadas. El país cuenta con un régimen integral de protección de datos personales basado en la Ley 29733 y su reglamento

actualizado en 2025, que introduce obligaciones reforzadas de seguridad, notificación de incidentes y designación de oficiales de datos, bajo supervisión de la autoridad nacional competente. En datos abiertos presenta un nivel medio-alto de madurez con 63/100 en ODIN 2024/2025, sustentado en un marco legal completo, portal nacional, estrategia de datos y participación en iniciativas internacionales, aunque persisten brechas en cobertura subnacional, licenciamiento y reutilización efectiva. En ciberseguridad, el país dispone de un entramado normativo sólido compuesto por la Ley de Gobierno Digital, el Marco de Confianza Digital, la Ley de Ciberdefensa y la Estrategia Nacional de Ciberseguridad 2026–2028, orientada a resiliencia, protección de infraestructuras críticas, capacidades técnicas y cooperación internacional, aunque el diagnóstico oficial reconoce déficits en cultura digital, coordinación institucional y protección de activos críticos. En infraestructuras digitales críticas no existe una ley integral específica, pero normas como el Decreto Legislativo 1412 y la Ley 30999 establecen obligaciones estatales de protección y continuidad de sistemas esenciales, configurando un esquema regulatorio funcional aunque disperso.

En el plano de implementación y acceso, Perú presenta resultados operativos relativamente avanzados dentro de la región. La interoperabilidad está formalmente establecida como componente obligatorio del gobierno digital en la Ley de Gobierno Digital, que define arquitectura tecnológica, gestión de identidad y servicios digitales para los tres niveles de gobierno. El país dispone además de un sistema de identidad digital robusto basado en el DNI electrónico con biometría, chip criptográfico y certificados digitales, complementado por la aplicación ID Perú, lo que lo ubica entre los modelos más desarrollados regionalmente en autenticación digital. En conectividad, Perú presenta infraestructura de nivel medio con 50,78 puntos y buen desempeño en velocidades móviles y fijas, lo que refleja un entorno técnico habilitante relativamente sólido. Finalmente, el derecho de acceso a la información pública se ejerce mediante un ecosistema digital centralizado y estandarizado compuesto por el Portal de Transparencia Estándar, el sistema de solicitudes de información y el portal estatal Gob.pe, conforme a la Ley Nº 27806. En conjunto, Perú configura un modelo de gobernanza digital normativamente avanzado y con institucionalidad especializada, cuyo principal desafío no radica en la ausencia de marcos regulatorios sino en la consolidación de capacidades operativas uniformes que permitan traducir su arquitectura estratégica en resultados consistentes a escala nacional.

Portugal

El ecosistema de gobernanza digital de Portugal se caracteriza por un alto grado de institucionalización, coherencia estratégica y alineación multinivel, configurando un modelo consolidado donde la digitalización constituye una política de Estado estructural y de largo plazo. El país presenta un esquema maduro en el que convergen planificación estratégica, regulación robusta, capacidades técnicas desarrolladas y mecanismos de implementación integrados, lo que permite observar una arquitectura digital consistente y articulada entre niveles normativos, institucionales y operativos.

En el plano estratégico, Portugal dispone de un marco nacional integral definido por el Programa Portugal Digital aprobado mediante la Resolución del Consejo de Ministros N.º 30/2020, con horizonte 2030 y alineación explícita con la Década Digital de la Unión Europea. Esta estrategia establece una visión multisectorial orientada a mejorar la calidad de vida, la competitividad y la interacción digital entre ciudadanía, empresas y Estado, estructurada en

dimensiones de personas, empresas, gobierno e infraestructura, y guiada por principios de inclusión, confianza, transparencia, sostenibilidad y seguridad. La transformación digital del Estado se concibe como modernización estructural dentro de esta estrategia, priorizando desmaterialización administrativa, interoperabilidad total, servicios proactivos, principio de solo una vez y fortalecimiento de la identidad digital mediante plataformas integradas como gov.pt. La gobernanza de Internet se apoya en un entramado regulatorio estrechamente vinculado al marco europeo, sin una ley nacional específica dedicada exclusivamente a este ámbito, aunque con una orientación estratégica explícita que reconoce a Internet como infraestructura habilitante. En inteligencia artificial, el país cuenta con la estrategia AI Portugal 2030 adoptada en 2019, coordinada por el programa público INCoDe.2030, que promueve investigación, innovación y adopción transversal de IA, consolidando un marco nacional programático para su desarrollo.

En cuanto a capacidades habilitadoras, Portugal exhibe uno de los ecosistemas más avanzados del entorno comparado. El régimen de gobernanza de datos se encuentra plenamente alineado con el GDPR y con la Ley 58/2019, complementado por normativa sectorial y supervisado por la CNPD, con facultades sancionadoras y obligaciones integrales en materia de derechos, bases legales, transferencias, evaluaciones de impacto y notificación de incidentes. En datos abiertos el país alcanza un nivel de madurez muy alto con 83/100 en ODIN 2024/2025 y posición 11 global, destacándose especialmente en apertura, formatos reutilizables y legibilidad automática, sustentado en un marco legal completo, estrategia nacional y portal consolidado. En ciberseguridad, Portugal dispone de una arquitectura estratégica y normativa sólida integrada por la Estratégia Nacional de Segurança do Ciberespaço, el régimen jurídico de seguridad del ciberespacio y la transposición de la Directiva NIS y NIS2, lo que amplía obligaciones sectoriales, refuerza supervisión y eleva estándares de gestión de riesgos. En infraestructuras digitales críticas, el país cuenta con uno de los marcos más avanzados de la Unión Europea, basado en la Lei 46/2018 y el Decreto-Lei 22/2025, que establecen procedimientos formales de identificación, evaluación de riesgos, designación y supervisión de infraestructuras críticas, junto con obligaciones técnicas y planes de resiliencia obligatorios.

En el plano de implementación y acceso, Portugal muestra un nivel de consolidación operativa elevado y coherente con su arquitectura estratégica. La interoperabilidad se gestiona mediante marcos institucionales claros coordinados por la Agência para a Modernização Administrativa, incluyendo el programa iAP y el portal único gov.pt, que integran estándares técnicos comunes y plataformas compartidas alineadas con los marcos europeos de interoperabilidad. El país dispone además de uno de los sistemas de identidad digital más avanzados de Europa, basado en el Cartão de Cidadão y la Chave Móvel Digital, que permiten autenticación multifactor y firma electrónica cualificada conforme a estándares eIDAS. En conectividad, Portugal presenta indicadores de infraestructura altamente desarrollados, con cerca del 89 por ciento de hogares con banda ancha fija, más del 90 por ciento de conexiones superiores a 100 Mbps y una penetración de fibra cercana al 81,9 por ciento, situándose entre los líderes europeos en acceso de alta capacidad. Finalmente, el acceso a la información pública se ejerce mediante un ecosistema digital estandarizado que integra el portal ePortugal, sistemas electrónicos de solicitud, portal nacional de datos abiertos y acceso digital a normativa oficial bajo supervisión de la CADA. En conjunto, Portugal configura un modelo de gobernanza digital altamente maduro, caracterizado por coherencia entre estrategia, capacidades e implementación, donde la principal fortaleza no radica únicamente en la

existencia de marcos regulatorios avanzados sino en su efectiva articulación institucional y operativa.

República Dominicana

El ecosistema de gobernanza digital de la República Dominicana presenta una configuración intermedia caracterizada por la coexistencia de avances estratégicos relevantes con brechas de articulación institucional y programática. El país dispone de instrumentos de planificación de largo plazo y de desarrollos sectoriales significativos, pero la arquitectura general evidencia una estructura parcialmente integrada, donde conviven políticas formales, iniciativas dispersas y marcos regulatorios heterogéneos que generan asimetrías entre visión estratégica, capacidades habilitadoras e implementación operativa.

En el nivel estratégico, la Agenda Digital 2030 aprobada en 2022 constituye el principal instrumento rector y define una hoja de ruta nacional orientada a insertar al país en la economía digital mediante un enfoque multisectorial alineado con la Estrategia Nacional de Desarrollo 2030, los ODS y la agenda eLAC. Su diseño se organiza en cinco ejes estratégicos y dos ejes transversales, priorizando gobernanza, conectividad, gobierno digital, capacidades y economía digital, con énfasis en reducción de brechas y mejora de competitividad. Sin embargo, la transformación digital del Estado carece de un plan nacional unificado, vigente y públicamente disponible que articule interoperabilidad, servicios digitales, datos y ciberseguridad en un solo instrumento, lo que genera dependencia de iniciativas sectoriales, mesas de trabajo y proyectos aislados. La gobernanza de Internet se estructura sobre una base normativa fragmentada y sectorial sin ley específica ni principios explícitos de gobernanza, aunque la Agenda Digital reconoce su rol habilitante. En contraste, la gobernanza de inteligencia artificial presenta mayor consolidación relativa: el país se clasifica como adoptante en el ILIA 2025 con 44,96 puntos y un nivel avanzado en gobernanza, sustentado en una Estrategia Nacional de IA de 2023 implementada por OGTIC, con pilares en gobierno inteligente, talento, infraestructura de datos e integración regional, además de sandboxes regulatorios e iniciativas legales en desarrollo, lo que posiciona a la IA como uno de los subcampos estratégicos más estructurados del ecosistema digital nacional.

En materia de capacidades habilitadoras, el país muestra avances formales con debilidades institucionales. El régimen de protección de datos se basa en la Constitución y la Ley 172-13, que regula principios y derechos, pero carece de una autoridad nacional especializada, lo que limita supervisión y aplicación efectiva. El desempeño en datos abiertos es medio, con 62/100 en ODIN 2024/2025 y buen nivel de cobertura, respaldado por marco legal completo, portal nacional y membresía en OGP, aunque persisten brechas en licencias abiertas y reutilización. En ciberseguridad, la Estrategia Nacional de Ciberseguridad 2030 establece prioridades claras de fortalecimiento normativo, capacidades, protección de infraestructuras críticas y respuesta a incidentes bajo coordinación del CNCS y operación del CSIRT-RD, configurando un marco estratégico formal cuya efectividad depende de su ejecución sostenida. En infraestructuras digitales críticas no existe una ley específica, pero su protección se integra como componente central dentro de dicha estrategia, lo que indica un abordaje programático más que regulatorio.

En el plano de implementación y acceso, la República Dominicana evidencia progresos institucionales acompañados de fragmentación operativa. El Decreto 92-22 establece el

Marco Nacional de Interoperabilidad Gubernamental para orientar el intercambio de información entre entidades públicas, sentando bases técnicas para el gobierno digital. El sistema de identidad se sustenta en una cédula biométrica robusta y en la Ley 126-02 de firma digital, que habilita autenticación electrónica con validez jurídica, aunque todavía no existe una identidad digital nacional integrada ni una plataforma unificada, manteniéndose mecanismos dispersos. En conectividad, el país registra infraestructura alta-media con 70,46 puntos y destaca regionalmente en banda ancha móvil y velocidad, con amplia cobertura territorial. El acceso a la información pública se ejerce mediante la Ley 200-04 y mecanismos digitales de transparencia, complementados por participación de actores de sociedad civil como ISOC-DO, lo que introduce elementos de diálogo multiactor no institucionalizado. En conjunto, la República Dominicana presenta un modelo de gobernanza digital en consolidación, con fortalezas claras en planificación estratégica general y en políticas sectoriales como IA y ciberseguridad, pero con desafíos persistentes en integración sistémica, institucionalidad especializada y coordinación transversal que condicionan la coherencia del ecosistema digital nacional.

Uruguay

El modelo de gobernanza digital de Uruguay se caracteriza por un alto grado de madurez sistémica y coherencia estructural entre estrategia, institucionalidad y despliegue operativo, configurando un ecosistema donde la digitalización se integra como política pública de Estado sostenida en el tiempo. La arquitectura nacional muestra consistencia entre visión estratégica, capacidades habilitadoras e implementación, lo que permite identificar un patrón de desarrollo incremental pero continuo, sustentado en una rectoría clara, estabilidad institucional y alineación entre instrumentos programáticos y regulatorios.

En el plano estratégico, la Agenda Uruguay Digital constituye el eje rector transversal que orienta la digitalización del país más allá del ámbito gubernamental, articulando inclusión, innovación, competitividad, datos, interoperabilidad, identidad digital y conectividad bajo coordinación de AGESIC. Aunque no posee rango legal, su continuidad política y su institucionalización le otorgan efectividad como instrumento de gobernanza, reforzada por la Agenda Uruguay Digital 2025, que organiza la acción pública en áreas y objetivos estratégicos con monitoreo permanente y alineación internacional. La transformación digital del Estado se concibe como política estructural sostenida en un entramado normativo coherente que establece la gestión electrónica como estándar administrativo, consolidando un modelo altamente maduro orientado a generación de valor público. En materia de gobernanza de Internet, el país dispone de bases normativas sólidas y rectoría institucional clara, aunque sin un marco específico dedicado exclusivamente a esta materia. En inteligencia artificial, Uruguay se posiciona como referente regional al clasificarse como país pionero en el ILIA 2025 con 62,32 puntos y 77,67 en gobernanza, sustentado en una Estrategia Nacional de IA vigente y en actualización, con altos puntajes en institucionalidad, evaluación, coordinación, ética y participación multiactor, lo que refleja un ecosistema estratégico avanzado y consolidado.

En capacidades habilitadoras, Uruguay presenta uno de los marcos más robustos de la región. Su régimen de protección de datos, basado en la Ley 18.331 y supervisado por la URCDP, establece estándares integrales alineados con buenas prácticas internacionales, incluyendo obligaciones de notificación de incidentes, registro de bases y control de

transferencias internacionales. En datos abiertos, el país alcanza 54/100 en ODIN 2024/2025, con fortalezas en estadísticas económicas y debilidades en cobertura social y territorial, aunque dispone de marco legal completo, portal nacional, estrategia de datos, adhesión a la Open Data Charter y membresía en OGP. En ciberseguridad, la Estrategia Nacional 2024–2030 define un enfoque integral que abarca gobernanza, protección de infraestructuras críticas, resiliencia, capacidades técnicas y cooperación internacional, con liderazgo institucional del CERTuy. En infraestructuras críticas, aun sin ley específica, existe un marco estratégico explícito que establece mecanismos de identificación, gestión de riesgos, monitoreo y continuidad operativa, apoyado en normativa que consolida la gobernanza del sector, lo que demuestra una aproximación programática sólida.

En la dimensión de implementación y acceso, Uruguay exhibe un ecosistema operativo altamente consolidado. La interoperabilidad es un componente normado y funcional, articulado institucionalmente por AGESIC y respaldado por decretos que regulan la plataforma nacional de intercambio de datos entre entidades públicas, lo que facilita servicios digitales integrados y centrados en el ciudadano. El sistema de identidad digital es uno de los más avanzados regionalmente, sustentado en la cédula electrónica con chip, biometría y certificados digitales, complementado por identidad digital móvil con niveles de seguridad equivalentes a la autenticación presencial y por un marco legal que reconoce plena equivalencia jurídica entre identidad física y electrónica. En conectividad, el país presenta infraestructura muy alta, con 70,46 puntos, liderazgo regional en suscripciones móviles, cobertura 5G extendida y velocidades elevadas, configurando un entorno tecnológico propicio para servicios digitales avanzados. El acceso a la información pública se ejerce mediante mecanismos electrónicos operativos vinculados a la Ley 18.381, aunque sin un portal único centralizado, lo que evidencia un sistema funcional pero distribuido. En conjunto, Uruguay configura un modelo de gobernanza digital altamente institucionalizado y coherente, donde la alineación entre estrategia, capacidades e implementación produce un ecosistema estable, resiliente y avanzado en términos comparativos.

Venezuela

El ecosistema de gobernanza digital de Venezuela se caracteriza por una estructura de baja institucionalización y fuerte fragmentación, donde la ausencia de una estrategia nacional vigente y de una hoja de ruta integral limita la articulación sistémica entre visión estratégica, capacidades habilitadoras e implementación. La arquitectura digital estatal se desarrolla principalmente a través de iniciativas sectoriales y marcos parciales, lo que genera un patrón de avance discontinuo, con esfuerzos puntuales pero sin un instrumento rector capaz de integrar interoperabilidad, servicios digitales, identidad digital, datos abiertos y ciberseguridad dentro de una política pública coherente.

En el plano estratégico, el país carece de una estrategia nacional de gobierno digital actualizada, manteniendo como referencia programática el Plan Nacional de Ciencia, Tecnología e Innovación 2005–2030, orientado al desarrollo científico-tecnológico pero no concebido como instrumento de gobernanza digital. La modernización estatal se impulsa desde el Ministerio del Poder Popular para Ciencia y Tecnología mediante una política centrada en infraestructura tecnológica, software libre, interoperabilidad de datos y ampliación del acceso a telecomunicaciones, lo que evidencia una orientación hacia soberanía tecnológica más que hacia una arquitectura integral de transformación digital. La gobernanza

de Internet se sustenta en un esquema sectorial basado en la Ley Orgánica de Telecomunicaciones y la rectoría del ministerio y de CONATEL, sin principios explícitos sobre neutralidad de la red, apertura del ecosistema digital o protección integral de datos. En inteligencia artificial, el país presenta uno de los niveles más bajos de la región: se clasifica como Explorador en el ILIA 2025 con 24,65 puntos generales y 12,46 en gobernanza, careciendo de estrategia, institucionalidad, participación social y regulación específica, lo que refleja un vacío estructural en la conducción de tecnologías emergentes.

En capacidades habilitadoras, el país exhibe debilidades institucionales relevantes. No dispone de una ley integral de protección de datos personales ni de una autoridad nacional especializada; la gobernanza del dato se sustenta en disposiciones constitucionales y jurisprudencia, complementadas por normas sectoriales dispersas, lo que configura un sistema fragmentado sin obligaciones sistemáticas de registro ni notificación de incidentes. En datos abiertos, el desempeño es muy bajo según ODIN 2024/2025, con 23/100 y puesto 194 global, evidenciando ausencia o interrupción de estadísticas clave y una publicación altamente fragmentada, sin portal nacional operativo ni licencias abiertas que permitan reutilización. En ciberseguridad, aunque se creó en 2024 el Consejo Nacional de Ciberseguridad y existe un Sistema Nacional de Seguridad Informática supervisado por SUSCERTE, el país carece de una estrategia nacional formal, operando con capacidades parciales y coordinación limitada. En infraestructuras críticas, no existe ley específica, pero normas técnicas sobre tecnologías libres establecen requisitos de seguridad, continuidad e integridad para sistemas estatales, lo que configura un marco técnico parcial sin institucionalidad integral.

En la dimensión de implementación y acceso, el modelo presenta avances legales puntuales pero sin integración sistémica. La Ley de Infogobierno define principios para el uso de tecnologías en el sector público y la interacción con la ciudadanía, aunque no se traduce en un ecosistema interoperable consolidado. El país no dispone de una identidad digital nacional integrada: la identificación se basa en la cédula física y en un régimen de firma electrónica que reconoce validez jurídica de transacciones digitales, pero sin plataforma estatal unificada de autenticación. En conectividad, la infraestructura es baja, con 24,46 puntos, limitada cobertura fija, baja penetración móvil y velocidades reducidas, lo que restringe el despliegue efectivo de servicios digitales. El acceso a Internet no es derecho constitucional, aunque se reconoce como prioridad nacional, y el acceso a la información pública carece de ley específica y de sistema nacional de solicitudes, operando mediante mecanismos fragmentados y discrecionales. En conjunto, Venezuela configura un modelo de gobernanza digital incipiente y discontinuo, donde la ausencia de coordinación estratégica y de marcos integrales limita la consolidación de un ecosistema digital coherente, interoperable y basado en estándares institucionales estables.

Análisis comparativo de los modelos

A partir de la matriz comparativa elaborada, es posible realizar una **primera lectura transversal de los modelos de gobernanza digital presentes en los 22 países de Iberoamérica**, identificando patrones, convergencias y diferencias relevantes. Si bien el estudio no propone en esta etapa un ranking exhaustivo ni una evaluación normativa del desempeño de los países, el análisis preliminar de las dimensiones relevadas permite

distinguir **trayectorias diferenciadas de institucionalización, integración y capacidad de implementación** de la gobernanza digital en un sentido amplio.

Desde esta perspectiva, los resultados muestran que el grado de avance de la gobernanza digital no depende exclusivamente de la existencia de marcos normativos o estrategias sectoriales, sino de la **coherencia del ecosistema digital en su conjunto**. En particular, los países que presentan mayores niveles de madurez relativa son aquellos que logran articular de manera consistente la definición de una visión estratégica de largo plazo, la construcción de capacidades habilitantes y la materialización de políticas en servicios, infraestructuras y derechos efectivos en el entorno digital.

Asimismo, cabe señalar que, los resultados de este análisis comparativo no necesariamente se condicen de manera lineal con los desempeños que arrojan el Índice de Gobierno Electrónico de Naciones Unidas (Anexo II) ni el Índice de Gobierno Digital de la OCDE (Anexos III y IV). Ello se explica, en primer lugar, porque nuestra metodología adopta un abordaje más integral y sistémico, orientado a examinar no sólo la provisión de servicios digitales o el grado de digitalización administrativa, sino la articulación entre visión estratégica de largo plazo, arquitectura institucional, capacidades habilitantes, infraestructura pública digital, **pero con especial atención a la presencia o ausencia de marcos regulatorios y normativas que permitan garantizar derechos en el entorno digital.** En segundo lugar, se trata de un análisis predominantemente cualitativo, que busca captar dinámicas institucionales, coherencia de políticas y capacidades de coordinación intergubernamental, dimensiones que no siempre son plenamente reflejadas en índices compuestos basados en indicadores estandarizados. En consecuencia, los hallazgos aquí presentados no son estrictamente comparables con dichos rankings, sino que los complementan, aportando una lectura más estructural sobre la madurez de los modelos de gobernanza digital en Iberoamérica.

Una primera observación transversal es la existencia de **desacoples frecuentes entre dimensiones**. En numerosos países se verifican avances significativos en la digitalización de servicios públicos y en la oferta de trámites en línea, que no siempre se corresponden con un desarrollo equivalente de capacidades habilitantes como la gobernanza de datos, la interoperabilidad de sistemas o la institucionalización de la ciberseguridad. Este patrón da lugar a ecosistemas digitales funcionales en el corto plazo, pero potencialmente frágiles desde el punto de vista de la sostenibilidad, la escalabilidad y la protección de derechos.

Asimismo, el análisis evidencia que la **institucionalización de la gobernanza digital** —entendida como la existencia de arreglos estables de rectoría, coordinación y responsabilidad— constituye un factor clave para explicar diferencias entre países con niveles similares de digitalización. En este sentido, la continuidad de las políticas, la claridad en la asignación de competencias y la capacidad de coordinar múltiples dimensiones y actores emergen como variables tan relevantes como los niveles de inversión o el desarrollo tecnológico.

Sobre la base de los criterios definidos en el marco metodológico, y con fines analíticos y exploratorios, el estudio propone una **tipología preliminar de modelos de gobernanza digital**, que agrupa a los países según el grado de madurez de sus enfoques en un sentido amplio. Esta tipología no pretende establecer jerarquías cerradas, sino identificar

trayectorias diferenciadas de desarrollo institucional, que serán profundizadas en etapas posteriores del estudio (Ver Tabla 1)[80].

Un primer grupo reúne a países que han logrado consolidar **modelos avanzados e integrales de gobernanza digital**, caracterizados por marcos estratégicos claros, alta institucionalización, mecanismos estables de coordinación y una fuerte capacidad de implementación. En estos casos, la gobernanza digital se concibe como una política de Estado, con articulación efectiva entre visión estratégica, capacidades habilitantes y provisión de servicios. En este grupo se ubican España, Uruguay, Brasil, Chile y Colombia que, con trayectorias y contextos distintos, presentan enfoques relativamente coherentes y sostenidos en el tiempo.

Un segundo grupo corresponde a **modelos en consolidación avanzada**, integrados por países que exhiben avances significativos y capacidades relevantes en múltiples dimensiones, con resultados concretos en la digitalización del Estado y en la provisión de servicios públicos digitales. No obstante, estos modelos enfrentan desafíos persistentes de integración transversal, coordinación institucional o continuidad, lo que limita su consolidación como enfoques plenamente sistémicos. En este grupo se incluyen Argentina, Portugal, Costa Rica y Perú. En particular, algunos de estos países combinan un alto nivel de desarrollo normativo y técnico con procesos de implementación fragmentados o dependientes de coyunturas políticas, lo que genera avances relevantes pero desiguales entre dimensiones y a lo largo del tiempo.

Un tercer grupo agrupa a países con **modelos intermedios o fragmentados de gobernanza digital**, donde conviven desarrollos normativos o estratégicos relevantes en algunas áreas con debilidades significativas en otras. En estos casos, la digitalización del Estado avanza de manera desigual, dependiendo en gran medida de iniciativas sectoriales o programas específicos, con menor articulación entre los niveles estratégico, habilitante y operativo. En este grupo se ubican, entre otros, México, Colombia, Ecuador, Panamá, Paraguay y República Dominicana.

Finalmente, un cuarto grupo incluye a países con **modelos incipientes o con brechas estructurales persistentes**, caracterizados por un bajo nivel de institucionalización transversal, marcos normativos incompletos o desactualizados y capacidades institucionales limitadas para la implementación sostenida de políticas digitales. En estos contextos, las brechas en conectividad, capital humano y recursos estatales condicionan fuertemente el desarrollo de ecosistemas digitales integrales. Este grupo comprende, entre otros, a Bolivia, Guatemala, Honduras, Nicaragua, Venezuela, Cuba y El Salvador.

Este análisis preliminar pone de manifiesto que las principales diferencias entre los países no se explican únicamente por el nivel de digitalización alcanzado, sino por la **capacidad de los Estados para articular de manera coherente la visión estratégica, las capacidades habilitantes y la implementación operativa**, así como por la estabilidad de los arreglos

[80] *Digital Government Index and Open, Useful and Re-usable Data Index: 2025 results and key findings* (OECD Working Papers on Public Governance No. 90). OECD, 2026. Disponible en https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/02/digital-government-index-and-open-useful-and-re-usable-data-index_dbe102ed/6347ec74-en.pdf

institucionales que sostienen dicha articulación. Estas conclusiones iniciales constituyen la base para el desarrollo de los estudios en profundidad y para la formulación de recomendaciones de política pública diferenciadas, orientadas a fortalecer la gobernanza digital en la región.

Tabla 1. Tipología preliminar de modelos de gobernanza digital en Iberoamérica

Grupo de países	Caracterización del modelo de gobernanza digital	Rasgos distintivos del enfoque	Países incluidos (preliminar)
Grupo I – Modelos avanzados e integrales	Países que presentan un enfoque **sistémico e integrado** de la gobernanza digital, con marcos estratégicos claros, alta institucionalización y una fuerte capacidad de implementación. La gobernanza digital se concibe como política de Estado y se sostiene en el tiempo.	Estrategias digitales nacionales integrales; gobernanza explícita de Internet e IA; capacidades habilitantes consolidadas (datos, ciberseguridad, identidad digital, interoperabilidad); provisión madura de servicios públicos digitales y fuerte enfoque en derechos y confianza.	España, Uruguay, Brasil, Chile, Portugal
Grupo II – Modelos en consolidación avanzada	Países con **avances significativos y marcos relevantes**, que muestran capacidad técnica e institucional, pero con desafíos pendientes de integración, continuidad o coordinación transversal.	Estrategias y marcos normativos robustos en varios ejes; buen desarrollo de gobierno digital; avances en datos, IA y ciberseguridad; persistencia de fragmentación institucional o brechas de implementación.	Colombia Argentina, Costa Rica, Perú, México
Grupo III – Modelos intermedios o fragmentados	Países con desarrollos parciales y **heterogéneos entre dimensiones**, donde conviven avances normativos con capacidades institucionales limitadas o implementación desigual.	Presencia de políticas o leyes sectoriales; menor articulación entre bloques estratégicos, habilitantes y operativos; servicios digitales en expansión, pero con restricciones de interoperabilidad, datos o gobernanza transversal.	Andorra, Ecuador, Panamá, Paraguay, República Dominicana

Grupo IV – Modelos incipientes o con brechas estructurales	Países donde la gobernanza digital presenta un **bajo nivel de institucionalización**, con marcos incompletos o desactualizados y capacidades limitadas para la implementación sostenida.	Ausencia o debilidad de estrategias integrales; rectoría digital poco definida; escasa articulación institucional; servicios digitales limitados y brechas significativas de acceso, capacidades y confianza.	Bolivia, Guatemala, Honduras, Nicaragua, Venezuela, Cuba, El Salvador

Hallazgos transversales

El análisis comparado de las distintas dimensiones de la gobernanza digital en los países iberoamericanos permite identificar una serie de **hallazgos transversales** que atraviesan el conjunto del estudio y aportan claves interpretativas para comprender las diferencias observadas entre modelos nacionales. Es importante destacar que estos hallazgos no constituyen conclusiones definitivas, sino **tendencias emergentes** que serán profundizadas en las siguientes etapas del trabajo:

- **Desacople entre digitalización de servicios y capacidades habilitantes.** Un primer patrón recurrente es el avance más acelerado de la digitalización de servicios públicos en relación con la consolidación de capacidades habilitantes como la gobernanza de datos, la interoperabilidad de sistemas o la institucionalización de la ciberseguridad. En varios países, la expansión de trámites y plataformas digitales no siempre se encuentra acompañada por marcos robustos de gestión de datos, coordinación interinstitucional y protección de derechos, lo que puede derivar en ecosistemas digitales funcionales en el corto plazo, pero frágiles desde el punto de vista de su sostenibilidad, escalabilidad y resiliencia.
- **La institucionalización como factor explicativo clave.** Más allá del nivel de desarrollo económico o de inversión tecnológica, el análisis sugiere que la **estabilidad y claridad de los arreglos institucionales** constituye un factor central para explicar diferencias entre países con desempeños similares en indicadores de digitalización. La existencia de rectorías claras, mecanismos de coordinación transversal y responsabilidades bien definidas emerge como un elemento determinante para sostener avances en el tiempo y evitar abordajes fragmentados o dependientes de coyunturas políticas.
- **Heterogeneidad interna en modelos aparentemente similares.** Incluso entre países ubicados en un mismo grupo de la tipología preliminar, se observa una **alta heterogeneidad en la profundidad y coherencia de las distintas dimensiones de la gobernanza digital**. Algunos países presentan desarrollos normativos avanzados pero capacidades limitadas de implementación, mientras que otros muestran resultados operativos relevantes con marcos estratégicos o regulatorios menos consolidados. Esta heterogeneidad refuerza la necesidad de evitar lecturas simplificadoras y de analizar los modelos de gobernanza digital como configuraciones complejas y dinámicas.

- **Gobernanza de la inteligencia artificial como proxy de madurez reciente.** La forma en que los países abordan la gobernanza de la inteligencia artificial —ya sea a través de estrategias nacionales, marcos éticos, arreglos institucionales o participación en espacios internacionales— aparece como un **indicador temprano de madurez institucional** en la agenda digital. Aquellos países que han avanzado en la definición de enfoques integrales de gobernanza de la IA tienden a mostrar mayores capacidades de coordinación intersectorial y de alineamiento con principios de derechos, lo que sugiere un potencial efecto catalizador sobre otras dimensiones de la gobernanza digital.
- **La dimensión internacional como acelerador de capacidades.** La participación activa en espacios internacionales y regionales de cooperación emerge como un **factor habilitante relevante**, especialmente para países con niveles intermedios de desarrollo. Estos ámbitos funcionan como plataformas de aprendizaje entre pares, armonización de enfoques normativos y fortalecimiento de capacidades técnicas e institucionales, contribuyendo a reducir asimetrías y a acelerar procesos de institucionalización de la gobernanza digital a nivel nacional.
- **Persistencia de brechas estructurales.** Finalmente, el análisis confirma la persistencia de **brechas estructurales** en conectividad, capital humano y capacidades estatales que condicionan el desarrollo de modelos integrales de gobernanza digital en varios países de la región. Estas brechas no solo afectan la provisión de servicios digitales, sino también la posibilidad de implementar marcos de gobernanza robustos y sostenibles, lo que plantea desafíos específicos para el diseño de políticas públicas y para la cooperación regional.

Capítulo 2. Hacia un modelo integral de gobernanza digital para Iberoamérica.

El análisis comparado desarrollado en el capítulo anterior puso en evidencia una realidad compleja: Iberoamérica ha avanzado de manera significativa en la construcción de fundamentos digitales, pero enfrenta desafíos persistentes vinculados a la heterogeneidad institucional, la fragmentación normativa, las brechas de capacidades estatales y la necesidad de articular la transformación digital con objetivos de desarrollo sostenible, legitimidad democrática y autonomía estratégica.

Proponer un modelo integral de gobernanza digital para la región exige, por tanto, partir de estos desafíos concretos. Un modelo no puede surgir como un diseño abstracto o normativo desligado de la realidad regional; debe ofrecer respuestas a las brechas identificadas, dialogar con las capacidades existentes y proyectar una arquitectura institucional capaz de anticipar las transformaciones tecnológicas en curso.

En este sentido, como punto de partida se revisa el modelo institucional recientemente propuesto por la CEPAL para América Latina y el Caribe. Dado su peso técnico y su influencia en la agenda Latinoamericana, resulta indispensable analizar sus fundamentos conceptuales, su arquitectura institucional y sus supuestos normativos. Este examen no persigue

desestimarlo, sino identificar sus aportes y límites a la luz de los desafíos actuales de la gobernanza digital en Iberoamérica.

A partir de este análisis crítico —y en diálogo con la literatura internacional y las experiencias comparadas examinadas en el Capítulo 1— el presente capítulo formula una propuesta superadora. El modelo que aquí se desarrolla no nace de cero: se apoya en los avances conceptuales existentes, pero los reinterpreta e integra en una arquitectura más amplia, que incorpora dimensiones estratégicas, multinivel, geopolíticas y de derechos digitales, con el objetivo de fortalecer la capacidad de los Estados iberoamericanos para conducir la transformación digital de manera coherente, inclusiva y orientada al desarrollo sostenible.

Desafíos de Iberoamérica para consolidar modelos robustos de Gobernanza Digital.

Los gobiernos operan en un entorno cada vez más complejo, caracterizado por transformaciones demográficas, ambientales y digitales de gran magnitud, en un contexto de bajos niveles de confianza ciudadana y crecientes restricciones fiscales[81]. La velocidad de adopción tecnológica, especialmente por parte de actores económicos y de la ciudadanía, está superando la capacidad de los Estados para regular, coordinar, implementar y supervisar el uso de tecnologías digitales y de inteligencia artificial [82] [83] [84].

Sin embargo, los desafíos de la gobernanza digital se manifiestan de manera distinta entre los países iberoamericanos, como así también a nivel intrarregional.

En Latinoamérica, los principales desafíos se relacionan con las capacidades estatales para sostener políticas digitales en el tiempo; la fragmentación institucional; la debilidad en la gobernanza de datos, como así también, con factores estructurales como las grandes desigualdades territoriales y sociales en el acceso y uso de servicios digitales. A ello se suma una mayor dependencia tecnológica de infraestructuras, plataformas y proveedores extra-regionales, que limita los márgenes de autonomía estratégica [85].

---

[81] Organización para la Cooperación y el Desarrollo Económicos (OCDE) & Banco Interamericano de Desarrollo (BID). (2024). Índice de Gobierno Digital OCDE-BID 2023: América Latina y el Caribe (OECD Public Governance Policy Papers). OCDE y BID. https://www.oecd.org/en/publications/government-at-a-glance-2025_0efd0bcd-en.html

[82] OECD (2021). *Governance of Digital Regulation*. OECD Publishing, Paris. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464

[83] CEPAL (2025). *Superar las trampas del desarrollo de América Latina y el Caribe en la era digital*. Santiago: Naciones Unidas. https://conferenciaelac.cepal.org/9/sites/elac9/files/s2401013_es.pdf

[84] Relatoria del Diálogo Regional “Los retos de la gobernanza digital en América Latina y el Caribe”.(CAF,2026). Disponible en: https://scioteca.caf.com/bitstream/handle/123456789/2586/Relator%C3%ADa%20del%20di%C3%A1logo%20regional.%20Los%20retos%20de%20la%20gobernanza%20digital%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf?sequence=1&isAllowed=y

[85] Relatoría del Diálogo Regional “Los retos de la gobernanza digital en América Latina y el Caribe”.(CAF, 2026). Disponible en: https://scioteca.caf.com/bitstream/handle/123456789/2586/Relator%C3%ADa%20del%20di%C3%A1logo%20regional.%20Los%20retos%20de%20la%20gobernanza%20digital%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf?sequence=1&isAllowed=y

Una caracterización reciente sobre los desafíos que enfrenta la gobernanza digital en América Latina y el Caribe se presentó en el Diálogo Regional “Los retos de la gobernanza digital en América Latina y el Caribe” organizado por la CAF y el PNUD en Montevideo a finales de diciembre de 2025.

A partir de la **Relatoría del Diálogo Regional “Los Retos de la Gobernanza Digital en América Latina y el Caribe”**[86], los principales retos de la gobernanza digital en la región se estructuran en torno a un diagnóstico compartido que trasciende lo tecnológico y se sitúa en el plano institucional, democrático y estratégico,

El punto de partida es una constatación central: la digitalización y la inteligencia artificial avanzan más rápido que la capacidad institucional de los Estados para regular, coordinar y supervisar su uso. Esta asimetría no es sólo normativa, sino estructural, y se expresa en déficits interrelacionados de infraestructura, capital humano e institucionalidad. En materia regulatoria, el diálogo identificó que el problema no radica en la ausencia de estrategias o declaraciones, sino en el déficit de implementación efectiva. El desafío principal es fortalecer autoridades con mandato claro, presupuesto y coordinación interinstitucional, evitando que la regulación quede en el plano declarativo .

Otro eje crítico es la fragmentación institucional para la adopción tecnológica. Ministerios y entidades adquieren soluciones sin una gobernanza técnica transversal, lo que genera duplicidades, riesgos de seguridad y pérdida de control estratégico. A ello se suman brechas en la retención de talento digital y limitaciones para sostener capacidades críticas, especialmente en ciberseguridad y mantenimiento tecnológico. La gobernanza de datos y la soberanía estratégica emergen como retos estructurales. Se señala la dependencia de infraestructura y procesamiento externos, la limitada capacidad regional para desarrollar modelos propios y el riesgo de reproducir dinámicas de “extractivismo digital”, donde se exportan datos y se importan soluciones de alto valor agregado.

En el plano democrático, los riesgos asociados a la desinformación, la microsegmentación, los deepfakes y la violencia digital (particularmente contra mujeres en política) ocupan un lugar central. El reto consiste en integrar salvaguardas democráticas desde el diseño, fortalecer agencias con autonomía técnica y evitar respuestas estatales que, bajo el argumento de combatir la desinformación, deriven en censura o restricciones indebidas de derechos[87].

Finalmente, el diálogo identifica desafíos persistentes de inclusión, participación y legitimidad. Las brechas de conectividad, habilidades digitales y usabilidad limitan la apropiación tecnológica y pueden erosionar la confianza institucional si la digitalización sustituye el trato humano sin garantías adecuadas. La legitimidad del Estado digital depende, según el documento, de asegurar acceso universal, derecho a la información sobre sistemas

[86] La relatoría del evento se encuentra disponible en: https://scioteca.caf.com/bitstream/handle/123456789/2586/Relator%C3%ADa%20del%20di%C3%A1logo%20regional.%20Los%20retos%20de%20la%20gobernanza%20digital%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf?sequence=1&isAllowed=y

[87] CAF – Banco de Desarrollo de América Latina y el Caribe & Programa de las Naciones Unidas para el Desarrollo (PNUD). (2026). Relatoría del Diálogo Regional “Los retos de la gobernanza digital en América Latina y el Caribe” (Montevideo, 26–28 de noviembre de 2025).

automatizados, derecho a atención humana y mecanismos efectivos de participación con devolución pública de resultados[88].

En consonancia con estos hallazgos, los resultados del ***Índice de Gobierno Digital 2023 (DGI 2023)*** **para América Latina y el Caribe** refuerzan este diagnóstico desde una perspectiva comparada[89] (Ver Anexo 4)**.** A través de esta herramienta, la OCDE identifica obstáculos estructurales que limitan la consolidación del gobierno digital en la región, especialmente en términos de alineación estratégica, coordinación transversal, gestión de datos y fortalecimiento institucional.

En primer lugar, la OCDE señala en ALC ciertas debilidades en la alineación de las Estrategias Nacionales de Gobierno Digital con otras políticas públicas, así como insuficiencias en la creación de mecanismos de gobernanza colaborativa y en el desarrollo y gestión del talento digital, elementos considerados clave para sostener la agenda de modernización del Estado[90].

En segundo término, si bien ALC ha avanzado en la habilitación del intercambio de datos entre instituciones públicas, los niveles de madurez siguen siendo inferiores al promedio de la OCDE. Persisten limitaciones en la cobertura gubernamental y en el alcance efectivo de los datos compartidos, así como en la publicación y (re) utilización de conjuntos de datos de alto valor. A ello se suma un progreso aún incipiente en materia de transparencia algorítmica, lo que puede afectar la rendición de cuentas y la confianza en los servicios y políticas públicas habilitados digitalmente[91].

Asimismo, el informe de OCDE advierte brechas relevantes en la integración sistemática de la retroalimentación de los usuarios y en la adopción de enfoques participativos para el diseño de servicios públicos digitales. ALC presenta avances limitados en la evaluación de barreras al co-diseño de servicios y en la incorporación de mecanismos estructurados de participación[92].

Finalmente, la OCDE destaca la falta de metas e iniciativas estratégicas orientadas a la prestación de servicios proactivos, el uso todavía insuficiente de datos para fortalecer el monitoreo de políticas públicas y la baja integración estratégica de inteligencia artificial confiable en el sector público. En conjunto, estos desafíos revelan la necesidad de reforzar los sistemas de monitoreo y evaluación de las políticas de gobierno digital como condición para avanzar hacia mayores niveles de madurez institucional[93].

En contraste, entre los países europeos que integran el espacio iberoamericano (España, Portugal y Andorra) los desafíos se sitúan en un plano distinto. Los resultados del ***Digital***

---

[88] Ídem.
[89] 2023 OCDE/BID Índice de Gobierno Digital de América Latina y el Caribe. Disponible en https://www.oecd.org/es/publications/2024/11/2023-oecd-idb-digital-government-index-of-latin-america-and-the-caribbean_5a9af6c4.html
[90] 2023 OCDE/BID Índice de Gobierno Digital de América Latina y el Caribe. Disponible en https://www.oecd.org/es/publications/2024/11/2023-oecd-idb-digital-government-index-of-latin-america-and-the-caribbean_5a9af6c4.html
[91] Ídem
[92] Ídem
[93] Ídem.

Government Index 2025[94] muestran trayectorias de mayor consolidación institucional (ver Anexo 3). España y Portugal presentan marcos estratégicos consolidados e infraestructura digital pública robusta, con un alto nivel de integración de tecnologías en la modernización del sector público. No obstante, enfrentan retos vinculados a la profundización del modelo, particularmente en la capacidad de transformar infraestructura y datos en servicios plenamente anticipatorios, fortalecer mecanismos sistemáticos de participación ciudadana y avanzar en transparencia en el uso de tecnologías avanzadas[95]. En estos casos, el desafío no reside en la construcción de capacidades básicas, sino en la sofisticación del uso estratégico de datos para el monitoreo de políticas, la automatización de procesos complejos y la prestación proactiva de servicios[96].

El caso de Andorra presenta un perfil distinto. Si bien ha avanzado en la digitalización administrativa y en la adopción de soluciones tecnológicas, los resultados muestran que enfrenta mayores desafíos para consolidar capacidades institucionales transversales, escalar la interoperabilidad y fortalecer la gobernanza estratégica de datos. Las limitaciones asociadas a la escala estatal se reflejan en la necesidad de reforzar coordinación, especialización técnica y sostenibilidad de las capacidades digitales, más que en la mera incorporación de nuevas herramientas[97].

Mientras que en los países ibéricos el reto principal se vincula con la profundización y sofisticación del modelo —particularmente en la prestación anticipatoria de servicios, el uso **Por lo tanto, la comparación muestra que los desafíos de gobernanza digital dentro de Iberoamérica se ubican en distintos estadios de desarrollo institucional: mientras que en los países ibéricos predominan retos asociados a la sofisticación y optimización de capacidades ya instaladas, en buena parte de América Latina persiste una agenda de consolidación estructural orientada a fortalecer coherencia estratégica, capacidades y mecanismos de implementación.**

A modo de síntesis, a continuación se mencionan los principales retos para la gobernanza digital iberoamericana:

- **Fragmentación normativa y asimetrías regulatorias.** La coexistencia de marcos legales dispares, niveles heterogéneos de madurez institucional y velocidades de adopción tecnológica dificulta la interoperabilidad regional, encarece el cumplimiento regulatorio y limita la construcción de un espacio digital iberoamericano coherente.
- **Capacidades estatales desiguales y brechas de implementación.** Si bien muchos países cuentan con estrategias, leyes o agendas digitales formales, persiste una brecha significativa entre el diseño normativo y su implementación efectiva, asociada a limitaciones técnicas, presupuestarias y de recursos humanos en el sector público.
- **Dependencia tecnológica y limitada autonomía estratégica digital.** La fuerte concentración de infraestructuras críticas, plataformas digitales y servicios de nube en actores extra-regionales como las grandes empresas tecnológicas reduce los márgenes de decisión soberana, incrementa riesgos de lock-in tecnológico y debilita

[94] OECD (2026). Digital Government Index and Open, Useful and Re-usable Data Index: 2025 Results and Key Findings. OECD Working Papers on Public Governance, No. 90. OECD Publishing.
[95] Ídem.
[96] Ídem.
[97] Ídem.

la capacidad de los Estados (principalmente entres los países iberoamericanos no europeos) para incidir en estándares y reglas globales.

- **Déficits en gobernanza de datos y uso estratégico de la información pública** Persisten problemas de calidad, interoperabilidad, reutilización y protección de datos, así como una adopción incipiente de enfoques de gobierno basado en evidencia, lo que limita el potencial transformador de la digitalización y de la inteligencia artificial en la gestión pública.
- **Brechas territoriales y sociales en el acceso y uso de servicios digitales.** La digitalización puede profundizar desigualdades preexistentes, especialmente en términos de conectividad, alfabetización digital, acceso a servicios públicos digitales y protección de derechos en entornos digitales (reto muy marcado entre los países iberoamericanos no europeos que parten de desigualdades estructurales).
- **Gobernanza de la inteligencia artificial aún incipiente y reactiva.** En muchos países, los marcos de gobernanza de la IA se encuentran en etapas tempranas, con enfoques fragmentados o sectoriales, escasa coordinación interinstitucional y capacidades limitadas para evaluar riesgos, impactos y oportunidades de manera integral.
- **Debilidad de los mecanismos de coordinación regional.** A pesar de la existencia de múltiples foros y espacios de diálogo, la cooperación regional en gobernanza digital sigue siendo fragmentada, con dificultades para traducir consensos políticos en instrumentos operativos, estándares comunes o proyectos conjuntos de alto impacto.
- **Tensiones entre innovación, regulación y protección de derechos.** Los Estados enfrentan el desafío de diseñar marcos regulatorios que promuevan la innovación y el desarrollo productivo, sin descuidar la protección de derechos fundamentales, la transparencia algorítmica, la no discriminación y la rendición de cuentas.
- **Limitada articulación público–privada y con el ecosistema tecnológico.** La gobernanza digital requiere mecanismos más sistemáticos de diálogo con empresas, academia y sociedad civil, que permitan anticipar tendencias tecnológicas, co-crear soluciones y reducir brechas entre regulación y realidad tecnológica.
- **Escasa inserción estratégica en la gobernanza digital global.** Los países no europeos de Iberoamérica enfrentan dificultades para incidir de manera coordinada en los espacios globales donde se definen estándares, principios y reglas del ecosistema digital, lo que refuerza una posición más reactiva que proactiva en la agenda internacional.

En este sentido, la gobernanza digital en Iberoamérica requiere modelos capaces de dialogar con realidades heterogéneas, pero articulados en torno a un núcleo común: **fortalecer las capacidades del Estado, garantizar derechos, promover la participación multiactor y asegurar que la transformación digital contribuya efectivamente a la legitimidad democrática y al desarrollo sostenible.**

Antecedentes conceptuales para la construcción del modelo propuesto

Como punto de partida se analiza el modelo institucional recientemente propuesto por CEPAL, publicado en septiembre de 2026, orientado a los desafíos de la gobernanza digital de ALC. Cabe destacar que este modelo se encuentra fuertemente alineado con los principios y recomendaciones de la OCDE en materia de gobierno digital, particularmente en lo referido a liderazgo político, coordinación transversal e interoperabilidad. Asimismo, es coherente con

la visión de la ONU sobre la transformación digital como instrumento del desarrollo sostenible. No obstante, su foco permanece predominantemente en la modernización administrativa del Estado, con menor desarrollo de las dimensiones de gobernanza digital sistémica, derechos digitales y regulación del ecosistema tecnológico global, que hoy ocupan un lugar central en la agenda multilateral.

A partir de este análisis, se identifican fortalezas y debilidades del modelo CEPAL, a fin de avanzar hacia una propuesta institucional superadora y adaptada a las particularidades de Iberoamérica. Concretamente, se busca ampliar el enfoque desde una perspectiva centrada en la eficiencia y la coordinación intraestatal hacia una concepción más integral de la gobernanza digital, que incorpore la dimensión multinivel, la economía política de la transformación tecnológica, la protección efectiva de derechos, la gobernanza de datos e inteligencia artificial, así como la inserción estratégica de la región en el ecosistema digital global. El modelo que aquí se propone se apoya en los avances conceptuales existentes, pero los reinterpreta a la luz de los desafíos contemporáneos, con el objetivo de ofrecer una arquitectura institucional más robusta, democrática y estratégicamente orientada al desarrollo sostenible de la región.

Sobre el modelo institucional de Gobierno Digital de CEPAL[98]

El modelo institucional que propone la **CEPAL** en la "*Guía para el establecimiento de un marco de gobernanza de gobierno digital"* es un **modelo jerárquico, integral y articulado en tres niveles de gobernanza**, diseñado para asegurar coherencia estratégica, capacidad normativa y ejecución efectiva de la transformación digital del Estado.

El núcleo del modelo institucional de la CEPAL se estructura en torno a una arquitectura jerárquica de tres niveles de gobernanza —estratégica, rectora y ejecutora— que delimitan con claridad funciones, atribuciones y responsabilidades. **Esta estructura es presentada explícitamente como una condición necesaria para evitar la fragmentación institucional y asegurar coherencia en la transformación digital del Estado[99]. Estas jerarquías son ámbitos diferenciados pero interdependientes, cuya articulación** debe **ser tanto horizontal como vertical.**

En la cúspide del modelo se sitúa la **gobernanza estratégica**, concebida como la instancia de conducción política de alto nivel. Este nivel tiene como funciones articular actores clave, establecer políticas y prioridades, comprometer recursos y facilitar acuerdos interinstitucionales[100]. Esta instancia debe contar con atribuciones para definir ámbitos estructurales, institucionalidad, recursos y competencias, asegurando coherencia en la estrategia digital del país[101]. La gobernanza estratégica puede materializarse en instancias como comisiones nacionales de transformación digital o comités de ministros, integrados por

[98] Esta sección fue elaborada en base a la siguiente publicación: Comisión Económica para América Latina y el Caribe. (2025). Guía para el establecimiento de un marco de gobernanza de gobierno digital para países de América Latina y el Caribe. Metodologías de la CEPAL (8) (LC/PUB.2025/13-P). Disponible en: https://www.cepal.org/es/publicaciones/82454-guia-establecimiento-un-marco-gobernanza-gobierno-digital-paises-america-latina
[99] Ídem, página 17.
[100] Ídem, página 17.
[101] Ídem, página 28

carteras clave (Presidencia, Ciencia y Tecnología, Hacienda, Planificación, Economía, Industria y Comercio, entre otras)[102]. Además, puede contemplar la articulación con actores del sector privado, la academia y la sociedad civil, ampliando su carácter multiactor[103]. La función sustantiva de este nivel es identificar prioridades nacionales en materia de modernización del Estado y asegurar que los proyectos estructurales cuenten con respaldo político y recursos para su implementación. Se trata, en consecuencia, de una instancia de dirección estratégica que debe operar más allá de los ciclos políticos de corto plazo[104].

El segundo nivel corresponde a la **gobernanza rectora**, encargada de establecer el marco normativo y técnico que habilita la implementación del gobierno digital. De acuerdo con el modelo, esta jerarquía tiene atribuciones para definir leyes, decretos, resoluciones y normas técnicas, así como para monitorear y auditar su cumplimiento[105]. Su función no se limita a producir normativa, sino que incluye la definición de estándares comunes, lineamientos técnicos y orientaciones metodológicas que permitan asegurar coherencia y compatibilidad entre las distintas iniciativas sectoriales (salud, educación, cultura, industria, etc).[106]. La gobernanza rectora constituye el nivel normativo-regulador del modelo: busca garantizar estabilidad jurídica, homogeneidad técnica y continuidad en la implementación, lo que esencial para evitar superposiciones y vacíos de responsabilidad[107], una problemática frecuente en los procesos de digitalización estatal en la región. En términos institucionales, esta instancia puede adoptar la forma de un ministerio, secretaría o agencia rectora con rango suficiente y mandato explícito en materia de transformación digital.

Finalmente, el tercer nivel corresponde a la **gobernanza ejecutora**, responsable de la implementación operativa de las iniciativas digitales. Según el modelo, esta jerarquía debe contar con atribuciones para definir, diseñar, implementar y mejorar soluciones transversales, así como para articular procesos, información y tecnología[108]. Esta instancia que puede adoptar la forma de secretaría, agencia o división especializada, tiene a su cargo la ejecución de proyectos transversales en coordinación con soluciones sectoriales y con instituciones descentralizadas, como gobiernos locales y organismos autónomos. Además, tiene funciones en áreas como gobernanza de datos e inteligencia artificial, gestión de interoperabilidad (normativa, organizacional, semántica y técnica), gestión de seguridad de la información, arquitectura de plataformas y gestión del cambio[109].

En la Tabla 2, se ofrece una síntesis comparativa de la arquitectura institucional de los tres niveles de gobernanza del modelo de CEPAL.

Tabla 2. Arquitectura institucional del modelo de gobernanza digital de CEPAL

[102] Ídem, página 31.
[103] Ídem, página 32.
[104] Ídem, página 31
[105] Ídem, páginas 17 y 28.
[106] Ídem, página 28.
[107] Idem, página 52.
[108] Ídem, página 28.
[109] ídem, páginas 80 y 82

Dimensión	Gobernanza estratégica	Gobernanza rectora	Gobernanza ejecutora
Naturaleza institucional	Instancia político-colegiada de alto nivel (comisión, consejo o comité interministerial).	Institución formal con mandato legal (ministerio, secretaría o agencia rectora).	Entidad técnica-operativa especializada (secretaría, agencia o división de implementación).
Ubicación jerárquica	Cercana al centro de gobierno o Presidencia.	Nivel ministerial o equivalente, con rango suficiente para emitir normas obligatorias.	Nivel técnico-operativo dependiente del órgano rector o del centro de gobierno.
Tipo de autonomía	Autonomía política-estratégica.	Autonomía técnica-normativa.	Autonomía técnica-operativa.
Fuente de autoridad	Liderazgo político y capacidad de comprometer recursos y prioridades nacionales.	Mandato legal explícito y atribuciones regulatorias.	Competencia técnica y capacidad de implementación.
Funciones principales	Definir visión país, prioridades y objetivos estratégicos; articular actores clave; resolver conflictos intersectoriales.	Establecer marco normativo; emitir estándares técnicos; garantizar interoperabilidad; monitorear y auditar cumplimiento.	Diseñar e implementar soluciones transversales; gestionar arquitectura tecnológica, datos, interoperabilidad y ciberseguridad.
Alcance transversal	Interministerial y multiactor (sector privado, academia, sociedad civil).	Transversal a todo el aparato estatal; fija reglas comunes para todos los sectores.	Coordina implementación con ministerios sectoriales y niveles subnacionales.
Capacidades requeridas	Capacidad de coordinación política y asignación presupuestaria; legitimidad institucional.	Capacidad jurídica y técnica; autoridad normativa; capacidad de supervisión.	Capacidades en arquitectura tecnológica, gestión de datos, interoperabilidad, gestión de proyectos y cambio organizacional.

Dimensión	Gobernanza estratégica	Gobernanza rectora	Gobernanza ejecutora
Elementos estructurantes	Estabilidad institucional; continuidad más allá de ciclos políticos; respaldo presupuestario.	Marco legal habilitante; estándares comunes; mecanismos de control y evaluación.	Estructura organizacional especializada; recursos humanos técnicos; infraestructura tecnológica.
Riesgos si es débil	Fragmentación estratégica; falta de visión común; discontinuidad política.	Superposición normativa; falta de estándares comunes; baja coherencia sistémica.	Implementaciones fragmentadas; baja calidad técnica; fallas en interoperabilidad y seguridad.

Fuente: Elaboración propia en base a Guía para el establecimiento de un marco de gobernanza de gobierno digital para países de América Latina y el Caribe, CEPAL, 2026.

Análisis crítico del modelo

El modelo institucional propuesto por la CEPAL constituye un aporte sustantivo y de gran calidad técnica para la ALC, al ofrecer una arquitectura clara, coherente y normativamente sólida para fortalecer la gobernanza del gobierno digital. Su sistematicidad, su alineación con estándares internacionales y su vocación de ordenar funciones y responsabilidades lo convierten en una referencia ineludible para cualquier discusión sobre institucionalidad digital en Iberoamérica. Precisamente por su relevancia, el presente estudio realiza un análisis crítico de sus principales supuestos y alcances, no con el objetivo de desestimarlo, sino de identificar áreas susceptibles de profundización y adaptación al contexto Iberoamericano. A partir de las debilidades o vacíos detectados, se propone un modelo que recoge sus aportes más valiosos, pero que busca ampliarlos e integrarlos en una concepción más integral, estratégica y orientada a derechos de la gobernanza digital. En este sentido, la crítica no se plantea como oposición, sino como punto de partida para una propuesta superadora.

Ofrece una arquitectura institucional sólida para la modernización del gobierno digital; su énfasis en la organización intraestatal y la estandarización administrativa pero deja relativamente subdesarrolladas las dimensiones de economía política, gobernanza multinivel, soberanía tecnológica y regulación del ecosistema digital en sentido amplio. Asimismo, debe tenerse en consideración que ha sido diseñado para fortalecer la gobernanza de los países de ALC y no de Iberoamérica.

Uno de los supuestos implícitos del modelo es la existencia de un nivel relativamente alto de capacidad estatal. La arquitectura propuesta descansa en la presencia de atribuciones claramente definidas, capacidad efectiva de coordinación interministerial, disponibilidad sostenida de recursos técnicos y financieros, así como continuidad política que permita sostener la estrategia digital en el tiempo. Sin embargo, en numerosos países de América Latina y el Caribe, estas condiciones no siempre se verifican: los órganos rectores

suelen ocupar un rango jerárquico limitado dentro de la estructura del Estado, carecen de presupuesto propio, enfrentan alta rotación de autoridades y presentan restricciones técnicas significativas. En este contexto, si bien el modelo resulta normativamente coherente y conceptualmente sólido, puede mostrar limitaciones de aplicabilidad en entornos de baja capacidad institucional. En particular, no desarrolla con suficiente detalle una estrategia de transición gradual que permita avanzar desde escenarios de debilidad estructural hacia el estándar institucional que propone como ideal.

Otro aspecto a considerar es el riesgo de una excesiva centralización derivada del esquema de tres jerarquías propuesto. Si bien la diferenciación entre gobernanza estratégica, rectora y ejecutora busca ordenar funciones y evitar fragmentación, en la práctica puede traducirse en una fuerte concentración de poder en la instancia rectora, con la consecuente subordinación de ministerios sectoriales y potenciales tensiones con gobiernos subnacionales. En países con estructuras federales (como en España, Argentina o Brasil) una implementación predominantemente vertical puede generar resistencias políticas, superposición de competencias y una baja apropiación territorial de las políticas digitales. En este sentido, aunque el modelo reconoce la necesidad de coordinación, su diseño resulta más naturalmente compatible con Estados unitarios que con sistemas federales complejos. La dimensión multinivel aparece mencionada, pero no se encuentra desarrollada con suficiente profundidad como para ofrecer lineamientos claros sobre cómo articular autonomía subnacional y coherencia estratégica nacional.

Un tercer aspecto crítico refiere al alcance conceptual del modelo, que presenta un enfoque predominantemente intraestatal. La propuesta es particularmente sólida en lo que respecta a la gobernanza del gobierno digital, esto es, la organización institucional, la interoperabilidad, la modernización administrativa y la provisión de servicios públicos digitales, pero resulta comparativamente menos desarrollada en dimensiones vinculadas a la gobernanza del ecosistema digital en sentido amplio. Temas como la regulación de plataformas, la economía de datos, la competencia en mercados digitales, la gobernanza de la inteligencia artificial en el sector privado o la gestión de infraestructuras tecnológicas críticas aparecen abordados de manera tangencial o indirecta. **En consecuencia, el modelo se centra principalmente en la digitalización del aparato estatal más que en una concepción sistémica de la gobernanza digital que incluya mercados, empresas tecnológicas, dinámicas geopolíticas y soberanía tecnológica.** Desde una perspectiva más amplia de gobernanza digital —como la que se propone en este estudio— este constituye un límite conceptual relevante, en la medida en que restringe el análisis al ámbito administrativo y no integra plenamente las interacciones entre Estado, sector privado y arquitectura tecnológica global.

Una cuarta limitación se vincula con la ausencia de un enfoque explícito en términos de poder y economía política. El modelo desarrolla con detalle aspectos relativos a la coordinación, la definición de atribuciones y la configuración institucional. Cuestiones como los conflictos interministeriales, la posible captura corporativa, las disputas presupuestarias, la resistencia burocrática o los incentivos políticos reales que moldean el comportamiento de los actores públicos y privados no son abordadas de manera sistemática. En este sentido, se trata de un modelo predominantemente técnico-administrativo, más centrado en el diseño organizacional que en la dimensión político-institucional de la transformación digital. En el contexto latinoamericano, donde los procesos de modernización estatal suelen verse

afectados por cambios de gobierno, inestabilidad de prioridades, uso político de la tecnología o debilidades en la coordinación fiscal, la falta de una estrategia explícita de gestión de la economía política constituye un vacío relevante. La experiencia regional muestra que las reformas digitales no fracasan por ausencia de organigramas formales, sino por la incapacidad de alinear incentivos, sostener acuerdos intersectoriales y garantizar continuidad política en el tiempo.

Una quinta limitación se relaciona con la escasa operacionalización del componente vinculado a datos e inteligencia artificial. Si bien el modelo incorpora nociones como inteligencia institucional, gobernanza de datos e incluso reconoce el carácter estratégico de la IA, el desarrollo conceptual de estas dimensiones permanece relativamente general. No se avanzan, por ejemplo, mecanismos concretos de rendición de cuentas algorítmica, marcos sistemáticos de evaluación de impacto, herramientas de gestión de riesgos ni esquemas de regulación adaptativa que permitan acompañar la rápida evolución tecnológica.

En un contexto post-2022, marcado por la expansión acelerada de modelos de inteligencia artificial generativa, la creciente centralidad de los datos masivos y la consolidación de plataformas digitales con poder estructural, esta falta de especificidad reduce la capacidad del modelo para dialogar con los debates más contemporáneos sobre gobernanza de IA. Desde una perspectiva orientada a la regulación responsable y democrática de tecnologías emergentes, la ausencia de instrumentos concretos para supervisar, auditar y mitigar riesgos algorítmicos constituye una limitación significativa, especialmente para enfoques que buscan integrar explícitamente la protección de derechos, la transparencia y la responsabilidad en el diseño institucional.

Una sexta observación refiere a la centralidad que el modelo otorga a la interoperabilidad, concebida en sus dimensiones legal, organizacional, técnica y semántica. En términos conceptuales, la interoperabilidad aparece como principio estructurante capaz de articular datos, sistemas y procesos, evitando la fragmentación y potenciando la eficiencia sistémica del Estado. Sin embargo, en la práctica, su implementación supone desafíos significativos: requiere inversión sostenida en infraestructura y capacidades, definición y adopción de estándares comunes, desarrollo de arquitecturas compartidas, disciplina institucional para sostener reglas de intercambio de información y, sobre todo, acuerdos políticos duraderos que trasciendan cambios de gobierno.

La experiencia comparada muestra que numerosos países han avanzado parcialmente en esta dirección, pero con resultados desiguales y frecuentemente limitados por restricciones presupuestarias o tensiones interinstitucionales. En este sentido, aunque el modelo reconoce la importancia estratégica de la interoperabilidad, no problematiza con suficiente profundidad los costos de implementación ni la sostenibilidad financiera y política de estas inversiones en el tiempo. La interoperabilidad aparece formulada como un ideal técnico-organizacional deseable, pero menos desarrollada en términos de viabilidad presupuestaria y secuenciación realista en contextos de recursos limitados.

Una séptima observación se vincula con la atención relativamente acotada que el modelo dedica a la dimensión ciudadana, los derechos digitales y la construcción de confianza. La propuesta se encuentra fuertemente orientada a mejorar la eficiencia,

fortalecer la coordinación institucional y modernizar la gestión pública, objetivos sin duda relevantes para la transformación digital del Estado. No obstante, las dimensiones vinculadas a la protección sustantiva de derechos digitales, la garantía robusta de protección de datos personales, la participación ciudadana en entornos digitales, la transparencia algorítmica y los mecanismos de control democrático aparecen desarrolladas con menor profundidad. En un contexto marcado por crisis de legitimidad institucional, desinformación y creciente escrutinio público sobre el uso de tecnologías por parte del Estado, estas dimensiones adquieren una centralidad estratégica. La confianza ciudadana no se construye únicamente a partir de eficiencia operativa, sino también mediante garantías claras de derechos, explicabilidad de decisiones automatizadas y espacios efectivos de participación. Desde esta perspectiva, el modelo podría fortalecer su enfoque incorporando de manera más explícita la dimensión democrática y de derechos como componente estructural, y no sólo complementario, de la gobernanza digital.

Una octava observación es la ausencia de una dimensión geopolítica explícita en el modelo. La propuesta se concentra en la organización interna del Estado y en la mejora de sus capacidades administrativas, pero no aborda de manera sistemática cuestiones como la dependencia tecnológica, la gestión de infraestructuras críticas, la concentración del mercado en proveedores globales, la soberanía sobre servicios en la nube o la geopolítica de los datos. Estos factores, que hoy configuran el entorno estructural en el que operan los Estados, condicionan de manera decisiva las posibilidades reales de autonomía y desarrollo digital. Para América Latina en 2026, en un escenario de creciente fragmentación tecnológica global, disputas por estándares, concentración de capacidades de cómputo e inteligencia artificial en pocas jurisdicciones, y creciente relevancia estratégica de los datos, esta omisión adquiere particular importancia.

Una novena observación se refiere al problema de la implementación secuencial. El modelo presenta una arquitectura institucional coherente y bien estructurada, pero no define con claridad el orden de prioridades, los pasos iniciales ni los criterios de gradualidad. No especifica qué componentes deberían implementarse primero, cuál podría considerarse un mínimo viable institucional, cómo escalar progresivamente las capacidades ni bajo qué criterios priorizar intervenciones en contextos de recursos limitados. Para muchos países de América Latina y el Caribe, donde las restricciones presupuestarias y las capacidades administrativas son heterogéneas, la secuenciación es una condición crítica de viabilidad. La ausencia de lineamientos claros sobre fases, hitos intermedios o trayectorias de implementación puede dificultar la traducción del modelo en políticas concretas y sostenibles en el tiempo.

Propuesta

De la modernización administrativa a la gobernanza digital estratégica iberoamericana

Durante las últimas dos décadas, gran parte de los modelos de transformación digital en la región se han estructurado en torno a la modernización administrativa del Estado: digitalización de trámites, interoperabilidad entre organismos, mejora de servicios públicos y optimización de procesos internos. Estos avances han sido fundamentales para mejorar la

eficiencia, transparencia y calidad de atención a la ciudadanía. Sin embargo, el contexto tecnológico actual, marcado por la expansión de plataformas globales, la concentración de infraestructura digital, el despliegue acelerado de inteligencia artificial y la creciente relevancia geopolítica de los datos— exige una concepción más amplia de la gobernanza digital.

La gobernanza digital actual ya no puede entenderse únicamente como una política sectorial de modernización del aparato estatal. Se configura en un entorno transnacional donde estándares tecnológicos, arquitecturas de nube, proveedores globales, cadenas de valor digitales e infraestructuras críticas condicionan las capacidades soberanas de los Estados. Las decisiones sobre datos, inteligencia artificial, interoperabilidad o ciberseguridad no son meramente técnicas: tienen implicancias económicas, regulatorias y geopolíticas.

En este escenario, los países iberoamericanos enfrentan desafíos estructurales compartidos: dependencia tecnológica externa, asimetrías en capacidades institucionales, fragmentación normativa y limitada capacidad de incidencia en la definición de estándares globales. Individualmente, muchos Estados poseen márgenes acotados para negociar con grandes proveedores tecnológicos o influir en marcos regulatorios internacionales. Colectivamente, sin embargo, la región representa un espacio significativo en términos demográficos, económicos y normativos.

Por ello, **el modelo propuesto en este estudio trasciende el enfoque de gobierno digital y se inscribe en una concepción de gobernanza digital estratégica iberoamericana.** Esto implica integrar la transformación digital del Estado con la política productiva, la autonomía tecnológica, la protección de derechos digitales, la regulación de mercados digitales y la cooperación regional. Supone reconocer que la arquitectura institucional nacional debe articularse con dinámicas multilaterales, mecanismos de coordinación regional y estrategias de posicionamiento internacional.

Esta ampliación conceptual no reemplaza la dimensión administrativa de la transformación digital —que sigue siendo indispensable—, sino que la integra en un marco más amplio donde el Estado no solo digitaliza servicios, sino que también gestiona datos como activos estratégicos, define estándares con proyección internacional, articula con el sector privado tecnológico y promueve bienes públicos digitales compartidos en el espacio iberoamericano.

En consecuencia, la arquitectura institucional que se presenta a continuación no se limita a ordenar competencias internas del aparato estatal, sino que incorpora mecanismos de articulación multiactoral, coordinación multinivel y proyección regional, con el objetivo de fortalecer la capacidad colectiva de los países iberoamericanos para gobernar su transformación digital en un entorno global altamente competitivo y tecnológicamente concentrado.

El modelo

Los objetivos del modelo se alinean con los principios establecidos en la **Carta Iberoamericana de Principios y Derechos en los Entornos Digitales de la SEGIB**[110], adoptando de manera explícita un enfoque basado en derechos humanos que coloca en el

[110] Adoptada en la XXVIII Cumbre Iberoamericana de Jefas y Jefes de Estado y de Gobierno, en Santo Domingo, República Dominicana, el 25 de marzo de 2023.

centro la dignidad y la autonomía de las personas, así como la inclusión, la transparencia, la rendición de cuentas y la cooperación regional como pilares de la gobernanza digital.[111].

En particular, se seleccionaron 5 grandes objetivos que buscan transformar patrones recurrentes identificados a lo largo del estudio, tales como la fragmentación institucional, el desacople entre la digitalización de servicios y las capacidades habilitantes, la persistencia de brechas estructurales y los desafíos emergentes asociados a la gobernanza de la inteligencia artificial.

Luego, la propuesta identifica ocho ejes estratégicos que operacionalizan los objetivos definidos y orientan su traducción en capacidades estatales, arreglos institucionales y mecanismos de intervención concretos. Estos ejes no implican la creación de estructuras adicionales, sino que estructuran la agenda sustantiva del modelo y se implementan a través de la arquitectura institucional propuesta. Cada uno contribuye de manera diferenciada a uno o varios de los objetivos, y puede ser abordado de forma modular y progresiva, facilitando su aplicación parcial o secuencial según las prioridades, capacidades y desafíos específicos de cada país, sin perder coherencia con una visión iberoamericana compartida.

Finalmente, la arquitectura institucional del modelo se concibe como el dispositivo organizacional que permite garantizar el cumplimiento efectivo de los objetivos y la implementación coherente de los ejes estratégicos. A diferencia de enfoques centrados exclusivamente en la creación de nuevas entidades, la propuesta parte de una definición previa de funciones esenciales —conducción estratégica, rectoría normativa, capacidad operativa e instancias de supervisión con garantías democráticas— y, a partir de ellas, plantea configuraciones institucionales posibles que pueden adaptarse a distintas trayectorias estatales. Esta arquitectura no busca uniformar estructuras ni imponer un diseño único, sino asegurar que, más allá de la forma organizativa adoptada, existan responsabilidades claramente asignadas, mecanismos de coordinación efectivos y capacidades suficientes para conducir la transformación digital de manera estratégica, multinivel y orientada a derechos.

De este modo, la propuesta responde directamente a los hallazgos del Capítulo 1, que evidencian la heterogeneidad institucional de Iberoamérica, las asimetrías en capacidades estatales y la persistencia de brechas estructurales que exigen soluciones flexibles pero conceptualmente coherentes a escala regional.

Objetivos del modelo

Los objetivos siguientes no se conciben como metas homogéneas sino como **orientadores estratégicos de trayectorias de transformación, capaces de estructurar prioridades, articular actores y guiar acciones concretas en contextos nacionales diversos:**

- **Objetivo 1. Fortalecer la capacidad del Estado para gobernar la transformación digital y la IA.** Reducir la brecha entre la velocidad de adopción tecnológica y la

[111] SEGIB, 2023. Carta Iberoamericana de Principios y Derechos en los Entornos Digitales de la SEGIB. https://www.segib.org/wp-content/uploads/2025/09/Carta_iberoamericana_derechos_digitales_ESP_web.pdf?_gl=1*1op0w7o*_ga*MTA4MDk2NDgzLjE3NjI0NTk0OTQ.*_ga_MCLNSVDYMK*czE3NzE0Mzc2MDIkbzEwJGcwJHQxNzcxNDM3NjAyJGo2MCRsMCRoMA..

capacidad estatal de diseñar, implementar, supervisar y sostener políticas digitales con valor público que garanticen la centralidad de las personas.

- **Objetivo 2. Proteger derechos, confianza e integridad democrática en entornos digitales.** Garantizar que la digitalización y el uso de la IA refuercen la legitimidad democrática, la transparencia, la seguridad y el ejercicio efectivo de derechos, evitando riesgos asociados a la desinformación, la automatización opaca y la pérdida de confianza institucional.
- **Objetivo 3. Asegurar inclusión digital universal y reducción de brechas estructurales.** Orientar la gobernanza digital a cerrar brechas de acceso, capacidades e infraestructura, evitando que lo digital amplifique desigualdades sociales, territoriales, etarias o de género preexistentes.
- **Objetivo 4. Aumentar la autonomía estratégica y la capacidad de decisión de los países iberoamericanos para contribuir al desarrollo sostenible.** Fortalecer la capacidad de los Estados para tomar decisiones informadas y soberanas sobre datos, infraestructuras tecnológicas y usos de la inteligencia artificial, promoviendo bienes públicos digitales, reduciendo dependencias críticas y favoreciendo esquemas de cooperación regional para el desarrollo.
- **Objetivo 5. Fortalecer una gobernanza digital participativa, multinivel y multiactor.** Construir arreglos institucionales estables que articulen a los distintos niveles de gobierno y a actores públicos, privados, académicos y de la sociedad civil, mediante mecanismos de coordinación y diálogo orientados a producir resultados concretos, sostenibles y verificables.

Ejes estratégicos para la gobernanza digital iberoamericana:

Eje 1. Capacidades estatales e institucionalidad para la gobernanza digital[112]

Uno de los principales condicionantes para el desarrollo de modelos sólidos de gobernanza digital en Iberoamérica es la **debilidad de los arreglos institucionales encargados de conducir la transformación digital**[113]. El diagnóstico comparado muestra que, en numerosos países, la digitalización de servicios y la adopción de nuevas tecnologías —incluida la inteligencia artificial— avanzan de manera fragmentada, impulsadas por iniciativas sectoriales, sin una rectoría clara, con escasa coordinación interinstitucional y con responsabilidades difusas en materia de supervisión, sostenibilidad y protección de derechos. Esta situación tiende a generar avances rápidos pero frágiles, dependientes de coyunturas políticas o de proveedores tecnológicos, y con limitadas capacidades de escalamiento y resiliencia.

En este sentido, la OCDE señala que la efectividad del liderazgo en la gobernanza digital depende de su **reconocimiento institucional, su respaldo legal y su ubicación dentro de la estructura del Estado**. Los mandatos establecidos por ley tienden a ofrecer mayor estabilidad y continuidad, mientras que aquellos definidos por decretos u otros instrumentos

[112] Este eje contribuye principalmente al **Objetivo 5**, al fortalecer una gobernanza digital participativa, multinivel y multiactor mediante arreglos institucionales estables y mecanismos de coordinación, y de manera secundaria aporta al **Objetivo 1**, al ordenar y robustecer la capacidad estatal, y al **Objetivo 4**, al facilitar posiciones estratégicas coordinadas en el plano regional.
[113] CEPAL, 2024. Agenda Digital para América Latina y el Caribe (eLAC2024 / eLAC2026).

administrativos permiten mayor flexibilidad, aunque con mayor exposición a los cambios de gobierno. Asimismo, la evidencia comparada muestra que las funciones de liderazgo digital situadas **cerca del centro del gobierno** cuentan con mayor capacidad para coordinar actores, alinear políticas y catalizar la adopción de soluciones digitales en el conjunto del sector público[114]. Además, sugiere que los países que han logrado avances sostenidos comparten, más allá de sus diferencias administrativas, **un conjunto de funciones básicas que estructuran la acción pública en el ámbito digital.**

En primer lugar, resulta indispensable contar con una **función de rectoría estratégica**, con jerarquía política suficiente para definir prioridades, alinear la agenda digital con los objetivos de desarrollo y ejercer capacidad de coordinación sobre el conjunto de la administración pública. Esta función puede estar alojada en un ministerio, una secretaría dependiente de la presidencia o un órgano central de gobierno, pero su efectividad depende menos de su denominación formal que de su capacidad real de incidir en decisiones presupuestarias, normativas y operativas.

En segundo lugar, la gobernanza digital requiere una **función de coordinación transversal e interoperabilidad**, encargada de establecer estándares comunes, evitar duplicaciones y ordenar la digitalización del Estado como un sistema integrado. Sin esta función, la proliferación de plataformas y soluciones aisladas tiende a reproducir silos institucionales en formato digital, debilitando la eficiencia y la calidad de los servicios públicos.

Un tercer componente clave es la **función de gobernanza de datos e inteligencia artificial**, orientada a definir reglas claras para el uso de datos, supervisar la adopción de sistemas automatizados y asegurar su alineamiento con principios de derechos, transparencia y responsabilidad. Esta función resulta particularmente relevante en un contexto en el que la IA opera como un acelerador de riesgos y oportunidades, y actúa como un indicador temprano de la madurez institucional de la agenda digital.

A estas funciones se suma la **capacidad de implementación técnica**, necesaria para desarrollar, operar y mantener infraestructuras y plataformas digitales, así como para acompañar a los distintos organismos del Estado en sus procesos de transformación. En este sentido, **es clave la disponibilidad de talento público especializado.** La gobernanza digital no puede sostenerse únicamente en arreglos organizativos o marcos normativos, sino que requiere equipos estatales con capacidades técnicas, estratégicas y de gestión suficientes para diseñar, implementar, supervisar y actualizar políticas digitales y sistemas basados en datos e inteligencia artificial. Esto incluye perfiles en gestión de datos, arquitectura digital, ciberseguridad, evaluación de riesgos y contratación tecnológica, así como capacidades de liderazgo y coordinación intersectorial. Sin estrategias deliberadas de atracción, formación y retención de talento, incluso los arreglos institucionales mejor diseñados tienden a volverse dependientes de proveedores externos y a perder capacidad de aprendizaje y adaptación en el tiempo.

Finalmente, el eje incorpora la **función de control, auditoría y rendición de cuentas**, indispensable para evaluar riesgos, auditar sistemas digitales y algorítmicos, y garantizar mecanismos efectivos de supervisión y protección de derechos.

[114] OECD. (2021). The digital transformation of governments. OECD Publishing.

En **Estonia**, por ejemplo, la gobernanza digital se apoya en una rectoría clara y en estándares obligatorios de interoperabilidad, con una separación funcional nítida entre el diseño de políticas, la provisión tecnológica y la supervisión. Sin concentrar todas las responsabilidades en una única institución, el país ha logrado sostener en el tiempo un modelo coherente, basado en reglas comunes y capacidades técnicas consolidadas[115]. Una lógica similar puede observarse en **Dinamarca**, donde la institucionalización de la agenda digital dentro del Ministerio de Finanzas ha otorgado a la transformación digital un anclaje fuerte en los procesos de planificación y asignación presupuestaria, reforzando su sostenibilidad y capacidad de implementación[116].

Otros casos ilustran la importancia de **combinar liderazgo político con capacidades técnicas especializadas**. En Singapur, la iniciativa *Smart Nation* es liderada desde la oficina del Primer Ministro y se apoya en agencias ejecutoras con mandatos claros, como GovTech, responsables de desarrollar infraestructuras digitales, plataformas de datos y servicios públicos integrados. Esta articulación entre visión estratégica de alto nivel y capacidad operativa ha permitido dotar de coherencia al ecosistema digital del Estado y alinear la transformación digital con objetivos económicos y sociales de largo plazo.

Por su parte, **Corea del Sur** ofrece un ejemplo de institucionalidad técnica sostenida en el tiempo. A través de agencias especializadas con mandato explícito para coordinar la digitalización del sector público y desarrollar capacidades en datos e infraestructura, el país ha consolidado un enfoque de *Digital Platform Government*, en el que la transformación digital se concibe como una política de Estado y no como una suma de proyectos aislados[117]. En un registro diferente, **Reino Unido** ha avanzado en la articulación de liderazgos políticos y técnicos mediante figuras como los *Chief Digital Officers* y *Chief Information Officers*, integrando la agenda digital con reformas administrativas más amplias y con mecanismos de coordinación a nivel central[118].

En Iberoamérica, las experiencias de **Brasil** y **España** muestran, además, que la fortaleza institucional resulta especialmente relevante en contextos de alta complejidad territorial y gobernanza multinivel.[119] En ambos casos, la existencia de rectorías digitales con capacidad de coordinación ha permitido ordenar la digitalización de servicios y articular estrategias nacionales en entornos descentralizados, evitando una fragmentación excesiva de iniciativas[120].

---

[115] Estonia, Ministry of Economic Affairs and Communications. (2025). Estonia's Digital Agenda 2030. https://www.justdigi.ee/sites/default/files/documents/2025-02/Digi%C3%BChiskonna%20arengukava_ENG.pdf

[116] Organización del Gobierno de Dinamarca – *Agency for Digital Government*. (s. f.). *About the Agency for Digital Government*. Recuperado de https://en.digst.dk/about-us/

[117] Prime Minister's Office, Singapore. (2018, junio 24). *Formation of Smart Nation and Digital Government Group – Prime Minister's Office*. Recuperado de https://www.pmo.gov.sg/newsroom/formation-smart-nation-and-digital-government-group-prime-ministers-office/

[118] Central Digital and Data Office. (s. f.). About Central Digital and Data Office. GOV.UK. Recuperado de https://www.gov.uk/government/organisations/central-digital-and-data-office/about

[119] Ver Capítulo 1: Caracterización por país, Matriz General

[120] Ver Capítulo 1: repositorio, matriz específica para la caracterización de la Gobernanza de Internet, anexo específico sobre mecanismos de acceso a la información pública.

En conjunto, este eje pone de relieve que **la clave de la gobernanza digital no reside en la adopción de una estructura institucional específica**, sino en la capacidad de los Estados para identificar, jerarquizar y articular funciones críticas de manera coherente con su arquitectura política y administrativa. Fortalecer estas capacidades institucionales (con especial atención sobre las competencias técnicas del factor humano) constituye una condición habilitante para el resto de los ejes del modelo y un paso indispensable para avanzar hacia una gobernanza digital más robusta, legítima y sostenible en el espacio iberoamericano.

Eje 2. Infraestructura tecnológica, interoperabilidad y digitalización del Estado[121]

El diagnóstico comparado muestra que uno de los principales riesgos en los procesos de digitalización del Estado es el **desacople entre la expansión de servicios digitales y la solidez de las infraestructuras tecnológicas que los sostienen**[122]. En numerosos países iberoamericanos, la digitalización ha avanzado a través de soluciones aisladas, desarrolladas por organismos individuales, sin una arquitectura común de interoperabilidad, sin estándares compartidos y con infraestructuras desiguales en términos de cobertura, seguridad y capacidad de escalamiento. Esto tiende a generar mejoras visibles en el corto plazo, pero limita la eficiencia sistémica del Estado y compromete la sostenibilidad de los servicios digitales en el tiempo.

Este eje parte de la premisa de que **la digitalización del Estado no puede entenderse como una suma de trámites en línea**, **sino como un proceso de transformación estructural que requiere infraestructuras tecnológicas robustas y una lógica de interoperabilidad como condición habilitante.** La interoperabilidad es un principio organizador que permite articular datos, sistemas y procesos entre organismos, reducir cargas administrativas, mejorar la experiencia de las personas y fortalecer la capacidad del Estado para diseñar políticas basadas en evidencia.

Desde esta perspectiva, el eje abarca tres dimensiones estrechamente interrelacionadas. En primer lugar, la **infraestructura tecnológica básica**, que incluye conectividad, centros de datos, capacidades de cómputo y servicios en la nube con criterios de seguridad y resiliencia. En segundo lugar, la **interoperabilidad de sistemas y datos**, sustentada en estándares comunes, identidades digitales confiables y marcos claros de intercambio de información entre organismos. En tercer lugar, la **digitalización de servicios públicos**, entendida como la reorganización de procesos administrativos y no solo como su traducción a interfaces digitales.

Las experiencias internacionales muestran que los países con mejores resultados han abordado estas dimensiones de manera integrada. En **Estonia**, la interoperabilidad constituye el núcleo del modelo de Estado digital, permitiendo que los distintos organismos

[121] Este eje contribuye principalmente al **Objetivo 3**, al reducir brechas estructurales de acceso, capacidades e infraestructura mediante el desarrollo de infraestructuras digitales públicas e interoperables, y secundariamente fortalece el **Objetivo 1**, al ampliar la capacidad operativa del Estado, y el **Objetivo 4**, al disminuir dependencias tecnológicas críticas.
[122] BID, 2023. Guía de transformación digital del gobierno, Recuperado de: https://publications.iadb.org/es/guia-de-transformacion-digital-del-gobierno

compartan información de manera segura y automática, y que los servicios públicos se diseñen a partir de procesos integrados y no de estructuras administrativas fragmentadas[123] [124]. Esta arquitectura ha sido clave para sostener una digitalización profunda con altos niveles de confianza y eficiencia.

En el caso del **Reino Unido**, la digitalización de los servicios públicos se ha estructurado a partir de un enfoque centrado en el usuario, impulsado desde el nivel central mediante el *Government Digital Service (GDS)*[125]. La consolidación de una plataforma única de acceso a servicios del Estado, junto con estándares comunes de diseño, identidad y datos, permitió simplificar trámites, reducir costos administrativos y mejorar la coherencia del ecosistema digital público. Este caso muestra que la digitalización efectiva no depende únicamente de la incorporación de tecnología, sino de la capacidad del Estado para rediseñar procesos y coordinar a los distintos organismos bajo una visión común.

En el contexto latinoamericano, **Brasil** ofrece un ejemplo relevante de cómo avanzar en interoperabilidad y digitalización. La consolidación de plataformas federales de servicios digitales y de identidad ha permitido ordenar la provisión de trámites en línea, reducir duplicaciones y establecer una base común sobre la cual los distintos organismos pueden construir soluciones propias, sin perder coherencia sistémica.

En conjunto, este eje pone de relieve que **la infraestructura tecnológica y la interoperabilidad no son condiciones técnicas**, sino decisiones estratégicas de política pública que determinan el alcance, la equidad y la sostenibilidad de la digitalización del Estado. Avanzar hacia modelos integrados de infraestructura e interoperabilidad permite no solo mejorar la eficiencia administrativa, sino también sentar las bases para una gobernanza de datos y de inteligencia artificial más robusta, reforzando la capacidad del Estado para responder a los desafíos estructurales y contemporáneos de la gobernanza digital en Iberoamérica.

Eje 3. Gobernanza de datos como infraestructura estratégica[126]

El análisis comparado muestra que la **gobernanza de los datos constituye uno de los principales cuellos de botella para el desarrollo de modelos integrales de gobernanza digital en el espacio iberoamericano**. En numerosos países, los datos públicos se encuentran fragmentados, con problemas de calidad, interoperabilidad, trazabilidad y acceso,

[123] Ministry of Economic Affairs and Communications. (2011). *Interoperability framework of the state information system: Version 3.0*. Recuperado de https://www.stat.ee/sites/default/files/2022-11/Estonian%20IT%20Interoperability%20Framework%20-%20Abridgement%20of%20Version%203.0.pdf

[124] e-Estonia. (s. f.). X-Road interoperability services. Recuperado de https://e-estonia.com/solutions/interoperability-services/x-road/

[125] Central Digital and Data Office & Government Digital Service. (s. f.). *Government Digital Service*. GOV.UK. Recuperado de https://www.gov.uk/government/organisations/government-digital-service

[126] Este eje contribuye principalmente al **Objetivo 2**, al proteger derechos, reforzar la transparencia y fortalecer la confianza e integridad democrática en el uso de datos e inteligencia artificial, y secundariamente aporta al **Objetivo 1**, al consolidar capacidades regulatorias y de supervisión estatal, y al **Objetivo 4**, al promover decisiones soberanas sobre datos e infraestructuras tecnológicas.

lo que limita su uso para el diseño de políticas públicas, la coordinación interinstitucional y la provisión de servicios más eficaces. Esta debilidad se vuelve especialmente crítica en un contexto en el que la inteligencia artificial y los sistemas automatizados dependen crecientemente de la disponibilidad y gestión de datos confiables.

Este eje parte de una premisa central: **los datos son un recurso estratégico del Estado**, no solo un insumo técnico o administrativo. Constituyen una infraestructura clave para la innovación pública, la toma de decisiones basadas en evidencia y el desarrollo de capacidades en inteligencia artificial. En este sentido, la forma en que los Estados gobiernan sus datos condiciona tanto su capacidad de generar valor público como su **grado de autonomía frente a proveedores tecnológicos, plataformas privadas y modelos externos**.

Desde esta perspectiva, la gobernanza de datos abarca un conjunto integrado de decisiones políticas, institucionales y técnicas. En primer lugar, implica establecer **reglas claras sobre la calidad, el acceso, el uso y la protección de los datos públicos**, diferenciando entre datos abiertos, datos compartidos entre organismos y datos sensibles. En segundo lugar, requiere **capacidades estatales para gestionar, integrar y reutilizar datos** de manera segura y responsable, incluyendo estándares comunes, mecanismos de interoperabilidad y responsabilidades definidas. En tercer lugar, supone reconocer explícitamente que los datos son la **materia prima de la inteligencia artificial**, y que sin una gobernanza sólida de los datos, el uso de IA en el sector público tiende a reproducir dependencias tecnológicas, sesgos y asimetrías de poder.

Las experiencias internacionales muestran que los países que han priorizado la gobernanza de datos como política de Estado han logrado avanzar de manera más consistente en la adopción de tecnologías avanzadas. En **Estonia**, la gobernanza de datos se articula en torno a *X-Road*, un **software de código abierto y una solución de ecosistema** que permite el intercambio de datos **seguro, estandarizado e interoperable** entre organizaciones, principalmente para la conexión de sistemas gubernamentales. X-Road actúa como una “carretera digital” encriptada que conecta fuentes auténticas de información, sin centralizar los datos, y garantiza principios clave como la confidencialidad, la integridad y el no repudio en los intercambios. Sobre esta infraestructura, el país ha construido servicios públicos integrados y ha avanzado en el uso de inteligencia artificial en el sector público con mayores niveles de control, confianza y autonomía, mostrando cómo una gobernanza sólida de los datos constituye la base para la innovación pública y el uso estratégico de tecnologías avanzadas.

En el ámbito iberoamericano, **España** ha comenzado a integrar la gobernanza de datos con su agenda de transformación digital y de inteligencia artificial, reconociendo explícitamente el valor estratégico de los datos públicos para la innovación y el desarrollo económico, en articulación con el marco europeo. Si bien persisten desafíos en términos de implementación y coordinación, este enfoque refuerza la idea de que la soberanía digital no se limita a la regulación de tecnologías, sino que se construye a partir del control efectivo sobre los datos.

Por lo tanto, **la gobernanza de datos es una condición estructural para la soberanía digital y la autonomía estratégica** en la era de la inteligencia artificial. Fortalecer esta dimensión permite no solo mejorar la calidad de las políticas públicas y los servicios digitales,

sino también posicionar a los Estados iberoamericanos como actores capaces de decidir cómo se utilizan sus datos, con qué fines y bajo qué reglas, evitando dinámicas de dependencia y asegurando que el valor generado a partir de los datos públicos se traduzca en beneficios para el desarrollo y la ciudadanía.

Eje 4. Transparencia, auditoría algorítmica y rendición de cuentas[127]

La aceleración del uso de sistemas digitales y de inteligencia artificial en el sector público plantea desafíos sustantivos para la **legitimidad democrática de la acción estatal**. A medida que los Estados incorporan algoritmos y sistemas automatizados para apoyar —o directamente adoptar— decisiones en ámbitos como políticas sociales, seguridad, justicia, fiscalidad o asignación de recursos, emergen riesgos asociados a la opacidad, la reproducción de sesgos, la dificultad de atribuir responsabilidades y la erosión de la confianza ciudadan[128]). Estos riesgos se ven amplificados en contextos de baja institucionalización, capacidades técnicas limitadas y marcos normativos de difícil aplicación.

Este eje parte de una premisa central: **la adopción de tecnologías digitales en el Estado debe ir acompañada de mecanismos efectivos de transparencia, auditoría y rendición de cuentas**. No se trata únicamente de conocer cómo funcionan los sistemas tecnológicos, sino de asegurar que su uso sea trazable, explicable, revisable y, en última instancia, responsable frente a la ciudadanía y a las instituciones democráticas. En ausencia de estos mecanismos, incluso soluciones técnicamente eficientes pueden generar efectos regresivos sobre la legitimidad del Estado y profundizar la desconfianza en las instituciones públicas.

Desde esta perspectiva, el eje aborda tres dimensiones complementarias. En primer lugar, la **transparencia algorítmica**, entendida como la obligación de documentar y comunicar de manera accesible los usos de sistemas automatizados en el sector público, incluyendo sus finalidades, fuentes de datos, criterios de decisión y márgenes de error. En segundo lugar, la **auditoría algorítmica**, que implica la existencia de capacidades técnicas y marcos institucionales para evaluar de manera periódica los sistemas utilizados por el Estado, identificar sesgos, riesgos o efectos no deseados, y corregirlos oportunamente. En tercer lugar, la **rendición de cuentas**, que supone definir responsabilidades claras (administrativas, políticas y, cuando corresponda, legales) por las decisiones apoyadas o automatizadas mediante tecnologías digitales.

Si bien estos principios se aplican de manera directa al uso de tecnologías digitales por parte del Estado, su efectividad depende crecientemente de la **capacidad pública para extenderlos al ecosistema tecnológico en su conjunto**, incluyendo a actores privados que desarrollan, proveen u operan sistemas algorítmicos con impacto público. En este sentido, la gobernanza algorítmica no se limita a la acción estatal directa, sino que involucra la definición de estándares, condiciones contractuales, mecanismos de supervisión y responsabilidades compartidas entre el sector público y el privado. Esto no implica exigir al sector privado las

[127] Este eje contribuye principalmente al **Objetivo 1**, al reducir la brecha entre la velocidad de adopción tecnológica y la capacidad del Estado para diseñar, implementar y sostener políticas digitales con valor público, y secundariamente apoya el **Objetivo 3**, al disminuir brechas de capacidades, y el **Objetivo 5**, al profesionalizar y estabilizar la gobernanza multinivel.

[128] CAF – Banco de Desarrollo de América Latina y el Caribe & Programa de las Naciones Unidas para el Desarrollo (PNUD). (2026). Relatoría del Diálogo Regional “Los retos de la gobernanza digital en América Latina y el Caribe” (Montevideo, 26–28 de noviembre de 2025).

mismas obligaciones que al Estado, sino establecer **reglas proporcionales al nivel de riesgo e impacto social**, especialmente cuando los sistemas algorítmicos afectan derechos, servicios esenciales o procesos democráticos.

Las experiencias internacionales muestran que estos mecanismos no surgen de manera espontánea, sino que requieren decisiones deliberadas de política pública. En **España,** la transparencia, la auditoría algorítmica y la rendición de cuentas en el uso de sistemas basados en datos e inteligencia artificial se están configurando como **funciones públicas formalmente integradas al aparato del Estado**. El enfoque español combina liderazgo desde el Poder Ejecutivo con la intervención de organismos reguladores y autoridades independientes, en particular en materia de protección de datos y derechos digitales. España fue el primer país de la Unión Europea en crear una agencia específica para la supervisión de la IA (AESIA)[129], adelantándose a las exigencias del Reglamento Europeo de IA (*AI Act*). Su modelo privilegia la **institucionalización temprana**, con reglas claras, mandatos explícitos y responsabilidades definidas dentro del Estado, aunque aún enfrenta desafíos en términos de capacidades técnicas y coordinación interinstitucional efectiva.

El **Reino Unido** ha optado por un **modelo pro-innovación, distribuido y basado en funciones[130]**, que rechaza explícitamente la creación de un regulador único de la inteligencia artificial. Esta orientación quedó plasmada en el *AI Regulation White Paper*, donde el gobierno británico define un enfoque **sectorial**, en el que la regulación y supervisión del uso de sistemas algorítmicos recae en los reguladores sectoriales existentes, por ejemplo, la *Information Commissioner's Office* (datos), la *Competition and Markets Authority* (competencia) o la *Financial Conduct Authority* (finanzas), la *Information Commissioner's Office* (datos), la *Competition and Markets Authority* (competencia) o la *Financial Conduct Authority* (finanzas), guiados por principios transversales de transparencia, seguridad y rendición de cuentas[131]. En paralelo, el Estado ha avanzado en mecanismos operativos de transparencia algorítmica, como el *Algorithmic Transparency Recording Standard (ATRS)*, un estándar obligatorio que exige a las entidades públicas registrar y publicar información sobre los sistemas automatizados que utilizan, habilitando formas de *accountability ex ante* por parte de la sociedad civil (Central Digital and Data Office, *ATRS*). La coherencia del modelo se refuerza a través del *Centre for Data Ethics and Innovation (CDEI)*, una entidad pública sin funciones sancionatorias cuya misión es producir lineamientos, marcos comunes y herramientas (como el *AI Assurance Toolkit)* que orientan tanto a organismos públicos como a reguladores sectoriales, evitando la fragmentación sin centralizar el mando (CDEI). Este esquema se complementa con un fuerte énfasis en el **escrutinio parlamentario**, en particular a través del *Science, Innovation and Technology Committee* de la Cámara de los Comunes, que realiza informes periódicos y convoca a ministros y equipos técnicos para rendir cuentas sobre el uso, la ética y la eficacia de los sistemas algorítmicos en el gobierno, reforzando así la legitimidad democrática del modelo (House of Commons). La producción de lineamientos

[129] Agencia Española de Supervisión de la Inteligencia Artificial (A ESIA). (s. f.). A ESIA. Recuperado de https://aesia.digital.gob.es/es

[130] Government Digital Service & Department for Science, Innovation and Technology. (2023). AI regulation: A pro-innovation approach (White Paper). GOV.UK. Recuperado de https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

[131] Fuente: Department for Science, Innovation and Technology, *A pro-innovation approach to AI regulation*). Recuperado de https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper#part-2-the-current-regulatory-environment

sobre uso responsable de algoritmos, la publicación de información sobre sistemas automatizados y el escrutinio parlamentario forman parte de un ecosistema institucional que privilegia la **accountability ex ante y ex post**, con fuerte énfasis en la claridad de responsabilidades más que en la centralización organizativa.

Brasil presenta un modelo **fragmentado pero dinámico**, en el que conviven distintos arreglos institucionales vinculados a la transparencia y la rendición de cuentas algorítmica. Por un lado, el Estado cuenta con órganos de control tradicionales, como por ejemplo, tribunales de cuentas y entidades de fiscalización, que han comenzado a incorporar el análisis de datos y sistemas automatizados en sus prácticas de auditoría. Una iniciativa pionera que ilustra cómo las tecnologías basadas en datos pueden contribuir a la **supervisión ciudadana de la acción estatal** es la *Operação Serenata de Amor*[132]. Se trata de un proyecto de inteligencia artificial y análisis de datos abierto y colaborativo, diseñado para **analizar gastos públicos federales y detectar posibles irregularidades** en reembolsos y desembolsos de parlamentarios y otros recursos públicos. El proyecto utiliza algoritmos para identificar discrepancias en el uso de fondos públicos, genera visualizaciones y reportes, y ha servido para presentar denuncias ante órganos de control, estimulando el escrutinio cívico de las decisiones presupuestarias del Estado. El desarrollo es mantenido de forma colaborativa en código abierto y ha logrado marcar la **agenda pública sobre transparencia de datos fiscales y auditoría algorítmica**, incluso impulsando debates sobre cómo los algoritmos pueden ser utilizados para fortalecer la vigilancia democrática del gasto público. Si bien esta experiencia no forma parte del Poder Ejecutivo ni tiene mandato formal, ha demostrado capacidad para incidir en la agenda pública y complementar los mecanismos estatales existentes. El caso brasileño ilustra un esquema de **gobernanza híbrida**, donde la innovación cívica precede y, en algunos casos, impulsa la adaptación de las instituciones formales de control.

En **Chile,** la sociedad civil y la academia han desempeñado un rol central como **actores catalizadores**, impulsando iniciativas que buscan visibilizar el uso de algoritmos por parte del Estado y abrir el debate público sobre sus impactos. Plataformas como *Algoritmos Públicos*[133] funcionan como registros externos y voluntarios, sin capacidad sancionatoria, pero con alto valor simbólico e informativo. Este modelo refleja una etapa incipiente de la gobernanza algorítmica, en la que la presión pública y la producción de conocimiento preceden a la institucionalización formal, generando insumos y aprendizajes relevantes para futuros arreglos estatales más robustos.

Estas experiencias muestran que la auditoría algorítmica no debe concebirse como un obstáculo a la innovación, sino como una **condición para su sostenibilidad democrática**, especialmente en sociedades marcadas por altos niveles de desigualdad, desconfianza institucional y brechas de poder.

[132] Serenata AI. (s. f.). *Serenata*. Recuperado de https://serenata.ai/

[133] Algoritmos Públicos. (s. f.). *Algoritmos Públicos*. Recuperado de https://algoritmospublicos.cl/

Eje 5. Ciberseguridad y resiliencia digital [134]

La expansión acelerada de la digitalización del Estado, la interconexión de sistemas, el uso intensivo de datos y la incorporación de inteligencia artificial han incrementado de manera significativa la **superficie de exposición a riesgos cibernéticos** en el sector público[135]. Ataques a infraestructuras críticas, filtraciones de datos sensibles, interrupciones de servicios digitales y campañas de desinformación coordinadas evidencian que la ciberseguridad ya no puede abordarse como una cuestión técnica o sectorial, sino como un **componente central de la gobernanza digital y de la seguridad democrática**.

La capacidad del Estado para garantizar la continuidad de servicios esenciales, proteger datos estratégicos y responder de manera coordinada a incidentes cibernéticos es una condición habilitante para todos los ejes anteriores. En contextos de alta dependencia tecnológica y de creciente interconexión público–privada, las fallas en ciberseguridad no solo generan costos operativos, sino que pueden erosionar la confianza ciudadana, afectar derechos fundamentales y comprometer la autonomía estatal[136].

Desde esta perspectiva, el eje abarca tres dimensiones interrelacionadas. En primer lugar, la **protección de infraestructuras digitales críticas**, incluyendo sistemas gubernamentales, plataformas de servicios públicos, registros, centros de datos y redes de conectividad. En segundo lugar, el **fortalecimiento de capacidades estatales de prevención, detección y respuesta a incidentes**, a través de marcos normativos claros, equipos especializados y protocolos de coordinación interinstitucional. En tercer lugar, la **resiliencia digital sistémica**, entendida como la capacidad de anticipar riesgos, recuperarse de eventos adversos y adaptarse a amenazas emergentes en un entorno tecnológico dinámico.

Las experiencias internacionales muestran que los enfoques más robustos combinan liderazgo estatal claro con mecanismos de coordinación transversal.

En **España**, la ciberseguridad se ha consolidado como una **política de Estado integrada a la Seguridad Nacional**, lo que explica su posicionamiento recurrente entre los países con mayor preparación a nivel global[137]. El país cuenta con un **marco estratégico nacional** que reconoce la interdependencia entre los sistemas digitales y la continuidad de los servicios esenciales, situando la ciberseguridad como un pilar de la estabilidad social y económica[138]. En segundo lugar, se sustenta en el **Esquema Nacional de Seguridad (ENS)**, que establece estándares obligatorios de protección para todas las entidades del sector público y extiende estas exigencias a sus proveedores privados, reforzando la confianza ciudadana en la

[134] Este eje contribuye principalmente al **Objetivo 1**, al traducir capacidades institucionales en soluciones digitales con impacto concreto y valor público, y secundariamente fortalece el **Objetivo 2**, al mejorar la transparencia y la confianza ciudadana, y el **Objetivo 3**, al facilitar el acceso inclusivo a servicios digitales.

[135] World Economic Forum. (2024). The Global Risks Report 2024 (19th ed.). https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

[136] CAF – Banco de Desarrollo de América Latina y el Caribe & Programa de las Naciones Unidas para el Desarrollo (PNUD). (2026). Relatoría del Diálogo Regional “Los retos de la gobernanza digital en América Latina y el Caribe” (Montevideo, 26–28 de noviembre de 2025).

[137] https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

[138] Presidencia del Gobierno. (2019). *Estrategia Nacional de Ciberseguridad 2019*. Gobierno de España.

administración digital (Real Decreto 311/2022). A ello se suma una **arquitectura institucional especializada y coordinada**, basada en centros de respuesta con mandatos diferenciados para el sector público, el sector privado y la seguridad interior, y una **cooperación público-privada formalizada** a través de la transposición de la Directiva NIS, que impone obligaciones de prevención y notificación de incidentes a los operadores de servicios esenciales (Real Decreto-ley 12/2018). En conjunto, este modelo combina institucionalización temprana, coordinación interinstitucional y corresponsabilidad público-privada como pilares de la resiliencia digital del Estado, reflejados en su desempeño en indicadores internacionales como el

De manera complementaria, **Estonia** ha desarrollado un modelo de resiliencia digital basado en redundancia, planificación de crisis y cooperación internacional, integrando la ciberseguridad como parte de su arquitectura de Estado digital desde etapas tempranas.Fue el primer país del mundo en crear una **Embajada de Datos**[139], una innovación institucional que permite al Estado **alojar y operar infraestructuras críticas fuera de sus fronteras manteniendo pleno control soberano**. La *Data Embassy* funciona como una extensión en la nube del gobierno estonio: se trata de un centro de datos ubicado en **Luxemburgo**, con nivel de seguridad Tier IV —el más alto para instalaciones de este tipo—, que almacena y protege información estatal crítica y puede operar servicios esenciales incluso ante ciberataques, desastres naturales o crisis geopolíticas[140]. A diferencia de los esquemas clásicos de respaldo de datos, la *Data Embassy* no se limita a copias de seguridad: está diseñada para **garantizar la continuidad operativa del Estado digital**, apoyándose en tecnologías avanzadas como *KSI Blockchain* para asegurar integridad, trazabilidad y protección frente a ataques. Este modelo, desarrollado desde 2015 en colaboración con empresas tecnológicas privadas, posiciona a Estonia y Luxemburgo como pioneros en la creación de mecanismos institucionales innovadores para asegurar la continuidad del Estado en la era digital y refuerza la idea de que la soberanía digital puede ejercerse también mediante infraestructuras distribuidas y cooperativas, sin perder control ni autonomía estratégica.

En **Brasil**, la ciberseguridad atraviesa una etapa de transición desde un esquema históricamente fragmentado hacia una **mayor jerarquización institucional**. El avance más relevante en este proceso ha sido la consolidación de la ciberseguridad bajo el ámbito del Gabinete de Seguridad Institucional (GSI) de la Presidencia, a través de la Secretaría de Seguridad de la Información y Ciberseguridad, lo que ha permitido elevar el tema al más alto nivel político del Estado. Esta orientación se refuerza con la aprobación de la **Política Nacional de Ciberseguridad (PNCiber)** a finales de 2023, que busca reducir la dispersión institucional mediante la creación del **Comité Nacional de Ciberseguridad (CNCiber)** y la definición de lineamientos comunes para el conjunto del sector público y actores estratégicos[141]. En paralelo, Brasil cuenta con **capacidades técnicas de alto nivel**,

[139] e-Estonia. (s. f.). X-Road interoperability services. Recuperado de https://e-estonia.com/solutions/interoperability-services/x-road/

[140] Aunque no constituye una embajada en el sentido diplomático tradicional, el acuerdo bilateral firmado en 2017 reconoce a esta infraestructura un estatus especial, inspirado en la Convención de Viena, que le otorga inmunidad y control exclusivo por parte del Estado estonio, inaugurando una figura novedosa en el derecho internacional.

[141] Governo do Brasil. (s. f.). *Estratégia Nacional de Cibersegurança e-Cyber*. Recuperado de https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-ciberseguranca-eciber

particularmente en el *Comando de Defesa Cibernética (ComDCiber)* y en el *CERT.br*, que constituyen núcleos de excelencia regional. No obstante, el desafío central sigue siendo traducir esta fortaleza técnica en un modelo plenamente coordinado y homogéneo a lo largo de un Estado federal altamente complejo.

En **Chile**, el avance reciente ha sido más nítido en términos de **institucionalización formal**, a partir de la aprobación de la **Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información (Ley 21.663)**. Esta norma representa un punto de inflexión en la región al crear la **Agencia Nacional de Ciberseguridad (ANCI)** como autoridad única con potestades de fiscalización y sanción, tanto sobre entidades públicas como sobre operadores privados de servicios esenciales. La ley define explícitamente qué sectores constituyen infraestructura crítica y establece obligaciones claras de prevención, reporte de incidentes y cooperación con el **CSIRT de Gobierno**, resolviendo uno de los principales déficits históricos de la región: la ausencia de una rectoría clara y de mecanismos coercitivos efectivos (Ley 21.663). Este enfoque posiciona a Chile como uno de los países latinoamericanos con mayor avance normativo e institucional en ciberseguridad, aunque su efectividad dependerá de la consolidación operativa de la ANCI y de la disponibilidad de capacidades técnicas sostenidas en el tiempo.

En conjunto, este eje subraya que **la ciberseguridad y la resiliencia digital no son objetivos aislados**, sino componentes estructurales de la gobernanza digital orientada al desarrollo. Fortalecer estas capacidades permite no solo reducir la exposición a amenazas cibernéticas, sino también **garantizar la continuidad del Estado digital**, proteger derechos, sostener la confianza ciudadana y preservar márgenes de autonomía estratégica en un entorno global crecientemente interdependiente y conflictivo.

Eje 6. Infraestructura digital crítica, capacidad de cómputo y soberanía tecnológica[142]

Las **infraestructuras físicas, energéticas y computacionales** constituyen la base material del ecosistema digital. Centros de datos, cables submarinos, redes de conectividad, capacidad de cómputo —incluyendo servicios de *cloud*, *edge computing* e inferencia— y los sistemas energéticos que los sostienen son hoy **infraestructuras críticas**, no solo por su función técnica, sino por su rol estructural en el funcionamiento del Estado, la economía y la vida social. A diferencia de los desafíos abordados en el eje de ciberseguridad, este eje no se centra en la protección frente a amenazas o en la respuesta a incidentes, sino en **quién controla, dónde se localiza y bajo qué reglas se gobierna** la infraestructura que hace posible lo digital.

Este eje parte de la premisa de que la **soberanía tecnológica** no se define únicamente por la capacidad normativa o por la adopción de tecnologías, sino por el **grado de control efectivo sobre las capas materiales del ecosistema digital**. Cuando la infraestructura crítica se encuentra altamente concentrada fuera del territorio nacional, bajo jurisdicciones extranjeras o dependiente de decisiones de un número reducido de actores privados globales,

[142] Este eje contribuye principalmente al **Objetivo 4**, al fortalecer la capacidad de decisión soberana y la construcción de bienes públicos digitales regionales, y secundariamente aporta al **Objetivo 3**, al reducir brechas mediante economías de escala y cooperación técnica, y al **Objetivo 5**, al consolidar esquemas regionales de articulación multinivel y multiactor.

los Estados ven limitado su margen de decisión sobre costos, prioridades, condiciones de acceso y continuidad de servicios. Esta dependencia estructural puede generar vulnerabilidades sistémicas incluso en ausencia de ataques o fallas de seguridad, condicionando la autonomía estatal y la capacidad de planificación de largo plazo.

En este contexto, la **capacidad de cómputo** emerge como un recurso estratégico. El acceso a infraestructura de procesamiento, almacenamiento y entrenamiento de modelos de inteligencia artificial se ha convertido en un insumo clave para la provisión de servicios públicos, la innovación productiva y la competitividad económica. La creciente concentración de estos recursos en plataformas globales plantea desafíos específicos para los países iberoamericanos, que suelen actuar como usuarios finales de infraestructuras sobre las cuales tienen escasa capacidad de incidencia. Frente a ello, los países que han avanzado en esta agenda han comenzado a desarrollar **estrategias explícitas de gobernanza del cómputo**, combinando esquemas de diversificación de proveedores, infraestructura pública o híbrida y cooperación regional para ampliar escala y reducir dependencias críticas.

Asimismo, la dimensión energética adquiere un carácter central de la infraestructura digital. Los centros de datos y las infraestructuras de cómputo intensivo requieren volúmenes crecientes de energía y agua, lo que introduce tensiones relevantes entre digitalización, sostenibilidad ambiental y seguridad energética. Abordar esta dimensión exige **articular políticas digitales con políticas energéticas, industriales y territoriales**, evitando que la expansión de la infraestructura digital reproduzca cuellos de botella estructurales o desigualdades territoriales.

Las experiencias internacionales muestran que los países que han avanzado en esta agenda lo han hecho mediante la **construcción de capacidades institucionales específicas**, reconociendo la infraestructura digital crítica como objeto de política pública y no como un resultado espontáneo del mercado.

En **España**, el desarrollo de infraestructura digital crítica se inscribe en una estrategia explícita de transformación productiva y modernización del Estado. A través del *Plan España Digital 2025*[143] y de la *Agenda España Digital 2026*[144], el país definió como prioridad el despliegue de conectividad de alta capacidad, la atracción y desarrollo de centros de datos y el fortalecimiento de capacidades de *cloud* y computación avanzada. Estas políticas se articulan desde el **Ministerio para la Transformación Digital y de la Función Pública**, que cumple un rol rector en la coordinación de inversiones, regulación y alineamiento con la política industrial y energética. En este marco, se impulsó el desarrollo de una **nube pública de la Administración General del Estado**, concebida como infraestructura común para los distintos organismos, con criterios de interoperabilidad, eficiencia y control institucional. De manera complementaria, España ha promovido activamente la **atracción y localización de centros de datos de gran escala**, articulando políticas digitales, energéticas y territoriales para posicionarse como nodo estratégico de infraestructura digital en el sur de Europa. Este enfoque refleja una concepción en la que el *cloud* y la capacidad de cómputo dejan de ser decisiones puramente tecnológicas y pasan a formar parte de la **planificación estatal de largo plazo**, vinculada a soberanía digital, competitividad y resiliencia del aparato público.

[143] https://avance.digital.gob.es/programas-avance-digital/paginas/espana-digital-2025.aspx
[144] https://espanadigital.gob.es/

Chile ha comenzado a avanzar de manera más explícita en el reconocimiento de la **infraestructura digital crítica como objeto de política pública**, incorporándola a su agenda de desarrollo productivo y transformación digital. Un hito relevante en este sentido es la definición de una **Política Nacional de Centros de Datos**, impulsada desde el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación en articulación con otros organismos del Estado, que busca posicionar al país como un *hub* regional de infraestructura digital. Esta política reconoce a los *data centers* como activos estratégicos para la economía digital, la provisión de servicios públicos, el desarrollo de capacidades de datos y la atracción de inversiones tecnológicas, y aborda de manera integrada aspectos regulatorios, territoriales, energéticos y ambientales.

En **Argentina**, el desarrollo de infraestructura digital crítica ha estado históricamente asociado a una **decisión estatal explícita de soberanía tecnológica**, materializada en la creación de la empresa pública **ARSAT cuyo mandato** es **diseñar, desplegar y operar infraestructura digital clave** para el Estado, incluyendo la Red Federal de Fibra Óptica, centros nacionales de datos y capacidades satelitales, con el objetivo de garantizar conectividad, alojamiento de información pública y provisión de servicios digitales bajo control estatal. En particular, el desarrollo de **centros de datos nacionales** y de una **nube pública estatal** respondió a la necesidad de contar con infraestructura propia para alojar datos sensibles del sector público y soportar la digitalización de servicios esenciales, evitando una dependencia exclusiva de proveedores externos. Si bien la experiencia argentina ha enfrentado desafíos de sostenibilidad, actualización tecnológica y coordinación interjurisdiccional, ARSAT constituye un caso relevante de **institucionalización temprana de la infraestructura digital crítica** en América Latina, y ofrece aprendizajes valiosos sobre el rol del Estado como desarrollador y operador de capacidades digitales estratégicas.

En **Brasil**, la infraestructura de *cloud* y centros de datos ha comenzado a incorporarse de manera explícita en el debate sobre **soberanía tecnológica y desarrollo nacional**, en un contexto marcado por la escala del mercado y la fuerte dependencia de proveedores globales. A través de la **Estrategia Brasileña para la Transformación Digital** y de lineamientos impulsados desde la Presidencia y los ministerios vinculados a economía, ciencia y tecnología, el Estado ha identificado la **capacidad de cómputo, el almacenamiento de datos y la localización de centros de datos** como activos estratégicos para el funcionamiento del sector público y para la competitividad de la economía digital. En este marco, se han promovido iniciativas orientadas a fortalecer el uso de *cloud* en el Estado bajo criterios de gobernanza pública, así como a incentivar la instalación de centros de datos en territorio nacional mediante instrumentos regulatorios y de política industrial. Si bien el modelo brasileño continúa siendo híbrido y enfrenta desafíos derivados de la heterogeneidad subnacional, el énfasis creciente en infraestructura de cómputo refleja un giro hacia una **visión más estratégica**, en la que el Estado busca ampliar su capacidad de decisión sobre infraestructuras digitales críticas y reducir dependencias estructurales en servicios esenciales para la administración pública y el desarrollo productivo.

Eje 7. Ciudadanía digital, alfabetización y legitimidad democrática

La legitimidad de la gobernanza digital depende crecientemente de la **capacidad de la ciudadanía para comprender, utilizar y cuestionar críticamente** las tecnologías digitales que median su relación con el Estado, el mercado y el espacio público. La expansión de

servicios digitales, el uso intensivo de datos y la incorporación de sistemas algorítmicos en decisiones públicas y privadas exigen **niveles básicos de alfabetización digital y capacidades cívicas** que permitan a las personas ejercer derechos, demandar explicaciones y participar de manera informada. Cuando estas capacidades están ausentes, la transformación digital tiende a profundizar desigualdades, debilitar la confianza institucional y erosionar la legitimidad democrática, incluso en contextos con marcos normativos e infraestructura avanzados.

Este eje parte de la premisa de que la gobernanza digital no puede sostenerse únicamente sobre reglas, instituciones o soluciones tecnológicas, sino que requiere una **base social de comprensión, inclusión y participación**. La alfabetización digital es una condición estructural de la democracia en la era digital, especialmente frente a fenómenos como la desinformación, la opacidad algorítmica y la creciente automatización de decisiones con impacto social.

En primer lugar, el eje pone el foco en el **desarrollo de capacidades ciudadanas** para interactuar con entornos digitales complejos. Esto incluye no solo habilidades instrumentales para el uso de tecnologías, sino también la comprensión básica de cómo funcionan los sistemas basados en datos y algoritmos, cuáles son sus límites y riesgos, y qué derechos asisten a las personas frente a su utilización. En la práctica, esto se traduce en iniciativas de alfabetización digital crítica tales como: programas educativos que incorporan nociones de datos, algoritmos y sesgos en los currículos escolares y universitarios; campañas públicas de sensibilización sobre privacidad, uso de datos personales y desinformación; instancias de formación ciudadana sobre derechos digitales y mecanismos de reclamo; y espacios de capacitación orientados a grupos específicos —como personas mayores, jóvenes, trabajadores del sector público o comunidades vulnerables— para fortalecer su autonomía frente a plataformas y servicios digitales. La experiencia comparada muestra que los ecosistemas digitales más robustos son aquellos que han invertido de manera sostenida en este tipo de iniciativas, orientadas a empoderar a la ciudadanía como sujeto activo de la transformación digital y no como usuaria pasiva de servicios.

En segundo lugar, este eje incorpora la **participación ciudadana y el diálogo multiactor** como componentes centrales de la gobernanza digital, reconociendo que la complejidad y transversalidad de las tecnologías digitales requieren espacios estables y estructurados de deliberación, consulta y co-creación. En la práctica, esto se materializa a través de mecanismos como plataformas digitales de participación ciudadana como por ejemplo, **Decidim**[145], utilizada por gobiernos locales y regionales en Europa para habilitar propuestas, debates y toma de decisiones colectivas. Otro mecanismo inter; procesos deliberativos informados que combinan provisión de información, discusión y emisión de recomendaciones, como las consultas ciudadanas coordinadas por la *Danish Board of Technology Foundation* en el marco de *World Wide Views*[146]; y esquemas institucionales de participación digital integrados en políticas públicas, como los planes de gobierno abierto que articulan consultas en línea por ejemplo, Danish Board of Technology Foundation en el marco de World Wide

[145] https://decidim.org/
[146] https://www.wwviews.org/

Views, implementadas de manera simultánea en múltiples países sobre temas complejos de interés público[147].

En tercer lugar, se consolida a través de esquemas institucionales de participación digital integrados en políticas públicas, como los planes de gobierno abierto que articulan consultas en línea, laboratorios de innovación pública y procesos de co-diseño con sociedad civil, academia y sector privado, tal como se observa en el V Plan de Gobierno Abierto de España 2025-2029[148]. A nivel internacional, destacan también los procesos multiactor impulsados por **UNESCO** para la elaboración de directrices sobre gobernanza de plataformas digitales, basados en amplias consultas públicas globales[149], así como las recomendaciones metodológicas de la **OECD** sobre mecanismos participativos —incluyendo consultas abiertas, talleres deliberativos y procesos de co-creación— como herramientas para mejorar la calidad, legitimidad y sostenibilidad de las decisiones públicas en el ámbito digital[150]. Estas experiencias muestran que la participación es un dispositivo clave para fortalecer la legitimidad social de la gobernanza digital, especialmente en contextos de alta desconfianza institucional y polarización, al incorporar de manera sistemática las voces de los actores afectados en el diseño y la implementación de políticas digitales.

En cuarto lugar, el eje reconoce la importancia de la **dimensión territorial y multinivel** de la ciudadanía digital. Las brechas de acceso, habilidades y uso efectivo de tecnologías digitales suelen reproducirse a nivel local y comunitario, afectando de manera diferenciada a grupos sociales y territorios. Un modelo iberoamericano de gobernanza digital requiere, por tanto, estrategias explícitas para reducir estas asimetrías, garantizando que la alfabetización digital y la participación no queden concentradas en sectores urbanos o altamente educados, sino que alcancen al conjunto de la población.

En **Finlandia**, la alfabetización digital se concibe explícitamente como una **estrategia de resiliencia democrática frente a la desinformación**. Lejos de apoyarse en mecanismos de censura o control algorítmico de contenidos, el modelo finlandés se fundamenta en el fortalecimiento sostenido de las capacidades de pensamiento crítico de la ciudadanía. Desde la reforma curricular de 2016, la “alfabetización mediática e informacional”[151] fue integrada como **competencia transversal en todas las materias y niveles educativos**, de modo que el pensamiento crítico frente a la información digital se trabaja en matemáticas (analizando la manipulación de estadísticas), en historia (estudiando propaganda) y en lengua (comprendiendo los usos persuasivos del lenguaje en redes sociales)[152]. Además, las bibliotecas públicas, con mandato legal de promover el aprendizaje permanente y la

[147] https://www.wwviews.org

[148] Ministerio para la Transformación Digital y de la Función Pública. (2025). V Plan de Gobierno Abierto de España 2025–2029. Gobierno de España.

[149] Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). (2023). Directrices para la gobernanza de las plataformas digitales: Salvaguardar la libertad de expresión y el acceso a la información con un enfoque de múltiples partes interesadas. UNESCO.

[150] Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2023). Directrices de la OCDE sobre procesos de participación ciudadana (Estudios de la OCDE sobre Gobernanza Pública).

[151] Es un concepto promovido por la UNESCO que refiere a las habilidades de la ciudadanía para utilizar la información de forma crítica, navegar por el entorno en línea de forma segura y responsable y garantizar la confianza en nuestro ecosistema de información y en las tecnologías digitales. Fuente: https://www.unesco.org/es/media-information-literacy

[152] https://okm.fi/en/media-literacy

ciudadanía activa, y el **Instituto Nacional Audiovisual (KAVI)**[153] coordinan una política nacional de alfabetización mediática que involucra a organizaciones de la sociedad civil y universidades, con programas orientados también a adultos mayores, uno de los grupos más vulnerables a la desinformación[154]. Como resultado de esta estrategia integral y de largo plazo, Finlandia ocupa de manera consistente el primer lugar en el *Media Literacy Index* del Open Society Institute, destacándose por la capacidad de su población para verificar fuentes, comprender el funcionamiento de los algoritmos de las plataformas digitales y reconocer contenidos sintéticos generados por inteligencia artificial[155].

En **Brasil**, el Comitê Gestor da Internet no Brasil (CGI.br)[156] constituye un caso ejemplar de **gobernanza democrática y multiactor de la infraestructura digital**. Creado en 1995 y reformado en 2003, el CGI.br no funciona como un órgano colegiado de 21 miembros en el que el gobierno es minoría, conviviendo en pie de igualdad con representantes del sector empresarial, la sociedad civil, la comunidad científica y expertos independientes[157]. Este diseño institucional, basado en voto igualitario y búsqueda de consensos técnicos y éticos, fue clave para que Brasil pudiera sancionar en 2014 el *Marco Civil da Internet*[158], considerado la "Constitución de Internet" del país. En 2009, el comité elaboró además un **decálogo de principios para la gobernanza y el uso de Internet**[159], que consagra valores como apertura, diversidad, libertad e interoperabilidad, y que sigue orientando debates regulatorios más recientes, incluyendo los vinculados a la inteligencia artificial. A través de su brazo ejecutivo (Núcleo de Información y Coordinación del Punto BR - **NIC.br)**[160] el Comité Gestor de Internet en Brasil (CGI.br) gestiona los recursos del dominio *.br* y los reinvierte en ciberseguridad, formación técnica e investigación sobre el uso de TIC, cerrando un círculo virtuoso de participación, sostenibilidad financiera e independencia relativa del presupuesto estatal, que refuerza la legitimidad social de la gobernanza digital en Brasil.

En **Colombia**, la construcción de legitimidad en torno a la inteligencia artificial ha avanzado a través de un **enfoque impulsado desde la sociedad civil y los compromisos de gobierno abierto**, que permitió anclar la agenda más allá de los ciclos políticos. A partir de sus compromisos en la **Open Government Partnership (OGP)**[161], el país fortaleció su **Marco**

---

[153] El Instituto Nacional Audiovisual (KAVI) y el Centro de Promoción de las Artes de Finlandia (Taike) se han fusionado para formar la Agencia Finlandesa de Arte y Cultura (Kuvi). La Ley de la Agencia Finlandesa de Arte y Cultura entró en vigor el 1 de enero de 2026, fecha en la que la nueva agencia inició sus operaciones. Esta agencia continúa las funciones que anteriormente desempeñaban KAVI y Taike.https://kavi.fi/en/

[154] Ministry of Education and Culture. (2019). Media literacy in Finland: National media education policy (Publications of the Ministry of Education and Culture, 2019:39). Ministry of Education and Culture.

[155] Lessenski, M. (2023). The Media Literacy Index 2023: "Bye, bye, birdie": Meeting the challenges of disinformation. Open Society Institute – Sofia.

[156] https://www.cgi.br/

[157] Fuente: https://www.cgi.br/membros/

[158] Ley nº 12.965/2014

[159] https://www.cgi.br/principios-para-la-gobernanza-y-el-uso-de-internet/

[160] El Núcleo de Información y Coordinación del Punto BR - NIC.br ha sido creado para implementar las decisiones y los proyectos del Comité Gestor de Internet en Brasil - CGI.br, que es el responsable por coordinar e integrar las iniciativas y servicios de Internet en el país.https://nic.br/quem-somos/

[161] https://www.opengovpartnership.org/
http://www.superservicios.gov.co/Participa/Colaboracion-e-innovacion-abierta/Laboratorio-de-innovacion

Ético para la IA[162] mediante procesos participativos liderados por el **Laboratorio de Innovación GovCo**[163], que convocó a funcionarios del Departamento Nacional de Planeación junto con comunidades de software libre, academia y expertos en derechos humanos para co-crear guías de uso responsable de sistemas algorítmicos en el sector público. Este diseño multiactor no solo mejoró la calidad técnica y ética de los lineamientos, sino que resultó clave para su **legitimidad política**: en un contexto de alta polarización, la discusión abierta y plural de la hoja de ruta de IA permitió que la estrategia mantuviera coherencia y continuidad a pesar del cambio de gobierno, mostrando cómo la participación ciudadana puede actuar como **mecanismo de estabilidad y confianza** en la gobernanza digital.

En conjunto, este eje pone de relieve que la gobernanza de las tecnologías digitales solo puede sostenerse democráticamente cuando existe una ciudadanía informada y participativa, con capacidad efectiva para comprender, interpelar e incidir en las decisiones que las regulan y orientan.

Eje 8. Cooperación regional, proyección internacional y autonomía estratégica digital

La gobernanza digital se configura crecientemente en un **entorno transnacional**, en el que estándares técnicos, marcos regulatorios, plataformas digitales y cadenas globales de valor desbordan la capacidad de injerencia de los Estados cuando actúan de manera individual[164] [165]. En este contexto, la **cooperación internacional** constituye una **oportunidad para ampliar la capacidad efectiva de incidencia de los países** en la definición de las reglas y los principios que moldean al ecosistema digital, especialmente frente a los riesgos de dependencia tecnológica y reducción de los márgenes de decisión soberana.

Este eje parte de la concepción de que la **autonomía estratégica** no implica autosuficiencia ni aislamiento, sino, por el contrario, la **capacidad colectiva de definir prioridades, establecer reglas y negociar en mejores condiciones** en un entorno digital global cada vez más interdependiente. Desde esta perspectiva, el espacio iberoamericano presenta una ventaja comparativa singular: articula países europeos con alta capacidad normativa y regulatoria con países de América Latina y el Caribe que enfrentan desafíos estructurales similares en materia de desarrollo, inclusión y fortalecimiento institucional.

La experiencia de la **Unión Europea** constituye un referente central en términos de construcción de poder normativo en el ámbito digital. A través de instrumentos como el Reglamento General de Protección de Datos y, más recientemente, el marco regulatorio sobre inteligencia artificial, la Unión Europea ha demostrado su capacidad de influir globalmente mediante estándares que combinan innovación, protección de derechos y seguridad jurídica[166] [167]. Para América Latina, la interacción con este proceso ha sido clave

[162] https://minciencias.gov.co/sites/default/files/marco-etico-ia-colombia-2021.pdf

[163]

[164] OECD. (2022). Global digital governance: Policy shaping the digital transformation. OECD Publishing.

[165] https://www.un-ilibrary.org/content/papers/10.18356/27082245-28

[166] European Commission. (2020). A European strategy for data. Brussels.

[167] European Commission. (2021). Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Brussels.

tanto como fuente de inspiración normativa como espacio de diálogo sobre adaptación contextual, favoreciendo procesos de convergencia regulatoria gradual en ámbitos como la protección de datos, la ciberseguridad y la ética de la inteligencia artificial.

En paralelo, los organismos multilaterales han desempeñado un rol catalizador en la articulación de lenguajes comunes y principios compartidos. La **UNESCO**, a través de la *Recomendación sobre la Ética de la Inteligencia Artificial*[168], ha proporcionado un marco normativo global que facilita la cooperación entre países con distintos niveles de desarrollo tecnológico, promoviendo una aproximación basada en derechos humanos, inclusión y sostenibilidad[169]. De manera complementaria, los marcos analíticos y las buenas prácticas impulsadas por la **OECD** han contribuido a estructurar el debate sobre gobernanza digital, capacidades estatales y confianza pública, funcionando como plataformas de aprendizaje entre pares para países de ambas regiones[170] [171].

En el ámbito específicamente iberoamericano, la **SEGIB** se posiciona como un actor clave para **articular una visión compartida de la gobernanza digital desde una lógica política y de derechos**, y no meramente técnica. Un hito relevante en este sentido es la **Carta Iberoamericana de Principios y Derechos Digitales**[172], impulsada en la Cumbre de Santo Domingo en 2023, que establece un marco común de referencia para la protección de derechos humanos en el entorno digital. Este instrumento funciona como una **brújula normativa** para los países del espacio iberoamericano, en particular para aquellos con menor desarrollo regulatorio, al ofrecer principios orientadores que facilitan la convergencia de enfoques y reducen el riesgo de fragmentación normativa. Al mismo tiempo, la capacidad de la SEGIB para convocar a gobiernos de Europa y América Latina, facilitar diálogos de alto nivel y promover iniciativas conjuntas permite anclar estos principios en procesos de cooperación concreta, reforzando la gobernanza digital como una agenda de interés compartido, vinculada tanto al desarrollo como a la calidad democrática del espacio iberoamericano.

En el ámbito latinoamericano, la **CEPAL** ha desempeñado un rol central en la conceptualización de la gobernanza digital como **una dimensión estructural del desarrollo económico y social** en América Latina y el Caribe. Esta institución ha promovido una visión de la infraestructura digital, los datos y las capacidades tecnológicas como **bienes públicos estratégicos**, y ha destacado la cooperación regional como condición necesaria para reducir asimetrías, fortalecer la autonomía estratégica y ampliar la capacidad de incidencia de los países de la región en el escenario digital global[173]. Este enfoque aporta una mirada

[168] https://www.unesco.org/es/articles/recomendacion-sobre-la-etica-de-la-inteligencia-artificial

[169] UNESCO. (2021). Recommendation on the ethics of artificial intelligence. Paris.
[170] OECD. (2021). The E-Leaders Handbook on the Governance of Digital Government. OECD Publishing. https://doi.org/10.1787/ac7f2531-en
[171] OECD. (2022). Global digital governance: Policy shaping the digital transformation. OECD Publishing.
[172] https://segib.org/es/publicacion/carta-iberoamericana-de-principios-y-derechos-en-entornos-digitales/

[173] CEPAL(2024). *Superar las trampas del desarrollo en la era digital: el potencial transformador de las tecnologías digitales y la inteligencia artificial*. Naciones Unidas. Recuperado de https://conferenciaelac.cepal.org/9/sites/elac9/files/s2401013_es.pdf#:~:text=Esta%20publicaci%C3%

complementaria a los marcos normativos europeos y multilaterales, anclando la gobernanza digital en los desafíos estructurales del desarrollo latinoamericano.

De forma complementaria, la **CAF** ha desempeñado un rol activo en la **operacionalización de la gobernanza digital en ALC**, combinando producción de conocimiento aplicado, asistencia técnica y espacios de articulación política. Un ejemplo relevante son los **encuentros regionales de legisladores y parlamentarios digitales**[174], que han reunido a representantes de distintos países para intercambiar experiencias y debatir marcos regulatorios vinculados a inteligencia artificial, protección de datos y derechos digitales. Estas instancias han contribuido a construir lenguajes comunes, reducir asimetrías de información y fortalecer la coordinación entre actores legislativos en un contexto de rápida evolución tecnológica, posicionando a CAF como una **plataforma de convergencia regional** que refuerza la coherencia normativa y la capacidad colectiva de incidencia de los países en los debates globales sobre gobernanza digital[175].

El modelo propone profundizar la **institucionalización de la cooperación regional** como parte de su arquitectura permanente, no solo para compartir experiencias exitosas, sino para **incidir de manera colectiva en la definición de estándares globales**, reducir dependencias críticas y ampliar los márgenes de autonomía estratégica. En un escenario de creciente fragmentación geopolítica y aceleración tecnológica, la cooperación UE–AL emerge así como un **activo político y estratégico** para construir una gobernanza digital más equitativa, resiliente y alineada con los valores democráticos del espacio iberoamericano.

Sin embargo, en los últimos años la cooperación internacional ha sido crecientemente cuestionada por su bajo impacto efectivo, asociado a iniciativas fragmentadas, de alcance limitado o excesivamente centradas en el intercambio de diagnósticos y buenas prácticas[176]. En este contexto, resulta necesario reorientar la cooperación hacia intervenciones más tangibles y verificables, que prioricen la co-creación de proyectos concretos, como el desarrollo de infraestructuras digitales compartidas, plataformas regionales, mecanismos conjuntos de formación y atracción de talento, o esquemas de financiamiento e implementación coordinada. Solo a partir de este giro hacia resultados materiales y capacidades duraderas la cooperación podrá recuperar legitimidad y constituirse en una herramienta efectiva para fortalecer la autonomía estratégica y el desarrollo digital de la región.

Arquitectura del modelo

B3n%20debe%20citarse%20como:%20Comisi%C3%B3n%20Econ%C3%B3mica,la%20inteligencia%20artificial%20(LC/CMSI.%209/3)%2C%20Santiago%2C%202024.

[174] https://www.caf.com/es/actualidad/noticias/caf-lanzo-el-foro-iberoamericano-de-parlamentarios-digitales-para-abordar-los-desafios-de-la-ia/

[175] CAF. (2023). Gobernanza digital y desarrollo en América Latina y el Caribe. Banco de Desarrollo de América Latina.

[176] *Roadmap for Digital Cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation* y el documento de antecedentes del *Global Digital Compact* (2023/2024)

La arquitectura del modelo propuesto se estructura a partir de una distinción analítica fundamental entre funciones y arreglos institucionales. En primer lugar, se identifican las funciones esenciales que todo sistema robusto de gobernanza digital debe cumplir —con independencia de su diseño organizacional específico— tales como la conducción estratégica, la rectoría normativa, la implementación operativa y la supervisión con garantías democráticas. Estas funciones definen el "qué" de la gobernanza digital: los roles sustantivos que deben estar claramente asignados para asegurar coherencia, capacidad de ejecución, coordinación multinivel y legitimidad democrática.

En segundo lugar, el modelo presenta posibles configuraciones institucionales a través de las cuales dichas funciones pueden materializarse. Esta secuencia —de las funciones hacia las estructuras— responde a una decisión metodológica deliberada: evitar que el debate organizacional preceda a la definición de responsabilidades sustantivas. De este modo, el modelo no prescribe una única solución institucional, sino que ofrece un marco adaptable a distintas trayectorias estatales, niveles de capacidad y tradiciones administrativas presentes en Iberoamérica.

Este enfoque funcional permite, además, compatibilizar el principio de coherencia estratégica con la diversidad institucional de la región. Países con estructuras altamente centralizadas, arreglos federales complejos o esquemas de capacidades intermedias pueden adoptar configuraciones distintas, siempre que garanticen el cumplimiento efectivo de las funciones identificadas. La flexibilidad del modelo es, por tanto, una condición necesaria para su viabilidad regional: no se trata de uniformar estructuras, sino de asegurar que, más allá de su forma, los Estados cuenten con los mecanismos adecuados para conducir la transformación digital de manera estratégica, inclusiva y sostenible.

Funciones

La arquitectura propuesta, en vez de crear necesariamente nuevas estructuras administrativas, busca garantizar que determinadas funciones estratégicas, rectoras, operativas y de control se encuentren claramente asignadas dentro del entramado institucional de cada país. En este sentido, el modelo es funcional y adaptable: define roles y responsabilidades indispensables para una gobernanza digital estratégica, pero permite que su materialización organizacional varíe según la tradición administrativa, el grado de madurez institucional y el contexto político de cada Estado iberoamericano.

El diseño se estructura en cuatro funciones diferenciadas y complementarias: conducción estratégica, rectoría normativa, implementación operativa y supervisión democrática.

1. Función de conducción estratégica

Esta función tiene por objeto definir la visión integral de gobernanza digital, establecer prioridades nacionales y asegurar coherencia intersectorial y multinivel. Debe estar ubicada en el centro de gobierno (Presidencia, Jefatura de Gabinete o equivalente) para garantizar jerarquía política y capacidad de coordinación.

Sus responsabilidades incluyen:

- Definir la estrategia nacional de gobernanza digital.

- Integrar la política digital con desarrollo productivo, innovación y derechos.
- Coordinar la dimensión internacional e iberoamericana.
- Establecer lineamientos de autonomía estratégica digital.
- Resolver conflictos interministeriales.
- Asegurar coherencia presupuestaria.

Esta función puede ejercerse mediante un Consejo Nacional de Gobernanza Digital u otro mecanismo equivalente ya existente, sin requerir necesariamente la creación de un nuevo órgano.

2. Función de rectoría normativa y coherencia sistémica

Esta función garantiza que la transformación digital del Estado se desarrolle bajo estándares comunes, arquitectura interoperable y criterios homogéneos en materia de datos e inteligencia artificial.

Sus responsabilidades incluyen:

- Definir estándares de interoperabilidad (legal, organizacional, semántica y técnica).
- Establecer lineamientos de gobernanza de datos en el sector público.
- Emitir marcos de uso responsable de inteligencia artificial.
- Integrar requisitos de ciberseguridad en la arquitectura digital.
- Establecer condiciones mínimas para proyectos digitales transversales.
- Promover armonización sectorial y territorial.

Además de emitir estándares, esta función tiene un carácter habilitante: debe acompañar a los organismos públicos en la adecuación progresiva de procesos, estructuras y sistemas para hacer viable la interoperabilidad.

Esta función puede ser asignada a una entidad existente fortalecida, a una secretaría especializada o, cuando el contexto lo permita, a una agencia con autonomía técnica reforzada. No implica necesariamente la creación de un nuevo organismo.

Opera bajo el principio de no sustitución competencial respecto de autoridades de protección de datos, agencias de ciberseguridad y reguladores sectoriales.

3. Función de implementación y capacidad operativa

Esta función asegura que los estándares y lineamientos definidos puedan traducirse en proyectos concretos, plataformas compartidas e infraestructura funcional.

Sus responsabilidades incluyen:

- Desarrollo de plataformas transversales.
- Integración técnica entre sistemas sectoriales.
- Asistencia técnica a organismos públicos.
- Gestión de infraestructura compartida.
- Implementación de proyectos estratégicos.
- Transferencia de capacidades.

Esta función puede estar concentrada en una agencia especializada, en una unidad técnica dentro del Ejecutivo o distribuida en varias entidades coordinadas, siempre que exista claridad en la responsabilidad operativa.

No emite estándares ni fiscaliza cumplimiento.

4. Función de supervisión y garantías democráticas

Para asegurar legitimidad y confianza pública, la arquitectura requiere una función independiente orientada a la protección de derechos digitales y al control de impactos de tecnologías emergentes.

Sus responsabilidades incluyen:

- Evaluación de impactos en derechos fundamentales.
- Supervisión de transparencia algorítmica.
- Recepción de reclamos ciudadanos.
- Articulación con autoridades de control existentes.
- Recomendaciones públicas sobre riesgos tecnológicos.

Esta función puede ejercerse mediante un órgano independiente específico o mediante el fortalecimiento de instituciones ya existentes (por ejemplo, defensorías, autoridades de protección de datos u organismos de control), siempre que se garantice autonomía funcional.

Dimensión transversal: articulación multiactor y cooperación iberoamericana

La arquitectura incorpora una dimensión transversal que reconoce que la gobernanza digital estratégica trasciende al aparato estatal.

Incluye:

- Mecanismos formales de consulta con sector privado, academia y sociedad civil.
- Coordinación con reguladores económicos y de competencia.
- Participación activa en instancias iberoamericanas de cooperación digital.
- Promoción de bienes públicos digitales compartidos.
- Armonización regional de estándares.

Esta dimensión puede materializarse a través de consejos consultivos, redes técnicas o mecanismos ya existentes de cooperación regional.

Modelos institucionales posibles

Las funciones definidas en la sección anterior constituyen los componentes mínimos necesarios para una gobernanza digital estratégica. No obstante, su materialización organizacional puede variar según la tradición administrativa, el grado de centralización del Estado, la capacidad institucional disponible y el contexto político de cada país iberoamericano.

El modelo propuesto no impone una estructura única, sino que admite diversas alternativas de diseño institucional, y tampoco presupone la creación obligatoria de nuevas entidades, siempre que se garantice la clara asignación de responsabilidades y la coherencia sistémica. En este sentido, pueden identificarse al menos tres configuraciones institucionales posibles.

1. Modelo de articulación sobre estructuras existentes

Este modelo parte del supuesto de que el país ya cuenta con un entramado institucional relativamente desarrollado y que la prioridad no es crear nuevas entidades, sino clarificar mandatos, fortalecer capacidades y formalizar mecanismos de coordinación.

En esta modalidad, las funciones necesarias se asignan y fortalecen dentro del entramado institucional ya vigente, sin creación de nuevas entidades.

- **La conducción estratégica se ejerce desde el centro de gobierno a través de un Consejo Nacional de Gobernanza Digital de carácter interministerial,** formalmente constituido en el ámbito de la Presidencia o la Jefatura de Gabinete. No se trata de la creación de una nueva estructura burocrática permanente, sino de un mecanismo institucionalizado de coordinación política, con mandato explícito, agenda definida y periodicidad regular de funcionamiento. Este Consejo integra a las áreas con incidencia directa en la agenda digital (Hacienda o Finanzas, Producción o Desarrollo Productivo, Ciencia y Tecnología, Justicia y Cancillería) con el objetivo de asegurar que la gobernanza digital se articule coherentemente con la política económica, la protección de derechos, la innovación tecnológica y la inserción internacional del país. Su efectividad depende, fundamentalmente, de tres condiciones: i) respaldo político sostenido del Poder Ejecutivo; ii) reglas claras de coordinación y resolución de conflictos interministeriales; y iii) capacidad real de incidir en la planificación presupuestaria y en la definición de prioridades estratégicas.
- **La rectoría normativa y de coherencia sistémica se asigna a una secretaría o unidad especializada ya existente dentro del Poder Ejecutivo,** por ejemplo, en materia de transformación digital, modernización o innovación pública, fortaleciendo explícitamente su mandato transversal. Esta instancia asume la responsabilidad de definir estándares comunes, lineamientos de interoperabilidad, criterios de gobernanza de datos y marcos de uso responsable de tecnologías emergentes en el sector público, asegurando coherencia técnica entre áreas y niveles de gobierno. Su actuación se rige por el principio de no sustitución competencial, lo que implica que no reemplaza ni absorbe las atribuciones legales de autoridades de protección de datos, agencias de ciberseguridad o reguladores sectoriales, sino que articula estándares y condiciones comunes que faciliten la interoperabilidad y la consistencia sistémica. La efectividad de esta función depende, principalmente, de la claridad formal de su mandato, de su capacidad técnica especializada, de la estabilidad de sus equipos profesionales y de la existencia de mecanismos que permitan vincular sus estándares con procesos presupuestarios, de planificación y de aprobación de proyectos digitales.
- **La implementación operativa se organiza de manera distribuida entre las capacidades técnicas ya existentes en el Estado.** Esto incluye agencias especializadas, áreas de tecnología dentro de los ministerios sectoriales y equipos

técnicos con competencias específicas en gestión de sistemas, datos e infraestructura digital. No se establece una agencia central única de ejecución, sino una red coordinada de unidades operativas que actúan bajo estándares comunes y lineamientos definidos por la instancia rectora. La coordinación técnica se asegura mediante marcos compartidos de interoperabilidad, mecanismos de asistencia interinstitucional y espacios formales de articulación técnica que permitan evitar duplicaciones, incompatibilidades y fragmentación tecnológica. La efectividad de este esquema depende de la claridad en la asignación de responsabilidades operativas, de la capacidad técnica instalada en cada sector, de la existencia de incentivos para adoptar estándares comunes y de mecanismos de seguimiento que permitan verificar el cumplimiento progresivo de las directrices establecidas.

- **La supervisión democrática se articula a través de los organismos de control ya existentes en el ordenamiento institucional, tales como la autoridad de protección de datos personales, defensorías del pueblo, tribunales administrativos y entidades de auditoría pública.** No se crea un nuevo órgano de control, sino que se fortalecen y coordinan las capacidades institucionales disponibles para garantizar la protección de derechos digitales, la legalidad en el uso de datos y tecnologías emergentes, y la rendición de cuentas en los procesos de transformación digital del Estado. Con el fin de abordar de manera específica los desafíos asociados a la inteligencia artificial y a los sistemas automatizados de decisión, puede incorporarse un mecanismo formal de coordinación entre estos organismos, que permita intercambiar información, armonizar criterios de evaluación y emitir recomendaciones conjuntas cuando corresponda. La efectividad de esta función depende de la autonomía real de los órganos de control, de su capacidad técnica para comprender tecnologías complejas, de la existencia de canales formales de cooperación interinstitucional y de la accesibilidad de mecanismos de reclamo y supervisión para la ciudadanía.

El modelo de articulación sobre estructuras existentes resulta particularmente adecuado en contextos donde el entramado institucional ya es amplio o complejo, y donde la creación de nuevas entidades podría generar fricciones políticas, solapamientos administrativos o resistencias burocráticas. Es especialmente pertinente en países que cuentan con organismos consolidados en materia de datos, ciberseguridad o modernización, pero carecen de una coordinación estratégica formalizada y transversal.

Fortalezas:

- Alta viabilidad política, al no requerir reformas estructurales profundas.
- Aprovechamiento de capacidades ya instaladas en el Estado.
- Implementación progresiva y adaptable.
- Respeto por el equilibrio institucional preexistente.
- Menor costo institucional y administrativo.

Desafíos:

- Persistencia de fragmentación si la coordinación no es efectiva.
- Ambigüedad en la delimitación de responsabilidades.
- Dependencia excesiva del liderazgo político del centro de gobierno.

- Dificultad para imponer estándares comunes sin instrumentos vinculantes.
- Riesgo de superposición funcional entre áreas sectoriales

Condiciones para su efectividad

La efectividad del modelo depende de ciertas condiciones institucionales mínimas que permitan mitigar sus riesgos estructurales:

- Mandato formal y explícito de coordinación estratégica.
- Claridad en la asignación de responsabilidades entre áreas.
- Existencia de estándares comunes obligatorios para interoperabilidad.
- Capacidad técnica suficiente en las áreas sectoriales.
- Mecanismos de seguimiento y evaluación del cumplimiento.
- Respaldo político sostenido desde el centro del gobierno.

Cuando estas condiciones se cumplen, el modelo puede ofrecer una gobernanza digital funcional y progresiva, aunque con menor grado de consolidación institucional que otras alternativas.

2. Modelo de integración funcional especializada

En esta modalidad, las funciones de rectoría normativa y de implementación operativa se concentran en una misma entidad especializada, mientras que la conducción estratégica permanece en el centro de gobierno y la supervisión continúa siendo ejercida por órganos independientes. El objetivo de este modelo es reducir la fragmentación, aumentar la coherencia técnica y acelerar la implementación, sin debilitar los contrapesos institucionales.

- **La conducción estratégica se institucionaliza, al igual que en el Modelo 1, a través de un Consejo Nacional de Gobernanza Digital ubicado en el centro de gobierno (Presidencia o Jefatura de Gabinete), con carácter interministerial y mandato formalizado.** Este Consejo define la visión estratégica, aprueba prioridades nacionales, articula la agenda digital con política productiva, derechos y posicionamiento internacional, y ejerce supervisión política sobre la entidad especializada. La diferencia clave es que el Consejo no coordina múltiples unidades técnicas dispersas, sino que interactúa con una entidad técnica unificada, lo que simplifica la gobernanza operativa. La efectividad de esta función depende de su capacidad real de orientación estratégica, de su vínculo con la planificación presupuestaria y de la claridad en la delimitación entre conducción política y autonomía técnica.
- **Las funciones de rectoría normativa y de implementación operativa se concentran en una misma entidad especializada dependiente del Poder Ejecutivo, dotada de autonomía técnica reforzada y mandato transversal**. Esta entidad puede adoptar la forma de una secretaría de alto rango ubicada en el centro de gobierno o de una agencia ejecutiva con personalidad jurídica propia, según la tradición administrativa y el grado de madurez institucional del país. Lo relevante no es su denominación formal, sino que cuente con rango suficiente, presupuesto propio y estabilidad técnica que le permitan ejercer simultáneamente funciones normativas y operativas sin perder coherencia estratégica. La entidad especializada asume la definición de estándares de interoperabilidad, lineamientos de gobernanza de datos,

marcos de uso responsable de inteligencia artificial en el sector público y criterios comunes de arquitectura digital. Al mismo tiempo, concentra la capacidad de desarrollo de plataformas transversales, integración técnica entre sistemas sectoriales, gestión de infraestructura compartida y asistencia técnica a organismos públicos. Esta integración busca reducir la fragmentación institucional, acelerar procesos de transformación digital y garantizar coherencia entre diseño normativo y ejecución técnica. Para evitar conflictos de interés y concentración indebida de poder técnico, la entidad debe asegurar una separación funcional interna clara entre el área responsable de la elaboración de estándares y marcos normativos y el área encargada de su implementación operativa. Esta diferenciación interna permite preservar objetividad regulatoria y trazabilidad de decisiones, al tiempo que mantiene la eficiencia derivada de la concentración de capacidades especializadas. La efectividad de esta función integrada depende, fundamentalmente, de la claridad formal de su mandato, de la estabilidad y profesionalización de sus equipos técnicos, de la existencia de mecanismos de coordinación obligatoria con autoridades sectoriales y reguladores existentes, y de su capacidad para vincular estándares normativos con procesos presupuestarios, de contratación y de aprobación de proyectos digitales en el sector público.

- **La supervisión se mantiene independiente de la entidad especializada.** Los organismos de control existentes continúan ejerciendo sus atribuciones, particularmente en materia de derechos digitales, protección de datos, legalidad administrativa y auditoría pública. La concentración de funciones técnicas hace aún más importante reforzar la capacidad técnica de los órganos de control y garantizar transparencia en estándares, algoritmos y contratación tecnológica. La efectividad de esta función depende de la autonomía real de los órganos de supervisión, del acceso a información técnica suficiente y de la existencia de mecanismos de rendición de cuentas públicos.

El modelo de integración funcional especializada puede resultar particularmente eficiente en contextos donde se requiere acelerar la transformación digital, reducir fricciones interinstitucionales y concentrar capacidades técnicas dispersas, manteniendo coherencia normativa y agilidad operativa.

Fortalezas

- Mayor coherencia técnica entre definición normativa y ejecución.
- Reducción de superposiciones burocráticas.
- Mayor agilidad en la implementación de proyectos transversales.
- Simplificación de la interlocución entre conducción estratégica y aparato técnico.

Riesgos y desafíos institucionales

- Concentración de poder técnico en una única entidad.
- Posible debilitamiento de controles si no existen contrapesos claros
- Riesgo de captura tecnológica o institucional.
- Tensión potencial entre autonomía técnica y orientación política.

Condiciones para su efectividad

La efectividad del modelo depende de la existencia de ciertas condiciones estructurales que permitan maximizar sus ventajas y mitigar sus riesgos:

- Claridad en la delimitación entre conducción política y autonomía técnica.
- Separación funcional interna real entre normativa e implementación.
- Presupuesto estable y profesionalización técnica.
- Mecanismos formales de coordinación con reguladores y órganos de control
- Transparencia y rendición de cuentas pública.

3. Modelo de institucionalización consolidada

En contextos de mayor madurez institucional y consenso político, las funciones pueden consolidarse en una entidad especializada con autonomía técnica reforzada, estabilidad presupuestaria y mandato legal claro. Este modelo supone un mayor grado de formalización normativa, estabilidad organizacional y autonomía técnica. La gobernanza digital deja de depender exclusivamente de mecanismos de coordinación política o arreglos administrativos flexibles y se institucionaliza mediante estructuras con base legal clara, mandato explícito y reglas de rendición de cuentas definidas.

- **La conducción estratégica continúa ubicada en el centro de gobierno, pero su institucionalidad se fortalece mediante una base legal formal (ley o norma de jerarquía equivalente) que define sus competencias, integración y mecanismos de rendición de cuentas.** Se institucionaliza como un Consejo Nacional de Gobernanza Digital mediante la creación por ley; un mandato estratégico plurianual; competencias explícitas para aprobar planes nacionales de gobernanza digital; capacidad de coordinar planificación presupuestaria digital; obligación de presentar informes periódicos ante el poder legislativo. Su composición interministerial se mantiene, pero se formalizan reglas de funcionamiento, periodicidad de reuniones y mecanismos de resolución de conflictos intersectoriales. El Consejo no ejecuta ni regula técnicamente, pero posee autoridad política vinculante en la definición de lineamientos estratégicos y prioridades nacionales. La efectividad de esta función depende de su respaldo político sostenido, de su integración real con los procesos presupuestarios y de su capacidad para articular la agenda digital con desarrollo productivo, inserción internacional y protección de derechos.
- **La rectoría normativa se ejerce desde una entidad especializada con base legal propia, autonomía técnica reforzada y mandato transversal explícito.** Esta entidad puede adoptar la forma de:i) Una agencia nacional especializada creada por ley; ii) Un ente descentralizado con personalidad jurídica propia; iii) Una autoridad administrativa independiente con autonomía técnica. Su marco legal define claramente: competencias en materia de interoperabilidad, arquitectura digital y estándares técnicos; lineamientos de gobernanza de datos en el sector público; marcos de uso responsable de inteligencia artificial; capacidad para emitir estándares obligatorios para organismos públicos; facultades de seguimiento y requerimiento de información. La rectoría normativa no es simplemente una coordinación administrativa, sino una función institucional consolidada con estabilidad organizacional, régimen de carrera técnica y previsibilidad presupuestaria. No sustituye competencias constitucionales de autoridades regulatorias sectoriales o de

protección de datos, pero coordina y armoniza estándares transversales mediante mecanismos formalizados de cooperación. La efectividad de esta función depende de la claridad competencial, de la estabilidad técnica y de la existencia de contrapesos institucionales que eviten concentración excesiva de poder.

- La **función de supervisión** se organiza de manera diferenciada y multinivel. En el plano técnico, una autoridad transversal supervisa el cumplimiento de estándares de interoperabilidad, gobernanza de datos, seguridad y uso responsable de tecnologías avanzadas. Esta entidad valida proyectos estratégicos, emite normas técnicas obligatorias y realiza auditorías periódicas para asegurar consistencia arquitectónica y reducción de riesgos sistémicos. Además, órganos independientes de control —como tribunales de cuentas o autoridades de protección de datos— ejercen supervisión externa sobre legalidad, contratación, protección de derechos y transparencia, reforzando la rendición de cuentas.

Este modelo resulta más adecuado en contextos de mayor madurez institucional, estabilidad administrativa y consenso político respecto de la centralidad estratégica de la agenda digital. Es especialmente pertinente en países que buscan consolidar la gobernanza digital como política de Estado, dotándola de mayor previsibilidad, autonomía técnica y estabilidad intergubernamental.Este modelo supone un entorno donde existen condiciones para reformas normativas de mayor alcance y donde la transformación digital ha dejado de ser una política sectorial para convertirse en una prioridad estructural del desarrollo.

Fortalezas:

- Alta estabilidad institucional y continuidad más allá de ciclos políticos.
- Claridad estructural en la asignación de competencias.
- Mayor capacidad de planificación estratégica de mediano y largo plazo.
- Profesionalización técnica sostenida.
- Señal política fuerte de priorización estatal de la gobernanza digital.
- Mayor previsibilidad regulatoria frente a actores públicos y privados.

Desafíos:

- Mayor complejidad jurídica y necesidad de reformas normativas formales.
- Riesgo de rigidez institucional que limite la adaptabilidad.
- Posible concentración excesiva de poder técnico si no existen contrapesos efectivos.
- Costos administrativos y presupuestarios más elevados.
- Potenciales tensiones con ministerios sectoriales si la delimitación competencial no es precisa.

Condiciones para su efectividad

La efectividad del modelo de institucionalización consolidada depende de un conjunto de condiciones estructurales que aseguren equilibrio entre estabilidad, autonomía y control democrático:

- Base legal clara que delimite competencias y establezca mecanismos de rendición de cuentas.

- Autonomía técnica acompañada de supervisión democrática robusta.
- Presupuesto estable y mecanismos de financiamiento previsibles.
- Profesionalización del cuerpo técnico y carrera especializada.
- Separación funcional interna entre definición normativa e implementación operativa.
- Coordinación formalizada con autoridades regulatorias existentes.
- Articulación explícita con la estrategia nacional de desarrollo productivo y política exterior.

Dimensión transversal

En un contexto donde estándares tecnológicos, flujos de datos, infraestructura digital y regulación de inteligencia artificial se configuran en ámbitos transnacionales, la gobernanza digital estratégica requiere una dimensión iberoamericana explícita.

Esta dimensión no implica la creación de nuevas estructuras supranacionales obligatorias, sino la articulación coordinada de capacidades nacionales para incidir colectivamente en la arquitectura digital global. Supone, entre otras acciones:

- Coordinación de posiciones en foros multilaterales.
- Desarrollo de bienes públicos digitales regionales.
- Armonización progresiva de estándares técnicos y regulatorios.
- Intercambio estructurado de capacidades técnicas.
- Estrategias compartidas en materia de autonomía tecnológica y gobernanza de la inteligencia artificial.

La incorporación de esta dimensión fortalece la capacidad de incidencia internacional de los Estados iberoamericanos y reduce asimetrías frente a actores tecnológicos globales.

Institucionalidad mínima de la dimensión iberoamericana

Con el fin de operacionalizar la dimensión estratégica iberoamericana, se propone una arquitectura ligera de tres niveles: un foro político-estratégico de coordinación entre órganos nacionales de conducción, una red técnica permanente entre autoridades digitales y un mecanismo de articulación entre órganos de supervisión en materia de derechos digitales. Esta estructura no implica cesión de soberanía ni creación de autoridad supranacional, sino un esquema de cooperación institucionalizada orientado a fortalecer la incidencia colectiva y la armonización progresiva de estándares.

Conclusión

El presente estudio partió de una premisa fundamental: la gobernanza digital no es un componente accesorio de la modernización del Estado, sino una dimensión estructural del desarrollo contemporáneo. En un contexto atravesado por transformaciones tecnológicas aceleradas, tensiones geopolíticas en torno a infraestructuras y datos, desafíos de legitimidad democrática y persistentes brechas sociales y territoriales, la manera en que los países

organizan institucionalmente su transformación digital incide directamente en sus trayectorias de desarrollo.

El análisis comparado de los 22 países de Iberoamérica permitió constatar avances significativos en la consolidación de agendas digitales, marcos normativos en ciberseguridad y protección de datos, desarrollo de servicios públicos digitales y construcción de capacidades técnicas. Sin embargo, también evidenció una heterogeneidad marcada en los arreglos institucionales, asimetrías en capacidades estatales, fragmentación estratégica, debilidades en la articulación multinivel y una brecha persistente entre la digitalización de servicios y las capacidades habilitantes que la sostienen.

Estos hallazgos confirman que la región no parte de cero, pero tampoco cuenta aún con modelos plenamente consolidados de gobernanza digital integral. En muchos casos, las arquitecturas existentes se concentran en la modernización administrativa del aparato estatal, sin integrar de manera sistemática dimensiones más amplias como la gobernanza de datos, la regulación del ecosistema digital, la inteligencia artificial, la soberanía tecnológica o la inserción estratégica en el escenario global.

Sobre esta base, el segundo componente del estudio asumió un carácter propositivo. Lejos de diseñar un modelo abstracto o desvinculado de la realidad regional, la propuesta desarrollada se construye como respuesta directa a los desafíos identificados. El examen del modelo institucional de CEPAL permitió reconocer un aporte técnico sólido y coherente para la gobernanza del gobierno digital, al tiempo que evidenció la necesidad de ampliar el enfoque hacia una concepción más sistémica y estratégica de la gobernanza digital en sentido amplio.

El modelo integral aquí propuesto se apoya en tres decisiones conceptuales centrales. En primer lugar, adopta un enfoque explícitamente basado en derechos, alineado con la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales, situando la dignidad, la autonomía, la inclusión, la transparencia y la rendición de cuentas como principios rectores. En segundo lugar, organiza su contenido a partir de objetivos estratégicos que buscan transformar patrones recurrentes observados en la región —fragmentación institucional, debilidades de coordinación, brechas estructurales y desafíos emergentes vinculados con la inteligencia artificial—. En tercer lugar, traduce estos objetivos en ocho ejes estratégicos que estructuran las prioridades sustantivas del modelo y orientan su implementación de manera modular y progresiva.

Un rasgo distintivo de la propuesta es la distinción analítica entre funciones y arreglos institucionales. Antes de definir estructuras, el modelo identifica funciones esenciales que todo sistema robusto de gobernanza digital debe garantizar: conducción estratégica, rectoría normativa y coherencia sistémica, capacidad operativa, supervisión con garantías democráticas y articulación multiactor. Esta decisión metodológica permite ofrecer un marco adaptable a distintas realidades estatales, evitando la prescripción de un diseño único y reconociendo la diversidad institucional de Iberoamérica.

La arquitectura resultante no busca uniformar estructuras ni promover soluciones estandarizadas, sino asegurar que, cualquiera sea la configuración adoptada, existan responsabilidades claramente asignadas, mecanismos efectivos de coordinación y capacidades suficientes para sostener la transformación digital en el tiempo. Esta flexibilidad constituye una condición de viabilidad regional, especialmente en un espacio caracterizado

por la coexistencia de Estados unitarios y federales, niveles dispares de capacidad institucional y trayectorias históricas diferenciadas.

El estudio también subraya que la gobernanza digital no puede concebirse exclusivamente como un asunto intraestatal. La creciente centralidad de plataformas globales, infraestructuras tecnológicas críticas, flujos transfronterizos de datos y sistemas de inteligencia artificial exige marcos de coordinación regional y proyección internacional. En este sentido, la cooperación iberoamericana emerge no solo como una dimensión complementaria, sino como un componente estratégico para fortalecer la autonomía, la capacidad de negociación y la incidencia normativa de la región en el ecosistema digital global.

La propuesta aquí desarrollada se inscribe plenamente en los objetivos de la SEGIB de promover una Iberoamérica más integrada, inclusiva y orientada al desarrollo sostenible. Al ofrecer un modelo integral, flexible y basado en derechos, el estudio busca contribuir a la consolidación de una agenda regional coherente que permita a los países avanzar hacia esquemas de gobernanza digital más robustos, democráticos y estratégicamente orientados.

En definitiva, el tránsito desde la modernización administrativa hacia una gobernanza digital estratégica constituye uno de los desafíos centrales para la próxima década. La consolidación de modelos institucionales capaces de articular capacidades técnicas, legitimidad democrática, visión de desarrollo y cooperación regional será determinante para que la transformación digital contribuya efectivamente al bienestar, la equidad y la sostenibilidad en Iberoamérica.

Este estudio no pretende clausurar el debate, sino ofrecer una base conceptual y metodológica para profundizarlo. La gobernanza digital es un campo dinámico, en permanente evolución, y su consolidación requerirá adaptación continua, aprendizaje institucional y articulación entre múltiples actores. Sin embargo, contar con un marco integral que ordene prioridades, funciones y responsabilidades constituye un paso imprescindible para avanzar desde diagnósticos fragmentados hacia estrategias regionales consistentes.

La oportunidad está abierta. La capacidad de aprovecharla dependerá de la voluntad política, la cooperación iberoamericana y la construcción sostenida de capacidades estatales que permitan conducir la transformación digital con una visión estratégica, democrática y orientada al desarrollo humano sostenible.

Anexo 1. Participación internacional en ámbitos de cooperación de la agenda digital

La gobernanza del entorno digital se configura crecientemente a través de **espacios internacionales de cooperación, diálogo político y coordinación técnica**, en los que los países intercambian experiencias, acuerdan principios comunes, desarrollan capacidades y construyen respuestas colectivas frente a desafíos que trascienden las fronteras nacionales. A diferencia de otras áreas de política pública, la agenda digital —que abarca desde la conectividad y el gobierno digital hasta la inteligencia artificial, la ciberseguridad y la protección de datos— presenta un **alto grado de interdependencia internacional**, tanto por la naturaleza global de las infraestructuras digitales como por la circulación transnacional de datos, servicios y riesgos.

En este contexto, la participación de los países en **ámbitos multilaterales, regionales y subregionales** constituye un componente clave de la gobernanza digital. Estos espacios cumplen múltiples funciones: permiten **alinear marcos normativos y estándares**, facilitan la **cooperación técnica y el fortalecimiento de capacidades institucionales**, promueven el **aprendizaje entre pares**, y contribuyen a posicionar las prioridades nacionales y regionales en los debates globales. Asimismo, ofrecen canales para incorporar enfoques basados en derechos, inclusión, sostenibilidad e innovación responsable en el diseño de políticas digitales.

Para los países de Iberoamérica, estos ámbitos de cooperación revisten una relevancia particular. Por un lado, funcionan como **plataformas de integración regional**, que permiten abordar brechas estructurales en conectividad, capacidades digitales y desarrollo tecnológico. Por otro lado, constituyen espacios estratégicos para **incidir colectivamente en la gobernanza global de lo digital**, fortaleciendo la voz de la región frente a actores y marcos normativos de alcance global. En este capítulo se presenta un relevamiento de los principales espacios internacionales de participación de los países iberoamericanos, organizados en cinco dimensiones temáticas centrales de la agenda digital.

1. Agenda digital

Agrupa a los espacios internacionales que desarrollan **marcos estratégicos amplios de digitalización**, y abordan de manera integrada aspectos como gobierno digital, infraestructura, economía digital, inclusión, innovación y confianza en el entorno digital. En este apartado se presentan los principales ámbitos de cooperación que estructuran la coordinación regional e iberoamericana en esta materia (Ver Tabla 3).

1.1. Agenda Digital para América Latina y el Caribe (eLAC – CEPAL)
eLAC constituye el principal marco regional de coordinación de políticas digitales en América Latina y el Caribe, estructurado en planes de acción plurianuales[177]. Su propósito es orientar el desarrollo del ecosistema digital regional mediante metas compartidas y líneas de acción concretas. Aborda de manera integrada temas como conectividad e infraestructura digital, gobierno digital, transformación productiva y

[177] eLAC2007, eLAC2010, eLAC2015, eLAC2024.https://desarrollodigital.cepal.org/es/elac

economía digital, inclusión y habilidades digitales, datos, ciberseguridad, inteligencia artificial y sostenibilidad ambiental. Una de sus particularidades es que combina una lógica política intergubernamental con una dimensión operativa de seguimiento y cooperación técnica, funcionando como referencia para otros organismos regionales.

1.2. Grupo de Agenda Digital del MERCOSUR (GAD)
El Grupo de Agenda Digital del MERCOSUR tiene como objetivo avanzar hacia un Mercosur digital mediante la coordinación de políticas públicas entre los Estados Parte. En este ámbito se trabajan temas vinculados a gobierno digital, infraestructura y conectividad, firma e identidad digital, ciberseguridad, economía digital y protección de datos personales. Se trata de un espacio subregional con foco en la convergencia regulatoria y la interoperabilidad, particularmente relevante para la facilitación del comercio digital y la integración productiva.

1.3. Red de Gobierno Electrónico de América Latina y el Caribe (Red GEALC – BID)
Red GEALC es una plataforma regional de cooperación técnica orientada a fortalecer la transformación digital del Estado en América Latina y el Caribe. Aborda temas como servicios públicos digitales, interoperabilidad de sistemas, identidad digital, datos abiertos, ciberseguridad, compras públicas digitales y soluciones GovTech. Se caracteriza por un fuerte énfasis en el aprendizaje entre pares, el intercambio de buenas prácticas y el desarrollo de pilotos y casos prácticos, operando a través de grupos de trabajo temáticos.

1.4. Agenda Digital Iberoamericana (SEGIB)
La Agenda Digital Iberoamericana establece un marco político común para la cooperación en materia de digitalización entre los 22 países iberoamericanos. Incluye temas como transformación digital del Estado, inclusión digital, innovación, tecnologías emergentes y cooperación birregional. Su principal particularidad es su carácter estratégico y no vinculante, funcionando como un espacio de alineamiento político y articulación entre agendas nacionales y regionales, así como entre América Latina y Europa.

Tabla 3. Espacios de cooperación internacional en la Agenda Digital

Espacio de cooperación	Tipo de participación	Países iberoamericanos participantes
Agenda Digital para América Latina y el Caribe (eLAC – CEPAL)	Intergubernamental regional	Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay, Venezuela

Grupo de Agenda Digital del MERCOSUR (GAD)	Subregional (Estados Parte y Asociados)	Argentina, Brasil, Paraguay, Uruguay (Estados Parte); Chile, Bolivia (asociados, con participación temática)
Red GEALC (BID)	Cooperación técnica regional	Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay, Venezuela
Agenda Digital Iberoamericana (SEGIB)	Marco político iberoamericano	Andorra, Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, España, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Portugal, República Dominicana, Uruguay, Venezuela

2. Gobernanza de Internet

Son espacios internacionales de **diálogo multipartito** en los que se discuten principios, políticas y desafíos asociados a la evolución y el uso de Internet. En este apartado se sintetizan los principales foros de participación de los países iberoamericanos en este campo (Tabla 4).

5.1. Internet Governance Forum (IGF – ONU)

El IGF es el principal foro global de diálogo multipartito sobre políticas públicas relacionadas con Internet. En este espacio se debaten temas como acceso y conectividad, derechos digitales, seguridad, datos y tecnologías emergentes. Se caracteriza por su naturaleza no vinculante y por la participación en pie de igualdad de gobiernos, sector privado, comunidad técnica, academia y sociedad civil.

5.2. Foro de Gobernanza de Internet de América Latina y el Caribe (LACIGF)

El LACIGF constituye el espacio regional multipartito de debate sobre gobernanza de Internet en América Latina y el Caribe. Aborda temas como inclusión digital, derechos, regulación y desarrollo, adaptando las discusiones globales a las prioridades y desafíos específicos de la región. Funciona como un puente entre los debates nacionales y el IGF global.

Tabla 4. Espacios de cooperación internacional en Gobernanza de Internet

Espacio de cooperación	Tipo de participación	Países iberoamericanos participantes
LAC4	Centro regional de capacidades	Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, México, Panamá, Paraguay, Perú, República Dominicana, Uruguay
Convenio de Budapest sobre Ciberdelito	Tratado internacional vinculante	Andorra, Argentina, Chile, Colombia, Costa Rica, República Dominicana, España, México, Panamá, Paraguay, Portugal, Uruguay *(Brasil: observador / proceso de adhesión)*
Counter Ransomware Initiative (CRI)	Iniciativa selectiva	España, Brasil, Chile *(participación variable según grupos de trabajo)*
Global Forum on Cyber Expertise (GFCE)	Plataforma multipartita	Argentina, Brasil, Chile, Colombia, Costa Rica, España, México, Uruguay
FIRST (CSIRT/CERT)	Red técnica especializada	Argentina, Brasil, Chile, Colombia, Costa Rica, España, México, Perú, Uruguay *(a través de CSIRT nacionales)*
Programa de Ciberseguridad del CICTE – OEA	Cooperación hemisférica	Todos los países de América Latina y el Caribe miembros de la OEA
OEWG sobre seguridad de las TIC (ONU)	Foro intergubernamental global	Todos los Estados miembros de Naciones Unidas (incluye los 22 países iberoamericanos)

3. Inteligencia Artificial

El eje de inteligencia artificial incluye los ámbitos de cooperación internacional centrados en la **gobernanza, los principios éticos y las políticas públicas asociadas al desarrollo y uso de sistemas de IA**. En esta sección se identifican los espacios relevantes para la región en este campo emergente (Tabla 5).

3.1. Implementación de la Recomendación de la UNESCO sobre Ética de la IA
Este proceso internacional promueve la adopción de marcos nacionales de inteligencia artificial alineados con principios éticos y de derechos humanos. Aborda cuestiones como transparencia, no discriminación, rendición de cuentas, impacto social y gobernanza de los sistemas de IA. Se ha consolidado como un marco de referencia central para el diseño de estrategias y políticas de IA en América Latina y el Caribe.

3.2. Espacios regionales de diálogo en IA (CEPAL / UNESCO)
Estos espacios facilitan el intercambio de experiencias y enfoques de política pública en materia de inteligencia artificial entre países de la región. En ellos se discuten estrategias nacionales de IA, capacidades institucionales, impactos productivos y sociales y desafíos regulatorios. Se caracterizan por su flexibilidad, su carácter no vinculante y su énfasis en el aprendizaje regional.

Tabla 5. Espacios de cooperación internacional en IA.

Espacio de cooperación	Tipo de participación	Países iberoamericanos participantes
Implementación Recomendación UNESCO sobre Ética de la IA	Marco normativo global	Todos los países iberoamericanos (Estados miembros de UNESCO)
Diálogos regionales CEPAL / UNESCO en IA	Cooperación regional flexible	Argentina, Brasil, Chile, Colombia, Costa Rica, México, Uruguay, Perú, Ecuador, España, Portugal *(participación variable por edición)*

4. Ciberseguridad

Esta dimensión reúne los espacios internacionales vinculados a la **seguridad en el uso de las tecnologías digitales**, incluyendo la prevención y respuesta a incidentes, el combate al ciberdelito y el fortalecimiento de capacidades técnicas e institucionales. A continuación, se detallan los principales foros y mecanismos de cooperación en ciberseguridad en los que participan los países iberoamericanos (Tabla 6).

2.1. Centro de Competencia Cibernética de América Latina y el Caribe (LAC4)
Es un centro regional orientado al fortalecimiento de capacidades en ciberseguridad y ciberdelito en América Latina y el Caribe. Su trabajo se concentra en la formación técnica especializada, la cooperación operativa y el desarrollo institucional, abordando temas como gestión de incidentes, ciberdelito, ciberdefensa y resiliencia cibernética. Una de sus particularidades es su fuerte vinculación con la Unión Europea y su organización en nodos y subsedes regionales.

2.2.Convenio de Budapest sobre el Ciberdelito
Es el principal instrumento internacional para la armonización de marcos legales en materia de ciberdelito y cooperación judicial transfronteriza. Establece estándares comunes para la tipificación de delitos informáticos, el tratamiento de la evidencia digital y los mecanismos de cooperación internacional, incorporando salvaguardas procesales y de derechos fundamentales. Su carácter jurídicamente vinculante lo convierte en una referencia central para las reformas legales nacionales.

2.3. Counter Ransomware Initiative (CRI)
Es una iniciativa internacional orientada a coordinar respuestas frente al crecimiento del ransomware como amenaza sistémica. En este espacio se trabajan enfoques de política pública, mecanismos de cooperación operativa, intercambio de información y fortalecimiento de la resiliencia cibernética. Se caracteriza por un enfoque pragmático y orientado a amenazas emergentes, con liderazgo de Estados Unidos y participación de países seleccionados.

2.4. Global Forum on Cyber Expertise (GFCE)
Funciona como una plataforma global de coordinación para el fortalecimiento de capacidades en ciberseguridad. Promueve el intercambio de buenas prácticas, el desarrollo institucional y la cooperación internacional en áreas como marcos normativos, políticas públicas y formación. Su enfoque es multipartito y opera principalmente como un hub de iniciativas y proyectos, más que como un foro normativo tradicional.

2.5. FIRST – Forum of Incident Response and Security Teams
FIRST es una organización global que promueve la cooperación técnica entre equipos de respuesta a incidentes de seguridad informática. Su actividad se centra en el intercambio de información técnica, el desarrollo de estándares operativos y la mejora de las capacidades de respuesta tanto reactiva como proactiva frente a incidentes de

ciberseguridad. Se caracteriza por su orientación altamente técnica y por una membresía institucional basada en CSIRT.

2.6. Programa de Ciberseguridad del CICTE (OEA)
Constituye el principal mecanismo hemisférico de fortalecimiento de capacidades en ciberseguridad. Sus actividades incluyen el apoyo al diseño de políticas nacionales de ciberseguridad, el desarrollo y fortalecimiento de CSIRT, la asistencia técnica en marcos legales y la concientización. Se destaca por su enfoque regional y por adaptar sus intervenciones a los distintos niveles de madurez de los países.

2.7. OEWG sobre seguridad de las TIC (ONU)
Es un espacio intergubernamental de las Naciones Unidas dedicado a la discusión de normas y principios relacionados con la seguridad en el uso de las tecnologías de la información y la comunicación. En este ámbito se abordan cuestiones vinculadas al derecho internacional aplicable, las amenazas cibernéticas, las medidas de fomento de la confianza y la creación de capacidades. Se trata de un foro de carácter político-estratégico orientado a la construcción de consensos globales.

Tabla 6. Espacios de cooperación internacional en Ciberseguridad

Espacio de cooperación	Tipo de participación	Países iberoamericanos participantes
LAC4	Centro regional de capacidades	Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, México, Panamá, Paraguay, Perú, República Dominicana, Uruguay
Convenio de Budapest sobre Ciberdelito	Tratado internacional vinculante	Andorra, Argentina, Chile, Colombia, Costa Rica, República Dominicana, España, México, Panamá, Paraguay, Portugal, Uruguay *(Brasil: observador / proceso de adhesión)*
Counter Ransomware Initiative (CRI)	Iniciativa selectiva	España, Brasil, Chile *(participación variable según grupos de trabajo)*
Global Forum on Cyber Expertise (GFCE)	Plataforma multipartita	Argentina, Brasil, Chile, Colombia, Costa Rica, España, México, Uruguay

FIRST (CSIRT/CERT)	Red técnica especializada	Argentina, Brasil, Chile, Colombia, Costa Rica, España, México, Perú, Uruguay *(a través de CSIRT nacionales)*
Programa de Ciberseguridad del CICTE – OEA	Cooperación hemisférica	Todos los países de América Latina y el Caribe miembros de la OEA
OEWG sobre seguridad de las TIC (ONU)	Foro intergubernamental global	Todos los Estados miembros de Naciones Unidas (incluye los 22 países iberoamericanos)

5. Datos y privacidad

Comprende a los espacios internacionales orientados a la **protección de datos personales, la privacidad y la gobernanza de los flujos de datos**, elementos centrales para la confianza en el entorno digital. La siguiente tabla presenta los principales ámbitos de cooperación en los que participan los países iberoamericanos en esta materia (Tabla 7).

4.1. Red Iberoamericana de Protección de Datos (RIPD)

La RIPD es un espacio de cooperación orientado a promover la convergencia normativa y el fortalecimiento institucional en materia de protección de datos personales. En su seno se abordan temas como privacidad, derechos de los titulares de datos, enforcement y flujos transfronterizos de información. Se trata de un ámbito clave para la armonización de estándares en el espacio iberoamericano.

4.2. Global Privacy Assembly (GPA)

La Global Privacy Assembly articula el diálogo global entre autoridades de protección de datos personales. Sus trabajos se centran en el desarrollo de estándares internacionales de privacidad, la cooperación regulatoria y el análisis de los desafíos que plantean las nuevas tecnologías para la protección de datos. Su alcance global permite a los países de la región participar activamente en debates internacionales de alto nivel.

Tabla 7. Espacios de cooperación internacional en Datos.

Espacio de cooperación	Tipo de participación	Países iberoamericanos participantes

Red Iberoamericana de Protección de Datos (RIPD)	Cooperación regulatoria	Andorra, Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, España, México, Perú, Portugal, República Dominicana, Uruguay
Global Privacy Assembly (GPA)	Foro global de autoridades de datos	Argentina, Brasil, Chile, Colombia, España, México, Perú, Portugal, Uruguay *(a través de autoridades nacionales)*

Anexo 2. Índice de Desarrollo del Gobierno Electrónico (EGDI) en Iberoamérica

El **Índice de Desarrollo del Gobierno Electrónico (EGDI)**, elaborado por Naciones Unidas, constituye la métrica internacional más utilizada para evaluar el grado de madurez del gobierno digital en los países. Este indicador ofrece una visión integral del ecosistema digital estatal, ya que combina tres dimensiones fundamentales:

- la disponibilidad y calidad de los servicios públicos digitales (*Online Service Index*, OSI),
- la infraestructura de telecomunicaciones que los sostiene (*Telecommunications Infrastructure Index*, TII),
- el nivel de capacidades de la población para utilizarlos (*Human Capital Index*, HCI).

Cada componente se normaliza en una escala de 0 a 1, y el EGDI final resulta del promedio simple de estos tres subíndices.

Esta metodología permite comparar países con realidades muy diversas, incorporando tanto factores tecnológicos como institucionales y sociales. El índice captura, por un lado, la oferta estatal de servicios digitales y, por otro, las condiciones estructurales que hacen posible su adopción y sostenibilidad. En este sentido, el EGDI funciona no solo como una medida de digitalización gubernamental, sino como un reflejo de la capacidad de los Estados para modernizar su gestión pública, producir valor público mediante el uso estratégico de tecnología y garantizar un acceso equitativo a servicios de calidad.

A partir de la información más reciente disponible (EGDI 2024), se elaboró un ranking de los **22 países de Iberoamérica**, incluyendo América Latina y el Caribe hispanohablante, junto con España, Portugal y Andorra (Tabla 8). Para facilitar la interpretación y resaltar las diferencias estructurales dentro de la región, se agruparon los países en cuatro niveles, según los siguientes umbrales: **muy alto** (EGDI > 0,90), **alto** (0,80–0,89), **medio** (0,65–0,79) y **bajo** (EGDI < 0,65).

Tabla 8. Índice de Gobierno Digital de Naciones Unidas (2024). Ranking de 22 países de Iberoamérica

Ranking	País	EGDI
1	España	0.92
2	Uruguay	0.90
3	Chile	0.88
4	Argentina	0.86
5	Portugal	0.84
6	Brasil	0.84
7	Perú	0.81
8	Costa Rica	0.80
9	México	0.78
10	Ecuador	0.78
11	Colombia	0.78
12	Panamá	0.73
13	Paraguay	0.73
14	República Dominicana	0.70
15	Andorra	0.69
16	Bolivia	0.67
17	El Salvador	0.60
18	Guatemala	0.57
19	Venezuela	0.54
20	Nicaragua	0.53
21	Cuba	0.49
22	Honduras	0.49

Fuente: Elaboración propia en base a UN EGDI 2024 vía statbase.org

En el **nivel muy alto** se ubican España (0,92) y Uruguay (0,90), dos países que han logrado consolidar ecosistemas digitales avanzados, con infraestructura robusta, altos niveles de capital humano y estrategias de digitalización sostenidas en el tiempo. Ambos combinan marcos institucionales sólidos con plataformas integradas y una visión estratégica de la transformación digital del Estado, lo que los posiciona no solo como líderes regionales, sino también como referentes a nivel global.

El **nivel alto** reúne a Chile, Argentina, Portugal, Brasil, Perú y Costa Rica, todos con valores entre 0,80 y 0,89. Este grupo conforma el núcleo emergente del gobierno digital en Iberoamérica. Son países que han logrado importantes avances en servicios en línea e interoperabilidad, y que cuentan con estrategias nacionales maduras, aunque aún enfrentan desafíos vinculados a desigualdades territoriales, sostenibilidad presupuestaria, continuidad

institucional o integración plena de sistemas de información. Aun así, su desempeño refleja un proceso de consolidación progresiva y una agenda de modernización relativamente estable.

En el **nivel medio** se encuentra el grupo más numeroso y heterogéneo: México, Ecuador, Colombia, Panamá, Paraguay, República Dominicana, Andorra y Bolivia, con puntajes entre 0,65 y 0,79. Estos países presentan avances significativos en digitalización gubernamental, pero todavía enfrentan limitaciones en infraestructura, capacidades técnicas, interoperabilidad o gobernanza de datos. Para muchos de ellos, el desafío principal no es iniciar procesos de digitalización -ya presentes- sino profundizarlos, escalarlos y dotarlos de una arquitectura institucional más estable.

Finalmente, el **nivel bajo** -aunque sin países extremadamente rezagados según la clasificación global de la ONU- incluye a El Salvador, Guatemala, Venezuela, Nicaragua, Cuba y Honduras, con valores inferiores a 0,65. Aquí se observan brechas estructurales persistentes en infraestructura digital, acceso equitativo a conectividad, alfabetización digital o capacidad estatal para sostener políticas de largo plazo. Estos países suelen desarrollar iniciativas puntuales o portales sectoriales, pero sin la consolidación de un ecosistema digital integral. La distancia respecto de los niveles superiores revela desigualdades profundas que condicionan la provisión de servicios públicos digitales y la capacidad de los Estados para adoptar tecnologías más avanzadas.

En conjunto, esta clasificación permite visualizar la **amplia heterogeneidad iberoamericana** en materia de gobierno digital. Mientras algunos países operan cerca de la frontera tecnológica global, otros permanecen limitados por condiciones estructurales o institucionales. Sin embargo, también evidencia oportunidades: los países con desempeños altos pueden servir como referentes de cooperación, transferencia de capacidades y desarrollo de estándares comunes para la región, contribuyendo a reducir brechas, fortalecer la gobernanza digital y avanzar hacia modelos más inclusivos y resilientes.

Anexo 3. Digital Government Index (DGI) 2025 de la OCDE[178].

El **OECD Digital Government Index (DGI)** constituye el principal instrumento comparado de la OCDE para medir la madurez de las políticas de gobierno digital en los países miembros y en proceso de adhesión. A diferencia de otros rankings internacionales centrados en la oferta o el uso de servicios digitales, el DGI no mide el nivel de digitalización de trámites específicos ni la adopción ciudadana de servicios en línea. Su foco está puesto en las **condiciones habilitantes estructurales** que permiten una transformación digital coherente, sostenible y

[178] Este anexo fue construido en base al documento "*Digital Government Index and Open, Useful and Re-usable Data Index: 2025 results and key findings* (OECD Working Papers on Public Governance No. 90). OECD, 2026. Disponible en https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/02/digital-government-index-and-open-useful-and-re-usable-data-index_dbe102ed/6347ec74-en.pdf

centrada en las personas en el conjunto del sector público. En este sentido, el índice evalúa la solidez del marco institucional, estratégico y operativo que sustenta el gobierno digital.

Hasta febrero de 2026, el **Digital Government Index (DGI)** ha tenido tres iteraciones principales, que reflejan una progresiva consolidación metodológica y ampliación temática. La primera edición, correspondiente a 2019 y publicada en 2020, funcionó como ejercicio piloto y línea de base, estableciendo el marco conceptual inicial y los primeros parámetros de medición comparada. La segunda edición, basada en la encuesta de 2023 y publicada en 2024, introdujo ajustes metodológicos relevantes, incorporando con mayor claridad dimensiones vinculadas a identidad digital, gobernanza de datos y uso estratégico de inteligencia artificial en el sector público. Sobre la base de esta misma encuesta se elaboró, además, una versión específica para la región, el **2023 OECD/IDB Digital Government Index of Latin America and the Caribbean**, desarrollada conjuntamente por la OCDE y el Banco Interamericano de Desarrollo, que permitió ampliar el análisis para países no miembros de la organización. Finalmente, la edición 2025 —publicada el 16 de febrero de 2026— constituye la actualización más reciente del índice, consolidando la estructura de seis dimensiones y mostrando, entre otros resultados destacados, el ascenso de Chile al Top 10 global.

El DGI 2025 identifica seis dimensiones clave para la transformación digital del Estado:

1. **Digital by design**: integración estratégica de lo digital en el diseño de políticas y servicios. Analiza si el país cuenta con estrategias nacionales de gobierno digital claras y coherentes, si existen marcos institucionales definidos con autoridad formal para coordinar la agenda digital, y si la transformación tecnológica se articula con prioridades de política pública más amplias. Asimismo, examina la gobernanza de las inversiones digitales, la existencia de mecanismos de coordinación interinstitucional y el desarrollo de capacidades y talento digital dentro del sector público. Un alto desempeño en esta dimensión indica que la digitalización no es periférica ni fragmentada, sino que forma parte del núcleo estratégico del Estado
2. **Data-driven public sector**: Se centra en la existencia de marcos de gobernanza de datos, estructuras de liderazgo dedicadas a su gestión, y mecanismos técnicos y legales que permitan el acceso, la interoperabilidad y la reutilización segura de información entre organismos públicos. También evalúa si los datos se utilizan efectivamente para diseñar políticas, monitorear resultados y mejorar la prestación de servicios. La lógica subyacente es que un gobierno digital maduro no solo acumula información, sino que la convierte en inteligencia pública para orientar decisiones y fortalecer la coordinación estatal.
3. **Government as a platform**: Evalúa la disponibilidad y cobertura de sistemas de identidad digital, plataformas comunes de servicios, estándares técnicos reutilizables, infraestructuras de interoperabilidad y estrategias para la adopción de tecnologías como el cloud. También considera los mecanismos de inversión y adquisición tecnológica que fomentan innovación y evitan duplicación de esfuerzos entre agencias. En esencia, analiza si el gobierno ofrece infraestructuras comunes para todo el sector público reduciendo la fragmentación.
4. **Open by default**: Incluye la disponibilidad y calidad de portales de datos abiertos, la accesibilidad de conjuntos de datos de alto valor, la promoción del uso de software de código abierto y la adopción de normas o directrices para la transparencia algorítmica.

Un alto desempeño en esta dimensión indica que la transformación digital se utiliza también como herramienta para fortalecer confianza pública y participación.

5. **User-driven**. Analiza si los gobiernos utilizan metodologías de diseño centrado en el usuario, realizan pruebas previas de servicios digitales, recogen retroalimentación sistemática y monitorean las necesidades de distintos grupos poblacionales. También examina la existencia de estrategias para reducir brechas digitales y garantizar inclusión. En esta dimensión, la madurez digital se refleja en la capacidad del Estado para adaptar políticas y servicios a las experiencias reales de la ciudadanía y no solo a lógicas administrativas internas.
6. **Proactiveness**: Evalúa la capacidad del gobierno para anticipar necesidades y ofrecer servicios antes de que sean solicitados explícitamente. Incluye el uso de analítica de datos y herramientas de inteligencia artificial para prever riesgos, personalizar intervenciones y mejorar la planificación pública. También considera la existencia de marcos estratégicos para el uso responsable de IA, instrumentos de gobernanza ética de algoritmos y mecanismos de evaluación de riesgos tecnológicos. Un alto desempeño en esta dimensión indica que el Estado no se limita a reaccionar ante demandas, sino que puede actuar de manera anticipatoria y estratégica, apoyado en datos y tecnologías avanzada

Cada una de las seis dimensiones tiene **igual peso (1/6 del total)** y el puntaje compuesto resulta del promedio simple de las dimensiones.

La información proviene de la **OECD Survey on Digital Government 3.0**, un cuestionario estructurado que incluye 94 preguntas dirigidas a altos funcionarios responsables de gobierno digital a nivel central o federal. La encuesta cubre ministerios y agencias del gobierno central y fue completada por:

- **36 países miembros de la OCDE**
- **6 países en proceso de adhesión**

El índice evalúa cada dimensión a lo largo de cuatro fases transversales del ciclo de política pública:

- **Enfoque estratégico** (existencia de estrategias y prioridades claras)
- **Instrumentos o policy levers** (marcos regulatorios, recursos, estándares y herramientas)
- **Implementación** (prácticas efectivamente desplegadas)
- **Monitoreo y evaluación** (mecanismos de seguimiento, evaluación de impacto y aprendizaje institucional)

De este modo, el DGI no sólo captura la existencia de estrategias formales, sino también la capacidad real de implementación y la institucionalización de mecanismos de seguimiento. Por lo tanto, refleja la **capacidad estatal para gobernar la transformación digital**, más que el nivel visible de digitalización de servicios.

Alcance y Cobertura

La edición 2025 del **OECD Digital Government Index (DGI)**, publicada en febrero de 2026, se basa en información relevada durante el primer semestre de 2025 y cubre políticas

e iniciativas implementadas entre el **1 de enero de 2023 y el 31 de diciembre de 2024**. Incluye un total de **42 países**, que participaron en la OECD Survey on Digital Government 3.0. La medición se circunscribe al nivel central o federal de gobierno y refleja exclusivamente la información provista y validada en el marco de dicho relevamiento.

Desde una perspectiva iberoamericana, la cobertura del índice resulta parcial. De los **22 países que integran el espacio iberoamericano** el DGI 2025 incluye únicamente **9 países**. En América Latina están representados **Argentina, Brasil, Chile, Colombia, Costa Rica, México y Perú**, mientras que en Europa iberoamericana participan **España y Portugal (Tabla 9)**.

Tabla 9. Ranking de los países Iberoamericanos en el DGI 2025.

N° Rank	País	Puntaje DGI 2025	Condición OCDE
3	Portugal	0.86	Miembro
10	Chile	0.79	Miembro
11	Brasil	0.79	En proceso de adhesión
13	España	0.75	Miembro
15	Colombia	0.71	Miembro
18	Perú	0.69	En proceso de adhesión
34	México	0.51	Miembro
35	Argentina	0.49	En proceso de adhesión
37	Costa Rica	0.45	Miembro

Elaboración propia en base a DGI 2025, OECD (2026)[179].

De acuerdo con los resultados oficiales del **OECD Digital Government Index (DGI) 2025**, el liderazgo global en materia de gobernanza digital lo encabeza **Corea**, con un puntaje de 0.95, consolidándose como el país con mayor nivel de madurez institucional en las políticas habilitantes de transformación digital. Le siguen **Australia** (0.88) y **Portugal** (0.86), que muestran desempeños altamente equilibrados en las seis dimensiones del marco de gobierno digital de la OCDE. En el cuarto lugar se ubica el **Reino Unido** (0.84), mientras que el quinto puesto es compartido por **Noruega**, **Estonia**, **Irlanda** y **Dinamarca**, todos con 0.83, reflejando trayectorias consolidadas en infraestructura digital pública, gobernanza de datos y enfoques proactivos de prestación de servicios. Completan el Top 10 **Francia** (0.80) y **Chile** (0.79), este último destacándose como el único país latinoamericano entre las diez economías con mayor madurez en las bases estructurales del gobierno digital.

En conjunto, estos resultados evidencian que el liderazgo en la materia se concentra principalmente en economías avanzadas con marcos estratégicos consolidados, aunque

[179] Fuente: https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/02/digital-government-index-and-open-useful-and-re-usable-data-index_dbe102ed/6347ec74-en.pdf

también muestra que algunos países de América Latina han logrado posicionarse en niveles de desempeño comparables a los referentes globales.

Anexo 4. Índice de Gobierno Digital OCDE-BID 2023 para América Latina y el Caribe[180]

Este índice fue implementado conjuntamente por la OCDE y el Banco Interamericano de Desarrollo (BID) en una edición especial que alcanza a los países de ALC. Los resultados tienen como objetivo apoyar a los gobiernos de la región mediante la comparación de sus avances hacia la transformación digital (OCDE, 2023)[181]. **La principal conclusión que arroja este índice es que los países de ALC han avanzado en la construcción de fundamentos institucionales y normativos del gobierno digital, pero aún deben fortalecer capacidades estratégicas, de implementación y de monitoreo para consolidar una transición plena desde el gobierno electrónico hacia un gobierno digital integral, centrado en las personas y sostenible en el tiempo.**

Tabla 10. Ranking en el GDI 2023 para países de ALC

Rank	País	Puntaje
1	Colombia	0,61
2	Uruguay	0,592
3	Perú	0,526
4	Brasil	0,51
5	México	0,503
6	Argentina	0,414
7	Chile	0,401
8	Costa Rica	0,382
9	República Dominicana	0,371
10	Panamá	0,358
11	Paraguay	0,338
12	Ecuador	0,335
13	El Salvador	0,316

[180] Este anexo se construyó enteramente sobre la base del documento de OCDE 2023: Índice de Gobierno Digital OCDE-BID América Latina y el Caribe. Disponible en: https://www.oecd.org/es/publications/2024/11/2023-oecd-idb-digital-government-index-of-latin-america-and-the-caribbean_5a9af6c4.html

[181] OCDE 2023: Índice de Gobierno Digital OCDE-BID América Latina y el Caribe. Disponible en: https://www.oecd.org/es/publications/2024/11/2023-oecd-idb-digital-government-index-of-latin-america-and-the-caribbean_5a9af6c4.html

14	Jamaica	0,302
15	Guatemala	0,28
16	Honduras	0,255
17	Bolivia	0,249

Fuente: elaboración propia en base a Índice de Gobierno Digital OCDE-BID América Latina y el Caribe.

En términos generales, el promedio regional (0.321) se ubica considerablemente por debajo del promedio de la OCDE (0.605), lo que indica que la mayoría de los países aún se encuentra en etapas iniciales o intermedias en la construcción de los fundamentos habilitadores del gobierno digital (p. 12-14). Solo cinco países (Colombia, Uruguay, Perú, Brasil y México) alcanzan resultados en la mitad superior del índice, con desempeños relativamente equilibrados en las seis dimensiones evaluadas (Anexo A, p. 27). La región muestra mejores resultados relativos en **Digital por diseño**, **Impulsado por los usuarios** e **Impulsado por los datos**, mientras que presenta mayores rezagos en **Gobierno como plataforma**, **Abierto por defecto** y, especialmente, **Proactividad** (Tabla 1 y Figura 3, p. 14).

En la dimensión **Digital por diseño**, que es la de mejor desempeño regional (0.453), los países han fortalecido la institucionalidad del gobierno digital mediante la adopción de estrategias nacionales y la designación de entidades responsables (p. 15-16). Sin embargo, persisten brechas importantes en monitoreo y evaluación de políticas, alineación estratégica con otras agendas nacionales y desarrollo de talento digital. En **Impulsado por los datos** (0.303), se observan avances en interoperabilidad y reconocimiento de los datos como activo estratégico, pero limitaciones significativas en inventarios de datos, monitoreo y liderazgo institucional en gobernanza de datos (p. 17-18).

En **Gobierno como plataforma** (0.312), los países han desarrollado algunos componentes de infraestructura pública digital —como identidad digital y marcos de interoperabilidad—, pero aún muestran debilidades en gestión estratégica de inversiones digitales, contratación adaptada y adopción de enfoques GovTech (p. 19-20). En **Abierto por defecto** (0.296), aunque existen mandatos de datos abiertos en muchos países, la publicación de conjuntos de alto valor, la evaluación de impacto y la transparencia algorítmica siguen siendo limitadas (p. 21-22). En **Impulsado por los usuarios** (0.353), se destaca el compromiso con la reducción de la brecha digital, pero la participación efectiva de usuarios en el diseño y co-creación de servicios es todavía incipiente (p. 23-24). Finalmente, **Proactividad** es la dimensión con menor puntaje (0.210), reflejando debilidades en servicios proactivos, uso estratégico de inteligencia artificial, gestión ética de algoritmos y anticipación basada en datos (p. 25-26).