



ALCALDÍA MAYOR
DE BOGOTÁ, D.C.

ACUERDO No. 003 DE 26 DIC 2025
()

"Por el cual se adoptan lineamientos y estándares para la preparación, desarrollo, implementación, supervisión y mejora continua de los sistemas de Inteligencia Artificial en las entidades y organismos del Distrito Capital"

LA COMISIÓN DISTRITAL DE TRANSFORMACIÓN DIGITAL – CDTD

En ejercicio de sus funciones legales y reglamentarias, en especial las conferidas en el artículo 5, numerales 1 y 6 del Decreto Distrital 025 de 2021, el artículo 28 del Decreto Distrital 575 de 2023, el artículo 13 del Acuerdo 001 de 2021 de la Comisión Distrital de Transformación Digital, y

CONSIDERANDO:

Que la Constitución Política de Colombia en su artículo 113 señala que los órganos del poder público deben colaborar armónicamente para el cumplimiento de los fines del Estado.

Que el artículo 209 de la Constitución Política de Colombia indica que las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado.

Que de conformidad con el numeral 1 del artículo 38 del Decreto Ley 1421 de 1993, corresponde al Alcalde Mayor hacer cumplir la Constitución, la ley, los decretos del Gobierno Nacional y los acuerdos del Concejo.

Que, el numeral 6 del artículo 38 del Decreto Ley 1421 de 1993 establece que corresponde al Alcalde Mayor distribuir los negocios según su naturaleza entre las secretarías, los departamentos administrativos y las entidades descentralizadas, facultad que garantiza una adecuada organización funcional y una gestión eficiente de los asuntos públicos.

Que, por su parte, el inciso segundo del artículo 53 del citado Decreto Ley señala que el Alcalde Mayor, en su calidad de Jefe de la Administración Distrital, ejerce sus atribuciones por medio de los organismos y entidades creados por el Concejo de Bogotá D.C., marco que faculta la adopción de lineamientos, directrices y disposiciones administrativas necesarias para orientar, coordinar y armonizar la gestión institucional en el territorio distrital.

Que el artículo 4 del Decreto 025 de 2021 de la Alcaldía Mayor de Bogotá, D.C dispone que la Comisión Distrital de Transformación Digital está integrada, entre otros, por "El/la Alcaldes/a Mayor de Bogotá, D. C., o su delegado/a, quien la presidirá."

Que el artículo 1 del Decreto Distrital 337 de 2025 delegó en el/la Secretario/a General de la Alcaldía Mayor de Bogotá, D.C., la participación del/la Alcalde/sa Mayor de Bogotá D.C., en la Comisión Distrital de Transformación Digital,

Que, conforme a lo dispuesto en el literal b) del artículo 48 del Acuerdo Distrital 257 de 2006, modificado por el artículo 6 del Acuerdo Distrital 638 de 2016, la Secretaría General de la Alcaldía Mayor de Bogotá Distrito Capital, tiene como función *"formular, adoptar, orientar y coordinar las políticas para el fortalecimiento de la*



ALCALDÍA MAYOR
DE BOGOTÁ, D.C.

ACUERDO No.

003

DE

26 DIC 2025

()

“Por el cual se adoptan lineamientos y estándares para la preparación, desarrollo, implementación, supervisión y mejora continua de los sistemas de Inteligencia Artificial en las entidades y organismos del Distrito Capital”

función administrativa distrital y su modernización, a través del mejoramiento de la gestión y de las estrategias de información y comunicación, de la utilización de los recursos físicos, financieros, tecnológicos e informáticos, y del desarrollo de las funciones de organización, dirección, control y seguimiento”. De igual manera, entre sus funciones, según el artículo 2 del Decreto Distrital 140 de 2021 está “liderar, orientar y coordinar la política del sistema integral de información y su desarrollo tecnológico”.

Que el Decreto 1078 de 2015, *“Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”, en su Capítulo 1 del Título 9 de la Parte 2 del Libro 2, establece los lineamientos generales de la Política de Gobierno Digital y dispone que su aplicación se desarrollará mediante un esquema que articula los elementos de gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, orientado a fortalecer la gestión pública, promover el uso de tecnologías emergentes y generar valor público mediante la transformación digital del Estado.*

Que, los numerales 1, 10 y 11 del artículo 11 del Decreto Distrital 140 de 2021, asignan a la Oficina Consejería Distrital de Tecnologías de la Información y las Comunicaciones – TIC funciones estratégicas esenciales para la orientación y coordinación de las políticas tecnológicas del Distrito Capital. En virtud del numeral 1, corresponde a dicha Oficina proponer y asesorar a la Alcaldía Mayor en materia de política pública distrital en Tecnologías de la Información y las Comunicaciones, así como expedir lineamientos, directrices, estrategias e instrumentos para guiar su implementación y seguimiento, con el propósito de fortalecer la función administrativa y misional de los sectores y entidades distritales.

Que, conforme al numeral 10 ibidem, compete igualmente a la Oficina Consejería TIC liderar la coordinación y articulación de las iniciativas de transformación digital en el Distrito Capital, rol que resulta determinante para garantizar coherencia, interoperabilidad, eficiencia y estándares comunes en el desarrollo tecnológico del Distrito.

Que, de acuerdo con el numeral 11 de la norma en cita, la Oficina Consejería TIC está facultada para implementar iniciativas tecnológicas de importancia estratégica a solicitud del/la Alcalde/sa Mayor, lo cual otorga soporte institucional a la adopción de directrices, lineamientos y actuaciones administrativas orientadas a promover el desarrollo tecnológico, la gestión digital y el uso responsable e innovador de las tecnologías emergentes en el ámbito distrital.

Que el artículo 228 del Acuerdo 927 de 2024 – Plan de Desarrollo Distrital “Bogotá Camina Segura 2024-2027” establece que la Secretaría General, por medio de la Oficina Consejería Distrital de Tecnologías de la Información y las Comunicaciones – TIC, debe orientar, definir estrategias y desarrollar acciones que impulsen la transformación digital y el modelo de ciudad inteligente en Bogotá, asegurando la eficiencia administrativa, el fortalecimiento del servicio a la ciudadanía y la adopción de soluciones tecnológicas de interés público.

Que el numeral 228.4 asigna expresamente a la Secretaría General, a través de la Oficina Consejería Distrital de TIC, la función de *“definir el plan de acción que permita impulsar la adopción de tecnologías emergentes, fomentando el desarrollo de Bogotá como epicentro de nuevas tecnologías especialmente (...) la implementación y aprovechamiento de la inteligencia artificial y la analítica de datos (...)”*, con el fin de mejorar la comunicación con la ciudadanía, promover el trabajo colaborativo, orientar mejores políticas públicas y apoyar decisiones más



ALCALDÍA MAYOR
DE BOGOTÁ, D.C.

ACUERDO No. 003 DE 26 DIC 2025
()

"Por el cual se adoptan lineamientos y estándares para la preparación, desarrollo, implementación, supervisión y mejora continua de los sistemas de Inteligencia Artificial en las entidades y organismos del Distrito Capital"

acertadas en asuntos estratégicos para la ciudad y la región. Esta habilitación conlleva, por su naturaleza, la facultad regulatoria interna para expedir lineamientos, estándares, directrices y guías técnicas que permitan a las entidades del Distrito implementar de manera uniforme, segura, transparente y eficaz las tecnologías de inteligencia artificial - IA.

Que, de igual manera, el numeral 228.6 dispone que la Secretaría General y la Oficina Consejería Distrital de TIC deben *"orientar y acompañar la implementación de soluciones basadas en tecnologías exponenciales o emergentes como inteligencia artificial (IA), Internet de las cosas y Blockchain, entre otras, en diversos sectores para mejorar la eficiencia y la toma de decisiones (...)"*. Esta competencia implica obligaciones de dirección, asistencia técnica y gobernanza que solo pueden materializarse mediante la emisión de lineamientos técnicos, metodológicos, operativos y éticos que permitan a las entidades distritales desarrollar y desplegar soluciones de IA bajo criterios uniformes de seguridad digital, protección de datos, transparencia, interoperabilidad, gestión de riesgos y valor público.

Que las funciones contenidas en los numerales 228.4 y 228.6 tienen naturaleza normativa-instrumental y de orientación técnica, lo que habilita a la Secretaría General, particularmente a la Oficina Consejería Distrital de TIC para dictar lineamientos de obligatorio cumplimiento en el marco de sus competencias, con fundamento adicional en el parágrafo del mismo artículo, según el cual todas las entidades distritales deben desarrollar acciones alineadas con las disposiciones que establezca la Oficina Consejería Distrital de TIC, configurándose un mandato expreso de coordinación y sujeción institucional respecto de los estándares emitidos por dicha dependencia.

Que, en consecuencia, la expedición de Lineamientos Técnicos de IA para el Distrito Capital constituye una actuación legítima, necesaria y directamente derivada de las competencias asignadas por el Acuerdo 927 de 2024, orientada a consolidar un marco común para la adopción responsable, segura, ética y eficiente de tecnologías de IA en Bogotá, en coherencia con las políticas nacionales de Gobierno Digital, seguridad digital, protección de datos y estrategias de ciudad inteligente.

Que el artículo 8 del Decreto Distrital 025 de 2021, estableció la competencia de la Comisión Distrital de Transformación Digital para impartir lineamientos o instrucciones en materia de transformación digital aplicables a todas las entidades y organismos del Distrito Capital.

Que el Acuerdo 001 de 2021 de la Comisión Distrital de Transformación Digital *"Por el cual se adopta el Reglamento Interno de la Comisión Distrital de Transformación Digital"* establece entre las funciones de esta Comisión, generar lineamientos en materia de transformación digital para el Distrito, en concordancia con los estándares que defina el Ministerio de TIC.

Que el Acuerdo Distrital 1017 de 2025 ordena la expedición de lineamientos para el uso responsable y ético de la Inteligencia Artificial en el Distrito Capital, y dispone en su artículo 2 que dichos lineamientos deberán orientarse conforme a la Política Nacional de Inteligencia Artificial vigente y al Marco Ético para la Inteligencia Artificial en Colombia, estableciendo como líneas de acción, entre otras, la adopción de modelos de clasificación y gestión de riesgos para los sistemas de IA; el fomento del uso responsable y ético de tecnologías de inteligencia artificial



ALCALDÍA MAYOR
DE BOGOTÁ, D.C.

ACUERDO No. 003 DE 26 DIC 2025
()

"Por el cual se adoptan lineamientos y estándares para la preparación, desarrollo, implementación, supervisión y mejora continua de los sistemas de Inteligencia Artificial en las entidades y organismos del Distrito Capital"

generativa en las entidades distritales; la promoción de mecanismos de participación ciudadana en soluciones de alto impacto social; el impulso de buenas prácticas de protección de datos personales; la implementación de mecanismos de supervisión humana para mitigar riesgos; y la documentación del ciclo de vida de los sistemas de IA, a efectos de garantizar su operación transparente, segura y orientada al interés público.

Que, en consecuencia, y para garantizar la observancia del principio constitucional de la función administrativa basado en la eficiencia, economía y celeridad, se hace indispensable expedir los lineamientos y estándares para la preparación, desarrollo, implementación, supervisión y mejora continua de los sistemas de Inteligencia Artificial en las entidades y organismos del Distrito Capital, en coherencia con el marco normativo nacional y distrital.

Que en sesión ordinaria adelantada el 10 de diciembre de 2025, la Comisión Distrital de Transformación Digital, en cumplimiento de sus funciones aprobó el presente Acuerdo, según consta en el Acta No. 04 de 2025.

En mérito de lo expuesto,

ACUERDA:

Artículo 1. Objeto: Adoptar los lineamientos y estándares para la preparación, desarrollo, implementación, supervisión y mejora continua de los sistemas de Inteligencia Artificial en las entidades y organismos del Distrito Capital.

En desarrollo de este objeto, los presentes lineamientos tienen como propósito garantizar un marco normativo, técnico y ético para la adopción de sistemas de IA en el Distrito Capital; su alcance es de obligatorio cumplimiento para los sujetos señalados en su ámbito de aplicación, y se articula con las políticas nacionales, distritales e internacionales vigentes en la materia. La implementación de estos lineamientos se efectuará bajo un enfoque de madurez institucional, progresividad en la adopción, promoción de la innovación y adaptación a la realidad del territorio y a las capacidades disponibles, de manera que se asegure su pertinencia, sostenibilidad y efectividad.

Parágrafo: Las entidades y organismos distritales deberán cumplir con los lineamientos y estándares técnicos de este acuerdo y sus anexos que hacen parte integral del mismo.

Artículo 2. Ámbito de aplicación: Son sujetos obligados a la aplicación del presente lineamiento las entidades del sector central, descentralizado y las localidades del Distrito Capital, correspondientes a los sectores administrativos, sus entidades adscritas y vinculadas, y los particulares que ejerzan funciones públicas dentro de la Administración Distrital conforme al Decreto Ley 1421 de 1993.

Tal como se establece en el parágrafo 2 del artículo 2.2.24.1.2 del Decreto 1078 de 2015, las personas jurídicas de derecho privado podrán aplicar las disposiciones contenidas en el presente Acuerdo siempre que no resulte contrario a su naturaleza y a las disposiciones que regulan su objeto, actividades y servicios.



ALCALDÍA MAYOR
DE BOGOTÁ, D.C.

ACUERDO No. 003 DE
(26 DIC 2025)

“Por el cual se adoptan lineamientos y estándares para la preparación, desarrollo, implementación, supervisión y mejora continua de los sistemas de Inteligencia Artificial en las entidades y organismos del Distrito Capital”

Artículo 3. Lineamientos y estándares para la preparación, desarrollo, implementación, supervisión y mejora continua de los sistemas de Inteligencia Artificial en las entidades y organismos del Distrito Capital. Los sujetos obligados deberán adoptar los lineamientos y estándares para la preparación, desarrollo, implementación, supervisión y mejora continua de los sistemas de Inteligencia Artificial en las entidades y organismos del Distrito Capital contenidos en el ANEXO LINEAMIENTOS TÉCNICOS Y ÉTICOS EN IA PARA EL DISTRITO CAPITAL DE BOGOTÁ y sus herramientas, que hacen parte integral de este Acuerdo.

Artículo 4. Actualización. Los lineamientos a que se refiere el presente Acuerdo serán actualizados cuando así se requiera. Para ello, la Oficina Consejería Distrital TIC, propondrá a la Comisión las actualizaciones del anexo aquí adoptado, para su revisión y aprobación.

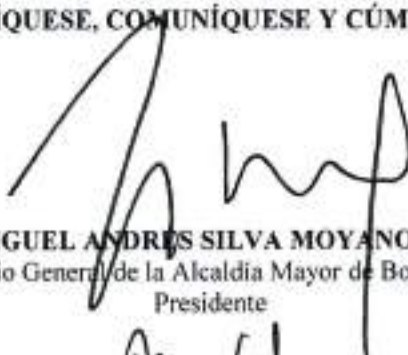
Parágrafo. Las distintas versiones deberán estar publicadas en la sede electrónica de la Secretaría General, por conducto de la Oficina Consejería Distrital de TIC.

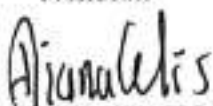
Artículo 5. Vigencia y derogatoria. El presente Acuerdo rige a partir del día siguiente a la fecha de su publicación, y deroga las disposiciones que le sean contrarias.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dado en Bogotá D. C., a los

26 DIC 2025


MIGUEL ANDRÉS SILVA MOYANO
Secretario General de la Alcaldía Mayor de Bogotá D.C.
Presidente


DIANA ROCIO CELIS MORA
Jefe Oficina Consejería Distrital de TIC
Secretaría General de la Alcaldía Mayor de Bogotá D.C.
Secretaría Técnica

Revisó: Felipe Valencia Serrano – Asesor 
Adriana Elena Martínez Díaz – Asesor 

ANEXO
LINEAMIENTOS TÉCNICOS Y ÉTICOS EN LA PARA EL DISTRITO CAPITAL
DE BOGOTÁ

003

1. ACRÓNIMOS

1.1. METODOLOGÍAS Y CICLO DE VIDA

Stage-Gate®: Marco de decisión por “puertas” (gates) para proyectos.

CRISP-DM: *Cross-Industry Standard Process for Data Mining* (Proceso Estándar para Minería de Datos).

TDSP: *Team Data Science Process* (Proceso de Ciencia de Datos en Equipo).

KDD: *Knowledge Discovery in Databases* (Descubrimiento de Conocimiento en Bases de Datos).

MLOps: *Machine Learning Operations*

OCDE / OECD: Organización para la Cooperación y el Desarrollo Económicos (ciclo de vida de IA de la OCDE).

1.2. ÍNDICES, PUNTAJES Y RUTAS

IGD: Índice de Gobierno Digital (promedio de 11 elementos/ subíndices).

PDP: Puntaje por Determinantes del Proyecto (ponderación de factores internos). Indicador que mide la preparación institucional y técnica de un proyecto de inteligencia artificial mediante la ponderación de ocho factores internos —planeación estratégica, financiación, alcance, sostenibilidad, estado de ejecución, criticidad, manuales y tratamiento de datos personales— valorados en una escala de 0, 5 o 10 (o 0/10 para infraestructura crítica) y ponderados con pesos que suman 100. Su cálculo se realiza aplicando la fórmula $(\text{Valor}/10) \times \text{Peso}$ para cada factor, obteniendo un resultado total entre 0 y 100 que refleja la madurez interna del proyecto y sirve como insumo para el Índice Compuesto de Madurez $(\text{ICM} = 0,40 \times \text{IGD} + 0,60 \times \text{PDP})$, donde el IGD representa el nivel de madurez de la Política de Gobierno Digital y el PDP la capacidad de gestión institucional del proyecto.

ICM: Índice Compuesto de Madurez $= 0,40 \times \text{IGD} + 0,60 \times \text{PDP}$.

ICC/SE: Infraestructura Crítica Cibernética / Servicio Esencial (Decreto Nacional 88/2022 y Decreto 472 de 2024 Alcaldía Mayor de Bogotá, D.C.).

EIA / AIA: Evaluación de Impacto Algorítmico / *Algorithmic Impact Assessment*.

DPIA: *Data Protection Impact Assessment* (Evaluación de Impacto en Protección de Datos).

KPI: *Key Performance Indicator* (Indicador Clave de Desempeño).

OKR: *Objectives and Key Results* (objetivos y resultados clave).

ODS: Objetivos de Desarrollo Sostenible de la ONU.

1.3. GOBERNANZA, DATOS Y SEGURIDAD

TIC: Tecnologías de la Información y las Comunicaciones.

PETI: Plan Estratégico de Tecnologías de la Información.

PEI: Plan Estratégico Institucional.
POAI: Plan Operativo Anual de Inversiones.
CDP: Certificado de Disponibilidad Presupuestal.
CRP: Registro/Compromiso de Recursos Presupuestales.
CAPEX / OPEX: Gasto de capital / gasto operativo.
SOP: *Standard Operating Procedure* (procedimiento operativo estándar).
RACI: *Responsible, Accountable, Consulted, Informed* (matriz de roles).
V&V: *Verification & Validation* (verificación y validación).
SLA: *Service Level Agreement* (Acuerdo de Nivel de Servicio).
IR: *Incident Response* (respuesta a incidentes).
MTTD / MTTR: *Mean Time to Detect / Mean Time to Restore* (Tiempo Medio de Detección / de Restauración).
US / OPS: Usuarios / Ops (Operaciones) — usado en “manuales US/OPS/Soporte”.

Nota. Para efectos de lo establecido en este lineamiento, se tendrán en cuenta las definiciones establecidas en la Resolución MinTIC 460 de 2022 y sus documentos técnicos, los Decretos Nacionales 1389 de 2022 y la Política de Gobierno Digital – Decreto Nacional 767 de 2022, ambos compilados en el Decreto Nacional 1078 de 2015 y los Decretos Distritales 76 de 2013, 608 de 2022, 575 de 2023 y en otras guías y marcos expedidos por el Gobierno Nacional o las señaladas en las normas técnicas que correspondan.

2. OBJETO

Establecer los lineamientos y estándares para la preparación, desarrollo, implementación, supervisión y mejora continua de los sistemas de Inteligencia Artificial en el Distrito Capital, con la finalidad de que su adopción contribuya de manera directa al cumplimiento de los fines esenciales del Estado.

En desarrollo de este objeto, los presentes lineamientos tienen como propósito garantizar un marco normativo, técnico y ético para la adopción de sistemas de IA en el Distrito Capital; su alcance es de obligatorio cumplimiento para los sujetos señalados en su ámbito de aplicación, y se articula con las políticas nacionales, distritales e internacionales vigentes en la materia. La implementación de estos lineamientos se realizará bajo un enfoque de madurez institucional, progresividad en la adopción, promoción de la innovación y adaptación a la realidad del territorio y a las capacidades disponibles, de manera que se asegure su pertinencia, sostenibilidad y efectividad.

3. ÁMBITO DE APLICACIÓN

Son sujetos obligados a la aplicación del presente lineamiento las entidades del sector central, descentralizado y las localidades del Distrito Capital, correspondientes a los sectores administrativos y sus entidades adscritas y vinculadas y los particulares que ejerzan funciones públicas dentro de la Administración Distrital conforme al Decreto Ley 1421 de 1993.

Tal como se establece en el parágrafo 2 del artículo 2.2.24.1.2 del Decreto Nacional 1078 de 2015, las personas jurídicas de derecho privado podrán aplicar las disposiciones contenidas en el presente Decreto siempre que no resulte contrario a su naturaleza y a las disposiciones que regulan su objeto, actividades y servicios.

4. MODELO DE PREPARACIÓN E IMPLEMENTACIÓN DEL LINEAMIENTO DISTRITAL DE INTELIGENCIA ARTIFICIAL (MPIA-BOGOTÁ)

4.1. Finalidad

El Modelo de Preparación e Implementación del Lineamiento Distrital de Inteligencia Artificial (MPIA-Bogotá) constituye el marco de gestión integral que orienta la adopción, despliegue y mejora continua de los proyectos de inteligencia artificial en el Distrito Capital.

Su finalidad es garantizar que la preparación e implementación de la inteligencia artificial se realice bajo principios de legalidad, transparencia, seguridad digital, protección de datos personales, ética pública y responsabilidad institucional, asegurando que cada fase del proceso sea trazable, verificable y sujeta a mejora continua.

El MPIA-Bogotá se estructura sobre el ciclo de gestión PHVA (Planear, Hacer, Verificar y Actuar), lo cual permite gestionar de manera progresiva y controlada todo el ciclo de vida de los proyectos de inteligencia artificial, conforme a los estándares de gestión pública distrital y las políticas nacionales de Gobierno Digital.

4.2. Alcance

Los presentes lineamientos se aplican a los sistemas, técnicas, modelos y soluciones tecnológicas que, en cualquier fase de su ciclo de vida (diseño, desarrollo, pruebas, despliegue, mantenimiento u operación), realicen tratamiento automatizado o semiautomatizado de datos mediante métodos estadísticos, reglas avanzadas, modelos de aprendizaje automático o técnicas generativas, y cuyos resultados tengan la potencialidad de apoyar, complementar o automatizar decisiones

institucionales, interactuar con la ciudadanía o producir efectos administrativos directos o indirectos.

El alcance se determina por la naturaleza técnica del sistema y por su impacto institucional y social, bajo un enfoque de riesgo que exige obligaciones diferenciadas según el nivel de impacto del sistema sobre derechos, servicios o procesos misionales.

Entre otros, quedan comprendidas las siguientes categorías de sistemas y tecnologías:

a) Automatización avanzada y Automatización Robótica de Procesos (RPA) con impacto administrativo

Incluye automatizaciones que generen efectos administrativos, modifiquen registros, realicen validaciones automatizadas o procesen información sensible o crítica. Cuando la automatización sea puramente mecánica y sin impacto en decisiones, podrá ser exceptuada salvo que interactúe con datos sensibles.

b) Analítica predictiva y modelos de aprendizaje automático

Sistemas que anticipan comportamientos, estiman probabilidades o predicen eventos relevantes para la gestión pública. Requieren validación periódica, gestión de sesgos y trazabilidad de variables.

c) Sistemas de recomendación o priorización algorítmica

Modelos que sugieren acciones, asignan recursos, priorizan beneficiarios o influyen en la toma de decisiones institucionales. Deben garantizar explicabilidad, criterios verificables y responsabilidad humana final.

d) Chatbots, asistentes virtuales y sistemas de interacción automatizada

Siempre que atiendan consultas, tramiten información o interactúen con la ciudadanía, deben cumplir obligaciones reforzadas de transparencia, derechos digitales del administrado, supervisión humana y protección de datos.

e) Visión por computador y análisis automatizado de imágenes o video

Aplicaciones utilizadas para verificación de obras, monitoreo de infraestructura, vigilancia ambiental o análisis urbano. Requieren controles de calidad, gestión del riesgo de identificación y supervisión humana significativa.

f) Reconocimiento óptico de caracteres (OCR) con extracción automatizada

Incluye OCR tradicional y OCR enriquecido con modelos lingüísticos, cuando sus resultados alimenten decisiones administrativas o procesos operativos. Requiere validación de exactitud y controles de integridad.

g) Sistemas de Inteligencia Artificial Generativa

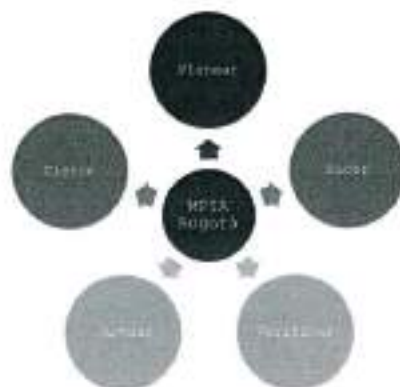
Modelos capaces de producir texto, audio, imágenes, video o código, cuando su uso esté asociado a comunicaciones oficiales, soporte a decisiones institucionales o interacción con la ciudadanía. Requieren supervisión humana, controles de calidad, salvaguardas éticas y trazabilidad.

h) Tecnologías emergentes o híbridas

003

Cualquier solución tecnológica que integre técnicas estadísticas avanzadas, aprendizaje automático, modelos generativos, reglas expertas o automatización inteligente para producir resultados relevantes en procesos administrativos, incluso si no encaja exactamente en las categorías anteriores.

4.3. Ciclo PHVA (Planear, Hacer, Verificar y Actuar)



Planear

Corresponde a la Fase 1 – Preparación y Planeación del Proceso, en la que se definen los objetivos, políticas, estrategias y capacidades institucionales necesarias para la adopción responsable de la inteligencia artificial. Comprende las siguientes actividades mínimas:

- Diagnóstico de madurez institucional mediante el Índice de Gobierno Digital (IGD).
- Valoración de los factores determinantes del proyecto (PDP) y cálculo del Índice Compuesto de Madurez ($ICM = 0,40 \times IGD + 0,60 \times PDP$).
- Clasificación de la iniciativa en una ruta de madurez (Exploratoria, Consolidación o Avanzada) y verificación de si aplica la Ruta Especial ICC/SE.
- Definición del plan de trabajo y cumplimiento los actores responsables, y el repositorio digital de evidencias.

Resultado exigible: documento de inicio del proyecto que consolida su viabilidad técnica y organizacional, su nivel de madurez y la trazabilidad de los insumos necesarios para avanzar.

Hacer

Corresponde a la Fase 2 – Desarrollo, Validación y Despliegue según Madurez, en la cual se ejecutan los planes definidos y se aplican los lineamientos técnicos, éticos y de control establecidos en la Guía. Incluye las siguientes acciones mínimas:

- Cumplimiento de los requisitos generales transversales (gobernanza, transparencia, protección de datos personales y seguridad digital).
- Aplicación de los lineamientos específicos por nivel de madurez (Exploratoria, Consolidación o Avanzada).

- c) Identificación de roles, conexión con el canal distrital de comunicaciones y documentación de controles y evidencias requeridas.
- d) Utilización de los artefactos definidos en la Guía.

Resultado exigible: sistema de inteligencia artificial listo para su despliegue operativo, con todos los controles técnicos y jurídicos aplicados y evidenciados en el expediente digital del proyecto.

Verificar

Corresponde a la Fase 3 – Implementación y Seguimiento, orientada a evaluar el desempeño, la efectividad de los controles y el cumplimiento normativo del sistema de inteligencia artificial. Comprende, entre otros y según el nivel de madurez alcanzado, los siguientes componentes:

- a) Monitoreo operativo y algorítmico continuo, incluyendo métricas de desempeño y detección de drift.
- b) Gestión de incidentes y vulnerabilidades conforme a la Estrategia Distrital de Ciberseguridad del Distrito.
- c) Evaluaciones de impacto algorítmico y de protección de datos (EIA/DPIA).
- d) Auditorías internas o externas y seguimiento a indicadores de desempeño (KPI y OKR).

Resultado exigible: evidencias consolidadas.

Actuar

Esta etapa se orienta al mejoramiento continuo, la sostenibilidad y la confianza pública en los sistemas de inteligencia artificial implementados en el Distrito Capital. Incluye, como mínimo, las siguientes acciones:

- a) Reentrenamiento o actualización de modelos conforme a resultados de desempeño o nuevas obligaciones normativas.
- b) Gestión de terceros y cadena de suministro, seguimiento de SLA, licencias y cláusulas de seguridad.
- c) Auditorías periódicas y ejecución de planes de continuidad y resiliencia documentados.
- d) Cierre de ciclo y desmantelamiento responsable de los sistemas que lleguen al final de su vida útil.
- e) Actualización de políticas, procedimientos y lecciones aprendidas para retroalimentar el ecosistema distrital de inteligencia artificial.

Resultado exigible: consolidación de una cultura de mejora permanente, en la cual los aprendizajes de cada ciclo retroalimentan la madurez institucional y fortalecen la seguridad, la ética y la transparencia en el uso de la inteligencia artificial.

4.4. Cierre del modelo

El MPLA-Bogotá articula de manera progresiva los tres niveles de madurez —Exploratoria, Consolidación y Avanzada— con el ciclo PHVA, permitiendo que la gestión de la inteligencia artificial en el Distrito Capital sea planificada, controlada y evolutiva, con evidencia verificable en cada etapa y un enfoque sostenido en la confianza pública, la mejora continua y la innovación responsable.

5. FASES EN PROYECTOS DE IA DEL DISTRITO DE BOGOTÁ

Este lineamiento deberá aplicarse de manera secuencial, progresiva e incremental, en las tres fases que lo integran, asegurando en todo momento la trazabilidad, registro y conservación de las evidencias en el expediente digital del proyecto.

Las entidades responsables no requerirán aprobación previa para avanzar entre las fases, pero estarán obligadas a cumplir íntegramente los requisitos establecidos en cada una, priorizando la innovación responsable, la mejora continua y la observancia de las políticas distritales.



5.1. Fase 1 – Preparación y planeación del proceso.

La entidad deberá verificar sus capacidades institucionales mínimas, preasignar la ruta de madurez correspondiente (Exploratoria, Consolidación o Avanzada) y organizar el proyecto con base en evidencias verificables. Estas evidencias comprenden, como mínimo:

- a) El diagnóstico del Índice de Gobierno Digital (IGD).
- b) La valoración de los Factores Determinantes del Proyecto (PDP).
- c) El Semáforo por dominio del IGD, instrumento que evalúa el nivel de cumplimiento de cada uno de los once subíndices del Índice de Gobierno Digital, clasificándolos en Rojo (0–39) cuando existe un cumplimiento bajo o deficiente, Ámbar (40–69) cuando el

cumplimiento es parcial o requiere ajustes, y Verde (70–100) cuando el cumplimiento es adecuado o completo, y

- d) El Dictamen de Ruta, entendido como el resultado técnico-jurídico derivado del cálculo del Índice Compuesto de Madurez ($ICM = 0,40 \times IGD + 0,60 \times PDP$), que determina la ruta de madurez aplicable al proyecto según su nivel de preparación institucional.

La salida de esta fase es el paquete de inicio del proyecto, que debe incluir, al menos:

1. La ficha técnica del proyecto, con su objetivo, alcance, valor público esperado y población beneficiaria.
2. La clasificación de madurez asignada y su justificación.
3. El plan de trabajo, cumplimiento, agenda de trabajo responsables, y
4. El repositorio digital de evidencias, donde se almacenará toda la documentación que soporte el cumplimiento de esta fase y sirva de base para las fases siguientes.

5.2. Fase 2 – Desarrollo, validación y despliegue según madurez.

La entidad deberá cumplir requisitos generales (gobernanza, transparencia algorítmica, protección de datos y seguridad digital) y controles específicos diferenciados por ruta (Exploratoria, Consolidación, Avanzada) en materias como datos, V&V, uso responsable, obligaciones de los terceros, auditoría, propiedad intelectual/industrial y seguridad por diseño.

La salida es el sistema listo para operación con controles aplicados y evidenciados.

5.3. Fase 3 – Implementación, seguimiento y mejora continua.

La entidad deberá operar el sistema con monitoreo continuo, gestionar incidentes y riesgos, ejecutar auditorías y mejorar iterativamente los controles y el desempeño, manteniendo la documentación y trazabilidad actualizadas.

Al final del lineamiento se incluye un conjunto de plantillas (formatos de diagnóstico, fichas de transparencia, registros de datos, checklists de V&V, matrices de licenciamiento y seguridad, entre otros) que deberán usarse para documentar el cumplimiento de cada actividad y consolidar el expediente digital del proyecto.

6. FASE 1 – PREPARACIÓN Y PLANEACIÓN

6.1. Objeto, alcance y obligatoriedad

La Fase 1 tiene por finalidad verificar la capacidad institucional de la entidad para ejecutar proyectos de inteligencia artificial y definir la ruta de madurez (Exploratoria, Consolidación o Avanzada) que determinará los requisitos técnicos y de control en las fases siguientes.

Esta fase deberá realizarse antes de cualquier desarrollo, compra, uso, contratación o despliegue de IA dentro de las entidades del Distrito Capital, incluidos los proyectos ejecutados con terceros.

El cumplimiento de esta fase es obligatorio para toda iniciativa de IA. El resultado de la Fase permite el avance a las fases siguientes.

6.2. Metodología única de la fase

La Fase 1 adopta exclusivamente la metodología Stage-Gate® como sistema de decisión secuencial y controlado. Esta metodología, reconocida internacionalmente para la gestión estructurada de proyectos, divide el proceso en etapas (stages) y puntos de decisión (gates).

Cada etapa agrupa las actividades técnicas, organizacionales y documentales requeridos; cada “puerta” constituye un punto formal de decisión donde se evalúa la evidencia y se determina si el proyecto puede avanzar.

En el contexto distrital, su aplicación garantiza que:

1. Las decisiones se adopten con base en información verificable, no en apreciaciones subjetivas.
2. Cada avance quede trazado y documentado en el expediente digital del proyecto.
3. Se priorice la innovación responsable y la mejora continua, sin exigir aprobaciones previas.
4. De esta manera, Stage-Gate® opera como marco de gobernanza y control del proceso de adopción de IA en el Distrito, fortaleciendo la trazabilidad, la transparencia y la rendición de cuentas.

La metodología Stage-Gate® es plenamente compatible con los principales ciclos de vida internacionales para proyectos de IA y analítica de datos, sin modificarlos:

- **CRISP-DM (Cross Industry Standard Process for Data Mining):** la Fase 1 coincide con las etapas de *entendimiento del negocio* y *comprensión de los datos*, garantizando claridad en objetivos, fuentes y necesidades de información.
- **TDSP (Team Data Science Process – Microsoft):** la Fase 1 cubre el bloque de *Business Understanding* y parte de *Data Acquisition & Understanding*, incorporando desde el inicio requisitos jurídicos y éticos.
- **KDD (Knowledge Discovery in Databases):** la Fase 1 actúa como marco de validación institucional previo a las fases de selección, preprocesamiento y minería de datos.

- **Modelo de Ciclo de Vida de la OCDE para Sistemas de IA:** la Fase 1 se alinea con el bloque *Diseño y Planificación Responsable*, que exige verificar capacidades institucionales, riesgos, legitimidad y protección de derechos antes del desarrollo.

Esta compatibilidad permite que el Distrito integre sus proyectos de IA con estándares técnicos y éticos globales, evitando duplicidades y fortaleciendo la coherencia metodológica.

6.3. Regla de decisión

El paso entre etapas se rige por una única regla de decisión basada en el **Índice Compuesto de Madurez (ICM)**:

$$\text{ICM} = 0,40 \times \text{IGD} + 0,60 \times \text{PDP}$$

6.4. Rangos de madurez:

- 0 – 39 → **Exploratoria**
- 40 – 69 → **Consolidación**
- 70 – 100 → **Avanzada**

Condición de criticidad (obligatoria):

- Si alguno de los elementos o subíndices de Gobernanza, Seguridad y Privacidad de la Información o decisiones basadas en datos del IGD obtiene un valor inferior a 40, la ruta no podrá superar Consolidación; si es inferior a 30, será Exploratoria.
- **Infraestructura crítica o servicios esenciales (ICC/SE):**
Si el proyecto afecta infraestructuras críticas cibernéticas o servicios esenciales conforme al Decreto Nacional 88 de 2022 y Decreto Distrital 472 de 2024 o la norma que los modifique, sustituya o reemplace, se deberá activar la Ruta Especial ICC/SE, que implica:
 - La aplicación obligatoria de controles de nivel Avanzado desde la Fase 2 (ciberseguridad, continuidad operativa, explicabilidad y supervisión humana).
 - La documentación motivada de esta clasificación en la Fase 1, y con el objetivo de llevar un registro de iniciativas, las entidades podrán comunicar en esta etapa sus proyectos, a fin de que, si corresponde, se solicite el acompañamiento técnico del CDTIC.

Esta metodología proporciona la base técnica, jurídica y procedimental que permite decidir de forma uniforme si un proyecto de IA está en condiciones de avanzar o requiere fortalecimiento institucional.

6.5. Obtención de valores aplicados a la metodología

6.5.1. Índice de Gobierno Digital (IGD)

El IGD mide la madurez digital institucional en once elementos o subíndices definidos por el Ministerio TIC. El procedimiento es el siguiente:

1. Consultar la fuente oficial: acceder al portal de mediciones del MinTIC
<https://gobiernodigital.mintic.gov.co/portal/Mediciones/>

003

y obtener los valores más recientes del IGD (escala 0–100) por elemento o sub-índice o los resultados FURAG en la página web de la Función Pública.

2. Si no existen datos vigentes: realizar una autoevaluación documentada (0–100) sustentada en evidencia verificable (acto, política, informe, tablero, captura). Para eso se utilizará el formato de autoevaluación para sujetos no obligados al IDG adjunto a este documento, titulado “Autoevaluación_IGD_IA NoObligados_PDP_V1a”.
3. Registrar: fuente, fecha, versión y responsable de cada valor.
4. Aplicar el semáforo por elemento o subíndice de la política de gobierno digital:
 - 1.1.1. Rojo (0–39): cumplimiento bajo.
 - 1.1.2. Ámbar (40–69): cumplimiento parcial.
 - 1.1.3. Verde (70–100): cumplimiento adecuado.
5. Calcular el IGD: resultado del IDG de los once elementos o sub-índices.
6. Determinar si se cumple condición de criticidad.

6.5.2. Puntaje por Determinantes del Proyecto (PDP)

El PDP evalúa las condiciones internas de preparación del proyecto mediante ocho factores ponderados:

Factor	Valor (0/5/10)	Peso (%)
Inclusión en PETI	0 / 5 / 10	10
Recursos económicos asignados	0 / 5 / 10	15
Alcance institucional	0 / 5 / 10	10
Modelo de sostenibilidad	0 / 5 / 10	15
Estado de ejecución y plan de cumplimiento	0 / 5 / 10	10
Infraestructura crítica / servicio esencial	0 / 10	20
Manuales de uso y operación	0 / 5 / 10	10
Tratamiento de datos personales	0 / 5 / 10	10
Total		100

Regla de cálculo:

$$PDP = \sum ((\text{Valor} / 10) \times \text{Peso})$$

Criterios generales de asignación de valores (0, 5 o 10 puntos)

Cada valor debe sustentarse con evidencia (actos administrativos, documentos oficiales, políticas vigentes, planes o presupuestos).

Los criterios aplicables son los siguientes:

Factor	0 puntos – No cumple	5 puntos – Cumplimiento parcial o en proceso	10 puntos – Cumplimiento completo
1. Inclusión en el PETI	El proyecto no figura en el Plan Estratégico de	El proyecto figura en el PETI, pero sin metas,	El proyecto está formalmente priorizado en el PETI, con metas,

Factor	0 puntos – No cumple	5 puntos – Cumplimiento parcial o en proceso	10 puntos – Cumplimiento completo
	Tecnologías de la Información (PETI) ni en instrumentos de planeación institucional.	cronograma ni presupuesto aprobado.	responsables y cronograma definido.
2. Recursos económicos asignados	No se han identificado recursos presupuestales ni fuente de financiación.	Existe financiación parcial o temporal (solo CAPEX u OPEX, o solo para piloto).	Cuenta con recursos asignados para todo el ciclo de vida (desarrollo, mantenimiento, evaluación y sostenibilidad).
3. Alcance institucional	Impacta una sola dependencia o área operativa.	Involucra varias dependencias o unidades funcionales de la entidad.	Tiene alcance transversal en la entidad o vincula varias entidades del sector o del Distrito.
4. Modelo de sostenibilidad	No existe modelo, plan o presupuesto de sostenibilidad.	Existe un modelo, plan o presupuesto preliminar o de corto plazo (< 1 año), o; dispone de modelo, plan o presupuesto formal aprobado superior a un año, que NO cubre operación, monitoreo, actualización y formación	Dispone de modelo, plan o presupuesto formal aprobado superior a un año, que cubre operación, monitoreo, actualización y formación.
5. Estado de ejecución y plan de trabajo y de cumplimiento	El proyecto no ha iniciado o carece de plan de trabajo y cumplimiento.	Se encuentra en ejecución con plan aprobado y plazo ≤ 60 días para evidenciar cumplimiento.	Está en ejecución activa, cumple los lineamientos de IA responsable y mantiene evidencia trazable del avance.
6. Infraestructura crítica / servicio esencial (ICC/SE)	El proyecto no afecta servicios esenciales ni infraestructuras críticas, o no existe relación directa con la continuidad de operaciones públicas.	<i>No aplica (escala binaria).</i>	El proyecto afecta directamente servicios esenciales o infraestructuras críticas según el Decreto 88 de 2022, debiendo activarse la Ruta Especial ICC/SE y aplicar controles de nivel Avanzado.
7. Manuales de uso y operación	No existen manuales o guías técnicas para el sistema o proceso asociado.	Existen borradores o versiones de manuales o guías técnicas preliminares en revisión o actualizaciones en trámite o manuales que no incluyen alguna de las siguientes variables roles, flujos, soporte y	Los manuales o guías técnicas están aprobados, actualizados y divulgados, incluyen roles, flujos, soporte y mecanismos de actualización.

003

Factor	0 puntos – No cumple	5 puntos – Cumplimiento parcial o en proceso	10 puntos – Cumplimiento completo
		mecanismos de actualización	
8. Tratamiento de datos personales	No existe base jurídica ni política de tratamiento de datos; no se han identificado riesgos o controles.	Existe base jurídica y evaluación de impacto preliminar (EIA/DPIA), sin finalizar o sin publicación o sin medidas de minimización o existe (EIA/DPIA) completa y medidas de minimización, pero no cláusulas contractuales	Se cuenta con EIA/DPIA completa, medidas de minimización, cláusulas contractuales de tratamiento y avisos de privacidad vigentes.

Reglas especiales de aplicación:

1. Si el proyecto ya está en ejecución y no tiene plan de trabajo y cumplimiento aprobado, la ruta no podrá superar Consolidación hasta su aprobación formal por quien ejerce la representante de la entidad.
2. Si el proyecto afecta infraestructura crítica o servicios esenciales (ICC/SE), la entidad deberá activar la Ruta Especial ICC/SE y aplicar controles de nivel Avanzado en la Fase 2, independientemente del resultado del ICM.
3. Los valores asignados deberán registrarse junto con la fuente de evidencia, fecha y responsable en el expediente digital del proyecto.

6.5.3. Acciones que debe ejecutar la entidad

1. **Delimitar el proyecto:** definir problema público, caso de uso, valor público esperado, alcance y población o servicios impactados.
2. **Identificar actores institucionales:** Jurídica, TIC/Infraestructura, Datos/Gobernanza, Seguridad de la Información y área misional responsable.
3. **Obtener o autoevaluar el IGD:** seguir el procedimiento anterior y documentar evidencias.
4. **Calcular el PDP:** asignar valores y pesos, obtener el total y conservar la evidencia.
5. **Calcular el ICM:** aplicar la fórmula $ICM = 0,40 \times IGD + 0,60 \times PDP$ y asignar la ruta correspondiente.
6. **Aplicar reglas obligatorias:** condición de criticidad e ICC/SE cuando proceda.
7. **Elaborar documento:** en el que se consolida IGD, PDP e ICM, justificar la ruta asignada y detallar las principales brechas.

8. **Gestionar el expediente digital:** cada sujeto obligado deberá crear, custodiar y conservar el expediente electrónico del proyecto, con control de versiones y conforme a la normativa institucional de gestión documental y administración electrónica.

6.5.4. Proyectos en curso y entidades no obligadas al Índice de Gobierno Digital

- Entidades sin obligación de medición del IGD. Las entidades que no hayan sido incluidas en el último reporte del FURAG para la medición del IGD, documentarán únicamente el PDP y comenzarán en ruta Exploratoria.
- Proyectos en curso. Los proyectos de inteligencia artificial que ya se encuentren en ejecución iniciarán obligatoriamente en la Ruta Exploratoria, debiendo consolidar el Puntaje por Determinantes del Proyecto (PDP) y reunir las evidencias mínimas exigidas en la Fase 1. Una vez cumplidos dichos requisitos, podrán avanzar a la Fase 2, bajo el principio de innovación responsable y mejora continua, asegurando que toda la información y resultados queden debidamente documentados en el expediente digital del proyecto.

Para realizar las actividades descritas en este numeral, utilizar la herramienta denominada "ICM_MPIA_Bogota_V1"

6.5.5. Resultados y cierre de la fase

Salida exigible: el paquete de inicio del proyecto, que incluirá al menos:

- Ficha técnica del proyecto: objetivo, alcance, valor público, población (beneficiarios de la solución) y servicios.
- Diagnóstico IGD: valores vigentes o autoevaluación con fuente, fecha, responsable y semáforo.
- Cálculo PDP: tabla de factores con valores, pesos y evidencias.
- Documento técnico-jurídico: IGD, PDP, ICM, ruta asignada, condición de criticidad y situación ICC/SE.
- Expediente digital: estructura, responsables, fechas y control de versiones.

Con la información anterior, la Fase 1 se considera cerrada y el proyecto habilitado para avanzar a la Fase 2 sin trámite de aprobación previa. La entidad conserva la responsabilidad total sobre la veracidad de la autoevaluación y la trazabilidad de las evidencias, sujetas a verificación posterior por los órganos de control.

7. FASE 2 – DESARROLLO, VALIDACIÓN Y DESPLIEGUE SEGÚN MADUREZ

7.1. Objeto

La Fase 2 tiene por objeto establecer los requisitos, controles y evidencias que deberán cumplir las entidades distritales durante el desarrollo, validación y despliegue de los sistemas de inteligencia artificial, garantizando la observancia de los principios de legalidad, transparencia, ética pública, protección de datos personales y seguridad digital.

Esta fase traduce los resultados obtenidos en la Fase 1 (Preparación y Planeación) en acciones verificables, que aseguran la ejecución responsable y la trazabilidad documental de cada decisión técnica, jurídica o administrativa adoptada durante la construcción y despliegue del sistema.

7.2. Alcance de aplicación

La Fase 2 comprende todas las actividades de diseño técnico, validación, prueba, integración, documentación, publicación y despliegue operativo del sistema de inteligencia artificial, incluyendo los ajustes derivados de procesos de prueba, auditorías o decisiones jurídicas posteriores.

Las disposiciones contenidas en esta fase son vinculantes para las entidades distritales que implementen proyectos de IA y también para aquellos sistemas que se encuentren en operación al momento de la entrada en vigor de estos lineamientos, los cuales deberán adaptarse progresivamente a los estándares definidos en la presente fase.

7.3. Obligatoriedad y condiciones de cumplimiento

1. El cumplimiento de la Fase 2 es condición para avanzar hacia la Fase 3 (Implementación y Seguimiento). Ningún proyecto podrá pasar a etapa operativa sin haber documentado y validado los controles previstos en esta fase.
2. Cada entidad deberá gestionar su propio expediente digital del proyecto conforme a las normas de gestión documental y administración electrónica vigentes, registrando:
 - a. La fuente de la evidencia.
 - b. La fecha y versión del documento.
 - c. El responsable institucional, y
 - d. El enlace o ubicación electrónica correspondiente.
3. En los proyectos clasificados como Infraestructura Crítica Cibernética o Servicio Esencial (ICC/SE), se aplicarán controles de nivel Avanzado, sin perjuicio de la ruta de madurez obtenida en la Fase 1, en cumplimiento del Decreto Nacional 88 de 2022 y la Estrategia Distrital de Ciberseguridad.

Los sujetos obligados podrán solicitar el acompañamiento de la Consejería Distrital de TIC, en su calidad de autoridad metodológica y articuladora del ecosistema de inteligencia artificial, la cual podrá verificar ex post el cumplimiento de los requisitos establecidos en esta fase y emitir observaciones o recomendaciones técnicas. Su intervención tendrá carácter orientador y no constituye un proceso de aprobación o validación previa, y su propósito será fortalecer la coherencia metodológica y documental de los proyectos.

4. Todas las actuaciones y resultados deberán estar soportados en evidencia verificable y trazable, bajo los principios de rendición de cuentas, mejora continua, innovación responsable y protección de derechos digitales.

7.4. Principios de aplicación y proporcionalidad

7.4.1. Principio de prevalencia

En caso de duda, conflicto o superposición entre los requisitos generales, los requisitos específicos por nivel de madurez o las políticas distritales vigentes, prevalecerá siempre la exigencia más estricta que brinde mayor protección al interés público, a los derechos fundamentales y a la integridad de la información.

Cuando el proyecto esté clasificado como Infraestructura Crítica Cibernética o Servicio Esencial (ICC/SE), se aplicarán los controles de nivel Avanzado en todos los casos, independientemente de la ruta de madurez asignada en la Fase 1, conforme al Decreto 338 de 2022, al Decreto Nacional 88 de 2022 y a la Estrategia Distrital de Ciberseguridad.

7.4.2. Principio de proporcionalidad

La aplicación de los controles y requisitos deberá ser proporcional al nivel de riesgo, al impacto potencial del sistema y a la ruta de madurez asignada mediante el Índice Compuesto de Madurez (ICM) (numeral 6.3 de este lineamiento).

Ningún requisito podrá implicar una carga desproporcionada o contraria al principio de eficiencia administrativa; sin embargo, no podrá reducirse el estándar mínimo fijado por los requisitos generales o por las políticas distritales obligatorias en materia de protección de datos personales, seguridad digital, transparencia pública y gobierno abierto.

7.4.3. Principio de coherencia metodológica

Los controles establecidos en esta fase deberán aplicarse de forma coherente con los resultados obtenidos en la Fase 1, garantizando que la ejecución técnica del proyecto se mantenga alineada con:

- a. La ruta de madurez (Exploratoria, Consolidación o Avanzada).
- b. La criticidad de los elementos o subíndices del IGD identificados, y
- c. Las acciones de mejora y mitigación de riesgos previstas en el dictamen técnico-jurídico de la fase anterior.

La coherencia metodológica busca evitar duplicidades, inconsistencias o retrocesos en la gestión del proyecto, asegurando una transición ordenada entre planeación, desarrollo y operación.

7.4.4. Principio de trazabilidad y evidencia

Toda acción, decisión o medida adoptada durante la Fase 2 deberá estar debidamente documentada, fechada y firmada por el responsable institucional correspondiente.

Las evidencias deberán conservarse en el expediente digital del proyecto, con identificación de:

003

- La fuente original del documento,
- La fecha y versión,
- El responsable técnico o jurídico, y
- El enlace o ubicación electrónica.

7.5. Requisitos Generales Transversales

Los requisitos generales transversales son de cumplimiento obligatorio para todas las entidades distritales, sin distinción de ruta de madurez. Constituyen el marco mínimo técnico-jurídico para la ejecución responsable de los proyectos de inteligencia artificial, y su cumplimiento verificable condiciona el avance de la Fase 2.

Cada entidad deberá conservar las evidencias respectivas en su expediente digital, con identificación de fuente, fecha, responsable y versión, conforme a las normas de gestión documental y administración electrónica.

7.5.1.1. Gobernanza institucional

Objeto

Garantizar que cada proyecto de IA se articule con las políticas distritales vigentes, los planes de transformación digital y los once elementos o subíndices del Índice de Gobierno Digital (IGD), en coherencia con las funciones, competencias y responsabilidades de la entidad.

Obligaciones

- Identificar las políticas, planes o lineamientos distritales aplicables al proyecto de IA, en relación con los once elementos del IGD.
- Elaborar y mantener actualizada una matriz de alineación institucional, que evidencie cómo el proyecto contribuye al cumplimiento de dichos elementos y políticas.
- Registrar y conservar en el expediente digital del proyecto la versión vigente de la matriz de alineación, indicando la fecha de actualización, responsables institucionales y fuentes de verificación.

Resultado exigible

Matriz de alineación institucional actualizada, archivada en el expediente digital, con trazabilidad de responsables, fecha de corte y evidencias que acrediten la articulación del proyecto con las políticas distritales y el IGD. Para ello, utilizar la herramienta denominada “Matriz_Alineacion_Institucional_IGD_IA_V1”.

7.5.2. Roles y responsabilidades institucionales

Objeto

Definir con claridad las funciones y competencias de todos los actores involucrados en el ciclo de vida del proyecto de IA.

Obligaciones

- Identificar a los puntos focales o responsables en las áreas de Jurídica, TIC/Infraestructura, Datos/Gobernanza, Seguridad de la Información y dependencia misional correspondiente. Cuando no existan dichas dependencias se identificará los responsables en virtud del cumplimiento de las obligaciones aquí señaladas.

- En proyectos con proveedores externos, incluir los contactos del contratista o socio tecnológico, y designar un responsable institucional de supervisión o interventor.

Resultado exigible

Listado oficial de roles y responsabilidades (“quién hace qué”) archivado y actualizado en el expediente digital. Para ello, utilizar la herramienta denominada “Matriz_Roles_Responsabilidades_IA_V1”.

7.5.2.1.1. Conexión con el canal distrital de comunicaciones

Objeto

Asegurar la interoperabilidad comunicativa con el canal distrital de atención y gestión de incidentes, PQRS, transparencia y seguridad digital, conforme a la Resolución 1519 de 2020 (MinTIC) o la que modifique, sustituya o reemplace y las disposiciones de la Secretaría General De la Alcaldía Mayor.

Obligaciones

- Integrar el proyecto al canal distrital de comunicaciones disponible en <https://bogota.gov.co/servicios/bogota-te-escucha> o el que haga sus veces, registrando su punto de conexión y responsable de escalamiento.
- Documentar el flujo de reporte, recepción, clasificación y cierre de inquietudes, solicitudes o incidentes asociados al sistema de IA.
- Verificar la operatividad del canal mediante una prueba de recepción (ticket o caso de prueba) y conservar la evidencia.

Resultado exigible

Conexión al canal distrital con evidencia de prueba operativa y responsable designado.

7.5.2.1.2. Línea base de factores determinantes del proyecto (PDP)

Objeto

Actualizar la línea base de los factores determinantes del proyecto definida en la Fase 1, para permitir el seguimiento continuo de la madurez institucional durante el desarrollo.

Obligaciones

- Registrar la línea base con fecha de corte, responsable, valor de cada factor y evidencia asociada.
- Actualizarla cuando se modifique cualquiera de los factores determinantes (financiación, alcance, sostenibilidad, plan de cumplimiento, infraestructura crítica, manuales, tratamiento de datos).
- Conservar la trazabilidad histórica de los cambios en el expediente digital.

003

- Si el proyecto es ICC/SE, consignar la justificación y mantener activa la conexión con el canal distrital para gestión de incidentes críticos.

Resultado exigible

Matriz de línea base PDP actualizada y archivada en el expediente digital con fecha de corte y validación institucional. Para ello, utilizar la herramienta denominada “Matriz_Línea Base_Factores Determinantes Proyecto_VI”.

7.5.2.2. Obligaciones Generales

Con el fin de asegurar la coherencia institucional, la protección de derechos y la adopción responsable de tecnologías de inteligencia artificial en el Distrito Capital, todas las entidades distritales deberán dar cumplimiento a las siguientes Obligaciones Generales, aplicables sin distinción de la fase del proyecto, del tipo de tecnología utilizada o de la ruta de madurez asignada. Estas obligaciones complementan los requisitos específicos ya definidos en este lineamiento y deberán reflejarse en las líneas de acción, políticas internas, documentos técnicos y expediente digital de cada iniciativa.

7.5.2.2.1. Modelo de clasificación de riesgos para sistemas de IA

Las entidades deberán adoptar un modelo institucional de clasificación de riesgos aplicable a todos los proyectos de IA, que permita identificar, valorar y categorizar los riesgos técnicos, jurídicos, éticos, sociales y operativos asociados al sistema.

El modelo deberá, como mínimo:

- Definir niveles de riesgo (por ejemplo: bajo, medio, alto, crítico).
- Establecer criterios objetivos de clasificación basados en impacto y probabilidad.
- Determinar los controles mínimos obligatorios según el nivel de riesgo identificado.
- Documentar los resultados de la evaluación en el expediente digital del proyecto.

Nivel de riesgo	Descripción general	Criterios de Impacto	Criterios de Probabilidad
1. Bajo	Sistemas de apoyo operativo o uso cotidiano, sin incidencia directa en decisiones institucionales ni afectación a derechos. Daños reversibles y alcance limitado.	• No afecta decisiones administrativas. • No procesa datos personales sensibles. • No interactúa directamente con la ciudadanía. • Impacto institucional menor o nulo.	• Baja probabilidad de error material. • Archivos y procesos de baja complejidad. • Poca exposición pública. • Baja posibilidad de sesgo o mal funcionamiento.
2. Medio	Sistemas que apoyan decisiones operativas internas o procesos administrativos no discrecionales, con impacto moderado en operaciones o servicios.	• Puede influir en clasificaciones o priorizaciones operativas. • Procesa datos personales no sensibles. • Genera efectos moderados sobre servicios internos.	• Probabilidad media de error o sesgo. • Dependencia parcial de datos de calidad variable. • Exposición operativa moderada.

Nivel de riesgo	Descripción general	Criterios de Impacto	Criterios de Probabilidad
3. Alto	Sistemas que influyen en decisiones administrativas, asignación de recursos, prestación de servicios o interacción directa con la ciudadanía.	• Afecta acceso a servicios o beneficios. • Procesa datos sensibles o información reservada. • Interactúa con ciudadanía y grupos vulnerables • Impacto significativo en derechos o procesos misionales.	• Probabilidad relevante de error con impacto institucional o jurídico. • Complejidad técnica alta. • Exposición pública considerable. • Riesgo elevado de sesgo o errores sistémicos.
4. Crítico	Sistemas cuyo mal funcionamiento puede generar afectación grave o irreversible a derechos fundamentales, seguridad pública, infraestructura crítica o servicios esenciales.	• Incide en decisiones de alto impacto social o jurídico. • Relacionado con servicios esenciales o infraestructura crítica. • Potencial daño grave o irreversible.	• Incluso baja probabilidad implica consecuencias severas. • Alta complejidad o inestabilidad técnica. • Riesgo extremo de impacto reputacional, jurídico o social.

7.5.2.2.2. Uso responsable y ético de sistemas de Inteligencia Artificial Generativa

Toda entidad que utilice, desarrolle o integre sistemas de IA Generativa como mínimo deberá:

- Establecer los usos permitidos y no permitidos de la IA Generativa en la entidad.
- Garantizar supervisión y validación humana previa a cualquier contenido o resultado que produzca efectos administrativos, comunicacionales o sobre la ciudadanía.
- Implementar salvaguardas para prevenir sesgos, errores significativos, desinformación, inferencias indebidas o afectaciones a derechos fundamentales.
- Conservar evidencia de dichas medidas en el expediente digital del proyecto.

7.5.2.2.3. Participación ciudadana en proyectos de alto impacto social

Los proyectos de IA que generen impactos significativos en derechos, acceso a servicios públicos, asignación de beneficios o poblaciones vulnerables deberán incluir mecanismos de participación ciudadana en su diseño, validación o implementación.

Las entidades deberán garantizar:

- Información clara y accesible sobre el proyecto y sus implicaciones.
- Mecanismos de diálogo, consulta o retroalimentación cuando corresponda.
- Registro documentado de los aportes recibidos y de su incorporación o tratamiento.

7.5.2.2.4. Etiquetado de contenido generado por IA en comunicaciones oficiales

Cuando una entidad utilice contenido creado, asistido o modificado mediante sistemas de IA, deberá adoptar estándares de etiquetado que permitan a la ciudadanía identificar de forma clara, visible y verificable el origen algorítmico del contenido.

Las obligaciones mínimas comprenden:

- a) Indicación explícita cuando el contenido oficial ha sido total o parcialmente generado por IA.
- b) Inclusión de metadatos o mecanismos técnicos de verificación cuando sea posible.
- c) Documentación de los procedimientos de etiquetado y validación en el expediente digital.

(Este punto completa lo que el lineamiento regula únicamente en relación con chatbots; aquí se incorpora la obligación respecto al contenido institucional generado por IA.)

7.5.2.2.5. Supervisión humana significativa en procesos automatizados

Además de los controles por nivel de madurez, toda entidad deberá contar con mecanismos de supervisión humana efectiva en cualquier proceso automatizado que pueda afectar derechos, decisiones administrativas o la prestación de servicios públicos.

Como mínimo, deberá garantizarse:

- a) Capacidad real de revisión, validación, corrección o reversión de resultados automatizados.
- b) Registro de las intervenciones humanas realizadas y de sus decisiones.
- c) Disponibilidad de personal responsable debidamente designado y capacitado.

(Este punto complementa lo existente en las rutas Consolidación y Avanzada, extendiéndolo como obligación general transversal.)

7.5.2.2.6. Criterios éticos y de responsabilidad en la contratación de soluciones de IA

En los procesos de adquisición, contratación, convenios o servicios relacionados con sistemas de IA, las entidades deberán incorporar criterios éticos, de integridad, transparencia y responsabilidad digital, incluyendo al menos:

- a) Requisitos de explicabilidad, trazabilidad y documentación técnica del sistema.
- b) Obligaciones de supervisión humana y gestión de riesgos por parte del proveedor.
- c) Garantías de cumplimiento en materia de protección de datos, seguridad digital y continuidad del servicio.
- d) Cláusulas explícitas sobre responsabilidades en caso de fallos, sesgos o resultados indebidos.

7.5.2.3. Transparencia Algorítmica

Objeto

Garantizar la transparencia activa y pasiva de los sistemas de inteligencia artificial utilizados por las entidades distritales, en los términos de la Directiva Conjunta No. 007 de 2025 de la Procuraduría General de la Nación y la Defensoría del Pueblo, o de la norma que la complemente, modifique o sustituya.

El cumplimiento de estas obligaciones constituye un requisito transversal de la Fase 2 y debe documentarse con evidencia verificable en el expediente digital del proyecto.

7.5.2.4. Transparencia activa y pasiva

Las entidades deberán garantizar la transparencia activa mediante la publicación periódica y accesible de información relevante sobre el diseño, propósito, funcionamiento y efectos del sistema de IA, y la transparencia pasiva mediante la atención oportuna, completa y comprensible de solicitudes de información relacionadas con el mismo.

Toda información publicada o entregada deberá presentarse en lenguaje claro y accesible, asegurando la comprensión por parte de la ciudadanía y el respeto a los principios de la Ley 1712 de 2014.

Contenido mínimo de divulgación

Las entidades deberán publicar, como mínimo, la siguiente información en sus sitios web oficiales y mantenerla actualizada en el menú de transparencia y acceso a la información pública de acuerdo con el artículo 2.4.2. del numeral 9 del anexo 2 de la Resolución 1519 de 2019 o la que haga sus veces:

- a) Nombre del sistema y versión.
- b) Propósito y uso previsto del sistema de IA.
- c) Función institucional o proceso en el que se utiliza.
- d) Estado del sistema (en desarrollo, implementado, suspendido o discontinuado).
- e) Indicación expresa sobre si el sistema trata datos personales.
- f) Tipología general de datos utilizados (sin incluir datos sensibles o identificables).
- g) Entidad o proveedor responsable del desarrollo o mantenimiento.
- h) Canales de contacto para objeciones, solicitudes o aclaraciones, con los plazos previstos en el artículo 12 de la Directiva y en el artículo 14 de la Ley 1755 de 2015.
- i) Fecha de última actualización de la información.

Esta publicación deberá realizarse con actualización anual o cada vez que el sistema sufra cambios sustanciales, asegurando que el contenido sea verificable y esté disponible en formato accesible.

Sistemas suspendidos o discontinuados

Cuando un sistema de IA sea suspendido o discontinuado, la entidad deberá publicar dentro de los tres (3) meses siguientes la información relativa a la fecha y las razones de la decisión, indicando si existe o no sustituto tecnológico. Esta información deberá permanecer disponible en los canales oficiales durante al menos doce (12) meses posteriores a la publicación. Dicha publicación se realizará en el menú de transparencia y acceso a la información pública de acuerdo con el artículo 2.4.2. del numeral 9 del anexo 2 de la Resolución 1519 de 2019 o la que haga sus veces.

Reutilización de componentes o código

Si el sistema de IA reutiliza componentes, módulos o código de otro sistema, la entidad deberá informar en los mismos términos del artículo anterior:

- El nombre y propósito del sistema de origen.

003

- Las funcionalidades heredadas o adaptadas, y
- Las razones técnicas o administrativas de la reutilización.

La información deberá conservarse en el expediente digital y estar disponible al público en los medios institucionales.

Canal para objeciones y solicitudes de revisión

Las entidades deberán disponer de canales de peticiones, quejas y reclamos del distrito capital para recibir objeciones o solicitudes de revisión frente a decisiones total o parcialmente automatizadas.

Deberán garantizar que:

- a) La ciudadanía conozca qué área es responsable de atender dichas solicitudes.
- b) Se definan plazos de recepción y respuesta que aseguren el debido proceso y la corrección o explicación de la decisión.
- c) Los canales sean interoperables con el canal distrital de PQRS y transparencia.

El trámite deberá documentarse con resolución o informe que contenga la respuesta de fondo y los fundamentos técnicos y jurídicos aplicados.

Sistemas con impacto o riesgo elevado

Cuando un sistema de IA se utilice para cualquiera de los siguientes fines, se aplicarán exigencias reforzadas de divulgación:

1. Asignación o denegación de beneficios, subsidios o servicios públicos.
2. Predicción o evaluación de riesgos (criminalidad, fraude, reincidencia, deserción, entre otros).
3. Elaboración de perfiles individuales o colectivos.
4. Inferencia de emociones o rasgos personales.
5. Atención de niños, niñas, adolescentes, personas mayores o poblaciones en situación de vulnerabilidad.
6. Diagnóstico, pronóstico o acompañamiento en salud física o mental.

Se deberá informar adicionalmente la siguiente información:

- a) Criterios o variables principales de decisión (sin divulgar secretos industriales o medidas de seguridad).
- b) Explicación del uso del sistema en lenguaje claro (técnico, jurídico o administrativo).
- c) Análisis de impacto algorítmico (AIA) que incluya hallazgos, sesgos, riesgos y afectaciones diferenciadas.

- d) Medidas de mitigación aplicadas (revisión humana, supervisión continua, mejoras).
- e) Procedimientos de objeción y revisión, con canales, plazos y posibles resultados.
- f) Información sobre entrenamiento o reentrenamiento, origen y tipo de datos, y medidas adoptadas para prevenir sesgos estructurales.

Los resultados de las auditorías o análisis de impacto deberán publicarse en resumen, manteniendo confidencialidad sobre los datos sensibles o información protegida.

Nota: La entidad podrá incorporar en la documentación pública de sus proyectos de inteligencia artificial la información relativa a las variables, heurísticas, limitaciones y supuestos del modelo, así como las métricas empleadas para evaluar su rendimiento y el margen de error o desviación estadística del sistema, de acuerdo con la naturaleza y finalidad del proyecto. Esta información se divulgará según corresponda, garantizando el equilibrio entre la transparencia técnica, la protección de la seguridad digital y la reserva legítima de información sensible, y atendiendo en todo caso al principio de máxima publicidad previsto en la Ley 1712 de 2014 y demás normas aplicables en materia de acceso a la información pública.

Análisis de impacto algorítmico y auditorías

Para los sistemas mencionados en el apartado anterior, la entidad deberá realizar un análisis de impacto algorítmico previo al despliegue, documentando riesgos, sesgos, afectaciones diferenciadas y medidas de mitigación. Asimismo, deberá prever auditorías algorítmicas periódicas y evaluaciones ex post sobre el impacto en derechos humanos, igualdad, no discriminación y género.

Las auditorías podrán ser internas o externas, y sus conclusiones deberán incorporarse al expediente digital y, cuando no existan causales de reserva, ser publicadas en el portal institucional.

Interacción con asistentes virtuales, chatbots y plataformas omnicanal.

Cuando la ciudadanía interactúe con un sistema automatizado, asistente virtual o plataformas omnicanal, la entidad deberá informarlo de forma clara, visible y previa al inicio de la interacción, indicando que la respuesta es generada por un sistema de IA.

El aviso deberá formularse en lenguaje comprensible, garantizar el consentimiento informado y asegurar la opción de escalamiento a intervención humana cuando sea pertinente.

Si a la fecha de entrada en vigor del presente lineamiento existen asistentes virtuales, chatbots o plataformas omnicanal, dicha obligación se cumplirá en dentro de los 12 meses siguientes.

Transparencia pasiva y respuesta a solicitudes

Los sujetos obligados deberán garantizar el derecho de acceso a información sobre sistemas de IA conforme a la Ley 1712 de 2014 y la Ley 1755 de 2015, respondiendo dentro de los plazos legales con información clara, completa y verificable.

Solo podrá denegarse el acceso mediante una causal de reserva expresa, debidamente motivada y sustentada en norma vigente.

El procedimiento, las solicitudes y las respuestas deberán quedar documentadas en el expediente digital del proyecto.

003

Código fuente o explicación significativa

Ante solicitudes relacionadas con el código fuente del sistema, la entidad deberá aplicar el test de daño para decidir si procede la publicación del código o la entrega de una “explicación significativa”, en lenguaje claro, que permita comprender cómo el sistema toma decisiones.

La explicación deberá incluir, de manera no técnica, los criterios, pesos o parámetros relevantes que influyen en los resultados, garantizando comprensión sin comprometer la seguridad, la propiedad intelectual o la integridad del sistema.

Entrega del código fuente

Si, tras aplicar el test de daño, la entidad decide entregar el código fuente, deberá hacerlo mediante acta de entrega que establezca expresamente:

- a) La prohibición de uso comercial.
- b) La prohibición de usos que afecten la seguridad o integridad del sistema.
- c) La prohibición de reproducción o redistribución no autorizada.

El incumplimiento de estas condiciones generará responsabilidad civil, penal o administrativa, conforme al régimen legal aplicable.

Excepciones y test de daño

El acceso podrá denegarse únicamente cuando la información solicitada esté amparada por una causal de reserva expresa y la entidad demuestre, mediante test de daño, que:

- a) Existe una finalidad constitucional o legalmente legítima para la reserva.
- b) La causal invocada está prevista en la ley.
- c) El acceso produciría un daño presente, probable y específico a un interés público o particular, y
- d) El daño potencial supera el interés público del acceso.

La carga de la prueba corresponde exclusivamente a la entidad que deniega la información.

7.5.2.5. Protección de Datos Personales

Objeto

Garantizar que todo sistema o proyecto de inteligencia artificial desarrollado, adquirido o utilizado por las entidades del Distrito Capital cumpla íntegramente con la Política Distrital de Protección de Datos Personales, y con las disposiciones contenidas en la Ley 1581 de 2012, su Decreto Reglamentario 1377 de 2013, y las normas que los modifiquen, complementen o sustituyan.

Obligaciones de las entidades

1. Aplicar la Política Distrital de Protección de Datos Personales, asegurando su cumplimiento en todas las fases del ciclo de vida del sistema de IA.
2. Verificar y dejar documentado si el sistema realiza o no tratamiento de datos personales, señalando la base jurídica, la finalidad y las medidas de seguridad implementadas.
3. Conservar evidencia verificable en el expediente digital del proyecto, incluyendo:
 - Enlace oficial a la Política Distrital de Protección de Datos Personales.
 - Identificación del responsable institucional de cumplimiento, y
 - Constancia o registro que acredite la aplicación de la política.
4. Cuando el tratamiento implique datos personales sensibles o datos de niños, niñas o adolescentes, deberán aplicarse los controles reforzados de seguridad, confidencialidad y minimización, conforme a la normatividad vigente.
5. En caso de contratación con terceros, la entidad deberá incorporar cláusulas específicas de protección de datos personales en los contratos o convenios que soporten el proyecto.

Evidencia y control

El cumplimiento de este requisito deberá estar documentado y trazable en el expediente digital del proyecto, con indicación de la fuente, fecha, responsable y versión.

7.5.2.6. Seguridad Digital

Objeto

Garantizar que todos los sistemas o proyectos de inteligencia artificial del Distrito Capital se desarrollen, desplieguen y operen conforme a la Estrategia Distrital de Ciberseguridad, aplicando controles que aseguren la confidencialidad, integridad, disponibilidad y resiliencia de la información y de los servicios digitales asociados.

Obligaciones de las entidades

1. Aplicar de forma íntegra Estrategia Distrital de Ciberseguridad, en concordancia con las normas nacionales y distritales sobre seguridad de la información, gestión del riesgo y ciberseguridad.
2. Designar un punto focal de seguridad digital para cada proyecto de IA, responsable de coordinar las acciones técnicas, preventivas y de respuesta ante incidentes.
3. Cuando el proyecto esté clasificado como Infraestructura Crítica Cibernética o Servicio Esencial (ICC/SE), deberán aplicarse los controles de nivel Avanzado, de conformidad con el Decreto Nacional 88 de 2022, Decreto Distrital 472 de 2024 y las directrices de la Consejería Distrital de TIC.
4. En los contratos con terceros, incluir cláusulas que obliguen al cumplimiento de la Estrategia Distrital de Ciberseguridad y a la adopción de medidas equivalentes de protección.

Evidencia y control

003

Cada entidad deberá conservar en el expediente digital del proyecto:

- La referencia o enlace a la Estrategia Distrital de Ciberseguridad.
- La identificación del punto focal o responsable de seguridad; y
- La constancia o documento que acredite la verificación de los controles aplicados.

7.5.3.Requisitos específicos según ruta de madurez

7.5.3.1. Nivel Exploratorio

Objeto

Definir los controles básicos que deben cumplir los proyectos de inteligencia artificial en etapa inicial o experimental, para garantizar que la innovación se realice de forma segura, responsable y documentada, sin afectar derechos ni generar riesgos no evaluados.

Alcance

Aplica a los proyectos que:

- Se encuentren en fase de idea, prototipo o piloto.
- Utilicen datos no personales o anonimizados.
- No tomen decisiones administrativas.

Controles específicos

Las entidades deberán cumplir los siguientes controles mínimos:

- Explicar con claridad qué problema público busca resolver el proyecto y cuál es el beneficio esperado para la entidad o la ciudadanía.
- Enumerar los principales riesgos técnicos, jurídicos o éticos y señalar las acciones preventivas básicas para controlarlos.
- Utilizar datos anonimizados, sintéticos o de dominio público.
- Si se requiere usar datos personales, deberá contarse previamente con autorización o evaluación de impacto en protección de datos.
- Registrar de manera sencilla el tipo de modelo o técnica utilizada (por ejemplo, clasificación, predicción, procesamiento de texto, etc.) y la fuente de datos empleada.
- Documentar las acciones anteriores, la fecha de inicio del piloto y los responsables del proyecto.

Evidencias mínimas

El expediente digital del proyecto deberá contener como mínimo:

- Documento con propósito y valor público.
- Listado de riesgos y medidas preventivas.
- Descripción técnica del modelo o herramienta utilizada.
- Evidencia del tipo y origen de los datos usados.
- Registro de comunicación al canal distrital.

7.5.3.2. Nivel Consolidación

Objeto

Fortalecer los controles técnicos, jurídicos y organizativos en proyectos de inteligencia artificial que ya superaron la fase exploratoria y cuentan con resultados o pilotos validados, garantizando que su implementación sea segura, trazable y conforme con las políticas distritales.

Alcance

Aplica a los proyectos de IA que:

- Utilizan datos reales o institucionales con base jurídica definida.
- Se encuentran en proceso de despliegue o validación ampliada, o
- Interactúan parcialmente con usuarios o procesos administrativos internos.

Controles específicos

Las entidades deberán cumplir, además de los requisitos generales, los siguientes controles adicionales:

- Elaborar un plan de trabajo con responsables, cronograma y resultados esperados, incluyendo indicadores de desempeño técnico y cumplimiento normativo.
- Revisar los riesgos identificados en la fase exploratoria, actualizarlos y clasificarlos según impacto y probabilidad, incorporando medidas de mitigación y control.
- Confirmar la existencia de una base jurídica válida y, cuando corresponda, de una Evaluación de Impacto en Protección de Datos (DPIA) de acuerdo con el artículo 2.2.17.5.2. del Decreto 1078 de 2015, vigente y archivada.
- Comprobar la precisión, estabilidad y confiabilidad del modelo mediante pruebas documentadas.

002

- Si el sistema aprende o se ajusta automáticamente, dejar registro de las condiciones de reentrenamiento.
- Si el sistema emite resultados que puedan influir en decisiones institucionales, dejar constancia de las decisiones revisadas y validadas por una persona responsable.
- Documentar, en lenguaje comprensible, cómo funciona el sistema, qué variables utiliza y cuáles son sus límites.
- Esta información deberá quedar disponible para revisión técnica, jurídica y ciudadana.
- Solicitar concepto a las áreas Jurídica y TIC sobre el cumplimiento de los lineamientos de IA, protección de datos, transparencia y seguridad digital.

Evidencias mínimas

El expediente digital deberá contener como mínimo:

- Plan de ejecución y seguimiento.
- Matriz de riesgos actualizada.
- Registro de pruebas de desempeño.
- Documentación de explicabilidad en lenguaje claro.
- Concepto jurídico-técnico de cumplimiento.

7.5.3.3. Nivel Avanzado

Objeto

Establecer los controles y evidencias exigibles para los proyectos de inteligencia artificial que se encuentren en fase operativa o de madurez avanzada, garantizando su confiabilidad, supervisión permanente, transparencia pública y mejora continua.

Alcance

Aplica a los proyectos que:

- Se encuentran en operación institucional o prestación de servicios públicos.
- Procesan datos personales o información sensible, o
- Inciden directamente en decisiones administrativas o de interés ciudadano.

En los proyectos clasificados como Infraestructura Crítica Cibernética o Servicio Esencial (ICC/SE), estos controles son obligatorios sin excepción.

Controles específicos

Las entidades deberán cumplir los siguientes controles adicionales de nivel avanzado:

- Someter el sistema a auditorías técnicas, jurídicas o algorítmicas internas o externas, al menos una vez por año o tras cambios significativos en el modelo o los datos.
- Garantizar que exista personal responsable de revisar, validar o revertir decisiones automatizadas cuando proceda, documentando los casos y actuaciones.
- Establecer un procedimiento formal para reentrenar o ajustar el modelo cuando cambien los datos, el entorno operativo o se detecten desviaciones de desempeño (drift).
- Mantener un plan documentado de continuidad del servicio y recuperación ante incidentes, que asegure la disponibilidad y la integridad del sistema.
- Implementar controles automatizados o manuales para supervisar el funcionamiento del sistema, el cumplimiento de los indicadores de desempeño (KPIs) y la detección de sesgos o errores.
- Asegurar que toda acción o decisión tomada por el sistema pueda ser rastreada y verificada, conservando los registros en el expediente digital o en los sistemas de log institucionales.
- Actualizar la evaluación de impacto (DPIA y análisis algorítmico) e incorporar las recomendaciones o acciones de mejora derivadas de auditorías o revisiones, cuando proceda. Como buena práctica puede seguirse los estándares internacionales técnicos sobre la materia, así como, las evaluaciones de impacto de protección de datos sugeridas por las autoridades de protección de datos pertenecientes a la Red Iberoamericana de Protección de Datos.

Evidencias mínimas

El expediente digital del proyecto deberá contener:

- Informe o acta de auditoría técnica o algorítmica (interna o externa).
- Registro de supervisión humana y revisiones de decisiones automatizadas.
- Procedimiento de reentrenamiento o actualización de modelo.
- Plan de continuidad y registro de pruebas de contingencia.
- Monitoreo continuo de desempeño (indicadores o reportes).
- Análisis de impacto actualizado.
- Evidencia de publicación de información de transparencia reforzada, cuando proceda.

8. FASE 3 – IMPLEMENTACIÓN, SEGUIMIENTO Y MEJORA CONTINUA

Esta fase se aplicará únicamente cuando el proyecto haya alcanzado la Ruta Avanzada (R3) y haya cumplido íntegramente todas las actividades y salidas exigibles de las Fases 1 y 2 (diagnóstico, determinación de madurez, lineamientos generales y específicos, artefactos y evidencias). Para proyectos en infraestructura crítica/servicios esenciales, esta fase deberá aplicarse con frecuencias y controles reforzados. La conformidad se presume por la existencia de evidencias verificables, sin trámites de aprobación adicionales.

8.1. Objeto y obligatoriedad

La Fase 3 – Implementación y Seguimiento tiene por objeto verificar, monitorear y mejorar el funcionamiento de los sistemas de inteligencia artificial implementados por las entidades del Distrito Capital, asegurando que su operación se mantenga dentro de los principios de legalidad, transparencia, seguridad digital, ética pública y protección de derechos.

Esta fase consolida la trazabilidad de los proyectos de IA e integra las actividades de monitoreo, gestión de incidentes, relación con terceros y mejora continua, cerrando el ciclo de gestión establecido en el Modelo de Preparación e Implementación del Lineamiento Distrital de Inteligencia Artificial (MPIA-Bogotá).

1. Cada entidad es responsable de conservar en su expediente digital los registros, reportes y auditorías que demuestren el cumplimiento de esta fase.
2. El seguimiento se realizará conforme al modelo PHVA (Planear, Hacer, Verificar y Actuar) del MPIA-Bogotá, garantizando la mejora continua del sistema.
3. El seguimiento deberá realizarse de manera coordinada entre las áreas TIC, Jurídica, Datos/Gobernanza, Seguridad de la Información y Dependencia Misional, según sus competencias.
4. Cuando participen proveedores o aliados tecnológicos, las actividades de seguimiento y reporte deberán incorporarse como obligaciones contractuales verificables.
5. Todo lo actuado deberá documentarse en el expediente digital del proyecto, con indicación de la fuente, fecha, responsable y resultado.

8.2. Monitoreo y desempeño

1. Cada entidad deberá implementar un seguimiento continuo del funcionamiento técnico y jurídico de los sistemas de inteligencia artificial en operación.
2. El monitoreo incluirá la verificación del desempeño, precisión, estabilidad y cumplimiento normativo del sistema.
3. Los indicadores mínimos de seguimiento deberán contemplar:
 - Desempeño técnico (exactitud, errores, resultados esperados).
 - Cumplimiento de políticas distritales (protección de datos, seguridad digital y transparencia).

- Registro de revisiones, reentrenamientos o ajustes realizados.
4. Las entidades podrán usar herramientas automatizadas o reportes manuales, siempre que los resultados queden documentados en el expediente digital.
 5. Cuando se detecten desviaciones, fallos o impactos no previstos, se deberán activar las acciones correctivas correspondientes y dejar constancia del seguimiento aplicado.

8.3. Gestión de incidentes y vulnerabilidades

1. Los incidentes o vulnerabilidades detectados durante la operación del sistema deberán registrarse, analizarse y resolverse conforme a la Estrategia Distrital de Ciberseguridad.
2. Los incidentes críticos deberán comunicarse de inmediato a la Consejería Distrital de TIC, siguiendo los procedimientos institucionales establecidos.

8.4. Gestión de terceros y cadena de suministro

1. Cuando el desarrollo, mantenimiento o soporte del sistema esté a cargo de proveedores, contratistas o aliados tecnológicos, se deberá comunicar el cumplimiento de las obligaciones técnicas, jurídicas y de seguridad previstas en estos lineamientos.
2. Todo contrato o convenio deberá incluir cláusulas sobre:
 - Protección de datos personales y confidencialidad.
 - Medidas de seguridad digital.
 - Trazabilidad de modelos y datos utilizados.
 - Obligación de informar incidentes o fallos.
3. La entidad deberá mantener un registro actualizado de terceros vinculados al proyecto, con sus responsabilidades, vigencias y evidencias de cumplimiento.
4. Los informes o reportes de los proveedores deberán conservarse en el expediente digital como soporte del seguimiento institucional.

8.5. Mejora continua y retroalimentación institucional

1. Las entidades deberán aplicar el enfoque de mejora continua (Actuar del ciclo PHVA) para mantener actualizados los sistemas de IA y evitar obsolescencia o pérdida de control.
2. Se deberán revisar periódicamente los resultados del monitoreo y las auditorías, actualizando los modelos o procesos cuando cambien los datos, la normativa o los objetivos institucionales.
3. Las lecciones aprendidas y los ajustes técnicos o normativos derivados del seguimiento deberán documentarse y comunicarse a la Consejería Distrital de TICE, como insumo para fortalecer el ecosistema distrital de IA.

4. Cuando corresponda, las entidades deberán actualizar sus políticas internas, manuales o protocolos, incorporando las mejoras identificadas.

8.6. Evidencia y trazabilidad

1. Todas las acciones de seguimiento, mantenimiento, auditoría o mejora deberán registrarse en el expediente digital del proyecto, con identificación de la fuente, fecha, responsable y resultado.
2. Los documentos, reportes y registros técnicos formarán parte de la trazabilidad integral del sistema y deberán conservarse conforme a las normas de gestión documental electrónica.

8.7. Cierre y efecto jurídico

1. La Fase 3 se considerará cerrada cuando la entidad haya documentado las actividades de monitoreo, gestión de incidentes, control de terceros y mejora continua.
2. El cierre deberá dejar evidencia verificable de que el sistema de IA opera de forma estable, segura y conforme con la normativa vigente.
3. Con el cierre de esta fase se completa el ciclo PHVA del Modelo de Preparación e Implementación del Lineamiento Distrital de Inteligencia Artificial (MPIA-Bogotá).
4. La entidad mantiene la responsabilidad integral sobre la operación, seguridad, transparencia y resultados del sistema, sin perjuicio de las verificaciones ex post que realicen los organismos de control.

9. LINEAMIENTOS EN EL PROCESO DE ESTRUCTURACIÓN TÉCNICA, FINANCIERA Y CONTRACTUAL DE LOS PROYECTOS DE INTELIGENCIA ARTIFICIAL

9.1. Naturaleza y objeto

El presente apartado tiene por objeto establecer los deberes y criterios que deberán aplicar las entidades distritales y los demás sujetos obligados en la planeación, estructuración técnica y financiera, contratación, ejecución y cierre de los proyectos de inteligencia artificial, en articulación con el Modelo de Preparación e Implementación del Lineamiento Distrital de IA (MPIA-Bogotá) y el Manual de Contratación Distrital, garantizando su desarrollo responsable, transparente y conforme a la normativa vigente.

Se encuentra debidamente articulado con las disposiciones contenidas en la Ley 80 de 1993, y normas reglamentarias, la Directiva 007 de 2025 de la Procuraduría General de la Nación (transparencia algorítmica) y demás normas que las modifiquen o sustituyan y tiene

9.2. Estructuración técnica y financiera (fase precontractual)

- Cada proyecto con componentes de IA deberá estructurarse conforme a la Fase I del MPIA-Bogotá, incorporando los resultados del IGD, los PDP y la ruta de madurez asignada.
- Definir el propósito, alcance, valor público y población beneficiaria.
- Identificar los datos a utilizar y su base jurídica.
- Evaluar riesgos técnicos, éticos, jurídicos y de seguridad digital.
- Verificar interoperabilidad con plataformas distritales, cuando proceda.
- Los estudios previos deberán reflejar los costos del ciclo de vida del sistema (desarrollo, validación, mantenimiento, reentrenamiento, auditorías, soporte, licencias y seguros) y garantizar sostenibilidad presupuestal por al menos tres años posteriores a la entrega.
- Cuando existan costos variables o proyectos cofinanciados, la entidad documentará el mecanismo de actualización presupuestal durante toda la vida útil del sistema.
- La modalidad contractual deberá corresponder al objeto y nivel de riesgo: consultoría IA, suministro tecnológico, servicio tecnológico o convenio interadministrativo.
- La entidad elaborará una matriz de riesgos que contemple factores técnicos, jurídicos, financieros y éticos, con medidas de mitigación y responsables de seguimiento, cuando proceda.
- La documentación exigida será proporcional a la complejidad y riesgo del proyecto, priorizando evidencia esencial verificable.
- En los procesos de selección, las entidades deberán incluir criterios técnicos de evaluación (idoneidad, modelo, seguridad, protección de datos, explicabilidad), cuando proceda.

003

9.3. Ejecución contractual (fase contractual)

- Durante la ejecución, las entidades, contratistas e interventores deberán aplicar estos Lineamientos Distritales de IA, la Estrategia Distrital de Ciberseguridad y la Política Distrital de Protección de Datos Personales.
- Todo contrato con IA incluirá, cuando proceda, cláusulas de explicabilidad, trazabilidad, documentación, propiedad intelectual, seguridad, reporte de incidentes y entrega de evidencias.
- Por regla general, los derechos patrimoniales sobre desarrollos financiados con recursos públicos pertenecerán al Distrito. Cuando se usen componentes de software libre o licencias abiertas, la entidad verificará su compatibilidad institucional, cuando proceda.
- Se exigirán garantías de cumplimiento, seguridad y continuidad del servicio proporcionales al valor y criticidad del proyecto, cuando proceda.
- El contratista desarrollará el sistema conforme a estándares técnicos, éticos y normativos; conservará evidencia en el expediente digital; cumplirá deberes de transparencia algorítmica; transferirá conocimiento y capacitará al personal designado, cuando proceda.
- El interventor verificará trazabilidad y cumplimiento técnico-jurídico; emitirá observaciones; reportará incidentes a la entidad y a la Consejería Distrital de TIC; documentará verificaciones en el expediente digital.

9.4. Cierre y sostenibilidad (fase postcontractual)

- Al cierre, el contratista entregará: código fuente, modelos entrenados, manuales y métricas; licencias, claves y configuraciones; plan de continuidad y mantenimiento posterior, cuando proceda.
- Las entidades registrarán modelos o licencias como activos intangibles conforme al marco contable público, cuando proceda; conservarán evidencia en el expediente digital.
- Las entidades documentarán las lecciones aprendidas y las remitirán a la Consejería Distrital de TIC, cuando proceda, para reforzar el ecosistema distrital de IA.
- Los proyectos en ejecución antes de la vigencia de estos lineamientos deberán adaptarse progresivamente, priorizando la documentación y la actualización de planes de cumplimiento.

9.5. Acompañamiento y coordinación institucional

La Consejería Distrital de Tecnologías de la Información y las Comunicaciones (TIC), en su calidad de autoridad metodológica y articuladora del ecosistema distrital de transformación digital e inteligencia artificial, desarrollará sus funciones en armonía con lo dispuesto en el Artículo 228 del Acuerdo Distrital 927 de 2024, en materia de transformación digital y ciudad inteligente. En cumplimiento de dicho mandato, la Consejería TIC asumirá las siguientes obligaciones institucionales y técnicas:

- Emitir lineamientos técnicos, metodológicos y operativos distritales para la adopción responsable de tecnologías emergentes—incluida la inteligencia artificial—, asegurando su coherencia con las políticas nacionales, los estándares de Gobierno Digital, la

Estrategia Distrital de Ciberseguridad y las disposiciones de protección de infraestructuras críticas y datos personales.

- Asesorar, orientar y acompañar a las entidades distritales en la formulación, ejecución y seguimiento de los proyectos de datos e inteligencia artificial, de conformidad con lo previsto en los numerales 228.4, 228.6 y 228.9 del Acuerdo 927 de 2024, promoviendo su alineación con los principios de innovación pública, transparencia y ética digital.
- Fomentar la cooperación interinstitucional y las alianzas con el sector académico, privado y social, para promover la investigación aplicada, la innovación pública digital y la experimentación tecnológica, en consonancia con el numeral 228.7 del citado Acuerdo.
- Garantizar el principio de coordinación y concurrencia entre los diferentes sectores administrativos y niveles territoriales del Distrito, de manera que todas las actuaciones en materia de tecnologías emergentes, inteligencia artificial y analítica de datos se desarrollen bajo un esquema de gobernanza común, conforme al parágrafo del Artículo 228.

10. USO COTIDIANO DE LA INTELIGENCIA ARTIFICIAL EN EL DISTRITO CAPITAL

El uso cotidiano de la inteligencia artificial corresponde a la utilización de modelos de lenguaje generativo, herramientas basadas en plataformas tipo GPT y tecnologías equivalentes, destinadas a apoyar tareas rutinarias dentro de las funciones diarias de los servidores públicos. Su naturaleza es asistencial, de bajo impacto institucional, y orientada a incrementar la productividad sin sustituir el juicio técnico, profesional o jurídico del funcionario responsable.

Se consideran actividades de uso cotidiano, entre otras:

- Generación y organización de ideas;
- Redacción, corrección, estructuración o síntesis de textos institucionales;
- Resúmenes, cálculos simples y análisis preliminares;
- Preparación de insumos para documentos, informes o presentaciones;
- Clasificación básica de información;
- Búsqueda, explicación rápida o verificación preliminar de conceptos técnicos o normativos;
- Organización de agenda, recordatorios o apoyo operativo documental.

El valor del uso cotidiano depende de la capacidad del funcionario para formular instrucciones precisas, verificar manualmente los resultados y aplicar criterio profesional antes de incorporar cualquier producto a documentos o actuaciones institucionales.

- ✓ La IA solo podrá emplearse como herramienta de asistencia para optimizar tiempos, mejorar la calidad del trabajo y facilitar tareas operativas. Está prohibido utilizar la IA cotidiana para sustituir procesos de análisis, interpretación, deliberación técnica, valoración probatoria, adopción de decisiones administrativas o formulación de políticas públicas.
- ✓ Todo contenido generado con apoyo de IA deberá ser revisado, corregido y validado por el funcionario responsable.
- ✓ La aprobación humana es condición necesaria para que cualquier producto pueda ser incorporado en:
 - Comunicaciones institucionales;
 - Documentos internos o externos;
 - Análisis administrativos o jurídicos;
 - Informes, borradores o materiales para toma de decisiones.
- ✓ El uso cotidiano de la IA no podrá:
 - Incidir en decisiones administrativas o en la motivación de actos;
 - Interpretar normas, jurisprudencia o regulaciones para producir efectos jurídicos;
 - Elaborar conceptos jurídicos, dictámenes técnicos o informes que generen efectos vinculantes;
 - Determinar prioridades, asignar recursos o producir decisiones automatizadas;
 - Sustituir a los funcionarios en tareas sustantivas de control, supervisión o evaluación.
- ✓ Está prohibido ingresar en herramientas abiertas o no institucionales de IA:
 - Datos personales o sensibles;
 - Información sujeta a reserva legal o clasificada;
 - Documentos oficiales no publicados;

- Información estratégica, contractual o financiera;
 - Archivos protegidos por propiedad intelectual o confidencialidad;
 - Datos o parámetros de sistemas críticos del distrito.
- ✓ Solo podrán tratarse insumos restringidos en entornos cerrados, seguros y aprobados institucionalmente, con:
- Autorización o a través de la ejecución de los proyectos de IA Distritales de las distintas dependencias,
 - Protocolos de anonimización o seudonimización, y
 - Registro en el expediente del proyecto o del proceso.
- ✓ Cuando un producto institucional haya sido elaborado con apoyo de IA, y la naturaleza del documento lo justifique, deberá dejarse constancia de:
- La herramienta utilizada,
 - El tipo de apoyo recibido, y
 - El alcance de la intervención humana.
- ✓ La trazabilidad es obligatoria especialmente en:
- Informes técnicos,
 - Documentos divulgados públicamente,
 - Comunicaciones oficiales, y
 - Insumos utilizados para toma de decisiones.
- ✓ La IA cotidiana solo podrá usarse para tareas de baja complejidad. No se permitirá su uso en actividades que:
- Requieran interpretación normativa,
 - Impliquen deliberación compleja,
 - Definan consecuencias jurídicas,
 - Supongan análisis de riesgos institucionales,
 - Afecten derechos fundamentales, o
 - Requieran criterios especializados.
- ✓ El servidor público es el único responsable por los contenidos producidos con apoyo de IA y por los efectos que su utilización genere en la gestión pública. La IA no genera responsabilidad autónoma ni desplaza la responsabilidad funcional del servidor.
- ✓ Queda prohibido utilizar herramientas de IA cotidiana para:
- Automatizar decisiones o acciones administrativas,
 - Generar actos administrativos o sus motivaciones,
 - Producir documentos jurídicos vinculantes,
 - Replicar información sin verificación,
 - Elaborar documentos que deban ajustarse a formatos oficiales específicos, sin revisión humana.

Cuando se requiera usar IA para estas actividades se deberá cumplir los lineamientos establecidos a partir de la ruta identificada.

- ✓ El juicio técnico, profesional y ético del funcionario prevalece siempre sobre cualquier contenido generado por IA. En caso de duda, el funcionario debe:

003

- Contrastar la información con fuentes oficiales;
 - Consultar a un superior o experto cuando corresponda;
 - Abstenerse de utilizar el resultado generado hasta que sea validado.
-
- ✓ Utilizar la IA únicamente en actividades autorizadas y de bajo impacto.
 - ✓ Revisar de manera exhaustiva los resultados antes de usarlos institucionalmente.
 - ✓ Registrar el uso de IA cuando corresponda por razones de transparencia.
 - ✓ Abstenerse de ingresar información sensible, reservada o estratégica.
 - ✓ Garantizar que el documento final refleje criterio humano claro y verificable.
 - ✓ Reportar cualquier error, riesgo o desviación observada durante su uso.
 - ✓ Cumplir las políticas internas de seguridad digital, protección de datos y uso de tecnología.

Factor determinante	Valor (0 / 5 / 10)	Peso (%)	Valor ponderado (automático)	Evidencia documental o enlace
Inclusión en PETI		10		0
Recursos económicos asignados		15		0
Alcance institucional		10		0
Modelo de sostenibilidad		15		0
Estado de ejecución y plan de cumplimiento		10		0
Infraestructura crítica / servicio esencial (ICC/SE)		20		0
Manuales de uso y operación		10		0
Tratamiento de datos personales		10		0
POP total (0-100)		0		0

Fecha de actualización Responsable Factor modificado Valor anterior Valor nuevo Motivo del cambio Evidencia (foto / archivo) Comentario Registro en expediente digital (si/no)

GUÍA DE DILIGENCIAMIENTO — MATRIZ DE LÍNEA BASE POP

Objeto:

Actualizar la línea base de los factores determinantes del proyecto de IA definidos en la Fase 1, para permitir el seguimiento continuo de la madurez institucional durante su desarrollo.

Instrucciones:

- 1) Registre la fecha de corte y el responsable institucional al diligenciar la matriz.
- 2) Asigne un valor de 0, 5 o 10 puntos a cada factor según el nivel de cumplimiento (0 = no existe, 5 = parcial, 10 = completo).
- 3) El valor ponderado se calcula automáticamente multiplicando el valor por el peso (%).
- 4) En la columna de evidencia, indique el enlace o documento que respalde la calificación.
- 5) Actualice la matriz cuando se modifique cualquiera de los factores determinantes (financiación, alcance, sostenibilidad, plan de cumplimiento, infraestructura crítica, manuales o tratamiento de datos).
- 6) Registre cada actualización en la hoja 'Histórico de actualizaciones' para conservar la trazabilidad.
- 7) Si el proyecto es ICC/SE, consigne la justificación en la columna de observaciones y mantenga activa la conexión con el canal distrital para la gestión de incidentes críticos.

Resultado exigible:

Matriz de línea base POP actualizada y archivada en el expediente digital con fecha de corte y validación institucional.

N°	Área / Dependencia	Tipo de entor (Interio / Exterio)	Entidad / Proveedor (el sellado)	Nombre del responsable (el sellado)	Cargo	Curso electrónico	Teléfono	Porcentaje de vida (%)	Funciones y competencias (qué hace)	Responsabilidades (qué debe hacer)	Decisiones que puede adoptar	Indicadores operativos	Evidencias en medios digitales (el sellado)	Fecha de designación	Área que la designa (responsable)	Vigencia (días)	Vigencia (meses)	Observaciones
1	Salida																	
2	TC / Subordinados																	
3	TC / Subordinados																	
4	TC / Subordinados																	
5	TC / Subordinados																	
6	TC / Subordinados																	
7	TC / Subordinados																	
8	TC / Subordinados																	
9	TC / Subordinados																	
10	TC / Subordinados																	
11	TC / Subordinados																	
12	TC / Subordinados																	
13	TC / Subordinados																	
14	TC / Subordinados																	
15	TC / Subordinados																	
16	TC / Subordinados																	
17	TC / Subordinados																	
18	TC / Subordinados																	
19	TC / Subordinados																	
20	TC / Subordinados																	
21	TC / Subordinados																	
22	TC / Subordinados																	
23	TC / Subordinados																	
24	TC / Subordinados																	
25	TC / Subordinados																	
26	TC / Subordinados																	
27	TC / Subordinados																	
28	TC / Subordinados																	
29	TC / Subordinados																	
30	TC / Subordinados																	
31	TC / Subordinados																	
32	TC / Subordinados																	
33	TC / Subordinados																	
34	TC / Subordinados																	
35	TC / Subordinados																	
36	TC / Subordinados																	
37	TC / Subordinados																	
38	TC / Subordinados																	
39	TC / Subordinados																	
40	TC / Subordinados																	
41	TC / Subordinados																	
42	TC / Subordinados																	
43	TC / Subordinados																	
44	TC / Subordinados																	
45	TC / Subordinados																	
46	TC / Subordinados																	
47	TC / Subordinados																	
48	TC / Subordinados																	
49	TC / Subordinados																	
50	TC / Subordinados																	
51	TC / Subordinados																	
52	TC / Subordinados																	
53	TC / Subordinados																	
54	TC / Subordinados																	
55	TC / Subordinados																	
56	TC / Subordinados																	
57	TC / Subordinados																	
58	TC / Subordinados																	
59	TC / Subordinados																	
60	TC / Subordinados																	
61	TC / Subordinados																	
62	TC / Subordinados																	
63	TC / Subordinados																	
64	TC / Subordinados																	
65	TC / Subordinados																	
66	TC / Subordinados																	
67	TC / Subordinados																	
68	TC / Subordinados																	
69	TC / Subordinados																	
70	TC / Subordinados																	
71	TC / Subordinados																	
72	TC / Subordinados																	
73	TC / Subordinados																	
74	TC / Subordinados																	
75	TC / Subordinados																	
76	TC / Subordinados																	
77	TC / Subordinados																	
78	TC / Subordinados																	
79	TC / Subordinados																	
80	TC / Subordinados																	
81	TC / Subordinados																	
82	TC / Subordinados																	
83	TC / Subordinados																	
84	TC / Subordinados																	
85	TC / Subordinados																	
86	TC / Subordinados																	
87	TC / Subordinados																	
88	TC / Subordinados																	
89	TC / Subordinados																	
90	TC / Subordinados																	
91	TC / Subordinados																	
92	TC / Subordinados																	
93	TC / Subordinados																	
94	TC / Subordinados																	
95	TC / Subordinados																	
96	TC / Subordinados																	
97	TC / Subordinados																	
98	TC / Subordinados																	
99	TC / Subordinados																	
100	TC / Subordinados																	

Actividad / Entregable	Origen	ITC / Interconexión	Ente / Gobierno	Seguridad de la información	Dependencia nacional	Proceder / Continúa	Interconexión / Superación	CERO
Identificación del problema público / caso de uso								
Definición de los límites y finalidad del tratamiento								
Gestión de datos (planes, roles, responsabilidades)								
Evaluación de impacto (IA/CPI)								
Desarrollo / Integración / Configuración del sistema								
Verificación y validación (V&V) / Pruebas								
Seguridad digital (gestión de riesgos e incidentes)								
Transparencia algorítmica (datos y parámetros)								
Configuración / Pruebas / Implementación								
Monitoreo de desempeño / O&M								
Gestión de incidentes y vulnerabilidades								
Auditoría técnica / Algoritmos								
Revisión de la arquitectura / Actualización del modelo								
Cierre / Desmantelamiento registrado								

GUÍA DE DILIGENCIAMIENTO — ROLES Y RESPONSABILIDADES EN PROYECTOS DE IA

Objetivo

Estandarizar la identificación de actores, funciones, competencias y responsabilidades a lo largo del ciclo de vida (PHVA) de los proyectos de IA, y consolidar el 'quién hace qué' en el expediente digital.

Hoja 1 — Matriz de roles y responsabilidades

- 1) Registre todas las áreas/actores internos y externos involucrados (mínimo: Jurídica, TIC/Infraestructura, Datos/Gobernanza, Seguridad de la Información, Dependencia misional).
- 2) Cuando haya proveedores o socios tecnológicos, consigne sus datos y designe un responsable institucional de supervisión o interventor.
- 3) Defina claramente funciones, competencias, responsabilidades, decisiones y entregables por actor. Vincule la evidencia (ruta o enlace) en el expediente digital.
- 4) Documente la designación (acto/resolución) y vigencias.

Hoja 2 — Matriz RACI

Use la codificación RACI: R = Responsable ejecutor / A = Aprobador último / C = Consultado / I = Informado.

Asigne una letra por celda, evitando vacíos en actividades críticas (EIA/OPMA, Seguridad, V&V, Transparencia, Incidentes).

Ciclo PHVA y trazabilidad

- Planear: definición de caso de uso, base jurídica, datos, riesgos y responsabilidades.
- Hacer: desarrollo, integración, pruebas controladas y documentación.
- Verificar: auditorías, monitoreo, desempeño, sesgos, seguridad y cumplimiento.
- Actuar: mejoras, mejoramiento, continuidad, cierre o desmantelamiento.

Resultado exigible

Listado oficial de roles y responsabilidades ("quién hace qué"), archivado y actualizado en el expediente digital del proyecto.

N°	Elemento / Subíndice KID	Política / Lineamiento Distrital aplicable	Relación con el proyecto de la (cómo contribuye)	Responsable Institucional	Fecha de actualización	Evidencia documental o enlace
1	1. Gobernanza					
2	2. Innovación Pública Digital					
3	3. Arquitectura					
4	4. Seguridad y Privacidad de la Información					
5	5. Servicios Ciudadanos Digitales					
6	6. Cultura y Apropiación					
7	7. Servicios y Procesos Inteligentes					
8	8. Estado Abierto					
9	9. Decisiones Basadas en Datos					
10	10. Proyectos de Transformación Digital					
11	11. Estrategias de Ciudades y Territorios Inteligentes					

GUÍA DE DILIGENCIAMIENTO DE LA MATRIZ DE ALINEACIÓN INSTITUCIONAL

Objetivo:

Estandarizar la forma en que las entidades distritales documentan la relación de sus proyectos de inteligencia artificial con las políticas, planes y subíndices del Índice de Gobierno Digital (IGD).

Instrucciones generales:

1. Complete cada fila correspondiente a los 11 subíndices del IGD.
2. En la columna 'Política / Lineamiento Distrital aplicable', indique la norma, plan o documento distrital que corresponda (ej. Decreto 767 de 2022, Estrategia de Seguridad Digital, etc.).
3. En la columna 'Relación con el proyecto de IA', describa brevemente cómo el proyecto contribuye o se articula con ese subíndice.
4. Registre al responsable institucional, la fecha de actualización y la evidencia (documento o enlace).
5. Esta matriz debe conservarse en el expediente digital del proyecto y actualizarse al menos una vez al año.

Ejemplo de diligenciamiento:

Elemento / Subíndice IGD: 4. Seguridad y privacidad de la información

Política / Lineamiento Distrital aplicable: Estrategia Distrital de Seguridad Digital (Decreto 88 de 2022)

Relación con el proyecto de IA: El sistema implementa controles de ciberseguridad y cifrado conforme a la estrategia distrital.

Responsable institucional: Oficina de Seguridad de la Información

Fecha de actualización: 15/10/2025

Evidencia documental o enlace: Informe de auditoría de seguridad digital 2025.

Integración con el expediente digital:

La matriz debe almacenarse en el expediente digital del proyecto de IA, junto con los actos administrativos, evidencias técnicas, informes y registros de seguimiento. Cada actualización de la matriz deberá incluir la fecha, responsable y enlace a la documentación de respaldo.

Relación con el ciclo PHVA del MPIA:

La matriz de alineación institucional constituye una herramienta transversal dentro del ciclo PHVA (Planear–Hacer–Verificar–Actuar):

- En la fase 'Planear', permite identificar las políticas y lineamientos aplicables.
- En la fase 'Hacer', documenta la ejecución y responsabilidades institucionales.
- En la fase 'Verificar', evidencia el cumplimiento y la coherencia con el IGD.
- En la fase 'Actuar', orienta la mejora continua y la actualización anual del proyecto.

Campo	Valor	Descripción/Notas
Entidad		Secretaría de Hacienda
Proyecto		Nombre del proyecto
Fuente IGD		Link de acceso
Fecha IGD		Fecha consulta
Responsable IGD		Innovación - Pedro López
ICC/SG		¿Afecta Infraestructura Crítica Cibernética o Servicio Esencial? ("SI"/"NO")
Proyecto en ejecución		Seleccione "SI" si ya está en operación/piloto activo
Plan de trabajo y cumplimiento aprobado		Si el proyecto está en ejecución, ¿cuenta con plan de trabajo y cumplimiento aprobado? ("SI"/"NO")

Elemento / Subíndice IGD	Valor (0-100)	Semáforo
Gobernanza		
Innovación Pública Digital		
Arquitectura		
Seguridad y Privacidad de la Información		
Servicios Ciudadanos Digitales		
Cultura y Apropiación		
Servicios y Procesos Inteligentes		
Estado Abierto		
Decisiones Basadas en Datos		
Proyectos de Transformación Digital		
Estrategias de Ciudades y Territorios Inteligentes		

IGD (promedio 11 subíndices)

Críticos para criticidad:

Gobernanza	0
Seguridad y Privacidad de la Información	0
Decisiones basadas en datos	0

Indicador	Valor	Unidad
Inclusión en PETI	10	0
Recursos económicos asignados	15	0
Alcance Institucional	10	0
Modelo de sostenibilidad	15	0
Estado de ejecución y plan de cumplimiento	10	0
Infraestructura crítica / servicio esencial (ICC/SE)	20	0
Manuales de uso y operación	10	0
Tratamiento de datos personales	10	0
POR total (0-100)	100	0

IGD (promedio) PDR (total) $ICM = 0.40 \cdot IGD + 0.60 \cdot PDR$	0				
Ruta preliminar (por ICM) Créditos por subíndices críticos IGD ICC/SE (Ruta Especial) Regla especial: ejecución sin plan aprobado		Exploratoria ICC/SE: No aplica	Gobernancia	0 Seg. & Priv.	0 Decisiones datos
Ruta final Comentarios automáticos					0

Campo	Valor
Entidad	0
Proyecto	0
IGD (promedio)	0
PDP (total)	0
ICM	
Ruta preliminar	
Criticidad	Exploratoria
ICC/SE	
Regla especial (ejecución/plan)	No aplica
Ruta final	
Comentario	

DICTAMEN TÉCNICO-JURÍDICO FASE 1 (MPIA-Bogotá)

Para macro y botón PDF, ver hoja 'Macro_VBA'.

Entidad: 0

Proyecto: 0

IGD (promedio): 0

PDP (total): 0

ICM (0,40*IGD + 0,60*PDP): 0

Ruta preliminar:

Criticidad: Exploratoria

ICC/SE: No aplica

Regla especial (ejecución/plan):

ruta final:

Comentario:

Evidencias clave (IGD/PDP):

- Fuente IGD: 0

- Fecha IGD: 0

- Responsable IGD: 0

Firmas / VoBo:

Responsable Proyecto Jurídica / TIC

N°	Pregunta	Valor (0-100)	Valor ponderado (20%)	Evidencia de soporte	Observaciones
	¿La entidad cuenta con una Política o Plan Institucional de Transformación Digital que incluya proyectos de IA?			0	
	1. Transformación Digital que incluya proyectos de IA?			0	
	¿Dispone de infraestructura tecnológica y mecanismos de seguridad digital que garanticen la protección de datos y la continuidad operativa del proyecto de IA?			0	
	2. La entidad ha definido roles y responsabilidades institucionales (TIC, jurídica, datos, misión) para desarrollar o supervisar proyectos de IA?			0	
	3. Cuenta con procesos o políticas de gestión y protección de datos personales aplicables al tratamiento de información en el proyecto de IA?			0	
	4. Información en el proyecto de IA?			0	
	¿Dispone de procesos documentados de seguimiento, evaluación o mejora en proyectos tecnológicos o de IA (indicadores, auditorías, reportes)?			0	
	5. (indicadores, auditorías, reportes)?			0	
	TOTAL			0	

Rango de puntaje	Nivel de madurez	Ruta MPJA	Descripción
0 - 39	Bajo o inicial	Exploratoria	La entidad presenta capacidades digitales incipientes. Requiere fortalecimiento institucional previo a cualquier desarrollo de IA.
40 - 69	Intermedio	Consolidación	La entidad dispone de capacidades parciales y puede avanzar con acompañamiento técnico en proyectos de IA.
70 - 100	Alto	Avanzada	La entidad cuenta con condiciones sólidas para desplegar proyectos de IA con supervisión, transparencia y seguridad digital.