

**Diálogo Regional**

# Los retos de la gobernanza digital en América Latina y el Caribe

Relatoría del Diálogo Regional  
**“Los Retos de la Gobernanza Digital  
en América Latina y el Caribe”**

26 al 28 de noviembre de 2025,  
Montevideo, Uruguay



## Los retos de la gobernanza digital en América Latina y el Caribe

Del 26 al 28 de noviembre de 2025 | Montevideo, Uruguay

### Edición:

CAF —banco de desarrollo de América Latina y el Caribe— y el Programa de las Naciones Unidas para el Desarrollo (PNUD) en América Latina y el Caribe

### Diseño gráfico:

Sandra Pérez, diseñadora gráfica, PNUD

Este documento ha sido preparado en el marco de la alianza “Gobernanza para el desarrollo” de CAF —banco de desarrollo de América Latina y el Caribe— y del Programa de las Naciones Unidas para el Desarrollo (PNUD).

Su elaboración fue responsabilidad del Buró Regional para América Latina y el Caribe del PNUD, bajo el liderazgo de Michelle Muschett, Subsecretaria General de la ONU y Directora Regional para América Latina y el Caribe, y María del Carmen Sacasa, Directora Regional Adjunta; y de CAF, bajo el liderazgo de Sergio Díaz-Granados, presidente ejecutivo, y Christian Asinelli, vicepresidente corporativo de Programación Estratégica.

La conducción del diálogo y la redacción de esta relatoría estuvo a cargo de un equipo multidisciplinario de especialistas del PNUD y CAF.

Se agradece también a los distintos participantes de los cuatro diálogos subregionales, que contribuyeron con tiempo, experiencias y recomendaciones de manera generosa y comprometida al desarrollo de los diálogos.

### Equipo del PNUD

Jairo Acuña-Alfaro, líder de Gobernabilidad en América Latina y el Caribe

Claudia Bresanovich, especialista en Alianzas

María Pinedo, analista de Alianzas

Marisol Palma, asociada de programa y administrativa

Rosana Pineda, asociada administrativa

Camila Da Rocha, asociada administrativa

### Equipo de CAF

Juan Fernando Londoño, ejecutivo senior de la Vicepresidencia Corporativa de Programación Estratégica

Hiroshi Wago Rojas, director de Alianzas Globales

Andrés Sarache, ejecutivo principal de la Vicepresidencia Corporativa de Programación Estratégica

Karla Molina, ejecutiva principal de la Dirección de Alianzas Globales

Maximiliano Peccia, ejecutivo de la Vicepresidencia Corporativa de Programación Estratégica

### Equipo técnico PNUD

Jairo Acuña-Alfaro, líder de Gobernabilidad en América Latina y el Caribe

Moema Dutra Freire, especialista en Políticas

Enrique Crespo, especialista Digital

### Equipo técnico CAF

Eduardo Chomali, ejecutivo senior de la Dirección de Transformación Digital y Servicio al Ciudadano (DTDSC)

Martín Olmos, ejecutivo principal de la Dirección de Transformación Digital y Servicio al Ciudadano (DTDSC)

Alejandro Forero, ejecutivo principal de la Dirección de Transformación Digital y Servicio al Ciudadano (DTDSC)

### Nota aclaratoria

Las conclusiones, análisis y recomendaciones de esta relatoría no representan la posición oficial del PNUD, CAF ni de ninguno de los Estados Miembros de las Naciones Unidas.

# Tabla de Contenido

<b>1.</b>	Introducción y contexto	5
<b>2.</b>	Propósito y objetivos del diálogo	6
<b>3.</b>	Participantes y metodología	8
<b>4.</b>	Escenario regional compartido	10
4.1.	Una promesa bajo presión: inclusión, confianza y trato humano	11
4.2.	Democracia en riesgo: desinformación, violencia digital y ciberseguridad	11
4.3.	Soberanía y extractivismo digital	11
4.4.	Regulación: del “qué” al “cómo” y la idea de prudencia estratégica	12
4.5.	Gobernanza multiactor y continuidad	13
<b>5.</b>	Principales resultados del Diálogo	15
5.1.	Regulación y ejecución efectiva	15
5.2.	Institucionalidad pública y coordinación estatal para adoptar tecnologías con gobernanza	16
5.3.	Gobernanza de datos, soberanía estratégica e infraestructura digital pública	16
5.4.	Integridad democrática, violencia digital y ciberseguridad como política de Estado	18
5.5.	Inclusión, participación efectiva y legitimidad del Estado digital	19
<b>6.</b>	Hoja de ruta	22
6.1.	Principios orientadores	22
6.2.	Acciones regionales	23
6.3.	Horizonte Temporal	24
<b>7.</b>	Referencias bibliográficas	26

# 1. Introducción y contexto

América Latina y el Caribe atraviesan una coyuntura decisiva: mientras la vida cotidiana, la economía y la esfera pública se digitalizan a una velocidad inédita, la región sigue enfrentando tensiones estructurales de legitimidad, representación, desigualdad y seguridad. En este escenario, la gobernanza digital deja de ser un tema sectorial para convertirse en un asunto estratégico del desarrollo humano sostenible: no se trata sólo de adoptar tecnología, sino de definir para qué, para quién y bajo qué reglas se despliega, con qué capacidades estatales, con qué salvaguardas democráticas y con qué cooperación regional. (Naciones Unidas, 2024b)

Este Diálogo Regional, «Los Retos de la Gobernanza Digital en América Latina y el Caribe» (Montevideo, 26-28 de noviembre de 2025), se realiza en el marco de la alianza estratégica entre el Banco de Desarrollo de América Latina y el Caribe (CAF) y el Programa de las Naciones Unidas para el Desarrollo (PNUD), que durante los últimos años ha impulsado una agenda de gobernanza para el desarrollo orientada a traducir deliberación plural en recomendaciones accionables y oferta programática para los países. La primera ronda de diálogos subregionales consolidó un diagnóstico compartido: la región necesita un renacimiento institucional que recupere confianza, fortalezca capacidades públicas, promueva gobernanza inclusiva y habilite pactos políticos y sociales para gestionar transiciones simultáneas de desarrollo, digital y ambiental, sin erosionar el estado de derecho (CAF y PNUD, 2024). Esta segunda ronda profundiza esa apuesta mediante talleres temáticos, con un objetivo práctico: construir rutas de acción y cooperación capaces de incidir en políticas públicas y en marcos regionales.

La temática digital impone un sentido de urgencia adicional. En el marco del Informe regional sobre desarrollo humano 2025: Bajo presión, el PNUD advirtió que la región no ha recuperado plenamente su trayectoria de desarrollo post-pandemia y que la tecnología, lejos de operar como “solución automática”, puede funcionar como punto de presión: lo digital no es neutral y, sin decisiones deliberadas, réplica y amplifica desigualdades. En América Latina y el Caribe, persisten brechas críticas de capacidades, infraestructura y acceso efectivo, junto con riesgos emergentes asociados a opacidad algorítmica, sesgos culturales, vigilancia, impactos sobre salud mental y huella ambiental. Al mismo tiempo, se identificó un desafío estratégico de soberanía y cadena de valor, marcado por procesamiento extrarregional de datos y baja capacidad computacional, que puede derivar en nuevas formas de «extractivismo digital», si la región no fortalece la tríada infraestructura + capital humano + gobernanza de datos (PNUD, 2025b). En paralelo, se reconocen oportunidades concretas: en diversos países, el sector público ya está innovando con IA para mejorar servicios, gestión y políticas.

Con este trasfondo, CAF y PNUD convocaron a una representación diversa y multisectorial: gobiernos, parlamentos, sector privado, academia y sociedad civil, con participación de múltiples países, para construir un lenguaje común, identificar tensiones reales y acordar prioridades regionales. Tal como enfatizaron las palabras de bienvenida, el propósito no es discutir la tecnología en abstracto, sino alinear una visión donde la transformación digital sea una palanca de desarrollo: ampliar oportunidades, cerrar brechas y fortalecer la democracia, con la persona en el centro. A la vez, se subrayó el valor político de estos espacios: la gobernanza digital no se resuelve en solitario; exige alianzas, cooperación técnica, redes de confianza y una infraestructura institucional capaz de sostener reformas y aprendizajes compartidos.

Esta relatoría recoge los resultados del diálogo con una finalidad institucional clara: ofrecer una lectura rigurosa y propositiva de lo acordado, y dejar instalados insumos utilizables que orienten programación, cooperación y posicionamiento regional en espacios de alto nivel. En suma, el diálogo

parte de una convicción compartida: la gobernanza digital es, una condición habilitante del desarrollo humano y de la legitimidad democrática; su dirección no puede quedar librada a la inercia tecnológica, sino que debe ser construida, con evidencia, con pluralidad y con responsabilidad pública, desde América Latina y el Caribe.

## 2. Propósito y objetivos del Diálogo

El Diálogo Regional se estableció como una plataforma estratégica para redefinir la relación entre el Estado, la sociedad y la tecnología en América Latina y el Caribe. Su propósito fundamental fue trascender la discusión meramente técnica para situar la gobernanza tecnológica como un pilar indispensable del desarrollo humano sostenible. Mediante una metodología diseñada para transitar desde la nivelación conceptual hasta la deliberación política, el espacio buscó superar la visión de la región como consumidora pasiva de tecnología, para posicionarla como un actor capaz de diseñar sus propios marcos regulatorios y éticos. El encuentro articuló una convergencia multisectorial, integrando los sectores público, privado, académico y de la sociedad civil, con el fin de construir una visión compartida que equilibre la promoción de la innovación con la protección de los derechos fundamentales y la soberanía digital.

Los objetivos estratégicos del Diálogo fueron:

- » Establecer un marco de comprensión común que permita alinear conceptos y lenguajes sobre los alcances, oportunidades y riesgos de las tecnologías emergentes (especialmente la Inteligencia Artificial), fundamentando el debate en evidencia empírica, como el Informe Regional de Desarrollo Humano 2025: Bajo Presión y el Atlas de IA para el Desarrollo Humano en ALC, para superar las asimetrías de información y cimentar bases sólidas para la toma de decisiones.
- » Analizar los desafíos institucionales y las brechas regulatorias que deben superarse para transitar de enfoques sectoriales fragmentados a modelos de gobernanza integrales y adaptativos. Esto implicó identificar mecanismos para garantizar la interoperabilidad, la ciberseguridad y la inclusión digital, asegurando que la modernización estatal no vulnere derechos ni profundice brechas de desigualdad.
- » Debatar los impactos de la digitalización y la automatización en la esfera pública, abordando la tensión entre la expansión de la participación ciudadana y los riesgos de manipulación informativa. El diálogo se centró en identificar principios éticos y mecanismos de responsabilidad compartida que permitan preservar la confianza pública, garantizar la transparencia y proteger la integridad del debate democrático frente a desafíos como la desinformación.
- » Cocrear una hoja de ruta regional que traduzca el diagnóstico compartido en una agenda de prioridades estratégicas que fomente la cooperación internacional y la coordinación multinivel. Se buscó trascender la deliberación para definir alianzas y compromisos de acción que permitan avanzar hacia una gobernanza tecnológica colaborativa, centrada en las personas y capaz de responder a los retos transfronterizos del siglo XXI.

De esta manera, el Diálogo Regional se planteó como un punto de convergencia y proyección. Sus resultados buscan alimentar procesos de toma de decisión, diseño de políticas públicas y cooperación regional promovidos por CAF, el PNUD y sus contrapartes, contribuyendo a posicionar a América Latina y el Caribe como una región capaz de gobernar la tecnología con visión estratégica, responsabilidad democrática, y sin dejar a nadie atrás.



### 3.

## Participantes y metodología

El Diálogo Regional convocó a un grupo selecto de 35 personas, 23 mujeres y 12 hombres provenientes de 9 países de la región: Argentina, Chile, Colombia, Ecuador, Guatemala, México, Panamá, República Dominicana y Uruguay. Este diverso grupo de especialistas hacen parte de autoridades gubernamentales, legisladores/as y representantes de la sociedad civil, academia y el sector privado.

La composición del grupo destacó por su carácter multisectorial y pluriestatal, integrando perfiles técnicos y políticos de alto nivel. Entre los asistentes se contaron directores de agencias de innovación y gobierno digital, legisladores miembros de comisiones de futuro, representantes de organismos electorales, académicos especializados en derecho digital y ética de la IA, así como líderes de cámaras de tecnología y organizaciones de la sociedad civil enfocadas en transparencia y género. Se procuró un equilibrio de género y una diversidad de perspectivas, con la participación activa de redes especializadas en mujeres en seguridad y defensa, y alianzas por una internet abierta. Esta heterogeneidad aseguró que el diálogo abordara la gobernanza no solo desde la eficiencia técnica, sino también desde los derechos humanos, la inclusión y la sostenibilidad democrática.

El taller se estructuró bajo la lógica de diálogos estratégicos, diseñados para transitar desde la comprensión conceptual hacia la acción colectiva. La dinámica metodológica se basó en tres momentos interconectados: (i) Inspirar, mediante presentaciones de expertos/as y marcos conceptuales; (ii) Dialogar, a través de conversaciones guiadas que fomentaron el intercambio; y (iii) Producir, enfocándose en la síntesis de propuestas concretas.

Durante las jornadas, el trabajo se organizó alternando sesiones plenarias y grupos de trabajo temáticos:

- » Sesiones Plenarias: Se utilizaron para establecer diagnósticos comunes sobre los alcances y riesgos de las nuevas tecnologías, así como para abordar el impacto de la IA y las redes sociales en la gobernanza democrática y la integridad informativa.
- » Grupos de Trabajo: Los participantes se dividieron en mesas especializadas para profundizar en dos ejes críticos. Primero, se analizaron tendencias regulatorias (niveles, modelos y prioridades regulatorias). Posteriormente, se abordó la modernización estatal, discutiendo en cinco subgrupos temas de acceso universal, interoperabilidad, ciberseguridad, uso ético de la IA y confianza ciudadana.

Como herramientas de sistematización, se contó con un equipo de relatoría que documentó los hallazgos en tiempo real y el uso de dinámicas participativas como el “Mapa de la Conversación” para identificar tensiones éticas e institucionales. El proceso culminó con la construcción colaborativa de una Hoja de Ruta Regional, identificando prioridades estratégicas, principios compartidos y mecanismos de cooperación entre el sector público, privado y la sociedad civil para una gobernanza tecnológica centrada en las personas.

Para fundamentar el diálogo las sesiones de análisis y deliberación tomaron como referencia directa cuatro documentos estratégicos recientes. Las discusiones sobre el estado del arte y las brechas estructurales se guiaron por los hallazgos del *Atlas de inteligencia artificial para América Latina y el Caribe* (PNUD 2025a) y el diagnóstico socioeconómico del *Informe regional sobre desarrollo humano 2025: Bajo presión* (PNUD, 2025b). Del mismo modo, para abordar los desafíos institucionales y los mecanismos de coordinación, el trabajo se nutrió de las recomendaciones de *Gobernanza para el desarrollo en América Latina y el Caribe* (CAF & PNUD, 2024), así como de los datos de opinión pública presentados en el informe sobre *Gobernanza de la inteligencia artificial en América Latina y el Caribe* (Alto Intelligence, 2025).



## 4. Escenario regional compartido

Las y los participantes coincidieron en que América Latina y el Caribe atraviesa un punto de inflexión en el que lo digital dejó de ser un capítulo sectorial para convertirse en un factor transversal de gobernanza y desarrollo. El diálogo partió de una premisa compartida, subrayada desde la apertura por CAF y PNUD: la digitalización y la inteligencia artificial (IA) no son un fin en sí mismas, sino un medio. Un medio que puede expandir libertades, mejorar servicios y cerrar brechas, pero que también puede amplificar desigualdades, erosionar la confianza institucional y acelerar riesgos democráticos si no se gobierna con criterios de derechos, capacidades estatales y coordinación multiactor.

Desde el primer día, el escenario común se configuró como una tensión central: la región se encuentra en una “ventana de vulnerabilidad” donde la velocidad de adopción tecnológica, especialmente por parte de la ciudadanía y del mercado, supera la capacidad institucional para responder con instrumentos de política pública, marcos legales aplicables y capacidades operativas de supervisión. Esa asimetría no se percibió únicamente como un rezago normativo, sino como un desajuste más profundo entre expectativas sociales y desempeño estatal, que afecta la legitimidad del Estado digital. La frase citada en plenaria sintetizó esa brecha:

*“Los ciudadanos se comunican con tecnología del siglo XXI, las instituciones responden con instrumentos del siglo XX y las políticas públicas se han diseñado con pensamientos del siglo XIX”*

En este marco, se consolidó un diagnóstico compartido: la gobernanza digital en ALC no puede construirse solamente “desde la regulación” ni únicamente “desde la innovación”. Requiere resolver condiciones estructurales que hoy limitan la autonomía tecnológica y la posibilidad de que lo digital sea realmente una palanca de desarrollo humano. La discusión reiteró tres déficits que se retroalimentan:



En otras palabras: sin el trípode de infraestructura + talento + gobernanza de datos, la región corre el riesgo de quedar atrapada en la adopción periférica y dependiente de soluciones externas, con beneficios desiguales y baja sostenibilidad.

#### 4.1. Una promesa bajo presión: inclusión, confianza y trato humano

El segundo elemento del escenario regional compartido fue el consenso sobre el carácter no neutral de la tecnología. La conversación descartó la idea de que lo digital sea automáticamente modernizador o democratizador: sin decisiones explícitas, lo digital tiende a replicar y amplificar patrones del mundo analógico. De ahí que, más que debatir herramientas, se debatió la relación Estado–ciudadanía: cómo sostener cercanía, comprensión y dignidad en servicios digitalizados; cómo proteger derechos cuando se automatizan decisiones; y cómo evitar que la digitalización se convierta en un nuevo filtro de exclusión.

En las mesas y grupos se insistió en que la legitimidad del Estado digital depende de su capacidad para “no dejar a nadie atrás” en términos de acceso, asequibilidad, habilidades y usabilidad. El acceso universal fue entendido como una condición política, no solo tecnológica: si el Estado migra trámites y servicios sin transiciones razonables, acompañamiento y alternativas, puede profundizar desigualdades y aumentar frustraciones. De forma reiterada se planteó que la confianza es un activo intangible central de la gobernanza que no se decreta; se construye con trazabilidad, lenguaje claro, canales comprensibles, rendición de cuentas y garantías concretas, incluyendo el derecho a saber cuando se interactúa con sistemas automatizados y el derecho a ser atendido por una persona.

#### 4.2. Democracia en riesgo: desinformación, violencia digital y ciberseguridad

Un tercer rasgo del escenario regional compartido fue el lugar predominante que ocupan los riesgos sobre integridad democrática y violencia digital. Tanto el análisis de conversación pública como los aportes del debate situaron la desinformación electoral, la manipulación mediante microsegmentación y la proliferación de *deepfakes* (incluidos los de contenido sexual) como amenazas inmediatas que avanzan más rápido que los marcos institucionales de respuesta. (PNUD, 2024) Esta preocupación se vinculó, además, con una lectura estructural: la IA no crea por sí sola la crisis de confianza, pero sí puede amplificar fragilidades preexistentes en sistemas políticos atravesados por la polarización, el deterioro del debate público, la inseguridad y el debilitamiento de las mediaciones institucionales.

La violencia digital, en particular la dirigida contra mujeres en política y liderazgos públicos, emergió como un fenómeno que trasciende lo virtual y tiene efectos concretos en la vida real: inhibe participación, genera autocensura, altera la representación democrática y puede traducirse en riesgos físicos. De ahí que se reitera el binomio indisoluble: no es posible hablar de IA sin hablar de ciberseguridad. La seguridad se entendió como gestión de riesgos que debe integrarse desde el diseño, con instituciones con mandato claro y autoridad suficiente, capacidades de respuesta a incidentes, cooperación regional operativa y salvaguardas de derechos, evitando que el paraguas de “combatir *fake news*” habilite derivas de censura o control estatal indebido. (Naciones Unidas, 2024a)

#### 4.3. Soberanía y extractivismo digital

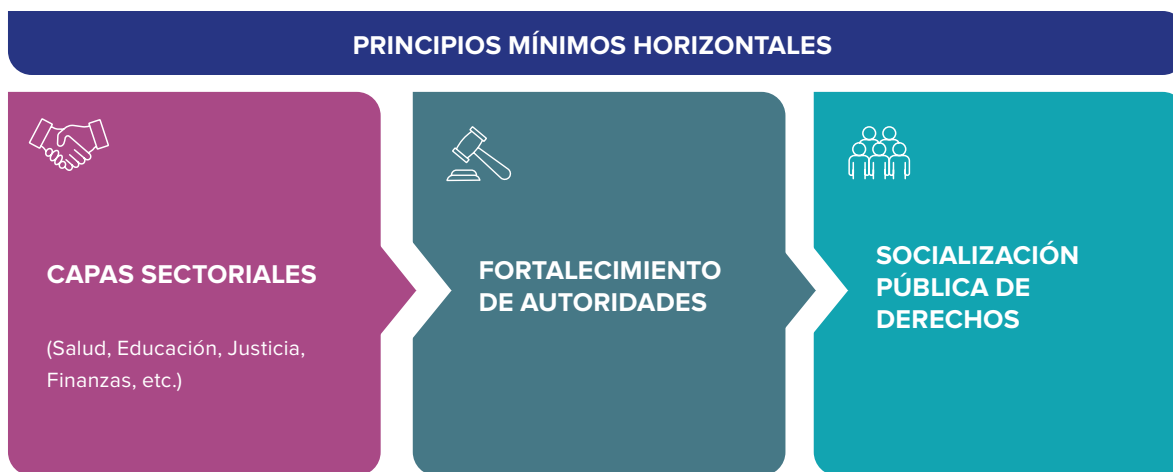
En el escenario común también se instaló un debate de fondo sobre soberanía: la región observa que el valor estratégico de lo digital se concentra en la infraestructura de cómputo y, sobre todo, en la gobernanza de los datos. Se discutió la posibilidad de que América Latina y el Caribe repita patrones históricos: exportar materias primas (datos y minerales críticos) e importar productos de alto valor agregado (modelos, software, servicios), quedando como consumidora de “cajas negras” que no reflejan su diversidad cultural y lingüística. Esta lectura, nombrada como “extractivismo digital” reforzó dos exigencias: (i) construir capacidades locales (datos, talento, infraestructura) y (ii) articularse regionalmente para negociar con mayor peso frente a corporaciones tecnológicas y dinámicas globales.

En ese punto, se reconoció la realidad de la infraestructura disponible en la región y la dependencia de nubes globales. Sin embargo, también se abrió un horizonte pragmático: desarrollar infraestructura digital pública y enfoques de “IA pública” entendida no como estatización, sino como bienes públicos digitales (open source, transparentes, auditables, con propósito social), junto con estrategias que prioricen modelos más pequeños y curados para problemas locales (salud, biodiversidad, productividad pública, justicia, educación), evitando entrar en una carrera inalcanzable por modelos masivos.

#### 4.4. Regulación: del “qué” al “cómo” y la idea de prudencia estratégica

Un quinto componente del escenario compartido fue el enfoque sobre regulación: se constató que la región tiene abundancia de estrategias, hojas de ruta y declaraciones, pero escasez de normativa operativa y, sobre todo, de capacidades de implementación. En ese sentido, se reiteró que el reto no es sólo redactar leyes, sino crear institucionalidad, presupuesto, competencias técnicas, coordinación y mecanismos de control que vuelvan aplicables las reglas.

La discusión evitó la dicotomía “regular vs innovar” y propuso una regulación habilitante: centrada en usos y riesgos, diferenciada por sectores y niveles de riesgo, con sandboxes regulatorios para aprender antes de normar de forma definitiva, y con estándares técnicos interoperables como camino realista para convergencias regionales. Se advirtió el riesgo de reproducir arquitecturas regulatorias complejas sin madurez institucional (el llamado “efecto copia” de modelos externos) y se valoró, en cambio, una progresión:



En el cierre del segundo día, esta mirada se conectó con una noción clave: la “prudencia estratégica” como oportunidad para comprender efectos, construir evidencia y evitar normas simbólicas o inaplicables. Esa prudencia, sin embargo, no se entendió como inacción: se vinculó a una hoja de ruta gradual con prioridades inmediatas: datos, transparencia, vigilancia, niñez, violencia digital, ciberseguridad; y metas verificables.

#### 4.5. Gobernanza multiactor y continuidad

Finalmente, el escenario regional compartido dejó una constatación transversal: la gobernanza digital no se sostiene sólo con marcos formales; requiere coordinación multinivel y mecanismos estables de diálogo multiactor con resultados tangibles. La región enfrenta fragmentación de iniciativas, disputa de liderazgos, duplicidades y discontinuidades asociadas a ciclos políticos. Por ello, se insistió en que el desafío es pasar de espacios deliberativos a arreglos institucionales con vocación vinculante, memoria institucional y productos concretos (estándares, guías, protocolos, observatorios, mecanismos de auditoría, acuerdos de interoperabilidad y cooperación).

En esa dirección, se valoró el rol de servidores públicos como nodos de continuidad, así como el aporte de academia y sociedad civil para sostener políticas de Estado, auditar sistemas, fortalecer marcos éticos y evitar que el “Estado digital” dependa exclusivamente de agendas políticas. También se reconoció la dificultad de construir una “visión latinoamericana” dada la heterogeneidad política y económica; aun así, se sostuvo que la ausencia de una narrativa regional coordinada debilita la capacidad de incidir en foros globales y de negociar condiciones más justas en la economía digital.

En síntesis, el escenario regional compartido que emergió del diálogo puede leerse como una encrucijada: o la región avanza hacia una gobernanza digital centrada en las personas, con reglas aplicables, instituciones capaces, datos bien gobernados y cooperación regional efectiva, o corre el riesgo de profundizar una adopción desigual y dependiente, donde lo digital opere como amplificador de exclusión, violencia y desconfianza.

La hoja de ruta delineada y expuesta en las siguientes secciones se apoya justamente en ese punto de partida: no se trata de elegir entre modernización y derechos, sino de construir capacidades y acuerdos para que la modernización sea, efectivamente, un camino de derechos, legitimidad y desarrollo humano.



# 5.

## Principales resultados del Diálogo

A lo largo de las plenarias, debates y grupos de trabajo se consolidó una lectura común: la gobernanza digital en América Latina y el Caribe ya no puede tratarse como un asunto tecnológico, sino como una decisión de política pública que define capacidad estatal, legitimidad democrática y las trayectorias del desarrollo. El diálogo mostró que los principales riesgos y oportunidades no dependen de la IA en abstracto, sino de cómo se gobierna: qué instituciones deciden, con qué datos, con qué capacidades, bajo qué salvaguardas y con qué mecanismos de rendición de cuentas.

De esa lectura emergió un mandato político y operativo: pasar de diagnósticos y marcos declarativos a arreglos de implementación. Es decir, traducir principios en:

- » Instrumentos aplicables: regulación por riesgos y usos (entendida no como la adopción automática de esquemas de clasificación externos, sino como un enfoque pragmático y contextual que prioriza la intervención estatal allí donde existen riesgos verificables para derechos, seguridad, integridad democrática o valor público, y habilita márgenes de experimentación responsable cuando dichos riesgos no son evidentes); sandboxes regulatorios; estándares; e institucionalidad con mandato claro y autoridad suficiente.
- » Fortalecer capacidades estatales: talento, coordinación, auditoría y justicia
- » Construir condiciones habilitantes: datos, interoperabilidad, ciberseguridad y acceso

Lo anterior, para que lo digital funcione como palanca de inclusión y no como amplificador de desigualdad, violencia o dependencia.

Esta sección sistematiza ese tránsito: del intercambio deliberativo hacia recomendaciones accionables para políticas públicas y reformas institucionales.

### Eje 1. Regulación y ejecución efectiva (del “qué” al “cómo”)

#### a) Diagnóstico compartido

Las intervenciones coincidieron en que el problema central no es la ausencia de ideas regulatorias, sino el déficit de implementación. Se identificó el riesgo de marcos vanguardistas sin capacidad real de cumplimiento (se usó la metáfora del “Ferrari regulatorio en una calle empedrada”); así como la tensión entre proteger derechos y evitar que normas rígidas terminen favoreciendo a grandes corporaciones con capacidad de cumplimiento, elevando barreras para PYMES y *startups*. También se advirtió que regular la tecnología es impreciso: los riesgos varían por uso, sector, actor y nivel de impacto.

#### b) Aprendizajes y consensos clave

Se propone entonces un enfoque de gobernanza dinámica: regular por riesgos y usos, con progresividad, evidencia y aprendizaje institucional. Hubo consenso en avanzar con modelos

por capas: principios mínimos horizontales + guías/obligaciones sectoriales. Promover el uso de *sandboxes* regulatorios para comprender efectos antes de fijar marcos definitivos. En el plano regional, se destacó la conveniencia de avanzar mediante marcos comunes no obligatorios, como principios, recomendaciones y lineamientos, junto con estándares técnicos interoperables, por considerarse una ruta más viable que la de negociar tratados formales y de difícil cumplimiento. Asimismo, se subrayó que, sin mecanismos efectivos de aplicación y cumplimiento, incluyendo autoridades con capacidades técnicas, presupuesto y coordinación interinstitucional, la regulación tiende a quedarse en el plano declarativo.

### c) Recomendaciones estratégicas

1. **Adoptar una regulación por capas y por riesgos**, combinando un plano horizontal de obligaciones mínimas con marcos sectoriales (salud, seguridad, finanzas, justicia, educación) según el impacto y la madurez institucional.
2. **Institucionalizar sandboxes regulatorios** con criterios públicos (riesgo, evaluación, salvaguardas) para generar evidencia, ajustar normas y evitar regulación obsoleta o inaplicable.
3. **Fortalecer autoridades de aplicación** con capacidad técnica, presupuesto, coordinación con el Ejecutivo y órganos de control, para asegurar supervisión y cumplimiento, especialmente en datos, transparencia algorítmica, vigilancia y protección de infancias.
4. **Diseñar la regulación como habilitadora**, incorporando incentivos y mecanismos proporcionales para no elevar barreras para PYMES/startups, implementando un marco de garantías consensuado.
5. **Alinear agendas legislativas y ejecutivas** mediante mecanismos formales de coordinación, incluidas comisiones de futuro o espacios anticipatorios para reducir fragmentación y duplicidades normativas.

Proposición: *La prioridad regulatoria debe ser construida considerando la capacidad de ejecución y regulación por riesgos, en lugar de adoptar marcos normativos complejos sin viabilidad institucional.*

## Eje 2. Institucionalidad pública y coordinación estatal para adoptar tecnologías con gobernanza

### a) Diagnóstico compartido

El diálogo evidenció fragmentación institucional: ministerios y entidades adquieren soluciones de forma unilateral, sin gobernanza técnica central, generando riesgos de seguridad, duplicidades y pérdida de control. Se identificaron obstáculos para retener talento, como brechas salariales, rigidez laboral, cultura del presencialismo y limitaciones para operar capacidades críticas, por ejemplo, ciberseguridad 24/7. También se señaló confusión conceptual: se etiqueta como IA a lo que muchas veces es transformación digital uso de big data, lo cual distorsiona decisiones de inversión y expectativas.

### b) Aprendizajes y consensos clave

Se consolidó la idea de que la gobernanza digital exige jerarquía institucional y mandatos transversales: las áreas de innovación y tecnología deben contar con capacidad real para transformar y ser implementadas desde el Estado, no solo para acompañar. Se reafirmó que adoptar IA sin bases de datos, gobernanza y mantenimiento local puede producir inversiones de alto costo, con

retorno de la inversión negativo o vulnerabilidades, incluida la obsolescencia. Al mismo tiempo, se propuso una lógica pragmática: avanzar con pilotos mientras se fortalecen, en paralelo, los datos y las capacidades.

### c) Recomendaciones estratégicas

1. **Elevar la función digital y tecnológica a nivel transversal** con mandato de coordinación, estándares, seguridad y compras públicas, para evitar la adopción fragmentada y reducir riesgos sistémicos.
2. **Establecer un modelo de gobernanza de adopción tecnológica** con definiciones comunes, criterios de riesgo, autorizaciones, trazabilidad, que distinga digitalización, automatización e IA y ordene prioridades.
3. **Reformar los esquemas de gestión de talento público digital**, habilitando perfiles, remuneraciones y modalidades de trabajo compatibles con funciones críticas, incluyendo turnos, teletrabajo y continuidad operativa.
4. **Implementar una estrategia de “doble carril”**: ejecutar pilotos de IA en procesos acotados, listos y evaluables, mientras se invierte en la calidad de los datos, la interoperabilidad y las capacidades de auditoría y de mantenimiento.
5. **Condicionar la inversión tecnológica a evaluaciones previas de sostenibilidad**, que incluyan costos de inversión y operación, necesidades de mantenimiento, disponibilidad de competencias locales y métricas verificables de impacto, con el fin de evitar adopciones impulsadas por tendencias y garantizar valor público.

Proposición: *Para que la tecnología genere valor público, los Estados deben contar con institucionalidad transversal y talento público especializado que permitan coordinar, supervisar y sostener su adopción.*

## Eje 3. Gobernanza de datos, soberanía estratégica e infraestructura digital pública

### a) Diagnóstico compartido

Se identificó una vulnerabilidad estructural: la dependencia de infraestructura y procesamiento externos, la escasez de capacidad local para desarrollar e implementar modelos de IA y la falta de digitalización de acervos públicos y culturales. Esto limita la autonomía, reproduce dinámicas de fuga de valor y debilita la posibilidad de contar con sistemas que reflejen la diversidad cultural y lingüística de la región. Se alertó, además, sobre incertidumbres normativas, como los derechos de autor, propiedad intelectual y el entrenamiento de modelos, que frenan iniciativas de interés público, académico y empresarial en la región.

### b) Aprendizajes y consensos clave

Emergió un consenso sobre soberanía: no se trata de autarquía, sino de capacidad de decisión sobre datos, infraestructura y usos. Se posicionó la noción de IA pública como bien público digital, abierto, transparente, auditable y con fin social. Se propuso enfocar esfuerzos en soluciones localizadas con modelos más pequeños y curados para problemas concretos en lugar de competir en la carrera de modelos masivos. También se reafirmó que la calidad y representatividad del dato es el cimiento de cualquier gobernanza incluida la mitigación de sesgos.

### c) Recomendaciones estratégicas

1. **Adoptar una política integral de gobernanza de datos** con calidad, representatividad, trazabilidad, acceso, seguridad y uso responsable como prerrequisito para la adopción de IA en el Estado.
2. **Acelerar la digitalización de archivos públicos y acervos culturales**, priorizando conjuntos de datos estratégicos para servicios, justicia, educación y políticas sociales, y garantizando resguardos de diversidad lingüística y cultural.
3. **Impulsar bienes públicos digitales e IA pública**, promoviendo soluciones abiertas, auditables y con propósito social, y fomentando modelos especializados para problemas locales.
4. **Establecer esquemas de negociación** mediante los cuales la provisión regional de recursos estratégicos, tales como energía, datos y minerales críticos asociados a la economía digital, se vinculen a contrapartidas claras, como capacidad de cómputo para uso público, transferencia tecnológica y acceso preferencial para investigación científica y servicios estatales.
5. **Actualizar marcos para habilitar innovación de interés público**, revisando obstáculos jurídicos que generan inseguridad para entrenamiento y desarrollo local, especialmente en investigación y soluciones con fin social.

Proposición: *Para avanzar en soberanía digital, los Estados deben priorizar la gobernanza de datos, la negociación de infraestructura crítica y la creación de bienes públicos digitales auditables y de carácter regional.*

## Eje 4. Integridad democrática, violencia digital y ciberseguridad como política de Estado

### a) Diagnóstico compartido

El intercambio situó riesgos inmediatos: desinformación electoral, microsegmentación, *deepfakes* y violencia digital, con énfasis en la violencia de género que inhibe participación y representación. Se advirtió que la IA amplifica debilidades democráticas preexistentes y que los principales riesgos siguen estando asociados a factores humanos, como brechas de capacidades, incentivos institucionales inadecuados, errores de diseño, uso indebido o manipulación mediante ingeniería social cada vez más sofisticada. A la vez, se alertó sobre el riesgo de respuestas estatales que, bajo el pretexto de combatir la desinformación, deriven en censura o control indebido.

### b) Aprendizajes y consensos clave

Se consolidó el binomio: no hay gobernanza de IA sin ciberseguridad. La ciberseguridad fue entendida no como una función técnica, sino como una política de gestión de riesgos que define qué activos se protegen, con qué recursos y bajo qué responsabilidades, decisiones que son inherentemente políticas. En ese marco, hubo acuerdo en que la dispersión institucional debilita la respuesta estatal, por lo que resulta prioritario ubicar las agencias de ciberseguridad en niveles estratégicos del Estado, dotarlas de autonomía técnica, presupuesto estable y mandatos claros de coordinación interinstitucional. Asimismo, se subrayó que, frente a amenazas transfronterizas, la cooperación regional sólo es efectiva si es operativa, interoperable y ágil, y no limitada a declaraciones o intercambios esporádicos. También se reafirmó que las salvaguardas democráticas deben integrarse desde el diseño y que la protección de infancias y la contención de violencia digital requieren marcos aplicables y rutas claras de respuesta

### c) Recomendaciones estratégicas

1. **Gestionar la ciberseguridad como política de Estado**, creando o fortaleciendo agencias con autonomía técnica y presupuesto, separadas de lógicas opacas de inteligencia que limiten cooperación y transparencia.
2. **Implementar capacidad operativa de respuesta a incidentes** con protocolos, equipos, coordinación interinstitucional. Además, elevar estándares de seguridad desde el diseño en servicios y sistemas automatizados.
3. **Actualizar marcos de respuesta frente a violencia digital y deepfakes**, priorizando protección de infancias y salvaguardas para mujeres en política y liderazgos públicos, con rutas de atención y coordinación con sector justicia.
4. **Construir cooperación regional operativa**, con mecanismos interoperables de alerta, intercambio técnico y aprendizaje conjunto, evitando solo acuerdos declarativos.
5. **Proteger la libertad de expresión mediante marcos de garantías claros**, asegurando que las políticas para enfrentar la desinformación no deriven en mecanismos de censura, control indebido del discurso público o restricciones desproporcionadas de derechos.

Proposición: *La protección de la democracia en entornos digitales exige integrar la ciberseguridad como una política pública orientada a la prevención y a la respuesta efectivas, con la implementación de un marco de garantías en respeto a derechos humanos.*

## Eje 5. Inclusión, participación efectiva y legitimidad del Estado digital

### a) Diagnóstico compartido

Se identificaron brechas persistentes de conectividad, costos de acceso, habilidades digitales y facilidad de uso, con impactos diferenciados entre territorios y generaciones. Estas brechas explican por qué la apropiación digital no ocurre de manera automática: invertir únicamente en plataformas, sin estrategias de difusión, sin claridad sobre cómo esa participación incide en decisiones públicas y sin devolución de resultados, tiende a generar frustración y desconfianza. En este marco, se subrayó que la digitalización puede erosionar la legitimidad institucional si no preserva la cercanía y la comprensión entre el Estado y la ciudadanía, especialmente cuando sustituye el trato humano o dificulta la rendición de cuentas.

### b) Aprendizajes y consensos clave

Se reafirmó una condición habilitante: el acceso digital universal es un asunto de equidad y legitimidad, no solo de tecnología. Hubo consenso en que la confianza se construye con medidas concretas: lenguaje claro, trazabilidad, interoperabilidad, derecho a saber cuándo se interactúa con sistemas automatizados y derecho a la atención humana. También se destacó el potencial de la IA para ampliar participación: procesar consultas masivas, identificar patrones; y para democratizar accesibilidad: traducción a lenguas indígenas, simplificación administrativa; siempre que exista diseño inclusivo y rendición de cuentas.

**c) Recomendaciones estratégicas**

- 1. Diseñar políticas de acceso universal centradas en personas**, con transiciones progresivas, acompañamiento y combinaciones de infraestructura (fibra, satelital, móvil) según territorio y población.
- 2. Garantizar derechos de interacción en el Estado digital**, incluyendo el derecho a ser informado cuando se use automatización o IA y el derecho a atención humana, con canales claros y comprensibles.
- 3. Institucionalizar la participación digital con la promesa de incidencia, asegurando la devolución pública**, respondiendo a la pregunta «¿Qué pasó con lo que dijeron?», mecanismos vinculantes cuando corresponda y diseño de comunicación para movilizar la participación.
- 4. Fortalecer la alfabetización digital y el pensamiento crítico** a lo largo del ciclo de vida y, de manera prioritaria, en el funcionariado que opera y supervisa sistemas.
- 5. Crear observatorios y esquemas descentralizados de auditoría**, con roles complementarios de academia y sociedad civil para continuidad, control social y memoria institucional, reduciendo dependencia de ciclos políticos.

Proposición: *La legitimidad del Estado digital depende de su capacidad para garantizar inclusión, transparencia y trato humano, más que de la sofisticación tecnológica de las plataformas para provisión de servicios. son más vulnerables a desplazamientos y pérdida de medios de vida (IPCC, 2022).*



## 6. Hoja de ruta

América Latina y el Caribe se encuentra en un punto de inflexión. La aceleración simultánea de la inteligencia artificial, la digitalización de los servicios públicos y la centralidad de los datos está reconfigurando en tiempo real las relaciones entre instituciones, ciudadanía, economía y democracia. No se trata de una transformación futura ni de una transición gradual, es una mutación en curso, con impactos inmediatos sobre derechos, capacidades estatales, cohesión social y desarrollo sostenible. En este contexto, la región enfrenta el riesgo de profundizar brechas históricas, territoriales, sociales y de capacidades o, por el contrario, de construir una gobernanza digital propia, cooperativa e inclusiva.

La presente Hoja de Ruta surge como respuesta a ese momento crítico. No es un documento prescriptivo ni un plan técnico, sino una narrativa estratégica de acción, construida a partir del diálogo. Reconoce la existencia de múltiples agendas, estrategias y hojas de ruta en materia digital en la región, y se propone articularlas y darles coherencia política y operativa, en particular en diálogo con procesos regionales ya en curso como la Agenda Digital eLAC de la CEPAL y la Hoja de Ruta de la Cumbre Ministerial de Inteligencia Artificial impulsada por CAF y UNESCO. En ese sentido, no busca superponer ni duplicar esfuerzos, sino contribuir a la alineación, priorización y traducción de dichos marcos en orientaciones accionables para los Estados.

### 6.1. Principios orientadores

#### **a. Centralidad de las personas, los derechos y las libertades**

La gobernanza digital no puede definirse únicamente por la eficiencia tecnológica. El diálogo reafirmó que las personas, en su diversidad, deben estar en el centro, y que los derechos humanos, libertades y garantías democráticas constituyen el marco irrenunciable de cualquier política de datos o IA.

#### **b. Inclusión efectiva y participación**

La participación no puede limitarse a la consulta. El consenso fue claro en la necesidad de cerrar el ciclo participativo: escuchar, decidir e informar, otorgando sentido y valor a la intervención ciudadana. La inclusión efectiva, especialmente de grupos históricamente excluidos, es una condición para la calidad de las políticas y su sostenibilidad en el tiempo.

#### **c. Gobernanza colaborativa, multiactor y multinivel**

La complejidad de la agenda digital exige cooperación, coordinación y colaboración entre Estados, cooperación internacional, sector privado, academia, sociedad civil, territorios y comunidades. Ningún actor puede avanzar solo. Este principio permite articular capacidades dispersas y evitar la fragmentación de esfuerzos.

#### **d. Coherencia entre política, recursos y capacidades**

El diálogo subrayó la brecha recurrente entre discurso y ejecución. La hoja de ruta se sostiene sólo si existe coherencia entre prioridades políticas, financiamiento, capacidades humanas e infraestructura. Sin esta alineación, la agenda digital corre el riesgo de convertirse en una suma de iniciativas aisladas.

#### **e. Innovación con enfoque ético, adaptativo y contextual**

Frente a la velocidad de la IA, se rechazó la idea de marcos rígidos y universales. La innovación debe ser ética, sensible a contextos culturales y territoriales, con mirada subnacional y capaz de adaptarse a cambios rápidos. Este principio reconoce que el aprendizaje continuo es parte estructural de la gobernanza digital.

## 6.2. Acciones regionales

A partir del trabajo colectivo, se establecen cuatro ejes prioritarios que articulan la agenda de gobernanza digital para la región:

### a. Gobernanza Colaborativa y Multidimensional (El Modelo 3C + 3M)

La prioridad identificada es la articulación política e institucional.

- » **Enfoque:** Adoptar el modelo de las **3C** (Cooperación, Coordinación, Colaboración) bajo una arquitectura **3M** (Multilateral, Multinivel, Multiactor).
- » **Acción:** Mapear y unificar los espacios de articulación existentes para evitar la duplicidad de esfuerzos, transformando los eventos en procesos continuos a través de comunidades de práctica permanentes.
- » **Soberanía:** Definir una postura regional estratégica que permita a los Estados regular y controlar sus infraestructuras y datos frente a poderes externos, pero estableciendo salvaguardas para evitar que estas herramientas se utilicen para la censura, la vigilancia masiva o la restricción de libertades. La soberanía debe entenderse como la capacidad de proteger a la ciudadanía, sus datos y su economía, no como un mecanismo para blindar al poder político del escrutinio público.
- » **Articulación de agendas regionales:** Alinear esta Hoja de Ruta con marcos existentes como la Agenda Digital eLAC (CEPAL) y la Hoja de Ruta de la Cumbre Ministerial de IA (CAF–UNESCO), promoviendo convergencia de prioridades, coherencia temporal y complementariedad de acciones.

### b. Infraestructura Pública Digital y Datos

Superar la dependencia tecnológica crítica mediante el desarrollo de ecosistemas propios.

- » **Infraestructura:** Abordar la obsolescencia tecnológica del sector público integrando obligatoriamente los costos de mantenimiento en la inversión.
- » **Economía de Datos:** Crear repositorios y catálogos de datos regionales compartidos que permitan capturar valor localmente, reducir la dependencia exclusiva de las *Big Tech* y fomentar ecosistemas locales de innovación.
- » **Ciberseguridad:** Implementar la seguridad y la privacidad desde el diseño en todas las capas de la infraestructura estatal.

### c. Inclusión y Democracia Algorítmica

Pasar de la consulta a la co-creación significativa.

- » **Cierre del Ciclo:** Garantizar que los procesos participativos informen a la ciudadanía sobre cómo sus aportes influyeron en la decisión final.
- » **Representación:** Crear directorios y espacios de voz propia para líderes y lideresas indígenas y comunidades vulnerables, sin intermediarios, transversalizando la perspectiva de género e interseccionalidad.
- » **Derechos:** Discutir el alcance de los derechos frente a la IA, reconociendo la diversidad cultural y ética de la región.

#### d. Capacidades Estatales y Talento Humano

Transformar la administración pública en organizaciones basadas en evidencia

- » **Alta Dirección:** Capacitar a los altos decisores políticos para asegurar el respaldo presupuestario y estratégico a las agendas técnicas.
- » **Alfabetización:** Establecer un nivel de competencias digitales mínimo para evitar que la brecha se amplíe entre funcionarios y ciudadanía.

### 6.3. Horizonte Temporal

Para operativizar los pilares anteriores, se propone la siguiente secuencia de hitos:

#### CORTO PLAZO: Diagnóstico y Cimientos (0 - 12 meses)

- » **Mapeo de Articulación:** Realizar un inventario de los espacios regionales, así como de los éxitos y fracasos en gobernanza digital, para establecer una línea de base y evitar duplicidades.
- » **Conversatorios Nacionales:** Iniciar diálogos locales para levantar demandas específicas de la sociedad civil, la academia y el sector privado local.
- » **Formación de Líderes:** Lanzar programas de capacitación dirigidos a altas autoridades sobre los riesgos y oportunidades de la IA.

#### MEDIANO PLAZO: Institucionalización y Estándares (1 - 3 años)

- » **Infraestructura Normativa:** Definición de glosarios comunes, métricas estandarizadas y guías de interoperabilidad para evitar disonancias interpretativas en la región.
- » **Observatorio Regional:** Puesta en marcha de un Observatorio/Repositorio regional de algoritmos públicos y desarrollos de IA latinoamericanos, desde sector público, academia y privado. Esto se puede alcanzar consolidando ejercicios ya existentes.
- » **Grupos de Trabajo Permanentes:** Consolidación de equipos técnicos, liderados por organismos como PNUD y CAF que den seguimiento a la agenda en su fase de implementación.
- »

#### LARGO PLAZO: Integración Estructural (3 - 5 años)

- » **Alianza Regional por una IA Inclusiva:** Establecimiento de un organismo o acuerdo vinculante que homologue estándares éticos y técnicos.
- » **Infraestructura Regional Compartida:** Operación de nubes públicas, infraestructuras de datos compartidas e inversiones realizadas bajo lógica de cooperación Sur-Sur.
- » **Sostenibilidad Financiera:** Consolidación de un modelo de financiamiento diversificado que no dependa exclusivamente de la cooperación internacional, asegurando recursos para la innovación pública y la sociedad civil.



# 7.

## Referencias bibliográficas

- Alto Intelligence.** (2025). Gobernanza de la inteligencia artificial en América Latina y el Caribe.
- CAF – Banco de Desarrollo de América Latina y el Caribe.** (2024a). Diseño de políticas públicas de inteligencia artificial: Desarrollo de habilitadores para su implementación en América Latina y el Caribe (Guía práctica). [scioteca.caf.com/bitstream/handle/123456789/2241/CAF%20-%20Gu%C3%ADa%20Dise%C3%B1o%20IA.pdf?isAllowed=y&sequence=3](https://scioteca.caf.com/bitstream/handle/123456789/2241/CAF%20-%20Gu%C3%ADa%20Dise%C3%B1o%20IA.pdf?isAllowed=y&sequence=3)
- CAF – Banco de Desarrollo de América Latina y el Caribe.** (2024b). Conectividad, inclusión y transformación digital para un mayor progreso. [scioteca.caf.com/bitstream/handle/123456789/2509/Conectividad%20inclusi%C3%B3n%20y%20transformaci%C3%B3n%20digital%20para%20un%20mayor%20progreso.pdf?isAllowed=y&sequence=1](https://scioteca.caf.com/bitstream/handle/123456789/2509/Conectividad%20inclusi%C3%B3n%20y%20transformaci%C3%B3n%20digital%20para%20un%20mayor%20progreso.pdf?isAllowed=y&sequence=1)
- CAF – banco de desarrollo de América Latina y el Caribe– & Programa de las Naciones Unidas para el Desarrollo.** (2024). Gobernanza para el desarrollo en América Latina y el Caribe: Recomendaciones a partir de los diálogos promovidos por CAF y PNUD. [www.undp.org/sites/g/files/zskgke326/files/2024-09/gobernanza\\_para\\_el\\_desarrollo\\_en\\_america\\_latina\\_y\\_el\\_caribe.pdf](https://www.undp.org/sites/g/files/zskgke326/files/2024-09/gobernanza_para_el_desarrollo_en_america_latina_y_el_caribe.pdf)
- Naciones Unidas.** (2024a). United Nations Global Principles for Information Integrity: Recommendations for multi-stakeholder action. [www.un.org/en/information-integrity/global-principles](https://www.un.org/en/information-integrity/global-principles)
- Naciones Unidas.** (2024b). The Pact for the Future (final). [www.un.org/pga/wp-content/uploads/sites/109/2024/09/The-Pact-for-the-Future-final.pdf](https://www.un.org/pga/wp-content/uploads/sites/109/2024/09/The-Pact-for-the-Future-final.pdf)
- Programa de las Naciones Unidas para el Desarrollo.** (2024). Information integrity for electoral institutions and processes: Reference manual for UNDP practitioners. [www.undp.org/sites/g/files/zskgke326/files/2024-03/24119\\_undp\\_information\\_integrity\\_v08\\_rc\\_002.pdf](https://www.undp.org/sites/g/files/zskgke326/files/2024-03/24119_undp_information_integrity_v08_rc_002.pdf)
- Programa de las Naciones Unidas para el Desarrollo.** (2025a). Atlas de inteligencia artificial para América Latina y el Caribe. [www.undp.org/es/latin-america/publicaciones/atlas-de-inteligencia-artificial-para-america-latina-y-el-caribe](https://www.undp.org/es/latin-america/publicaciones/atlas-de-inteligencia-artificial-para-america-latina-y-el-caribe)
- Programa de las Naciones Unidas para el Desarrollo.** (2025b). Informe regional sobre desarrollo humano 2025: Bajo presión. Recalibrando el futuro del desarrollo en América Latina y el Caribe. [www.undp.org/sites/g/files/zskgke326/files/2025-10/58590\\_lac\\_hdr\\_sp\\_web.pdf](https://www.undp.org/sites/g/files/zskgke326/files/2025-10/58590_lac_hdr_sp_web.pdf)



**CAF**  
BANCO DE DESARROLLO  
DE AMÉRICA LATINA  
Y EL CARIBE

