Articulo original

Gobernanza de datos para una inteligencia artificial generativa soberana y segura

Data governance for a sovereign and secure generative artificial intelligence

Omara Aldama López[1] https://orcid.org/0000-0002-6192-5061

Alfredo Rodríguez Díaz[1] https://orcid.org/0000-0002-3111-2692

[1]Palacio de la Revolución, La Habana, Cuba.

*Autor para la correspondencia: omara@palacio.cu

RESUMEN

Introducción: La Inteligencia Artificial Generativa ofrece oportunidades transformadoras para la administración pública, pero su implementación plantea riesgos críticos para la seguridad de la información y la soberanía tecnológica, especialmente en contextos de asimetría tecnológica.

Objetivo: Proponer un marco de gobernanza de datos específico para el uso de la IAG en el sector gubernamental cubano, diseñado para proteger la información sensible del Estado mientras se aprovechan sus beneficios.

Métodos: Se realizaron una revisión sistemática de la literatura (2019-2025), un análisis crítico del marco normativo cubano y una sistematización de experiencias prácticas en el gobierno central mediante estudios de caso, entrevistas semiestructuradas a 29 funcionarios y observación participante.

Resultados: Se identificaron brechas normativas y operativas significativas, como la ausencia de una Estrategia Nacional de Gobernanza de Datos y la inadecuación de las normas vigentes frente a los riesgos específicos de la Inteligencia Artificial Generativa. Como

respuesta, se proponen cuatro pilares interdependientes para un marco de gobernanza: gobernanza de datos con enfoque en la soberanía y la clasificación unificada; ética institucionalizada y supervisión humana; seguridad técnica de los modelos; y desarrollo del talento y alfabetización crítica en IAG.

Conclusiones: El marco presentado se distingue por su operacionalización en un contexto de asimetría tecnológica, integrando las normativas nacionales existentes y estructuras institucionales, como el Consejo Técnico Asesor de IA. Constituye una hoja de ruta concreta para materializar los postulados de la Estrategia cubana de Inteligencia Artificial, posicionando la soberanía de los datos como condición previa para una transformación digital autónoma y segura en el sector público cubano.

Palabras clave: inteligencia artificial generativa; gobernanza de datos; soberanía de datos; ética de la inteligencia artificial; seguridad nacional; Cuba

ABSTRACT

Introduction: Generative Artificial Intelligence offers transformative opportunities for public administration, but its implementation raises critical risks related to information security and technological sovereignty, especially in contexts of technological asymmetry.

Objective: To propose a specific data governance framework for the use of GAI in the Cuban public sector, designed to protect sensitive state information while harnessing its benefits.

Methods: A systematic literature review (2019-2025), a critical analysis of the Cuban regulatory framework, and a systematization of practical experiences within the central government were conducted through case studies, semi-structured interviews with 29 officials, and participant observation.

Results: Significant regulatory and operational gaps were identified, such as the absence of a National Data Governance Strategy and the inadequacy of current regulations to address specific GAI risks (e.g., prompt injection, data extraction). In response, four interdependent pillars for a governance framework are proposed: data governance with a focus on

sovereignty and unified classification; institutionalized ethics and human oversight; technical security of models; and talent development and critical AI literacy.

Conclusions: The presented framework is distinguished by its operationalization in a context of technological asymmetry, integrating existing national regulations and institutional structures such as Cuba's AI Technical Advisory Council. It provides a concrete roadmap to implement the tenets of the Cuban Artificial Intelligence Strategy, positioning data sovereignty as a prerequisite for an autonomous and secure digital transformation in the Cuban public sector.

Keywords: generative artificial intelligence; data governance; data sovereignty; artificial intelligence ethics; national security; Cuba

Recibido: 05/03/2026

Aprobado: 17/04/2026

Introducción

La Inteligencia Artificial Generativa (IAG) emerge como una tecnología disruptiva con el potencial de redefinir la eficiencia, la transparencia y la calidad de los servicios públicos a nivel global. Mediante modelos avanzados como los Grandes Modelos de Lenguaje (LLM), la IAG permite la automatización de trámites complejos, la generación de contenido contextualizado y la mejora de la interacción ciudadano-Estado, lo que se alinea con los objetivos de la Política de Transformación Digital cubana.[1] Sin embargo, esta promesa tecnológica conlleva riesgos críticos para países del Sur Global, particularmente en lo relativo a la seguridad de la información, la soberanía tecnológica y la dependencia de infraestructuras externas.

En el contexto cubano, la adopción de la IAG en el sector gubernamental se ve amenazada por una asimetría tecnológica estructural y por un escenario geopolítico adverso. La dependencia de modelos extranjeros, la jurisdicción extraterritorial sobre datos nacionales y la posibilidad de fugas de información sensible mediante técnicas como el *prompt injection* representan amenazas directas a la seguridad nacional.[2,3] Estos riesgos se exacerban por la ausencia de un marco de gobernanza de datos robusto y unificado, a pesar de la existencia de normativas como el Decreto-Ley 78/2023 sobre información clasificada[4] y la Ley 149/2022 de protección de datos personales,[5] el Decreto-Ley 6/2020 "Del Sistema de Información del Gobierno" [6] y el Decreto-Ley 98/2024 "De la Estadística Oficial".[7]

No obstante, a pesar de la existencia del marco legal señalado, la falta de una Estrategia Nacional de Gobernanza de Datos genera un panorama fragmentado en el que, por un lado, la información protegida no recibe la debida custodia y, por otro, se limita el acceso a datos que podrían ser de valor público, lo que frena la innovación y la eficiencia estatal.

La gobernanza de datos, por tanto, trasciende su función técnica para erigirse en un pilar de la seguridad nacional y de la soberanía. El principio de soberanía de datos —la capacidad de una nación para controlar los datos generados en su territorio[8]— se convierte en un imperativo estratégico para Cuba, donde la información estatal sensible debe residir bajo jurisdicción e infraestructuras nacionales. Como advierten Couldry y Mejías,[9] la extracción y procesamiento de datos de naciones periféricas reproducen dinámicas neocoloniales, donde los flujos de información benefician predominantemente a actores del Norte tecnológico, socavando la autonomía cognitiva y la capacidad de definir agendas digitales propias.

Este artículo se propone abordar esta brecha crítica mediante la formulación de un marco de gobernanza de datos específico para la IAG en el sector público cubano. Su objetivo es operacionalizar los principios de soberanía, seguridad y accesibilidad, integrando componentes clave como una arquitectura de clasificación unificada, protocolos de

anonimización y una estrategia de infraestructura híbrida que segregue el entrenamiento base del *fine-tuning* con datos sensibles. La contribución de este trabajo radica en ofrecer una hoja de ruta concreta y contextualizada para materializar los postulados de la Estrategia cubana de IA, transformando la gobernanza de datos de un desafío regulatorio en una ventaja estratégica.

Métodos

Este estudio adopta un diseño de investigación cualitativa para desarrollar un marco teórico-normativo. El diseño se articula como un proceso iterativo y de triangulación, combinando evidencia teórica internacional, análisis de normativas nacionales y experiencia práctica contextualizada. El proceso constó de cuatro fases.

Revisión sistemática de la literatura especializada

Se realizó una búsqueda exhaustiva en bases de datos académicas (Scopus, SciELO, Google Scholar) y en repositorios institucionales, utilizando cadenas de búsqueda basadas en operadores booleanos: ("data governance" OR "sovereign data") AND ("generative AI" OR "large language models") AND ("public sector" OR "government") AND ("Global South" OR "technological sovereignty"). Se priorizaron los documentos publicados entre 2019 y 2024. Esta revisión permitió identificar principios y mejores prácticas internacionales, tomando como referencias marcos como DAMA[10] y COBIT 2019,[11] modelos que constituyen referentes de gobernanza sólidos y ampliamente adoptados, incluidos en el sector público. Adicionalmente, se analizaron marcos más recientes para contextos de transformación digital, como el DCAM [12] y el CDMC.[13]

El DCAM (*Data Management Capability Assessment Model*) del EDM Council, recientemente convertido en EDM Association, según describe Projectiv Group [12] se enfoca en la capacidad organizacional para gestionar datos, proporciona un modelo de madurez específico para evaluar y mejorar capacidades de gobierno de datos. Su enfoque en capacidades lo hace

particularmente útil para diagnosticar el estado de la gobernanza de datos en las organizaciones.

Complementariamente, el CDMC (Cloud Data Management Capability) aborda los desafíos de la gestión de datos en entornos cloud,[13] lo que resulta relevante para la implementación de plataformas gubernamentales en infraestructuras en nubes soberanas.

Valorar la integración de estos marcos proporciona un sustento teórico robusto para abordar las problemáticas específicas identificadas en la gestión pública cubana: la falta de estandarización, la baja calidad de los datos y la limitada interoperabilidad.[14] Por lo tanto, constituyen una base conceptual para el diseño de la gobernanza de datos y para el uso de una IA generativa, soberana y segura en el sector público, con datos confiables y alineados con la estrategia nacional.

Análisis crítico del marco normativo cubano

Se realizó un escrutinio exhaustivo de la legislación nacional vigente con incidencia directa en la gestión de datos estatales, incluyendo: Decreto-Ley 6/2020,[6] Decreto-Ley 78/2023,[4] Ley 149/2022,[5] Decreto-Ley 98/2024[7] y la Política de Transformación Digital y Estrategia de IA nacional.[1] Este análisis permitió identificar fortalezas, brechas y oportunidades de integración.

Sistematización de la experiencia práctica

Con el objetivo de recoger evidencia empírica sobre los desafíos reales en la gestión de datos gubernamentales en Cuba, se diseñó un enfoque de investigación-acción que incluyó:

- Estudios de caso en dos instituciones clave: MINSAP y MINEM.
- Entrevistas semiestructuradas con 29 funcionarios técnicos y decisores involucrados en proyectos de automatización y de uso de datos.
- Revisión de documentos internos (informes, actas, protocolos).

Los datos cualitativos se analizaron mediante un análisis de contenido.

De manera crucial, se utilizó la observación participante, con los autores actuando como investigadores inmersos desde sus roles en el gobierno central. Esto permitió el acceso a contextos y dinámicas de procesos internos, nutriendo el estudio con la experiencia acumulada en la implementación y asesoría de proyectos tecnológicos.[14,15]

Consideraciones éticas y limitaciones metodológicas

Todos los participantes en las entrevistas dieron su consentimiento informado de forma oral. Los datos personales y la identidad de las instituciones fueron anonimizados.
Los documentos internos se utilizaron únicamente para el análisis de procesos. Las limitaciones incluyen:
1) El muestreo no es estadísticamente representativo de todo el sector público cubano.
2) La rápida evolución de la IAG implicará actualizaciones del marco.
3) La posición institucional de los autores, mitigada mediante triangulación y validación por expertos externos.

Diagnóstico del Contexto Normativo Cubano

El análisis del marco jurídico-institucional cubano revela un panorama en el que conviven avances normativos significativos y brechas críticas en la gobernanza de datos para IAG.

Fortalezas del marco normativo existente

La base jurídica cubana presenta elementos positivos.

El Decreto-Ley 6/2020 establece las bases para el tratamiento de información de interés nacional [6], definiendo como tal aquella que "forma parte del Sistema Nacional Estadístico o de los Sistemas de Información institucionales" y que resulta demandada para evaluar el desempeño de las políticas públicas y los programas priorizados. Este instrumento reconoce el valor estratégico de los datos para la gestión gubernamental.

El Decreto-Ley 78/2023 constituye el marco más específico para el tratamiento de información sensible, estableciendo categorías de clasificación [4]. Su existencia marca un piso mínimo para la protección de datos críticos.

La Ley 149/2022 introduce principios modernos de protección de la privacidad [5], alineándose parcialmente con estándares internacionales, aunque con limitaciones en su implementación práctica, teniendo en cuenta que la Ley no aborda específicamente los riesgos asociados al procesamiento de datos personales por sistemas de inteligencia artificial, ni establece salvaguardas técnicas para escenarios donde los datos son utilizados para entrenamiento de modelos generativos.

El Decreto-Ley 98/2024 establece el marco para la producción y difusión de estadísticas oficiales [7].

Brechas críticas identificadas

El contexto normativo propicia que los datos identificados tengan establecida su forma de recolección y almacenaje, a lo que se suman datos generados automáticamente. Con la implementación de la Política de Transformación Digital [1] se ha avanzado en la digitalización de procesos en sectores como Salud Pública y Educación, aunque persisten desafíos.

Aunque se reconoce que el camino de la digitalización es un proceso complejo, especialmente ante las dificultades económicas y si bien esto no se ha detenido y además se trabaja en la capacitación del capital humano y en el desarrollo de soluciones nacionales adaptadas a la realidad del país, también es necesario reconocer que se está aún lejos de una captación,

preservación y utilización eficiente de los datos, y que se comporte con un nivel de desarrollo similar en las diferentes esferas.

Se identifican vacíos sustanciales que obstaculizan una gobernanza efectiva para IAG:

- **Ausencia de Estrategia Nacional de Gobernanza de Datos**: No existe un marco unificador para el ciclo completo de vida de los datos. Esta carencia genera duplicidad, inconsistencia y ambigüedad en los protocolos aplicables.
- **Fragmentación institucional**: Cada organismo aplica sus propios criterios, resultando en silos informacionales que impiden el flujo seguro y eficiente de información entre entidades estatales, así como limita la interoperabilidad de herramientas digitales..
- **Inadecuación a los riesgos específicos de la IAG**: Las normativas actuales no abordan vulnerabilidades técnicas como el *prompt injection*, la extracción de datos mediante ingeniería inversa de modelos o los requisitos específicos para el entrenamiento y *fine-tuning* con información sensible.
- **Limitaciones en el acceso a datos de valor público**: Falta de mecanismos ágiles para la liberación controlada de datos no sensibles, lo que frena la innovación y la reutilización de información para fines de investigación y desarrollo.

Casos concretos de riesgo

La falta de gobernanza unificada se manifiesta en situaciones de riesgo tangible, por solo citar algunos ejemplos:

Investigaciones médicas: Datos y metadatos resultantes de estudios en el sector salud, que debidamente anonimizados podrían ser reutilizados para entrenar modelos de IAG especializados, permanecen inaccesibles o con protocolos de protección insuficientes.

Información patrimonial empresarial: Datos estratégicos de empresas estatales carecen de clasificación uniforme, exponiéndolos potencialmente a procesos de IAG en plataformas no soberanas.

Expedientes ciudadanos: La gestión fragmentada de información personal en diferentes silos como parte de los procesos de trámites gubernamentales crea vulnerabilidades de seguridad de la información.

Consecuencias para la seguridad nacional

Esta situación de fragmentación normativa no constituye solo un problema técnico-administrativo, sino una vulnerabilidad estratégica. La imposibilidad de garantizar la protección uniforme de datos sensibles, combinada con la falta de protocolos específicos para IAG, expone al Estado cubano a riesgos de:

- Fuga de información clasificada o patrimonial
- Dependencia tecnológica crítica de proveedores extranjeros
- Vulneración de la privacidad ciudadana a escala
- Erosión de la capacidad de toma de decisiones autónomas

El diagnóstico evidencia que, si bien Cuba cuenta con elementos normativos valiosos, la ausencia de una gobernanza de datos integral y específica para IAG representa una brecha crítica que debe ser abordada con urgencia para materializar una adopción segura y soberana de estas tecnologías.

Principios fundamentales para una Gobernanza Soberana de Datos en IAG

Como señala Janssen,[16] una gobernanza de datos sólida constituye la base esencial para el desarrollo de sistemas de inteligencia artificial confiables en el ámbito público. Diseñar un marco específico de gobernanza de datos para la IAG en el sector público cubano y que esté alineado con una estrategia integral de Gobernanza de Datos requiere de principios rectores que articulen la visión estratégica con la operatividad práctica.[17,18]

Estos principios, derivados del análisis normativo y la experiencia práctica, constituyen los cimientos conceptuales del modelo propuesto.

Soberanía de Datos como Imperativo de Seguridad Nacional

La soberanía de datos representa la capacidad del Estado cubano para ejercer control efectivo sobre los datos generados en su territorio, tratándolos como un recurso estratégico de interés nacional [8]. En el contexto de IAG, este principio se materializa en:

- Control jurisdiccional absoluto sobre datos sensibles y patrimoniales utilizados en procesos de entrenamiento y *fine-tuning* de modelos generativos.
- Infraestructura nacional preferente para el almacenamiento y procesamiento de información clasificada o de alto valor estratégico.
- Autonomía decisional en la definición de estándares y protocolos de gestión de datos, independiente de presiones o condicionamientos externos. **Es el principio que defiende que las reglas del juego sobre los datos cubanos las debe definir Cuba, en función de su interés nacional y no de agendas externas.** No es un llamado al aislacionismo, sino a la cooperación en condiciones de igualdad y respeto a la soberanía.

Seguridad por Diseño y por Defecto

- La protección de los datos debe estar integrada en el diseño mismo de los sistemas de IAG, no añadida como medida posterior. Este principio implica:
- Evaluación proactiva de riesgos en todas las fases del ciclo de vida de los datos, desde su recolección hasta su destrucción.
- Cifrado *end-to-end* de información sensible durante procesos de entrenamiento e inferencia.
- Mecanismos de contención para prevenir fugas mediante técnicas como *prompt injection* o extracción por ingeniería inversa. [3]

Minimización y Finalidad Específica

En línea con los estándares internacionales de protección de datos, pero adaptados al contexto de IAG se debe garantizar:

- Recolección limitada a lo estrictamente necesario para los fines específicos del proyecto de IAG.
- Prohibición de reaprovechamiento de datos para fines distintos a los originalmente autorizados, sin consentimiento explícito.

Transparencia Regulada y Auditoría

Equilibrio entre la necesaria transparencia en el uso de datos y la protección de información sensible:

- Documentación exhaustiva de los conjuntos de datos utilizados en entrenamiento, incluyendo metadatos que recojan origen, metodología de recolección y transformaciones aplicadas.
- Mecanismos de auditoría independiente que permitan verificar el cumplimiento de los protocolos de gobernanza.
- Transparencia diferenciada según la categoría de datos, con mayores niveles de apertura para información de carácter público, según la clasificación definida en el Decreto Ley 78/2023.[4]

Calidad como Fundamento de Confiabilidad

La efectividad de los sistemas de IAG depende críticamente de la calidad de los datos que los alimentan, por lo que es indispensable garantizar:

- Definición clara de las fuentes de información autorizadas para cada tipo de dato a utilizar.
- Exactitud e integridad como requisitos no negociables para datos utilizados en procesos decisorios.

- Actualización periódica de conjuntos de datos para reflejar la realidad cambiante.
- Metadatos estandarizados que permitan evaluar la procedencia y calidad de los datos.

Accesibilidad Regulada y Gobernada

Balance entre la necesaria disponibilidad de datos para la innovación y la protección de información sensible:

- Catalogación centralizada de datos disponibles para proyectos de IAG, respetando el marco legal establecido.
- Protocolos de acceso diferenciados según perfiles de usuario y categorías de datos.
- Mecanismos ágiles para la solicitud y concesión de accesos especiales para investigación.

Ética e Interés Público

Los datos deben gestionarse en función del bien común y la protección de derechos establecidos y los principios éticos acogidos:

- Evaluación de impacto ético previa a la implementación de proyectos de IAG que involucren datos sensibles.
- Mitigación proactiva de sesgos en conjuntos de datos de entrenamiento.
- Preservación de la autonomía cognitiva nacional mediante el desarrollo de modelos contextualizados con realidad cubana.

Este último punto no es meramente técnico, sino epistemológico: como señalan Mohamed, Png y Isaac,[19] **el diseño de sistemas de IAG no puede limitarse a aspectos técnicos** (como algoritmos, datos o infraestructura), **sino que debe considerar también cómo se construye, interpreta y valida el conocimiento en un contexto cultural, histórico y político específico**, que reflejen no solo los datos cubanos, sino también sus marcos interpretativos, históricos y sociales.

Integridad Contextual

Reconocimiento de que el valor y riesgo de los datos dependen del contexto específico de uso:

- Clasificación dinámica que considere no solo la naturaleza intrínseca de los datos, sino también su uso potencial en sistemas de IAG.
- Protocolos específicos para diferentes dominios de aplicación (salud, educación, seguridad nacional).
- Evaluación continua de riesgos emergentes asociados a nuevas capacidades de la IAG.

Estos ocho principios constituyen un sistema integrado que orienta el diseño e implementación del marco de gobernanza de datos para IAG en Cuba. Su aplicación conjunta y balanceada permitirá avanzar hacia un modelo que combine innovación tecnológica con seguridad nacional, aprovechamiento de oportunidades con gestión proactiva de riesgos, y eficiencia operativa con preservación de la soberanía digital.

Marco de Gobernanza de Datos para IAG: componentes clave operativos

Arquitectura de clasificación unificada para IAG

Se deben proponer clasificaciones de información, expandiendo el Decreto-Ley 78/2023 [4] para contextos de IA. Definir criterios específicos de clasificación no solo para datos de entrenamiento sino también para los modelos de IAG a desarrollar, teniendo en cuenta los objetivos de utilización.

Igualmente, los flujos de trabajo y permisos asociados a cada categoría deben quedar esclarecidos y procedimentados.

Protocolos para anonimización y generación de datos sintéticos

Con la definición de protocolos de anonimización y el establecimiento de la generación de datos sintéticos, se concreta la "estrategia de soberanía cognitiva", mencionada en principio, con la elaboración de:

- Metodologías validadas para anonimización robusta.
- *Framework* para la creación y validación de *datasets* sintéticos.
- Casos de uso específicos

Todo proceso de anonimización debe incluir pruebas de re-identificación realizadas por un "adversario ético" interno para verificar su robustez, especialmente ante la capacidad de los LLM de memorizar y revelar datos de entrenamiento.[20]

Criterios de soberanía y almacenamiento

Con el objetivo de operacionalizar el principio de soberanía de datos se deben definir:

- Matriz de decisión: qué datos pueden procesarse y dónde.
- Especificaciones técnicas para infraestructuras nacionales calificadas.
- Protocolos para acuerdos de nube soberana con jurisdicción garantizada, previa consulta del marco legal vigente para la protección de la información y las infraestructuras críticas.
- Qué aspectos, procesos o partes, no se podrán trabajar con el uso de la IA.

Este componente operacionaliza el principio de soberanía de datos, definiendo reglas claras e innegociables sobre el "dónde" y el "cómo" se procesa la información, con especial énfasis en la protección de las infraestructuras críticas.

Gobierno institucional: Comité de Gobernanza de Datos para IAG

Se propone la evaluación del actual Consejo Técnico Asesor (CTA) de IA para asumir estas funciones, creando un Comité de Gobernanza de Datos para IAG como su brazo ejecutor especializado. Su composición debe ser multidisciplinaria (MINCOM, CITMA, MINJUS, UIC, academia, gobierno central) y sus atribuciones clave incluirán: aprobar proyectos de IAG con datos sensibles, certificar protocolos, organizar auditorías preventivas y de cumplimiento, y certificar modelos como requisito para su despliegue.

Gobernanza de Datos e Infraestructura

El principio de correspondencia entre gobernanza e infraestructura

La efectividad del marco de gobernanza está supeditada a la existencia de una infraestructura tecnológica que permita materializar sus principios. La soberanía de datos exige un control físico y lógico sobre el almacenamiento y procesamiento, lo que se traduce en la necesidad de infraestructuras nacionales o acuerdos de nube soberana que garanticen la jurisdicción cubana.

Implicaciones de la gobernanza para la infraestructura

El marco de gobernanza define los requisitos funcionales y de seguridad que debe cumplir la infraestructura:

Confinamiento de datos: La infraestructura debe permitir implementar la segregación entre el entrenamiento base (que puede usar recursos distribuidos) y el *fine-tuning* con datos sensibles (que exige entornos aislados y certificados).

Cumplimiento normativo: La infraestructura debe facilitar la auditoría y el monitoreo para verificar el cumplimiento de los protocolos de gobernanza (ej.: que los datos clasificados como "Confidenciales" nunca salgan de un entorno nacional).

Sostenibilidad y Continuidad: La infraestructura debe ser suficientemente robusta para garantizar la disponibilidad de los servicios de IAG críticos, alineándose con los principios de seguridad nacional.

Implicaciones Prácticas y Recomendaciones

Para la política digital cubana

Integración con la Estrategia Nacional de IA: El marco propuesto proporciona el componente faltante de gobernanza de datos, operacionalizando los ejes de la Estrategia existente. Se recomienda su adopción formal mediante su integración a la Agenda Digital cubana en construcción. Además, su alineamiento con los Principios sobre Inteligencia Artificial para América Latina y el Caribe[21] -que enfatizan la inclusión, la transparencia y la soberanía tecnológica adaptadas a capacidades institucionales locales- posiciona a Cuba como actor proactivo en la construcción de una gobernanza regional de la IA.

Articulación Normativa: Se sugiere la emisión de una "Guía de Gobernanza de Datos para IAG" que sirva como instrumento vinculante para todos los organismos de la administración pública y que se integre con la Estrategia de Gobernanza de datos del país que se apruebe.

Para los organismos estatales

Cada organismo debe utilizar el marco para diagnosticar su madurez en gobernanza de datos y desarrollar un plan de adecuación progresivo.

Para la inversión y priorización

Se recomienda focalizar los recursos en:

(1) infraestructura nacional aislada para fine-tuning;

(2) herramientas de anonimización robusta, y;

(3) programas de capacitación.

Incluir en los proyectos impulsores identificados por el MINCOM, el desarrollo de modelos y asistentes virtuales para validar el marco y generar confianza.

Hoja de ruta de implementación sugerida

- Corto Plazo (0-12 meses): Formalización del Comité de Gobernanza, emisión de la guía de clasificación unificada, y lanzamiento de proyectos piloto.
- Mediano Plazo (1-3 años): Desarrollo de capacidades de infraestructura soberana, implementación de protocolos de anonimización a escala, y establecimiento del sistema de auditoría continua.
- Largo Plazo (>3 años): Consolidación de un ecosistema soberano de IAG, con modelos contextualizados cubanos y participación en iniciativas de soberanía de datos a nivel regional.

Limitaciones y Trabajo Futuro

Limitaciones del estudio

- Validación Empírica: El marco propuesto es, en esta etapa, una construcción conceptual y normativa que requiere validación mediante su aplicación en proyectos piloto dentro de organismos del gobierno central.
- Dinámica Tecnológica: La velocidad de evolución de la IAG es extremadamente rápida. El marco deberá contar con mecanismos de revisión y adaptación periódica.
- Contexto Específico: El marco está profundamente contextualizado para Cuba, por lo que su transferibilidad a otros países requeriría adaptaciones significativas.

Líneas de trabajo futuro

- Validación en Campo: Implementar el marco de forma controlada en una institución estatal.
- Desarrollo de Herramientas: Crear herramientas derivadas, como una guía de implementación detallada, listas de verificación (*checklists*) para auditores y materiales de capacitación estandarizados para funcionarios.
- Gobernanza Multinacional: Explorar modelos de gobernanza de datos para IAG con países aliados, que permitan compartir mejores prácticas, recursos e infraestructura dentro de un marco de soberanía colectiva.
-

Conclusiones

La adopción de la Inteligencia Artificial Generativa en el sector público cubano trasciende lo tecnológico para constituirse en un asunto de seguridad nacional y soberanía. Este artículo ha demostrado que la ausencia de un marco de gobernanza de datos específico para la IAG representa una brecha crítica.

La propuesta presentada proporciona una hoja de ruta concreta y contextualizada para cerrar esta brecha. Su principal contribución radica en operacionalizar el principio de soberanía de datos dentro de una arquitectura de gobernanza viable, que se integra con la normativa nacional existente y las estructuras institucionales vigentes.

El marco no busca frenar la innovación, sino encauzarla para garantizar que el proceso de Transformación Digital pilar del Modelo de Gobierno cubano sea autónomo, seguro y resiliente.

La verdadera inteligencia, en la era de la IAG, no reside solo en los algoritmos, sino en la capacidad colectiva de gobernarlos con sabiduría y en función del interés nacional. La

implementación de este marco es, por tanto, un imperativo estratégico para un desarrollo digital soberano.

Referencias Bibliográficas

1. Ministerio de Comunicaciones. Política para la transformación digital, Agenda digital cubana y la Estrategia de inteligencia artificial [Internet]. La Habana: MINCOM; 2024 [citado 27 Nov 2025]. Disponible en: http://media.cubadebate.cu/wp-content/uploads/2024/06/Politica_de_Transformacion_Digital_de_Cuba_Agenda_Digital_y_Estrategia.pdf

2. Bommasani R, Hudson DA, Adeli E, Altman R, Arora S, von Arx S, et al. On the opportunities and risks of foundation models [Preprint en Internet]. Ithaca: arXiv; 2021 [citado 27 Nov 2025]. Disponible en: https://arxiv.org/abs/2108.07258

3. European Union Agency for Cybersecurity. Cybersecurity of AI and standardisation [Internet]. Atenas: ENISA; 2024 [citado 27 Nov 2025]. Disponible en: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation

4. Cuba. Consejo de Estado. Decreto-Ley 78/2023, sobre la seguridad y protección de la información clasificada y limitada. Gaceta Oficial de la República de Cuba. 2024;(88 Ordinaria).

5. Cuba. Consejo de Estado. Ley 149/2022, de Protección de Datos Personales. Gaceta Oficial de la República de Cuba. 2022;(77 Ordinaria).

6. Cuba. Consejo de Estado. Decreto-Ley 6/2020, del Sistema de Información del Gobierno. Gaceta Oficial de la República de Cuba. 2020;(54 Ordinaria).

7. Cuba. Consejo de Estado. Decreto-Ley 98/2024, de la Estadística Oficial. Gaceta Oficial de la República de Cuba. 2025;(51 Ordinaria).

8. Hintze M, De La Chapelle B. The sovereignty of data: a European perspective. In: Chalaby AB, editor. Data governance in the digital age. Ontario: Centre for International Governance Innovation; 2019. p. 15-34.

9. Couldry N, Mejias UA. Data colonialism: rethinking big data's relation to the contemporary subject. Telev New Media. 2019;20(4):336-49.

10. DAMA International. The DAMA guide to the data management body of knowledge. 2nd ed. New Jersey: Technics Publications; 2017.

11. ISACA. COBIT 2019 framework: governance and management objectives [Internet]. Illinois: ISACA; 2018 [citado 27 Nov 2025]. Disponible en: https://www.isaca.org/resources/cobit

12. Beange S. DCAM v3.1: the future-ready framework for strategic data management [Internet]. [Países Bajos]: Projective Group; 2025 [citado 27 Nov 2025]. Disponible en: https://www.projectivegroup.com/dcam-v3-1-the-future-ready-framework-for-strategic-data-management/

13. BigID. What is the Cloud Data Management Framework (CDMC)? [Internet]. New York: BigID; 2021 [citado 27 Nov 2025]. Disponible en: https://bigid.com/blog/cdmc/

14. Aldama O, Delgado M, Díaz-Canel M, Rodríguez A. Implementación de tableros de mando integral en la gestión gubernamental: impacto en la toma de decisiones sanitarias basada en datos. INFODIR. 2025;(41):e1768.

15. Aldama López O, Delgado Fernández M, Díaz-Canel Bermúdez M. Metodología de los tableros y cuadro de mando integral en la gestión de gobierno orientada a la innovación. Rev Cubana Adm Pública Empresarial. 2022;6(3):e236.

16. Janssen M, Brous P, Estevez E, Barbosa LS, Janowski T. Data governance: organizing data for trustworthy artificial intelligence. Gov Inf Q. 2020;37(3):101493.

17. Organisation for Economic Co-operation and Development. Enhancing access to and sharing of data: reconciling risks and benefits for data re-use across societies. París: OECD Publishing; 2019.

18. UNESCO. Recomendación sobre la ética de la inteligencia artificial [Internet]. París: UNESCO; 2021 [citado 27 Nov 2025]. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000381137

19. Mohamed S, Png MT, Isaac W. Decolonial AI: decolonial theory as sociotechnical foresight in artificial intelligence. Philos Technol. 2020;33:655-84.
20. Carlini N, Tramer F, Wallace E, Jagielski M, Herbert-Voss A, Lee K, et al. Extracting training data from large language models. In: Proceedings of the 31st USENIX Security Symposium; 2022; Boston. Berkeley: USENIX Association; 2022. p. 2633-50.
21. Organización para la Cooperación y el Desarrollo Económicos, CAF – Banco de Desarrollo de América Latina. Uso estratégico y responsable de la inteligencia artificial en el sector público de América Latina y el Caribe. París: OECD Publishing; 2022.

Conflicto de intereses

Los autores declaran que no existe conflicto de intereses.

Contribuciones de los autores

Los autores trabajaron de conjunto en todo el proceso de desarrollo del trabajo.