

Marco para la gobernanza y el uso ético, responsable y seguro de la inteligencia artificial

Asociación Colombiana de Ciudades Capitales

Principios, clasificación de riesgos, obligaciones, procedimientos y arquitectura de gobernanza para el diseño, la adquisición, el despliegue, el uso, la supervisión y el retiro de sistemas de inteligencia artificial en Asocapitales, y referente adaptable para las 32 ciudades capitales.

FICHA DEL DOCUMENTO

TÍTULO	Marco para la gobernanza y el uso ético, responsable y seguro de la inteligencia artificial
CÓDIGO	MDE-PI-PLT-03
TIPO DE DOCUMENTO	Política
MACROPROCESO	Dirección Estratégica
PROCESO	Planeación Institucional
VERSIÓN	01
VIGENTE A PARTIR DE	24 de julio de 2026
RESPONSABLE POR EL DOCUMENTO	Planeación Institucional, Gestión Tecnológica y Comité de Gobernanza de IA de la Asociación Colombiana de Ciudades Capitales – Asocapitales
ELABORÓ	Andrés Santamaría Garrido Director General, Asocapitales
REVISÓ Y COMPLEMENTÓ	Planeación Institucional de Asocapitales María Virginia Jordán, Jefe de Planeación Institucional
APROBÓ	Dirección General de Asocapitales Andrés Santamaría Garrido, Director General

MARCO DE REFERENCIA

Este Marco se inscribe en el Sistema de Gestión de Calidad de la Asociación y en la Política Integral de Transparencia y Ética de Asocapitales – PITEA. Como criterio de interpretación complementario se alinea con la Recomendación de la UNESCO sobre la Ética de la Inteligencia Artificial (2021), los Principios de IA de la OCDE (2019, actualizados en 2024), el Reglamento de Inteligencia Artificial de la Unión Europea (2024), el Marco de Gestión de Riesgos de IA del NIST (2023) y los Principios para el uso ético de la IA en el Sistema de las Naciones Unidas (2022).

Asociación Colombiana de Ciudades Capitales – Asocapitales. Documento del Sistema de Gestión de Calidad. Su reproducción parcial o total debe conservar la referencia al código y a la versión vigente.

TABLA DE CONTENIDO

Contenido

1	Objetivos	4	10.4	Comunicación pública responsable	16
2	Alcance	4	11	Empleo, talento humano y reconversión	17
3	Normatividad	4	11.1	La nómina adentro	17
4	Definiciones	5	11.2	No sustitución por defecto	17
5	Principios rectores del uso de inteligencia artificial	6	11.3	Formación continua	17
6	Clasificación de usos por nivel de riesgo	8	11.4	Diálogo con el equipo	17
6.1	Niveles de riesgo y sentido del enfoque	8	12	Adquisiciones y proveedores	18
6.2	Usos de riesgo inaceptable (prohibidos)	10	12.1	Debida diligencia	18
6.3	Usos de alto riesgo	10	12.2	Cláusulas obligatorias	18
6.4	Usos de riesgo moderado	11	12.3	Compras públicas como palanca	18
6.5	Usos de riesgo mínimo	11	13	Arquitectura de gobernanza	19
7	Gestión del ciclo de vida de los sistemas de IA	12	13.1	Comité de Gobernanza de IA	19
7.1	Evaluación de impacto algorítmica (EIA)	12	13.2	Oficial de IA	19
7.2	Pilotos y despliegue gradual	13	13.3	Auditoría independiente	19
7.3	Monitoreo en operación	13	13.4	Canal de consultas y denuncias	19
7.4	Retiro y sustitución	13	14	Relación con las ciudades capitales	20
8	Datos, privacidad y seguridad	13	14.1	Referente de adopción territorial	20
8.1	Régimen de protección de datos	13	14.2	Acompañamiento gremial	20
8.2	Regla de no entrenamiento	13	14.3	Articulación con los observatorios de empleo e IA	20
8.3	Clasificación de la información	14	14.4	Interlocución nacional e internacional	20
8.4	Seguridad de la información	14	15	Régimen de incumplimiento e interpretación	21
8.5	Soberanía y localización de datos	14	15.1	Régimen de incumplimiento	21
9	Supervisión humana y responsabilidad	14	15.2	Interpretación	21
9.1	Verificación humana obligatoria	14	16	Mecanismos de divulgación, seguimiento y vigencia	21
9.2	Responsable de sistema y cadena de responsabilidad	14	16.1	Plan de comunicación	21
9.3	Declaración de uso y explicabilidad	15	16.2	Capacitación	22
9.4	Gestión de incidentes	15	16.3	Monitoreo y seguimiento	22
10	Transparencia y rendición de cuentas	15	16.4	Vigencia y revisión	22
10.1	Inventario público de sistemas	15	17	Responsable por el documento	23
10.2	Trazabilidad	15	18	Control de cambios	23
10.3	Informe anual de gobernanza de IA	16	19	Firmas	23

1

CAPÍTULO 1

Objetivos

Establecer los principios, la clasificación de riesgos, las obligaciones, los procedimientos y la arquitectura de gobernanza que rigen el diseño, la adquisición, el despliegue, el uso, la supervisión y el retiro de sistemas de inteligencia artificial (IA) en Asocapitales, y ofrecer a las 32 ciudades capitales un referente adaptable a sus propios actos administrativos. Lo anterior, enmarcando este Marco en el Sistema de Gestión de Calidad de la Asociación, en coherencia con la Política Integral de Transparencia y Ética de Asocapitales – PITEA.

2

CAPÍTULO 2

Alcance

Este Marco aplica a todos los servidores, contratistas, asesores, pasantes y aliados de la Asociación que utilicen sistemas de IA en ejercicio de sus funciones; a todos los sistemas de IA operados por la Asociación o por terceros en su nombre; y a todos los productos institucionales elaborados total o parcialmente con asistencia de IA, cualquiera que sea la herramienta empleada.

3

CAPÍTULO 3

Normatividad

Constitución Política de Colombia: en particular los derechos a la intimidad y al habeas data (art. 15), a la libertad de expresión e información (art. 20), al trabajo en condiciones dignas (art. 25) y al acceso a documentos públicos (art. 74).

Ley 1581 de 2012 y sus decretos reglamentarios (incluido el Decreto 1377 de 2013): régimen de protección de datos personales.

Ley 1712 de 2014: transparencia y acceso a la información pública.

CONPES 4144 de 2025: Política Nacional de Inteligencia Artificial.

Acuerdo 003 de 2025 de Bogotá D.C.: referente territorial de adopción de IA en el Distrito Capital.

ESTÁNDARES INTERNACIONALES DE REFERENCIA

Como criterio de interpretación complementario, este Marco se alinea con los siguientes estándares internacionales: la Recomendación de la UNESCO sobre la Ética de la Inteligencia Artificial (2021), los Principios de IA de la OCDE (2019, actualizados en 2024), el Reglamento de Inteligencia Artificial de la Unión Europea (2024), el Marco de Gestión de Riesgos de IA del NIST (2023) y los Principios para el uso ético de la IA en el Sistema de las Naciones Unidas (2022).

4 CAPÍTULO 4
Definiciones

Sistema de inteligencia artificial

sistema basado en máquinas que, con objetivos explícitos o implícitos, infiere a partir de la información que recibe cómo generar resultados —predicciones, contenidos, recomendaciones o decisiones— que pueden influir en entornos físicos o virtuales (definición OCDE, 2024).

IA generativa

sistemas que producen texto, imagen, audio, video o código.

Agente de IA

sistema con capacidad de planificar y ejecutar secuencias de tareas con autonomía delegada.

Supervisión humana efectiva

intervención de una persona competente, con tiempo, información y autoridad reales para revisar, corregir, revertir o detener las salidas de un sistema.

Evaluación de impacto algorítmica (EIA)

análisis previo y documentado de los riesgos de un sistema sobre derechos, equidad, seguridad y empleo, y de las medidas de mitigación correspondientes.

Responsable de sistema

servidor designado que responde por la operación conforme de cada sistema de IA.

Ciclo de vida

etapas de diseño o adquisición, prueba, despliegue, operación, monitoreo y retiro de un sistema.

Incidente

todo evento en que un sistema de IA produce un resultado erróneo, discriminatorio, inseguro o contrario a este Marco, con efectos institucionales o sobre terceros.

Comité de Gobernanza de IA

órgano colegiado responsable de la clasificación de riesgos, la autorización de herramientas y usos, y la actualización de este Marco.

Oficial de IA

servidor designado como secretario técnico del Comité de Gobernanza de IA.

5

CAPÍTULO 5

Principios rectores del uso de inteligencia artificial

Alineados con la Recomendación de la UNESCO (2021) y los Principios de la OCDE (2019, actualizados en 2024).

Todo diseño, adquisición, despliegue y uso de sistemas de IA en Asocapitales se rige por los siguientes principios:

01

Dignidad humana y primacía del criterio humano

La IA asiste a las personas; no las sustituye en el juicio ni las subordina a decisiones automatizadas.

02

Proporcionalidad e inocuidad

Ningún uso excede lo necesario para un fin legítimo, y ningún sistema recibe más autonomía que la que la institución puede supervisar.

03

Seguridad y robustez

Los sistemas operan de manera fiable, protegidos frente a fallos, ataques y usos indebidos, durante todo su ciclo de vida.

04

Equidad y no discriminación

Se previenen, detectan y corrigen los sesgos que puedan excluir o dañar a personas o territorios, con especial atención a mujeres, jóvenes y capitales de la periferia.

05

Privacidad y protección de datos

El tratamiento de datos personales observa los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso restringido, seguridad y confidencialidad (Ley 1581 de 2012).

CAPÍTULO 5 · PRINCIPIOS RECTORES (CONTINUACIÓN)**06 Transparencia y explicabilidad**

El uso de IA es declarable; las decisiones asistidas son explicables en un lenguaje comprensible para el afectado.

07 Supervisión humana efectiva

Toda salida con efectos institucionales pasa por verificación humana competente.

08 Responsabilidad y rendición de cuentas

Cada sistema tiene un responsable humano identificable; los procesos son trazables y auditables.

09 Sostenibilidad y beneficio social

La adopción se orienta al mejor servicio de las ciudades y sus habitantes, incluida la protección del empleo digno.

10 Gobernanza multiactor

La Asociación coopera con el Gobierno Nacional, la academia, el sector privado y los organismos internacionales en la construcción de estándares.

6

CAPÍTULO 6

Clasificación de usos por nivel de riesgo

Enfoque basado en riesgos, conforme al Reglamento de IA de la Unión Europea (2024).

6.1 Niveles de riesgo y sentido del enfoque

El enfoque basado en riesgos parte de una idea simple: no todos los usos de la IA son iguales, y por eso no todos merecen las mismas reglas. Redactar un borrador con un asistente no plantea los mismos riesgos que decidir con un algoritmo quién recibe un subsidio. Regular todo con la misma severidad frenaría la innovación en lo inofensivo; regular todo con la misma laxitud desprotegería a las personas en lo delicado. La solución es graduar: a mayor capacidad de un sistema de afectar derechos, más exigentes las condiciones para usarlo.

En consecuencia, todo uso de IA en la Asociación se clasifica, antes de su despliegue, en uno de cuatro niveles: **riesgo inaceptable** (prohibido siempre), **alto riesgo** (permitido solo con evaluación de impacto, autorización y vigilancia reforzada), **riesgo moderado** (permitido con registro y transparencia) y **riesgo mínimo** (permitido bajo los principios generales). La clasificación corresponde al Comité de Gobernanza de IA conforme a la siguiente matriz y a la guía de cuatro preguntas.

GUÍA DE CLASIFICACIÓN EN CUATRO PREGUNTAS · RESPONDER EN ORDEN

1

¿El uso puntúa, vigila masivamente, manipula o decide solo sobre personas, o expone datos sensibles o información reservada en herramientas no autorizadas?

→ **Inaceptable, prohibido, no continúe.**

2

Si el sistema se equivoca, ¿una persona determinada sufre la consecuencia, o el sistema actúa por sí mismo sobre otros sistemas, o trata datos personales sensibles?

→ **Alto riesgo.**

3

¿El resultado sale al público o circula institucionalmente como información confiable?

→ **Riesgo moderado.**

4

¿La salida queda siempre en manos de quien la pidió, sin datos de terceros ni información reservada?

→ **Riesgo mínimo.**

CAPÍTULO 6 · MATRIZ DE CLASIFICACIÓN POR NIVEL DE RIESGO

NIVEL	CRITERIO Y PREGUNTA CLAVE	EJEMPLOS EN ASOCAPITALES Y LAS CIUDADES	RIESGO QUE SE CONTROLA	OBLIGACIONES QUE SE ACTIVAN
● Inaceptable	El daño potencial es incompatible con los derechos; ninguna mitigación lo compensa. <i>¿La persona queda reducida a objeto de cálculo?</i>	Ranquear ciudadanos “confiables” para priorizar trámites; videovigilancia indiscriminada; descartar hojas de vida sin revisión humana; cargar historias clínicas a un chatbot público.	Daño irreversible a la dignidad, la igualdad y la presunción de inocencia.	Prohibido de plano. No admite EIA ni autorización; su práctica activa el régimen de incumplimiento.
● Alto	El error del sistema recae sobre una persona concreta, o el sistema ejecuta acciones por sí mismo. <i>¿Si se equivoca, alguien determinado paga la consecuencia?</i>	Focalización de beneficiarios; priorización de atención en salud o subsidios; agentes que responden PQRS o modifican registros; evaluación de desempeño asistida; tratamiento de datos sensibles.	Exclusión por sesgo; error automatizado que se materializa antes de que un humano lo vea.	EIA previa + autorización del Comité + piloto evaluado + supervisión humana de doble instancia + inventario + auditoría anual.
● Moderado	No decide sobre personas, pero su producto circula con apariencia de verdad. <i>¿El resultado sale al público o informa a la institución?</i>	Informes, boletines y comunicados asistidos por IA; presentaciones institucionales; asistentes internos de consulta documental.	El error publicado: cifras inventadas, fuentes mal citadas, tono impropio.	Registro en inventario + verificación humana documentada contra fuente primaria + declaración de uso + reglas de datos.
● Mínimo	Asistencia personal cuya salida siempre revisa quien la pidió. <i>¿Queda todo en manos del usuario, sin datos de terceros?</i>	Borradores de trabajo, lectura y resumen de documentos, corrección de estilo, traducción, organización de agenda y tareas.	Prácticamente ninguno institucional; riesgo residual de dependencia acrítica.	Principios generales + herramientas del listado autorizado. Uso fomentado como alfabetización práctica.

TRES REGLAS PRÁCTICAS DE CLASIFICACIÓN

1

Ante la duda, el nivel superior.

2

Se clasifica el uso, no la herramienta.

3

La clasificación es viva y se revisa cuando cambian la herramienta, los datos tratados o el efecto del uso.

6.2 ● Usos de riesgo inaceptable (prohibidos)

Son usos cuyo daño potencial sobre la dignidad, la libertad o la igualdad de las personas es tan grave que ninguna medida de mitigación lo compensa; por ello no se someten a evaluación, sino que se prohíben de plano. Se consideran de riesgo inaceptable, entre otros:

Calificación social (scoring social): puntuar personas o poblaciones combinando datos de contextos distintos para condicionar su acceso a derechos o servicios.

Vigilancia masiva indiscriminada o identificación biométrica remota sin fundamento legal expreso.

Decisiones definitivas exclusivamente automatizadas sobre personas —laborales, contractuales, disciplinarias o de acceso a servicios—: un algoritmo puede informar la decisión, pero jamás tomarla solo.

Manipulación del comportamiento que explote vulnerabilidades de personas o grupos (edad, condición económica, discapacidad).

Desinformación y suplantaciones: generar o difundir contenidos engañosos o que atribuyan afirmaciones falsas a personas o instituciones.

Fuga de información: introducir datos personales sensibles o información reservada en herramientas no autorizadas.

6.3 ● Usos de alto riesgo

Son usos legítimos y a menudo valiosos, pero cuyo error afecta a personas concretas o compromete seriamente a la institución. Entre otros: (i) los sistemas que apoyen decisiones con efectos sobre personas determinadas, focalización de beneficiarios, priorización de atención, evaluación de desempeño; (ii) los agentes con autonomía para ejecutar acciones sobre sistemas institucionales; (iii) los usos que traten datos personales sensibles; y (iv) las aplicaciones cuyo error pueda afectar derechos de terceros o la posición pública de la Asociación.

CONDICIONES ACUMULATIVAS PARA SU USO

Evaluación de impacto algorítmica previa, autorización expresa del Comité, piloto con evaluación documentada antes de escalar, supervisión humana reforzada de doble instancia durante la operación, y registro en el inventario con auditoría anual.

6.4 ● Usos de riesgo moderado

Son usos que no deciden sobre personas, pero cuyo producto sale al público o circula dentro de la institución con apariencia de verdad: IA generativa aplicada a informes, boletines, comunicados y presentaciones institucionales, así como asistentes internos de consulta con acceso a información no reservada. Se exige registro en el inventario, verificación humana documentada de toda cifra contra su fuente primaria, declaración de uso conforme al numeral 9.3 de este Marco y cumplimiento de las reglas de datos del Capítulo 8.

Registro en
inventario

Verificación humana
contra fuente
primaria

Declaración de uso
(9.3)

Reglas de datos
(Cap. 8)

6.5 ● Usos de riesgo mínimo

Corresponden a la asistencia personal a la productividad, búsqueda y lectura de documentos, borradores de trabajo, corrección de estilo, traducción, organización de tareas, cuyo rasgo común es que la salida siempre pasa por las manos de quien la pidió antes de tener cualquier efecto, y que no involucra datos personales de terceros ni información reservada. Estos usos se permiten y fomentan bajo los principios generales y el listado de herramientas autorizadas.

Búsqueda y
lectura de
documentos

Borradores de
trabajo

Corrección de
estilo

Traducción

Organización de
tareas

7

CAPÍTULO 7

Gestión del ciclo de vida de los sistemas de IA

Conforme al Marco de Gestión de Riesgos de IA del NIST: gobernar, mapear, medir, gestionar.

CICLO DE VIDA DE UN SISTEMA

7.1 Evaluación de impacto algorítmica (EIA)

La EIA es el equivalente, para un sistema de IA, de lo que un estudio de impacto ambiental es para una obra: un examen previo, escrito y verificable, que obliga a responder antes de desplegar las preguntas que de otro modo se responderían después del daño: ¿para qué exactamente se usará el sistema?, ¿con qué datos y de dónde salen?, ¿a quién puede perjudicar si se equivoca y cómo?, ¿quién lo vigila y con qué poder real de detenerlo? Sin EIA aprobada, ningún sistema de alto riesgo entra en operación.

Es obligatoria para todo sistema de alto riesgo, y para los de riesgo moderado cuando el Comité lo determine. La elabora el área que propone el uso con apoyo del Oficial de IA, y la decide el Comité. Como contenido mínimo, la EIA documenta:

CONTENIDO MÍNIMO DE LA EIA

1 • Identificación Identificación del sistema, proveedor, versión y responsable designado.	2 • Finalidad Finalidad, base jurídica y nivel de riesgo propuesto.
3 • Datos Datos tratados: categorías, origen, licitud, minimización y ciclo de retención.	4 • Riesgos Riesgos identificados sobre derechos, equidad, seguridad, empleo e imagen institucional, con probabilidad e impacto.
5 • Mitigación Medidas de mitigación y mecanismo de supervisión humana (quién revisa, qué revisa, con qué autoridad).	6 • Métricas Métricas de desempeño, plan de monitoreo y umbrales de suspensión.
7 • Retiro Plan de retiro y continuidad manual del proceso.	8 • Decisión Concepto del Oficial de IA y decisión del Comité.

La EIA se actualiza ante cualquier cambio sustancial del sistema, de sus datos o de su uso.

7.2 Pilotos y despliegue gradual

Los nuevos usos institucionales se implementan mediante pilotos con línea base, métrica de éxito y evaluación publicada al Comité: lo que la evaluación pruebe se escala con la Dirección Administrativa, Financiera y Gestión Humana para validar disponibilidad de presupuesto; lo que no, se descarta y se documenta la lección. Ningún sistema pasa de piloto a operación sin decisión expresa del Comité.

7.3 Monitoreo en operación

Los sistemas en operación se monitorean de forma continua sobre exactitud, deriva del modelo, sesgos, incidentes y uso efectivo. Los sistemas de alto riesgo reportan indicadores trimestrales al Comité.

7.4 Retiro y sustitución

Un sistema se retira cuando su desempeño, su seguridad o su proveedor dejen de cumplir este Marco. El retiro incluye la recuperación de los datos institucionales, la documentación del cierre y, cuando aplique, el plan de continuidad manual del proceso.

8

CAPÍTULO 8

Datos, privacidad y seguridad

8.1 Régimen de protección de datos

Todo tratamiento de datos personales mediante IA cumple la Ley 1581 de 2012, el Decreto 1377 de 2013 y las instrucciones de la Superintendencia de Industria y Comercio, incluidos los deberes frente a datos sensibles y de niños, niñas y adolescentes. La Asociación actúa como responsable del tratamiento y exige a los proveedores de IA condición de encargados con contratos de transmisión conformes.

8.2 Regla de no entrenamiento

Solo se autorizan herramientas cuyos términos garanticen que la información institucional no se emplea para entrenar modelos de terceros sin consentimiento expreso, y que permitan la eliminación efectiva de los datos cargados.

CAPÍTULO 8 · DATOS, PRIVACIDAD Y SEGURIDAD (CONTINUACIÓN)

8.3 Clasificación de la información

Antes de introducir información en un sistema de IA, el usuario verifica su clasificación: la información pública puede tratarse en herramientas autorizadas; la información clasificada o reservada (Ley 1712 de 2014) solo en entornos expresamente aprobados por el Comité; y los datos personales sensibles, únicamente en sistemas de alto riesgo autorizados con EIA vigente.

8.4 Seguridad de la información

Las herramientas autorizadas se integran al esquema de seguridad digital de la Asociación: autenticación reforzada, control de acceso por roles, registro de actividad, cifrado en tránsito y en reposo, y evaluación periódica de vulnerabilidades, en línea con los lineamientos de seguridad digital del Gobierno Nacional.

8.5 Soberanía y localización de datos

En las adquisiciones se preferirán soluciones que permitan conocer y pactar la jurisdicción de almacenamiento de los datos y que faciliten la portabilidad plena, evitando dependencias que comprometan el control institucional de la información de las ciudades.

9

CAPÍTULO 9

Supervisión humana y responsabilidad

9.1 Verificación humana obligatoria

Ninguna salida de IA se incorpora a decisiones, comunicaciones o documentos institucionales sin revisión humana competente que comprenda: exactitud y verificación de cifras contra fuente primaria, detección de invenciones o alucinaciones, sesgos, pertinencia jurídica y tono institucional. En los sistemas de alto riesgo, la verificación es de doble instancia.

9.2 Responsable de sistema y cadena de responsabilidad

Cada sistema tiene un responsable designado que mantiene su documentación, atiende incidentes y responde por su operación conforme. La responsabilidad final por los productos y decisiones de la Asociación es siempre humana e institucional: el uso de IA no atenúa la responsabilidad de quien firma, aprueba o publica.

CAPÍTULO 9 · SUPERVISIÓN HUMANA Y RESPONSABILIDAD (CONTINUACIÓN)

9.3 Declaración de uso y explicabilidad

Los productos institucionales elaborados con asistencia significativa de IA incluyen una nota metodológica que declara las herramientas empleadas, su función de asistencia y la dirección, verificación y redacción final humanas, con el siguiente modelo de referencia:

MODELO DE REFERENCIA · NOTA METODOLÓGICA

[Espacio reservado para el modelo de nota metodológica que adopte el Comité de Gobernanza de IA.]

Cuando un sistema apoye decisiones que afecten a una persona, esta tiene derecho a una explicación comprensible y a solicitar revisión humana.

9.4 Gestión de incidentes

Los incidentes se reportan a través del correo incidentes.IA@asocapitales.co y se remiten a los miembros del Comité dentro de los tres (3) días hábiles siguientes a su detección; los que involucren datos personales o efectos sobre terceros, de inmediato. El Comité ordena la corrección, documenta la causa raíz, ajusta los protocolos y, cuando la ley lo exija, informa a las autoridades competentes. El reporte de buena fe no genera sanción para quien reporta.

10

CAPÍTULO 10

Transparencia y rendición de cuentas

10.1 Inventario público de sistemas

La Asociación mantiene un inventario actualizado de sus sistemas de IA con: denominación, finalidad, nivel de riesgo, datos tratados, responsable, estado de evaluación y fecha de última auditoría. El inventario es de acceso público, salvo la información legalmente reservada.

10.2 Trazabilidad

Los procesos asistidos por IA conservan trazabilidad razonable, herramientas, versiones de trabajo, verificaciones realizadas suficientes para reconstruir y auditar el proceso.

CAPÍTULO 10 · TRANSPARENCIA Y RENDICIÓN DE CUENTAS (CONTINUACIÓN)

10.3 Informe anual de gobernanza de IA

El Comité presenta a la Dirección General y esta dirección podrá entregar a la Asamblea el informe anual sobre sistemas en operación, incidentes, auditorías, formación impartida y recomendaciones, cuyo resumen se publica.

Sistemas en operación	Incidentes	Auditorías	Formación impartida	Recomendaciones
--------------------------	------------	------------	------------------------	-----------------

10.4 Comunicación pública responsable

La comunicación institucional no exagera capacidades de la IA ni induce a error sobre la autoría humana de las posiciones de la Asociación. Los contenidos sintéticos de apariencia realista se etiquetan como tales.

11

CAPÍTULO 11

Empleo, talento humano y reconversión

Énfasis colombiano: coherencia con la alerta temprana sobre IA y empleo en las 32 capitales.

11.1 La nómina adentro

Toda automatización de procesos internos se aprueba junto con su plan de reconversión del talento: qué funciones pasan del trámite al análisis, la fiscalización, los datos y el servicio complejo, con qué formación y en qué plazo. En la Asociación, la IA se adopta con la nómina adentro: automatizar sin despedir.

REGLA INSTITUCIONAL

La IA se adopta con la nómina adentro: automatizar sin despedir.

11.2 No sustitución por defecto

La incorporación de IA no constituye causal automática de supresión de empleos. Las ganancias de productividad se orientan prioritariamente a ampliar la capacidad técnica y de servicio de la Asociación a las 32 capitales.

11.3 Formación continua

Todo el personal, incluido el nivel directivo, podrá recibir formación periódica en las cinco competencias de la transición: pensamiento crítico frente a salidas de IA, alfabetización en datos, colaboración humano-IA, ética digital y habilidades socioemocionales. La regla institucional es formar antes que comprar.

Pensamiento
crítico frente a
salidas de IA

Alfabetización en
datos

Colaboración
humano-IA

Ética digital

Habilidades
socioemocionales

11.4 Diálogo con el equipo

Los planes de adopción de IA con efectos organizacionales se socializan previamente con el equipo humano, cuyas observaciones se documentan y responden.

SECUENCIA DE ADOPCIÓN

Reglas primero, gente segunda, pilotos después.

12

CAPÍTULO 12

Adquisiciones y proveedores

12.1 Debida diligencia

Antes de contratar una solución de IA se evalúan: seguridad y tratamiento de datos, sesgos conocidos del modelo, condiciones de uso y de no entrenamiento, soporte, jurisdicción aplicable y sostenibilidad del proveedor.

Seguridad y datos	Sesgos conocidos	Uso y no entrenamiento	Soporte	Jurisdicción	Sostenibilidad
-------------------	------------------	------------------------	---------	--------------	----------------

12.2 Cláusulas obligatorias

Los contratos de soluciones de IA incluyen: transferencia de conocimiento, portabilidad de datos y configuraciones, prohibición de uso de la información institucional para entrenamiento sin consentimiento, niveles de servicio, auditabilidad y salida ordenada sin dependencia injustificada de un único proveedor.

12.3 Compras públicas como palanca

La Asociación promoverá entre las capitales el uso de las compras públicas como incentivo a la adopción responsable de IA por las empresas locales, con criterios de innovación, empleo y transferencia de capacidades, en línea con el CONPES 4144.

13

CAPÍTULO 13

Arquitectura de gobernanza

13.1 Comité de Gobernanza de IA

Créase el Comité de Gobernanza de IA, integrado por la Dirección General quien lo preside, Planeación Institucional, Dirección Administrativa, Financiera y Gestión Humana, Dirección Jurídica, el Área de Comunicaciones y Relacionamento Institucional y el responsable del Área de Gestión Tecnológica. Puede sesionar en cualquier momento (si hay algún incidente o necesidad) o al menos trimestralmente y decide sobre: clasificación de riesgos, autorización de herramientas y usos, evaluación de pilotos, incidentes, auditorías y actualizaciones de este Marco.

13.2 Oficial de IA

La Dirección General designa un Oficial de IA, secretario técnico del Comité, encargado de mantener el inventario, tramitar autorizaciones, coordinar las evaluaciones de impacto algorítmicas y las auditorías, gestionar la formación y servir de punto de contacto con las áreas, ciudades y las autoridades.

13.3 Auditoría independiente

Los sistemas de alto riesgo se auditan anualmente y los demás al menos cada dos años, sobre desempeño, seguridad, sesgos y cumplimiento. Cuando la criticidad lo amerite, la auditoría será externa e independiente, con informe al Comité y a la Dirección General.

13.4 Canal de consultas y denuncias

Existirá un canal permanente para consultas sobre este Marco y para denunciar usos contrarios a él, con garantía de confidencialidad y no represalia para el denunciante de buena fe. Este canal es el correo incidentes.IA@asocapitales.co y a través del formulario de PQRS de la página web de Asocapitales.

14

CAPÍTULO 14

Relación con las ciudades capitales**EL ÉNFASIS TERRITORIAL****De reglamento interno a estándar gremial de las 32 capitales.****14.1 Referente de adopción territorial**

Este Marco se pone a disposición de las 32 ciudades capitales como referente adaptable mediante acto administrativo local, junto con el Acuerdo 003 de 2025 de Bogotá D.C., para que cada capital adopte sus reglas antes de desplegar sistemas de IA: reglas primero, gente segunda, pilotos después.

14.2 Acompañamiento gremial

La Asociación acompañará a las capitales en la adaptación del Marco, la formación de servidores, el diseño de las evaluaciones de impacto y la estructuración de pilotos de alto retorno, atención ciudadana y gestión tributaria, con prioridad en las capitales de menor capacidad institucional: Quibdó, Mitú, Inírida, Puerto Carreño, Mocoa, San José del Guaviare, Arauca, Yopal, Riohacha, Leticia y Providencia.

Quibdó	Mitú	Inírida	Puerto Carreño	Mocoa	San José del Guaviare
Arauca	Yopal	Riohacha	Leticia	Providencia	

14.3 Articulación con los observatorios de empleo e IA

Los datos de adopción y sus efectos sobre el empleo público y privado alimentarán los observatorios locales de empleo e IA y el sistema de alerta temprana coordinado por la Asociación, de modo que la gobernanza tecnológica y la política laboral operen como un solo sistema.

14.4 Interlocución nacional e internacional

La Asociación representará la voz de las capitales ante el Gobierno Nacional en el desarrollo del CON-PES 4144 y de la regulación de IA, y cooperará con organismos internacionales, UNESCO, OCDE, BID, Banco Mundial, Naciones Unidas en la adopción territorial de estándares.

UNESCO	OCDE	BID	Banco Mundial	Naciones Unidas
--------	------	-----	---------------	-----------------

15

CAPÍTULO 15

Régimen de incumplimiento e interpretación

15.1 Régimen de incumplimiento

El incumplimiento de este Marco da lugar a las medidas administrativas, contractuales o disciplinarias correspondientes, graduadas según la naturaleza de la vinculación, la clasificación de riesgo del uso y la gravedad y reiteración de la conducta, sin perjuicio de las responsabilidades legales. Este régimen opera de manera articulada con el Procedimiento Interno de Investigación y Sanción de la PITEA.

Naturaleza de la vinculación

Clasificación de riesgo del uso

Gravedad y reiteración de la conducta

15.2 Interpretación

Las dudas de interpretación se resuelven por el Comité de Gobernanza de IA conforme a los principios rectores del Capítulo 5 y a los estándares internacionales de referencia, aplicando siempre la lectura más protectora de los derechos de las personas.

CAPÍTULO 16

16

Mecanismos de divulgación, seguimiento y vigencia

16.1 Plan de comunicación

El Comité de Gobernanza de IA, con apoyo del Área de Comunicaciones y Relacionamento Institucional, construirá las piezas y ayudas necesarias para que el contenido de este Marco sea apropiado por los colaboradores de Asocapitales y por las ciudades capitales, promoviendo una cultura de uso ético, responsable y seguro de la IA.

CAPÍTULO 16 · MECANISMOS DE DIVULGACIÓN, SEGUIMIENTO Y VIGENCIA (CONTINUACIÓN)

16.2 Capacitación

El Oficial de IA, con apoyo de la Dirección Administrativa, Financiera y Gestión Humana, podrá realizar espacios de inducción a todos los nuevos colaboradores sobre los elementos esenciales de este Marco. Anualmente, el Comité podrá realizar al menos una sesión de capacitación y actualización, en la que se identificarán necesidades de ajuste de los lineamientos aquí contenidos.

16.3 Monitoreo y seguimiento

El seguimiento continuo a la clasificación de riesgos, al inventario de sistemas, a los incidentes y a las acciones de mitigación será realizado por el Oficial de IA y presentado al Comité en sus sesiones trimestrales. Los resultados se documentan en las actas del Comité y alimentan el informe anual de gobernanza de IA de que trata el numeral 10.3.

16.4 Vigencia y revisión

Este Marco rige desde su expedición, deroga las disposiciones internas que le sean contrarias y se revisa al menos anualmente, o antes si la evolución tecnológica o normativa lo exige, por iniciativa del Comité y con aprobación de la Dirección General.

17

CAPÍTULO 17

Responsable por el documento

Planeación Institucional, Gestión Tecnológica y Comité de Gobernanza de IA de la Asociación Colombiana de Ciudades Capitales – Asocapitales.

18

CAPÍTULO 18

Control de cambios

VERSIÓN	DESCRIPCIÓN DE LOS CAMBIOS	ELABORACIÓN Y REVISIÓN	FECHA
01	Documento nuevo. Consolidación del Marco para la Gobernanza y el Uso Ético, Responsable y Seguro de la Inteligencia Artificial de Asocapitales.	Elaborado por Andrés Santamaría Garrido, Director General. Revisado y complementado por Planeación Institucional de Asocapitales.	24/07/2026

19

CAPÍTULO 19

Firmas

ELABORÓ

Andrés Santamaría Garrido

Director General
Asociación Colombiana de
Ciudades Capitales – Asocapitales

REVISÓ Y COMPLEMENTÓ

María Virginia Jordán

Jefe de Planeación Institucional
Asociación Colombiana de
Ciudades Capitales – Asocapitales

APROBÓ

Andrés Santamaría Garrido

Director General
Asociación Colombiana de
Ciudades Capitales – Asocapitales



Asociación Colombiana de Ciudades Capitales – Asocapitales

Sistema de Gestión de Calidad

DOCUMENTO	Marco para la gobernanza y el uso ético, responsable y seguro de la inteligencia artificial
CÓDIGO	MDE-PI-PLT-03
VERSIÓN	01
VIGENTE A PARTIR DE	24 de julio de 2026
MACROPROCESO · PROCESO	Dirección Estratégica · Planeación Institucional

Elaborado por Andrés Santamaría Garrido, Director General. Revisado y complementado por Planeación Institucional de Asocapitales.

Documento del Sistema de Gestión de Calidad de Asocapitales. Su reproducción parcial o total debe conservar la referencia al código y a la versión vigente.