

DOI: <https://doi.org/10.46296/rc.v9i18.0457>

Retos de la gobernanza tecnológica y ciberseguridad en el sector público en el Ecuador: Una revisión sistemática de la literatura

Challenges of technological governance and cybersecurity in Ecuador's public sector: A systematic literature review

Flores-Cedeño Pablo Ramon

Universidad Técnica de Manabí. Portoviejo, Ecuador.

Correo: pablo.flores@utm.edu.ec

ORCID ID: <https://orcid.org/0009-0008-6092-1342>

RESUMEN

La transformación digital del sector público ecuatoriano ha avanzado mediante políticas de gobierno digital, marcos de seguridad de la información, regulación de datos personales y modernización de servicios; sin embargo, la expansión tecnológica también amplía las exigencias de gobernanza, interoperabilidad, capacidades institucionales y ciberseguridad. Este artículo revisa críticamente literatura científica y documentos oficiales recientes para examinar tres ejes: gobernanza digital y capacidad estatal, ciberseguridad y protección de datos, e interoperabilidad e infraestructura pública digital. La evidencia muestra una situación dual. Ecuador presenta fortalezas normativas y de madurez GovTech, pero mantiene brechas en proactividad, articulación interinstitucional y desarrollo de capacidades. En el Global Cybersecurity Index 2024 el país alcanza valores altos en medidas legales, organizacionales, técnicas y de cooperación, mientras que el desarrollo de capacidades constituye el componente más rezagado. Se concluye que el reto central no consiste únicamente en incorporar tecnología, sino en consolidar una gobernanza tecnológica que articule estándares, talento humano, datos, interoperabilidad, gestión de riesgos y rendición de cuentas. La sostenibilidad de la transformación digital pública depende de convertir estos componentes en capacidades permanentes del Estado.

Palabras claves: gobernanza tecnológica; ciberseguridad; gobierno digital; sector público; interoperabilidad; Ecuador.

ABSTRACT

Digital transformation in Ecuador's public sector has advanced through digital-government policies, information-security frameworks, personal-data regulation and service modernization. Yet technological expansion also increases governance, interoperability, institutional-capacity and cybersecurity demands. This review critically examines recent scientific literature and official documents around three axes: digital governance and state capacity; cybersecurity and data protection; and interoperability and public digital infrastructure. Evidence reveals a dual picture. Ecuador shows regulatory and GovTech-maturity strengths while persistent gaps remain in proactiveness, inter-institutional coordination and capacity development. In the 2024 Global Cybersecurity Index, Ecuador performs strongly in legal, organizational, technical and cooperation measures, whereas capacity development is its weakest pillar. The central challenge is therefore not merely adopting technology, but consolidating technological governance that connects standards, human talent, data, interoperability, risk management and accountability. Sustainable public-sector digital transformation requires these components to become permanent state capabilities rather than isolated projects.

Información del manuscrito:

Fecha de recepción: 13 de julio de 2026.

Fecha de aceptación: 10 de septiembre de 2026.

Fecha de publicación: 10 de octubre de 2026.



Keywords: technological governance; cybersecurity; digital government; public sector; interoperability; Ecuador.

1. INTRODUCCIÓN

La digitalización del Estado ha dejado de ser un proceso asociado exclusivamente a la informatización de trámites. En la actualidad implica rediseñar servicios, compartir datos entre instituciones, crear plataformas comunes, establecer identidades digitales y proteger infraestructuras cuya indisponibilidad puede afectar derechos y servicios esenciales. La Agenda de Transformación Digital del Ecuador 2022–2025 ubicó dentro de una misma hoja de ruta la infraestructura digital, los sistemas de información, el gobierno de tecnologías de información, la identidad digital, la interoperabilidad y la seguridad digital, lo que evidencia que la transformación pública debe entenderse como un problema de gobernanza y no únicamente de equipamiento (MINTEL, 2022a).

La literatura regional coincide en que el gobierno digital requiere capacidades institucionales que permitan coordinar actores, gestionar datos, diseñar servicios centrados en las personas y evaluar el desempeño de las inversiones tecnológicas. La OCDE y CAF (2024) destacan que la digitalización pública produce mejores resultados cuando existe una visión de gobierno completo, reglas claras de gobernanza, capacidades del sector público y mecanismos de inclusión. Desde una perspectiva latinoamericana, Aguerre y Bonina (2024) agregan que las plataformas digitales también reconfiguran relaciones entre gobierno y ciudadanía, por lo que los modelos de gobernanza deben considerar participación, transparencia y responsabilidad institucional.

En Ecuador, el marco reciente incorpora la Ley Orgánica para la Transformación Digital y Audiovisual de 2023, el Reglamento General a la Ley Orgánica de Protección de Datos Personales de 2023 y el Esquema Gubernamental de Seguridad de la Información —EGSI— actualizado en 2024. Estos instrumentos amplían la responsabilidad pública sobre servicios digitales, tratamiento de datos, continuidad operativa y gestión de seguridad. No obstante, la existencia de normas no elimina las brechas de implementación. Vera Ortega y Yong Amaya (2025) identifican barreras vinculadas con interoperabilidad, capacidades institucionales, equidad territorial y gobernanza, mientras Moreira et al. (2024)

subrayan la necesidad de articular legislación, sistemas de información y cooperación frente a delitos informáticos y protección de datos.

El propósito de este artículo es sintetizar los principales retos de gobernanza tecnológica y ciberseguridad del sector público ecuatoriano, organizándolos en tres subtemas derivados de las variables centrales del problema: gobernanza digital y capacidad institucional; ciberseguridad y protección de datos; e interoperabilidad, infraestructura pública digital y confianza ciudadana. La revisión se orienta a identificar convergencias, tensiones y prioridades de fortalecimiento para una administración pública digital sostenible.

2. GOBERNANZA DIGITAL, INSTITUCIONALIDAD Y CAPACIDADES DEL ESTADO

La gobernanza tecnológica define quién decide, con qué reglas se priorizan inversiones, cómo se coordinan las instituciones y de qué manera se evalúan los efectos de la tecnología sobre la ciudadanía. En este sentido, Cedeño-Bazurto y Vegas-Meléndez (2024) relacionan la gobernanza institucional con el desempeño, la infraestructura inteligente y el desarrollo sostenible, destacando que el gobierno digital exige mecanismos de coordinación que trasciendan la simple disponibilidad de plataformas. Muñoz-Pallaroso et al. (2025) sostienen, de forma convergente, que la gobernanza digital transforma la gestión pública cuando logra integrar eficiencia, inclusión y procesos administrativos apoyados en tecnología.

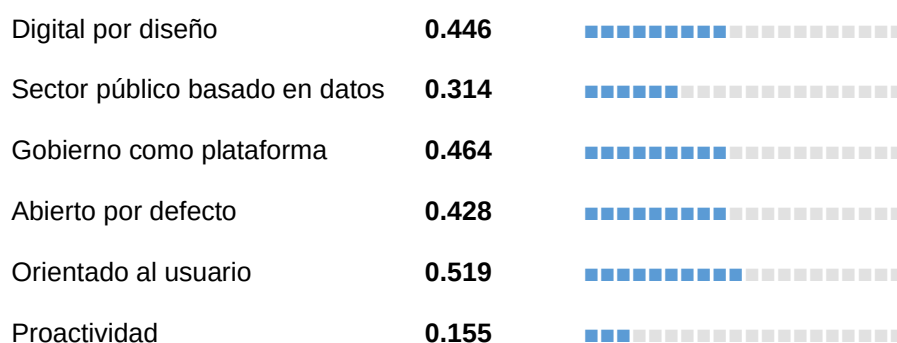
Los indicadores internacionales muestran avances, pero también una posición intermedia frente a los países líderes. En el Índice de Gobierno Digital 2023 de la OCDE/BID, Ecuador obtuvo un puntaje compuesto de 0,387 y se ubicó décimo entre los países latinoamericanos y caribeños evaluados. Sus mejores componentes fueron orientación al usuario (0,519), gobierno como plataforma (0,464) y digital por diseño (0,446); la proactividad alcanzó 0,155, revelando una brecha en la capacidad de anticipar necesidades y ofrecer servicios antes de que el ciudadano deba solicitarlos (OECD/IDB, 2024).

Esta lectura se complementa con el GovTech Maturity Index 2025, que ubica a Ecuador dentro del grupo de economías con madurez GovTech extensa. El valor agregado es relevante porque indica que existen sistemas básicos, capacidades de prestación digital y habilitadores institucionales. Sin embargo, la madurez tecnológica no debe confundirse con gobernanza consolidada: la sostenibilidad requiere presupuestos, perfiles profesionales, arquitectura empresarial, evaluación de riesgos y coordinación efectiva entre entidades (World Bank, 2025).

La literatura ecuatoriana insiste en la misma tensión. Vera Ortega y Yong Amaya (2025) identifican que la interoperabilidad, el marco regulatorio, la gobernanza, las capacidades institucionales y la equidad territorial siguen condicionando la transformación. Esto implica que el desafío no es únicamente aumentar el número de trámites en línea, sino garantizar que las instituciones compartan estándares, responsabilidades y modelos de gestión. Un servicio digital aislado puede mejorar una interacción puntual, pero no necesariamente modifica la capacidad estatal si no se conecta con datos, sistemas y decisiones de otras entidades.

La Ley Orgánica para la Transformación Digital y Audiovisual fortalece esta perspectiva al promover simplificación, medios digitales y modernización de servicios públicos y judiciales. Su relevancia para la gobernanza radica en que reconoce la transformación digital como un proceso transversal. No obstante, la efectividad depende de la institucionalización de mecanismos de seguimiento y de la capacidad de convertir políticas nacionales en planes, portafolios de proyectos e indicadores comparables a escala institucional.

Figura 1. Índice de Gobierno Digital 2023: dimensiones de Ecuador



Puntaje compuesto 0.387 

Nota. Fuente: OECD/IDB (2024), *Índice de Gobierno Digital para América Latina y el Caribe*.
Gráfico construido con elementos nativos y editables de Word.

Tabla 1. Retos de gobernanza tecnológica y respuestas institucionales

Reto	Manifestación	Respuesta prioritaria
Fragmentación institucional	Sistemas y decisiones tecnológicas gestionados por entidades con niveles desiguales de madurez.	Gobernanza de gobierno completo, arquitectura común y coordinación interinstitucional.
Baja proactividad	Servicios digitales que responden a solicitudes, pero anticipan poco las necesidades ciudadanas.	Datos interoperables, automatización responsable y diseño de servicios centrado en el usuario.
Capacidades desiguales	Brechas en talento digital, gestión de proyectos, datos y seguridad.	Planes permanentes de formación y perfiles especializados en el sector público.
Equidad territorial	Diferencias de infraestructura y capacidades entre instituciones y territorios.	Estándares mínimos, servicios compartidos y apoyo técnico a entidades con menor madurez.

Nota. Síntesis elaborada a partir de OECD/CAF (2024), Vera Ortega y Yong Amaya (2025), World Bank (2025) y MINTEL (2022a).

3. CIBERSEGURIDAD, GESTIÓN DE RIESGOS Y PROTECCIÓN DE DATOS

La expansión del gobierno digital aumenta la superficie de exposición a incidentes de seguridad. Bases de datos, servicios web, identidades digitales, redes institucionales y plataformas de interoperabilidad se convierten en activos críticos. La Estrategia Nacional de Ciberseguridad del Ecuador plantea una visión multisectorial y reconoce que la protección del ciberespacio requiere coordinación entre Estado, sector privado, academia y sociedad civil (MINTEL, 2022b). Esta orientación es coherente con el enfoque de gobernanza del riesgo: la ciberseguridad no puede reducirse al área técnica, porque las decisiones sobre activos, continuidad, privacidad y respuesta a incidentes involucran responsabilidades directivas.

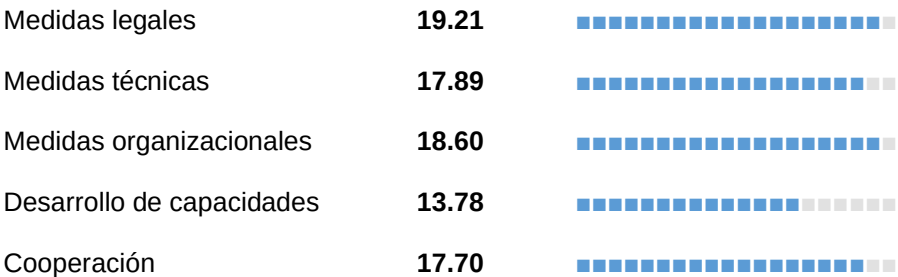
El EGSi 3.0, expedido en 2024, fortalece esta dimensión al establecer un mecanismo gubernamental para implementar sistemas de gestión de seguridad de la información en el sector público. Su alineación con ISO/IEC 27001:2022 facilita una estructura basada en identificación de activos, valoración de riesgos, controles, políticas, roles y mejora continua. Desde esta perspectiva, el reto no es únicamente cumplir listas de controles, sino incorporar la seguridad a la planificación institucional, la contratación tecnológica, el desarrollo de software y la gestión de proveedores.

El Global Cybersecurity Index 2024 ubica a Ecuador en el nivel T2 “Advancing”. Las medidas legales alcanzan 19,21 sobre 20; las técnicas, 17,89; las organizacionales, 18,60; la cooperación, 17,70; y el desarrollo de capacidades, 13,78. La estructura del índice sugiere que el marco normativo y organizacional es comparativamente sólido, mientras que la formación, las competencias y el desarrollo sostenido de talento especializado constituyen la brecha principal (ITU, 2024).

La protección de datos personales amplía las obligaciones de seguridad. El Reglamento General a la Ley Orgánica de Protección de Datos Personales exige una gestión responsable de tratamientos, medidas de seguridad y garantías para los titulares. En el sector público, donde los datos pueden incluir información tributaria, social, sanitaria, registral o judicial, la gobernanza debe integrar privacidad desde el diseño, minimización, trazabilidad y controles de acceso. Moreira et al. (2024) advierten que la aplicación efectiva de la regulación y la cooperación son indispensables para enfrentar delitos informáticos y riesgos asociados a los sistemas de información.

La principal implicación institucional es que las inversiones en seguridad deben acompañarse de cultura organizacional. El menor desempeño del país en desarrollo de capacidades dentro del GCI refuerza la necesidad de programas continuos de formación para directivos, responsables de procesos, desarrolladores, administradores de infraestructura y usuarios finales. La seguridad depende de controles técnicos, pero también de decisiones humanas, procedimientos y mecanismos de respuesta.

Figura 2. Global Cybersecurity Index 2024: desempeño de Ecuador por pilar



Nota. Fuente: International Telecommunication Union (2024). Puntaje máximo por pilar: 20. Gráfico construido con elementos nativos y editables de Word.

4. INTEROPERABILIDAD, INFRAESTRUCTURA PÚBLICA DIGITAL Y CONFIANZA CIUDADANA

La interoperabilidad constituye el puente entre digitalización institucional y transformación del Estado. Cuando cada entidad mantiene sistemas cerrados, el ciudadano debe repetir datos, presentar documentos que ya posee otra institución y adaptarse a procedimientos fragmentados. La Agenda de Transformación Digital incorporó específicamente un eje de interoperabilidad y tratamiento de datos, junto con servicios de interoperabilidad, datos personales y datos abiertos (MINTEL, 2022a). Este diseño reconoce que el valor de la tecnología pública aumenta cuando la información puede circular de forma segura, trazable y legítima.

OECD/CAF (2024) señala que los gobiernos digitales maduros se apoyan en infraestructura pública digital y componentes reutilizables que evitan duplicar inversiones. El enfoque de gobierno como plataforma implica servicios comunes de identidad, pagos, notificaciones, datos y autenticación que puedan ser utilizados por distintas entidades. En Ecuador, el puntaje de 0,464 en “gobierno como plataforma” dentro del DGI 2023 muestra una base relevante, aunque la baja proactividad evidencia que esa infraestructura aún puede generar mayor valor mediante automatización y servicios integrados.

La interoperabilidad también exige gobernanza de datos. No basta con conectar aplicaciones: deben definirse bases jurídicas de intercambio, responsabilidades de tratamiento, calidad, catálogos, metadatos, trazabilidad y mecanismos de

auditoría. El Reglamento de Protección de Datos Personales introduce límites y obligaciones que impiden concebir la integración de sistemas como libre circulación irrestricta de información. La arquitectura tecnológica debe operar bajo principios de finalidad, proporcionalidad, seguridad y responsabilidad demostrada.

La confianza ciudadana es, por tanto, una variable de resultado de la gobernanza tecnológica. Servicios más simples y coordinados pueden mejorar la experiencia de las personas, pero una filtración de datos, una interrupción masiva o una decisión automatizada opaca puede deteriorar esa confianza. Por ello, la ciberseguridad y la interoperabilidad no son objetivos independientes: la primera protege la infraestructura que hace posible la segunda, mientras la segunda multiplica el impacto de cualquier debilidad de seguridad.

La consolidación de infraestructura pública digital debe ir acompañada de evaluación de desempeño. El GovTech Maturity Index y el Digital Government Index ofrecen referencias comparativas útiles, pero las instituciones necesitan indicadores propios sobre disponibilidad, interoperabilidad, incidentes, calidad de datos, uso de servicios, satisfacción ciudadana y tiempos de atención. Convertir esos indicadores en ciclos de mejora es una condición para que la transformación digital permanezca más allá de programas o períodos administrativos.

Tabla 2. Instrumentos recientes que estructuran la gobernanza digital y la seguridad pública en Ecuador

Instrumento	Año	Aporte principal
Agenda de Transformación Digital del Ecuador 2022–2025	2022	Integra infraestructura, gobierno TI, interoperabilidad, datos y seguridad digital.
Estrategia Nacional de Ciberseguridad	2022	Define coordinación multisectorial y prioridades para fortalecer el ciberespacio ecuatoriano.
Ley Orgánica para la Transformación Digital y Audiovisual	2023	Impulsa simplificación, servicios y adopción de tecnologías digitales en el Estado.
Reglamento General a la Ley Orgánica de Protección de Datos Personales	2023	Desarrolla obligaciones para tratamiento y protección de datos personales.

Esquema Gubernamental de Seguridad de la Información 3.0	2024	Establece el marco para sistemas de gestión de seguridad de la información en el sector público.
---	------	---

Nota. *Elaboración propia con base en normativa y documentos oficiales ecuatorianos.*

5. SÍNTESIS CRÍTICA E IMPLICACIONES PARA LA GESTIÓN PÚBLICA

La revisión permite identificar una convergencia clara: Ecuador dispone de una base normativa e institucional significativa, pero el siguiente ciclo de transformación depende de la capacidad de ejecutar, coordinar y sostener. Los puntajes del GCI muestran que el país ha avanzado en legislación, organización y cooperación; al mismo tiempo, el DGI evidencia una proactividad limitada. Ambas mediciones apuntan al mismo problema: el marco formal debe transformarse en capacidades operativas y servicios integrados.

En términos de política pública, la prioridad debería ser articular gobernanza, seguridad e interoperabilidad en un mismo modelo. Los comités de transformación digital requieren capacidad para priorizar inversiones, gestionar arquitectura y datos, evaluar riesgos y medir resultados. Si estas funciones se distribuyen sin coordinación, la digitalización puede reproducir la fragmentación burocrática en una nueva capa tecnológica.

El fortalecimiento de capacidades merece especial atención. La brecha identificada por ITU en desarrollo de capacidades y las barreras institucionales reportadas por Vera Ortega y Yong Amaya (2025) sugieren que la disponibilidad de tecnología supera, en algunos ámbitos, la capacidad de apropiación. Programas de formación diferenciados por rol, comunidades de práctica y carreras técnicas públicas podrían reducir esa brecha y mejorar la sostenibilidad de las inversiones.

Finalmente, la confianza debe ser tratada como un activo público. La transformación digital solo produce valor cuando la ciudadanía percibe que los servicios son útiles, accesibles y seguros. Esto exige transparencia sobre el uso de datos, respuesta ante incidentes, canales de soporte y mecanismos de

evaluación. La gobernanza tecnológica madura combina eficiencia con protección de derechos y capacidad de rendición de cuentas.

6. CONCLUSIONES

La gobernanza tecnológica del sector público ecuatoriano se encuentra en una etapa de consolidación. Las políticas y normas recientes han construido una base para gobierno digital, protección de datos, interoperabilidad y seguridad de la información, mientras los indicadores internacionales muestran niveles relevantes de madurez y compromiso.

No obstante, las brechas de proactividad, capacidades institucionales y articulación interinstitucional limitan la conversión de esa base normativa en valor público. La ciberseguridad presenta fortalezas en componentes legales y organizacionales, pero requiere mayor inversión sostenida en competencias, cultura de seguridad y gestión de riesgos.

La interoperabilidad debe asumirse como componente de gobernanza y no como proyecto técnico aislado. Su desarrollo demanda estándares comunes, bases jurídicas claras, calidad de datos, trazabilidad y privacidad desde el diseño. De la misma manera, la infraestructura pública digital debe medirse por su contribución a servicios simples, integrados y confiables.

En consecuencia, el principal reto para Ecuador consiste en transformar la digitalización en capacidad estatal permanente. Esto supone integrar estrategia, arquitectura, datos, ciberseguridad, talento humano y evaluación bajo una gobernanza común que preserve derechos y fortalezca la confianza ciudadana.

Declaraciones

Conflicto de intereses. El autor declara no mantener conflictos de intereses relacionados con el contenido de este artículo.

Financiamiento. El artículo no reporta financiamiento externo específico.

Originalidad. El manuscrito se presenta como artículo de revisión y síntesis crítica de literatura científica, normativa y fuentes institucionales recientes.

Adecuación editorial. La estructura se preparó siguiendo criterios académicos compatibles con REICOMUNICAR y referencias en formato APA 7.

REFERENCIAS

- Aguerre, C., & Bonina, C. (2024). Open government, civic tech and digital platforms in Latin America: A governance study of Montevideo's urban app "Por Mi Barrio". *Information Systems Journal*, 34(4), 1037–1067. <https://doi.org/10.1111/isj.12468>
- Asamblea Nacional del Ecuador. (2023). Ley Orgánica para la Transformación Digital y Audiovisual. Registro Oficial, Tercer Suplemento No. 245.
- Cedeño-Bazurto, J. D., & Vegas-Meléndez, H. J. (2024). Gobernanza institucional como estrategia del gobierno digital para fomentar ciudades inteligentes. *593 Digital Publisher CEIT*, 9(1), 138–153. <https://doi.org/10.33386/593dp.2024.1.2167>
- International Telecommunication Union. (2024). Global Cybersecurity Index 2024. ITU.
- Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022a). Agenda de Transformación Digital del Ecuador 2022–2025. Acuerdo MINTEL-MINTEL-2022-0022.
- Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022b). Estrategia Nacional de Ciberseguridad del Ecuador. MINTEL.
- Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2024). Esquema Gubernamental de Seguridad de la Información (EGSI). Acuerdo MINTEL-MINTEL-2024-0003.
- Moreira Moreira, I. A., Navia Mendoza, M., & Parraga-Alava, J. (2024). El derecho informático y la influencia en los sistemas de información: un análisis bibliográfico bajo la perspectiva jurídica y tecnológica en Ecuador. *Revista Tecnológica - ESPOL*, 36(1), 162–178. <https://doi.org/10.37815/rte.v36n1.1151>
- Muñoz-Pallaroso, E. K., Romero-Vásquez, X. M., Pallaroso-Granizo, R. Y., & Oviedo-Bayas, B. (2025). Gobernanza digital y transformación del Estado. Impacto de la tecnología en la gestión pública. *Revista Metropolitana de Ciencias Aplicadas*, 8(3), 96–100. <https://doi.org/10.62452/hctsy763>

- 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>
- OECD/IDB. (2024). 2023 OECD/IDB Digital Government Index of Latin America and the Caribbean: Results and key findings. OECD Public Governance Policy Papers, 64. <https://doi.org/10.1787/10b82c83-en>
- Presidencia de la República del Ecuador. (2023). Reglamento General a la Ley Orgánica de Protección de Datos Personales. Decreto Ejecutivo No. 904, Registro Oficial Suplemento No. 435.
- Vera Ortega, R., & Yong Amaya, L. (2025). Barreras institucionales para la gobernanza digital en Ecuador: Evidencia desde la Cuarta Revolución Industrial. *Revista Española de la Transparencia*, 22, 313–333. <https://doi.org/10.51915/ret.407>
- World Bank. (2022). GovTech Maturity Index, 2022 Update: Trends in public sector digital transformation. World Bank.
- World Bank. (2025). GovTech Maturity Index 2025: Tracking public sector digital transformation worldwide. World Bank.