Guía para la Reglamentación

Introducción: de la norma a la política pública

La regulación de la inteligencia artificial en el ámbito municipal no debe entenderse como una iniciativa tecnológica aislada, sino como un proceso de institucionalización de capacidades estatales. En este sentido, la ordenanza constituye el instrumento jurídico que permite transformar el uso de IA en una **política pública formal**, dotándola de legitimidad, continuidad y alineación estratégica.

El enfoque adecuado no es restrictivo. La regulación no tiene por objeto limitar el uso de la IA, sino **habilitar su adopción bajo condiciones de gobernanza**, asegurando que su implementación contribuya efectivamente a mejorar la gestión pública, proteger derechos y generar valor público.

Las experiencias municipales muestran una convergencia hacia una estructura normativa común, que organiza la política de IA en torno a cuatro componentes principales.

En primer lugar, la creación de un **Programa Municipal de Innovación con IA**, que actúa como eje articulador de la política. Este programa establece las líneas de acción prioritarias, incluyendo la identificación de oportunidades de uso, el desarrollo de proyectos piloto, la articulación con actores externos y la capacitación del personal.

En segundo lugar, la incorporación de **instrumentos de implementación**, que permiten operacionalizar la política. Entre los más relevantes se encuentran los laboratorios de innovación, los entornos de prueba controlados (sandbox), los registros de algoritmos, los gemelos digitales y los mecanismos de convocatoria a soluciones tecnológicas.

En tercer lugar, la definición de **principios de uso ético, responsable y seguro**, que establecen estándares mínimos en materia de transparencia, explicabilidad, protección de datos, no discriminación y supervisión humana.

Finalmente, la inclusión de mecanismos de **monitoreo y evaluación**, que permiten medir resultados, identificar aprendizajes y ajustar la política en función de la evidencia.

Esta arquitectura refleja una idea central: la regulación de la IA no es solo normativa, sino también **organizacional y operativa**.

Es importante destacar que la ordenanza no agota la regulación. Por el contrario, funciona como un marco general que define principios, objetivos e instrumentos, mientras que su **reglamentación es la que determina el impacto real**, al traducir esos principios en reglas operativas, procedimientos y decisiones concretas.

La reglamentación constituye el paso más relevante en el proceso de institucionalización. Mientras la ordenanza define “qué hacer”, la reglamentación establece “cómo hacerlo”.

Una reglamentación robusta debe estructurarse en torno a cinco dimensiones clave:

- Gobernanza
- Priorización estratégica
- Implementación operativa
- Control y gestión de riesgos
- Evaluación de resultados

Estas dimensiones no son independientes, sino que conforman un sistema integrado que determina la capacidad real del municipio para adoptar IA de manera sostenible.

Gobernanza: liderazgo, roles y capacidades

La gobernanza constituye el componente estructural sobre el cual se apoya toda política de inteligencia artificial en el ámbito municipal. No se trata únicamente de definir una autoridad formal, sino de construir un **sistema de toma de decisiones, ejecución y control** que permita operar la IA como política pública transversal, con coherencia institucional y capacidad efectiva de implementación.

En la mayoría de los municipios, la adopción de IA enfrenta tres riesgos típicos:

- **Fragmentación organizacional**: múltiples áreas impulsan iniciativas sin coordinación, generando duplicación de esfuerzos, incompatibilidades tecnológicas y uso ineficiente de recursos.
- **Vacío de responsabilidad**: nadie tiene la autoridad clara para decidir, priorizar o detener proyectos.
- **Asimetría de capacidades**: áreas técnicas avanzan más rápido que las jurídicas o de gestión, lo que genera riesgos regulatorios y de legitimidad.

La gobernanza debe diseñarse precisamente para evitar estos escenarios, asegurando que la IA se implemente bajo un esquema **coordinado, responsable y controlado**.

Autoridad de aplicación: el centro de gravedad de la política

El primer elemento crítico es la designación de una **autoridad de aplicación con mandato explícito**. Esta figura no debe limitarse a un rol administrativo, sino que debe constituirse como el **órgano rector de la política de IA**.

Funciones estratégicas

- Definir lineamientos y estándares para el uso de IA en el municipio.
- Coordinar la implementación intersectorial (todas las áreas).
- Priorizar proyectos y asignar recursos.
- Supervisar riesgos, cumplimiento normativo y resultados.

Requisitos institucionales

Para que esta autoridad sea efectiva, debe cumplir tres condiciones:

1. **Jerarquía política suficiente**: idealmente una secretaría o subsecretaría con capacidad de incidencia transversal.
2. **Capacidad técnica**: conocimiento en datos, tecnología y regulación.
3. **Poder de coordinación**: facultades para intervenir en proyectos de otras áreas.

En términos de diseño institucional, ubicar esta función en áreas de modernización, transformación digital o jefatura de gabinete suele ser más efectivo que en áreas puramente tecnológicas, porque la IA no es solo infraestructura, sino **gestión pública**.

Unidad operativa: de la estrategia a la ejecución

La autoridad de aplicación necesita un brazo operativo. Sin este componente, la política queda en el plano declarativo.

Características de la unidad

- Equipo pequeño, altamente especializado.
- Capacidad de trabajo transversal con todas las áreas.
- Orientación a proyectos (no a burocracia).
- Flexibilidad organizacional.

Funciones principales

- Identificación y formulación de casos de uso.
- Coordinación de pilotos con áreas sectoriales.
- Vinculación con startups y proveedores.
- Soporte técnico y metodológico.
- Seguimiento de implementación.

Un error frecuente es intentar crear estructuras grandes desde el inicio. La evidencia muestra que es más efectivo comenzar con un **equipo ágil** que actúe como catalizador interno.

Modelo de gobernanza transversal: articulación con las áreas

La IA no debe centralizarse completamente ni dispersarse. Requiere un modelo híbrido:

- **Centralización estratégica**: la autoridad de aplicación define reglas, estándares y prioridades.
- **Descentralización operativa**: cada área implementa casos de uso en su dominio (salud, movilidad, atención ciudadana, etc.).

Esto implica establecer mecanismos formales de articulación:

- Puntos focales de IA en cada área.
- Mesas de coordinación intersectorial.
- Procedimientos de validación y aprobación de proyectos.

El objetivo es evitar tanto el “cuello de botella central” como la “anarquía tecnológica”.

Comité de ética y gobernanza: institucionalización del control

Los principios éticos no son suficientes si no se traducen en procedimientos. Por ello, es recomendable crear un **comité de ética y gobernanza de IA**.

Composición

- Perfil jurídico (protección de datos, derecho administrativo).
- Perfil técnico (IA, datos).
- Perfil institucional (gestión pública).
- Opcional: participación académica o externa.

Funciones

- Evaluar proyectos de IA antes de su implementación.
- Analizar riesgos de sesgo, discriminación o impacto en derechos.
- Revisar cumplimiento de estándares.
- Emitir recomendaciones (vinculantes o no, según diseño).

Momento de intervención

El comité debe intervenir en:

- proyectos de alto impacto;
- sistemas con incidencia en decisiones administrativas;
- uso de datos sensibles.

Este órgano permite pasar de una lógica declarativa a una lógica de **control institucionalizado**.

Consejo consultivo: apertura institucional y construcción de inteligencia colectiva

Además de los mecanismos formales de control, como el comité de ética y gobernanza, la reglamentación puede prever la creación de un **consejo consultivo en materia de inteligencia artificial**, orientado a ampliar la base de actores involucrados en el diseño e implementación de la política.

A diferencia del comité de ética —cuyo rol es analizar riesgos, evaluar impactos y eventualmente emitir dictámenes sobre sistemas específicos—, el consejo consultivo tiene una función **no vinculante y de carácter estratégico**, centrada en aportar conocimiento, anticipar tendencias y enriquecer la toma de decisiones públicas.

Su conformación puede incluir representantes del ámbito académico, del sector tecnológico, de organizaciones de la sociedad civil y, eventualmente, de otros niveles de gobierno. Esta diversidad permite incorporar miradas interdisciplinarias y fortalecer la calidad del diseño de políticas en un campo caracterizado por su rápida evolución y complejidad técnica.

Entre sus funciones principales pueden destacarse:

- emitir recomendaciones sobre lineamientos generales de la política de IA;
- identificar oportunidades de innovación y tendencias tecnológicas relevantes;
- contribuir al desarrollo de estándares y buenas prácticas;
- promover instancias de diálogo entre el municipio y el ecosistema externo;
- aportar insumos para la evaluación de impacto y mejora continua.

La existencia de un consejo consultivo no reemplaza las funciones decisorias de la autoridad de aplicación ni los mecanismos de control institucional, sino que las complementa, permitiendo incorporar una lógica de **gobernanza abierta**.

Desde el punto de vista regulatorio, su diseño debe contemplar:

- su carácter asesor (no vinculante);
- criterios de selección y duración de sus integrantes;
- periodicidad de funcionamiento;
- mecanismos de articulación con la autoridad de aplicación.

La incorporación de este tipo de instancias contribuye a fortalecer la legitimidad de la política de IA, mejorar la calidad de las decisiones y reducir el riesgo de capturas tecnológicas o enfoques excesivamente cerrados dentro de la administración.

Distribución de responsabilidades: principio clave

Un aspecto crítico de la gobernanza es evitar la “irresponsabilidad algorítmica”.

Debe quedar explícito que:

- La IA es **instrumental**, no decisoria.
- El **agente público conserva la responsabilidad** sobre las decisiones.
- La validación humana es obligatoria en casos relevantes.

Esto implica definir claramente:

- quién diseña;
- quién implementa;
- quién valida;
- quién responde ante errores.

Sin esta claridad, se genera un vacío jurídico que debilita la política.

Capacidades institucionales: el factor determinante

La gobernanza no es solo estructura, sino también capacidades.

Un municipio puede tener una ordenanza avanzada y, sin embargo, fracasar en su implementación si no desarrolla capacidades en tres niveles:

a) Capacidades técnicas

- comprensión básica de IA y datos;

- habilidades para interpretar resultados;
- criterios para evaluar proveedores.

b) Capacidades organizacionales

- trabajo transversal;
- gestión de proyectos de innovación;
- adaptación a metodologías ágiles.

c) Capacidades regulatorias

- conocimiento en protección de datos;
- evaluación de riesgos;
- comprensión de impactos legales.

La formación del personal no es un complemento, sino un **componente estructural de la gobernanza**.

Gobernanza como sistema dinámico

Finalmente, la gobernanza de IA no debe diseñarse como un esquema rígido, sino como un sistema adaptable.

Esto implica:

- revisión periódica de roles y procesos;
- ajuste de estructuras según aprendizaje;
- actualización de estándares frente a cambios tecnológicos.

La IA evoluciona rápidamente, por lo que la gobernanza debe incorporar mecanismos de **flexibilidad y mejora continua**.

Conclusión Gobernanza

Una buena gobernanza no se limita a designar una autoridad, sino que construye un sistema coherente de liderazgo, ejecución y control.

Cuando este sistema está bien diseñado:

- la IA deja de ser experimental,
- se integra a la gestión pública,
- y se convierte en una capacidad institucional sostenible.

Cuando no lo está:

- la política queda fragmentada,
- los riesgos aumentan,
- y el impacto es marginal.

Por eso, la gobernanza es, en la práctica, el **principal determinante del éxito o fracaso** de la regulación de IA en gobiernos locales.

Priorización: definición de casos de uso

La priorización de casos de uso constituye el punto de inflexión entre la estrategia y la implementación. Es, en términos prácticos, el momento en el que la política de IA deja de ser un marco general y se traduce en decisiones concretas sobre **dónde intervenir, con qué objetivos y en qué secuencia**.

Una mala priorización conduce a dispersión, proyectos irrelevantes o fallas tempranas que erosionan la legitimidad de la política. Una buena priorización, en cambio, permite generar resultados visibles en el corto plazo y construir capacidades institucionales de manera progresiva.

En ausencia de un proceso estructurado de priorización, los municipios tienden a caer en tres sesgos:

- **Sesgo tecnológico**: se eligen proyectos por disponibilidad de herramientas, no por relevancia pública.
- **Sesgo oportunista**: se priorizan iniciativas impulsadas por proveedores o actores externos.
- **Sesgo político de corto plazo**: se seleccionan casos de alto impacto comunicacional pero baja viabilidad.

La priorización introduce un criterio técnico-político que permite ordenar la adopción de IA bajo una lógica de **valor público, factibilidad y sostenibilidad**.

Principio rector: la IA como herramienta para resolver problemas públicos

El punto de partida no debe ser “dónde aplicar IA”, sino **qué problemas públicos vale la pena resolver**.

Esto implica invertir la lógica habitual:

- No partir de la tecnología → partir del problema.
- No pensar en soluciones → pensar en necesidades.
- No buscar innovación por sí misma → buscar impacto.

En este sentido, los casos de uso deben definirse como **problemas de gestión o de servicio**, en los cuales la IA puede aportar una mejora sustantiva (no marginal).

Construcción del Directorio de Oportunidades

Una herramienta clave es la creación de un **Directorio de Oportunidades de IA**, que funcione como un inventario estructurado de posibles casos de uso en el municipio.

Cada oportunidad debería describirse con una ficha técnica que incluya:

- Área responsable (ej. salud, movilidad, atención ciudadana).
- Problema a resolver.
- Proceso actual (cómo funciona hoy).
- Tipo de mejora esperada (automatización, predicción, clasificación, etc.).
- Disponibilidad y calidad de datos.
- Nivel de impacto esperado.
- Complejidad técnica e institucional.

Este directorio permite transformar la identificación de casos en un proceso sistemático, evitando decisiones ad hoc.

Criterios de priorización: el núcleo de la decisión

La selección de casos de uso debe basarse en criterios explícitos. En términos generales, se recomienda trabajar con al menos cuatro dimensiones:

a) Impacto en la gestión o en la ciudadanía

- ¿Reduce tiempos de respuesta?
- ¿Mejora la calidad del servicio?
- ¿Aumenta la eficiencia o reduce costos?
- ¿Afecta a un volumen significativo de personas?

b) Viabilidad técnica

- ¿Existen datos disponibles?
- ¿Los datos tienen calidad suficiente?
- ¿La solución es tecnológicamente factible?

c) Viabilidad institucional

- ¿El área responsable tiene capacidad de implementar?
- ¿Existen resistencias organizacionales?
- ¿El proceso es modificable o está altamente rigidizado?

d) Riesgo

- ¿El sistema puede afectar derechos?
- ¿Involucra datos sensibles?
- ¿Requiere altos niveles de explicabilidad?

Matriz esfuerzo–impacto: herramienta operativa

Una práctica ampliamente utilizada es la construcción de una **matriz de priorización**, que cruce:

- **Impacto esperado** (alto / bajo)

- **Esfuerzo requerido** (alto / bajo)

Esto permite identificar tres tipos de proyectos:

1. **Quick wins** (alto impacto, bajo esfuerzo): deben ser la prioridad inicial.
2. **Proyectos estratégicos** (alto impacto, alto esfuerzo): requieren planificación.
3. **Proyectos de baja prioridad** (bajo impacto): deben postergarse.

Este enfoque permite construir una **hoja de ruta progresiva**, comenzando por casos que generen resultados rápidos y visibles.

Tipología de casos de uso en gobiernos locales

La experiencia comparada muestra que los casos de uso de IA en municipios tienden a concentrarse en ciertas categorías:

a) Automatización de procesos administrativos

- clasificación de expedientes;
- generación de documentos;
- gestión de trámites.

b) Mejora de la atención ciudadana

- chatbots;
- priorización de reclamos;
- análisis de consultas.

c) Análisis predictivo

- detección de riesgos (ej. inundaciones, fallas);
- planificación de servicios;
- asignación de recursos.

d) Optimización operativa

- rutas de recolección;
- gestión de tránsito;
- mantenimiento urbano.

Esta tipología ayuda a orientar la identificación de oportunidades, evitando empezar desde cero en cada municipio.

Priorización política vs. priorización técnica

La priorización no es un proceso puramente técnico. Requiere una articulación entre:

- **criterios técnicos** (viabilidad, datos, impacto);
- **criterios políticos** (agenda del gobierno, prioridades estratégicas).

El rol de la autoridad de aplicación es precisamente mediar entre ambos planos, evitando que uno anule al otro.

Un enfoque exclusivamente técnico puede derivar en proyectos irrelevantes políticamente. Uno exclusivamente político puede derivar en proyectos inviables.

Secuenciación: construir una curva de aprendizaje

La priorización no es solo seleccionar proyectos, sino también definir **en qué orden implementarlos**.

Se recomienda una lógica de secuencia:

1. **Etapa inicial**: proyectos de bajo riesgo y alta visibilidad (quick wins).
2. **Etapa intermedia**: proyectos con mayor complejidad técnica.
3. **Etapa avanzada**: sistemas con impacto en decisiones o derechos.

Esta progresión permite desarrollar capacidades institucionales antes de abordar casos más sensibles.

Integración con el modelo de pilotos

La priorización está directamente vinculada con el modelo de pilotos.

Cada caso priorizado debería transformarse en un piloto con:

- objetivos claros;
- indicadores definidos;
- duración acotada;
- criterios de evaluación.

La lógica no es implementar directamente a escala, sino **testear, aprender y escalar**.

Riesgo de dispersión y cómo evitarlo

Uno de los principales riesgos es intentar implementar múltiples casos de uso en paralelo.

Esto genera:

- sobrecarga institucional;
- pérdida de foco;
- baja calidad en la ejecución.

La recomendación es clara: **pocos proyectos, bien ejecutados**, en lugar de muchos proyectos inconexos.

Conclusión sobre Priorización

La priorización es el mecanismo que traduce la política de IA en resultados concretos.

Cuando está bien diseñada:

- orienta recursos hacia donde generan mayor valor;
- reduce riesgos de implementación;
- permite construir capacidades progresivamente.

Cuando no lo está:

- la IA se convierte en un conjunto de iniciativas aisladas;
- el impacto es marginal;
- y la política pierde legitimidad.

En definitiva, priorizar no es elegir proyectos. Es **definir el camino de adopción de la IA en el municipio**.

Implementación: diseño y gestión de pilotos

La implementación de inteligencia artificial en gobiernos locales no debe abordarse como un despliegue directo a escala, sino como un proceso iterativo basado en **experimentación controlada**. En este contexto, los pilotos constituyen el mecanismo central para reducir incertidumbre, validar soluciones y generar aprendizaje institucional antes de escalar.

Un piloto no es una versión “pequeña” de una política, sino un **instrumento de decisión pública**: permite determinar si una solución tecnológica es pertinente, viable y segura en el contexto real del municipio.

La adopción directa de soluciones de IA a gran escala presenta riesgos significativos:

- implementación de tecnologías no adaptadas al contexto local;
- dependencia temprana de proveedores sin validación previa;
- exposición a riesgos legales, reputacionales o de derechos;
- inversión de recursos en soluciones de bajo impacto.

El enfoque de pilotos permite mitigar estos riesgos mediante una lógica de **probar antes de adoptar**, transformando la implementación en un proceso gradual y basado en evidencia.

Naturaleza jurídica y operativa del piloto

Desde el punto de vista técnico-jurídico, un piloto debe ser entendido como:

- una **instancia experimental controlada**, con alcance limitado;
- una **fase previa a la contratación o adopción definitiva**;
- un proceso con objetivos, indicadores y duración definidos.

Esto implica que la reglamentación debe diferenciar claramente entre:

- pilotos (prueba, validación);
- implementación (adopción operativa);

- escalamiento (integración estructural).

La ausencia de esta distinción suele generar confusión normativa y riesgos contractuales.

Ciclo completo de un piloto

La implementación de pilotos debe estructurarse como un ciclo con etapas definidas:

a) Definición del problema

Todo piloto debe partir de un problema claramente delimitado, previamente priorizado. Esta etapa incluye:

- descripción del proceso actual;
- identificación de ineficiencias o limitaciones;
- definición del resultado esperado.

Un error frecuente es definir el piloto en términos tecnológicos (“implementar un chatbot”), en lugar de hacerlo en términos de problema (“reducir tiempos de respuesta en atención ciudadana”).

b) Diseño del piloto

En esta etapa se establecen las condiciones de la prueba:

- alcance (qué área, qué proceso, qué volumen de casos);
- duración (generalmente entre 8 y 16 semanas);
- datos a utilizar;
- indicadores de evaluación;
- condiciones de éxito o fracaso.

También deben definirse aspectos críticos como:

- requisitos de seguridad y protección de datos;
- nivel de intervención humana;
- criterios de explicabilidad.

El diseño debe asegurar que el piloto sea **lo suficientemente acotado para ser controlable**, pero lo suficientemente representativo para generar evidencia válida.

c) Convocatoria y selección de soluciones

La reglamentación debe definir cómo se identifican las soluciones tecnológicas.

Existen distintos mecanismos posibles:

- convocatorias abiertas a startups y empresas;
- desafíos públicos de innovación;
- selección directa en casos justificados;
- articulación con ecosistemas GovTech.

Independientemente del mecanismo, es clave definir:

- criterios de evaluación (madurez de la solución, antecedentes, adecuación al problema);
- requisitos mínimos (seguridad, cumplimiento normativo);
- condiciones de participación.

Este componente es central para estructurar una relación transparente y eficiente con proveedores.

d) Implementación del piloto

Durante la ejecución, el piloto debe operar en un entorno controlado:

- acceso limitado a datos;
- supervisión permanente;
- monitoreo de desempeño;
- registro de incidencias.

Es fundamental garantizar que:

- no se comprometan datos sensibles sin resguardos;
- exista intervención humana en decisiones relevantes;
- se documenten todos los procesos.

En esta etapa, la coordinación entre el equipo técnico, el área sectorial y el proveedor es determinante.

e) Evaluación

Al finalizar el piloto, debe realizarse una evaluación estructurada, basada en los indicadores definidos.

La evaluación debe responder preguntas clave:

- ¿Se resolvió el problema identificado?
- ¿La solución es técnicamente robusta?
- ¿Existen riesgos no previstos?
- ¿Es viable escalar la solución?

La evaluación no debe ser solo técnica, sino también:

- operativa (impacto en procesos);
- jurídica (cumplimiento normativo);
- organizacional (aceptación interna).

f) Decisión de escalamiento

El piloto culmina con una decisión:

- escalar la solución;
- rediseñar y repetir el piloto;
- descartar la solución.

Esta decisión debe estar formalizada y basada en evidencia, evitando que los pilotos queden como experiencias aisladas sin impacto real.

Relación con proveedores y startups

Uno de los aspectos más sensibles de los pilotos es la relación con actores externos.

La reglamentación debe establecer reglas claras para:

- participación de startups;
- uso de datos municipales;
- propiedad intelectual de desarrollos;
- confidencialidad;
- condiciones de continuidad.

Un riesgo frecuente es que los pilotos generen dependencia tecnológica sin un marco contractual adecuado.

Por ello, es recomendable que:

- los pilotos no impliquen compromisos de contratación automática;
- se establezcan condiciones claras para una eventual escalabilidad;
- se definan estándares abiertos cuando sea posible.

Estándares técnicos y de seguridad

Todo piloto debe cumplir estándares mínimos, incluso en fase experimental.

Entre los más relevantes:

- protección de datos personales;
- anonimización cuando corresponda;
- seguridad de la información;
- trazabilidad de decisiones;
- control de accesos.

La lógica no es relajar los estándares por tratarse de pruebas, sino **adaptarlos proporcionalmente al nivel de riesgo**.

Supervisión humana y control

Un principio transversal en los pilotos es la supervisión humana.

Esto implica que:

- ningún sistema debe operar de forma completamente autónoma en decisiones relevantes;
- los resultados deben ser validados por agentes públicos;
- debe existir capacidad de intervención y corrección.

Este componente no solo reduce riesgos, sino que también facilita la adopción organizacional.

Gestión del conocimiento institucional

Uno de los principales valores de los pilotos es el aprendizaje.

Sin mecanismos de sistematización, ese aprendizaje se pierde.

Por ello, es clave:

- documentar procesos, resultados y errores;
- generar reportes de cada piloto;
- difundir buenas prácticas dentro del municipio;
- alimentar el diseño de futuros proyectos.

Esto convierte a los pilotos en una herramienta de **acumulación de capacidades institucionales**.

Integración con la política pública

Los pilotos no deben ser experiencias aisladas, sino parte de una estrategia.

Esto implica que:

- deben estar alineados con prioridades definidas;
- deben alimentar decisiones de política pública;
- deben integrarse con sistemas existentes (cuando escalan).

El objetivo final no es experimentar, sino **transformar la gestión pública**.

Riesgos frecuentes en la implementación de pilotos

Algunos errores recurrentes:

- pilotos sin problema claro;
- falta de indicadores de evaluación;
- ausencia de control sobre datos;
- dependencia de proveedores;
- falta de decisión posterior (pilotos que “quedan en el aire”).

La reglamentación debe anticipar estos riesgos y establecer mecanismos para evitarlos.

Conclusión sobre Pilotos

Los pilotos son el puente entre la regulación y la transformación real.

Cuando están bien diseñados:

- reducen incertidumbre;
- generan evidencia;
- permiten escalar con menor riesgo;
- construyen capacidades institucionales.

Cuando no lo están:

- consumen recursos sin impacto;
- generan frustración organizacional;
- y debilitan la política de IA.

Por eso, la implementación mediante pilotos no es una opción metodológica más, sino el **mecanismo central para una adopción responsable y efectiva de la IA en gobiernos locales**.

Control y gestión de riesgos

El control y la gestión de riesgos constituyen el núcleo regulatorio de la política de inteligencia artificial en gobiernos locales. Mientras la gobernanza organiza la toma de decisiones y la implementación habilita la acción, el sistema de control es el que garantiza que dicha acción se mantenga **dentro de límites jurídicos, éticos y operativos aceptables**.

En términos estrictos, no hay política de IA sin un esquema explícito de gestión de riesgos. La ausencia de este componente transforma a la IA en una fuente potencial de daño institucional, más que en una herramienta de mejora de la gestión.

Naturaleza del riesgo en sistemas de IA

A diferencia de otras tecnologías, los sistemas de IA presentan riesgos específicos que deben ser abordados de manera diferenciada:

- **Riesgos sobre derechos**: decisiones que pueden afectar acceso a servicios, beneficios o trato igualitario.
- **Riesgos de sesgo y discriminación**: derivados de datos o modelos.
- **Riesgos de opacidad**: dificultad para explicar cómo se generan resultados.
- **Riesgos operativos**: errores, fallas o comportamientos no previstos.
- **Riesgos de seguridad y datos**: filtración, uso indebido o acceso no autorizado.
- **Riesgos reputacionales**: pérdida de confianza ciudadana.

Estos riesgos no son homogéneos. Por ello, la regulación debe adoptar un enfoque **proporcional**, ajustando los controles según el nivel de impacto del sistema.

Registro de sistemas de IA: punto de partida del control

No es posible gestionar riesgos sobre sistemas que no se conocen.

Por ello, el primer instrumento indispensable es la creación de un **Registro de Sistemas de Inteligencia Artificial**, que permita identificar, documentar y monitorear todas las aplicaciones de IA utilizadas por el municipio.

Contenido del registro

Cada sistema debería incluir, como mínimo:

- finalidad y área de aplicación;
- tipo de sistema (apoyo, recomendación, decisión);
- datos utilizados;
- proveedor o desarrollo interno;
- nivel de riesgo asignado;
- estado (piloto, implementado, descontinuado).

Este registro cumple una doble función:

- interna: ordenar y gestionar el portafolio de sistemas;
- externa: habilitar mecanismos de transparencia.

Clasificación de riesgos: el principio de proporcionalidad

Una vez identificado el universo de sistemas, el siguiente paso es su **clasificación según nivel de riesgo**.

Un esquema básico distingue tres categorías:

a) Bajo riesgo

Sistemas de apoyo sin incidencia directa en decisiones (ej. análisis descriptivo, automatización interna).

- Requieren controles mínimos.
- No afectan derechos directamente.

b) Riesgo medio

Sistemas de recomendación o priorización (ej. ordenamiento de reclamos, sugerencias de acción).

- Requieren supervisión humana.
- Deben garantizar trazabilidad y explicabilidad básica.

c) Alto riesgo

Sistemas con incidencia material en decisiones o que afectan derechos (ej. asignación de beneficios, controles, sanciones).

- Requieren evaluación previa de impacto.
- Deben contar con revisión humana obligatoria.
- Exigen mayores estándares de transparencia y control.

La clasificación no es un ejercicio teórico: define **qué controles aplicar en cada caso**.

Evaluación de impacto: control previo a la implementación

Para sistemas de riesgo medio y alto, es necesario implementar un mecanismo de **evaluación de impacto previa**.

Esta evaluación tiene como objetivo anticipar riesgos antes de que el sistema entre en funcionamiento.

Contenido mínimo

- identificación de derechos potencialmente afectados;
- análisis de sesgos o discriminación;
- evaluación de proporcionalidad (¿es necesaria la IA?);
- identificación de medidas de mitigación;
- definición de mecanismos de supervisión.

La evaluación debe integrarse formalmente al expediente administrativo y constituir un requisito para la aprobación del sistema.

Comité de ética y gobernanza: control institucionalizado

El control no puede depender únicamente de áreas técnicas.

La creación de un **comité de ética y gobernanza** permite institucionalizar la revisión de riesgos desde una perspectiva multidisciplinaria.

Rol en la gestión de riesgos

- revisar evaluaciones de impacto;
- analizar casos complejos o de alto riesgo;
- emitir recomendaciones o dictámenes;
- proponer ajustes en políticas y estándares.

El valor del comité radica en introducir **deliberación institucional** en decisiones que, de otro modo, quedarían en manos técnicas.

Política de datos: base estructural del control

La mayoría de los riesgos de IA están vinculados a los datos.

Por ello, la gestión de riesgos requiere una **política de datos explícita**, que establezca:

- qué datos pueden utilizarse;
- bajo qué condiciones;
- con qué mecanismos de anonimización;
- con qué estándares de calidad;
- con qué medidas de seguridad.

Además, deben definirse restricciones claras, como:

- prohibición de uso de datos en sistemas externos no controlados;
- limitaciones en el uso de datos sensibles;
- requisitos contractuales con proveedores.

Sin esta base, cualquier control sobre la IA resulta insuficiente.

Control en el uso interno: conducta de los agentes públicos

Un vector crítico de riesgo es el uso informal de IA por parte de empleados públicos.

La regulación debe abordar este punto mediante:

- definición de usos permitidos, prohibidos y condicionados;
- prohibición de carga de datos personales en herramientas no autorizadas;
- exigencia de validación humana;
- lineamientos sobre uso de IA generativa.

Este componente es clave porque muchos riesgos no provienen de sistemas institucionales, sino de **usos no regulados en la práctica cotidiana**.

Transparencia como mecanismo de control

La transparencia no es solo un principio, sino un instrumento de gestión de riesgos.

Permite:

- control ciudadano;
- detección de errores;
- legitimación del uso de IA.

Los mecanismos pueden incluir:

- publicación del registro de sistemas;
- identificación de procesos asistidos por IA;
- información accesible sobre funcionamiento y finalidad.

La transparencia reduce el riesgo reputacional y fortalece la confianza institucional.

Monitoreo continuo y auditoría

El control no termina con la implementación.

Los sistemas de IA deben ser objeto de **monitoreo permanente**, que permita detectar:

- desviaciones en el comportamiento;
- degradación del rendimiento;
- aparición de sesgos no previstos.

Esto puede complementarse con:

- auditorías internas periódicas;
- auditorías externas en sistemas críticos;
- revisión de indicadores de desempeño.

El enfoque debe ser dinámico: los riesgos pueden cambiar con el tiempo.

Responsabilidad y rendición de cuentas

Un principio clave es que la IA no elimina la responsabilidad administrativa.

Debe establecerse claramente que:

- las decisiones siguen siendo responsabilidad de los agentes públicos;
- los errores del sistema no eximen responsabilidad;
- existe obligación de rendición de cuentas.

Esto evita la “delegación algorítmica” de decisiones y refuerza el principio de legalidad.

Gestión de incidentes

La reglamentación debe prever mecanismos para actuar ante fallas o incidentes:

- detección y reporte;
- análisis de causas;
- medidas correctivas;
- comunicación interna y, cuando corresponda, externa.

Esto es especialmente relevante en casos que involucren datos personales o afectación de derechos.

Conclusión sobre control y gestión de riesgos

El control y la gestión de riesgos no buscan frenar la innovación, sino hacerla viable.

Cuando están bien diseñados:

- permiten adoptar IA con menor incertidumbre;
- protegen derechos y datos;
- fortalecen la legitimidad institucional.

Cuando no lo están:

- los riesgos se materializan;
- la confianza se deteriora;
- y la política de IA pierde sostenibilidad.

En definitiva, el control no es un obstáculo para la IA. Es la condición que permite su **uso responsable, seguro y sostenido en el tiempo**.

Uso interno de IA: regulación de los agentes públicos

El uso interno de herramientas de inteligencia artificial por parte de agentes públicos constituye hoy uno de los principales puntos ciegos de la regulación. A diferencia de los sistemas institucionales —que suelen estar sujetos a procesos formales de evaluación—, el uso cotidiano de IA generativa y otras herramientas ocurre de manera **descentralizada, espontánea y, muchas veces, no regulada**.

La paradoja es clara: mientras el municipio regula la IA como política pública, sus propios agentes ya la utilizan sin lineamientos claros. Por ello, este componente no es accesorio, sino crítico para garantizar coherencia normativa, protección de datos y responsabilidad institucional.

Naturaleza del problema

El uso interno de IA presenta características específicas que lo diferencian de otros ámbitos:

- **Alta difusión**: herramientas accesibles, muchas veces gratuitas.
- **Baja trazabilidad**: difícil registro de qué se usa y para qué.
- **Uso individual**: decisiones tomadas a nivel del agente, no institucional.
- **Riesgos invisibles**: carga de datos, generación de contenido no verificado, automatización informal.

Esto genera una situación en la que el riesgo no proviene únicamente de sistemas formales, sino de prácticas cotidianas no reguladas.

Objetivo de la regulación interna

La regulación del uso interno no debe tener un enfoque prohibitivo, sino **ordenador y habilitante**.

El objetivo no es impedir el uso de IA, sino:

- establecer condiciones claras de uso;
- reducir riesgos legales y operativos;
- asegurar calidad en la producción administrativa;
- alinear prácticas individuales con la política institucional.

En este sentido, la regulación debe permitir aprovechar el potencial de la IA como herramienta de productividad, sin comprometer la integridad del accionar público.

Clasificación de usos: marco básico de regulación

Una forma efectiva de estructurar la regulación es clasificar los usos en tres categorías:

a) Usos permitidos

Corresponden a aplicaciones de bajo riesgo, donde la IA actúa como herramienta de apoyo.

Ejemplos:

- redacción preliminar de documentos;
- síntesis de información pública;
- generación de borradores;
- asistencia en tareas administrativas.

Condición clave: siempre con validación humana posterior.

b) Usos condicionados

Requieren autorización o cumplimiento de condiciones específicas.

Ejemplos:

- uso de datos internos no sensibles;
- generación de informes técnicos;
- interacción con sistemas institucionales.

Condiciones típicas:

- uso de herramientas autorizadas;
- cumplimiento de estándares de seguridad;
- registro o trazabilidad del uso.

c) Usos prohibidos

Involucran riesgos significativos para el municipio o la ciudadanía.

Ejemplos:

- carga de datos personales o sensibles en herramientas no autorizadas;
- uso de IA para tomar decisiones sin intervención humana;
- generación automática de actos administrativos sin revisión;
- uso de herramientas sin garantías de confidencialidad.

Esta clasificación permite traducir principios generales en reglas operativas concretas.

Principios rectores del uso interno

Más allá de la clasificación, la regulación debe basarse en principios claros que orienten la conducta de los agentes:

a) Principio de asistencia: La IA es una herramienta de apoyo, no de sustitución del criterio profesional.

b) Principio de validación humana: Todo contenido generado por IA debe ser revisado por un agente público responsable.

c) Principio de confidencialidad: No deben compartirse datos personales o información sensible en sistemas no controlados.

d) Principio de responsabilidad: El agente público es responsable por el uso que hace de la IA y por los resultados que valida.

e) Principio de transparencia interna: Debe ser posible identificar cuándo y cómo se utilizó IA en procesos administrativos.

Uso de IA generativa: regulación específica

Las herramientas de IA generativa requieren una regulación particular, dado su uso extendido.

Riesgos específicos

- generación de contenido incorrecto o inventado;
- incorporación de sesgos;
- exposición de información sensible;
- dificultad para verificar fuentes.

Lineamientos recomendados

- uso restringido a tareas de apoyo;
- prohibición de ingreso de datos personales;
- obligación de verificación de contenido;
- identificación interna del uso en documentos relevantes.

La regulación debe reconocer que estas herramientas son útiles, pero no neutrales ni infalibles.

Integración con la normativa existente

El uso interno de IA no debe regularse en forma aislada, sino integrarse con:

- normativa de protección de datos personales;
- régimen de procedimiento administrativo;

- políticas de seguridad de la información;
- normativa de ética pública.

Esto permite evitar contradicciones y asegurar coherencia jurídica.

Capacitación obligatoria: condición de efectividad

La regulación sin capacitación es, en la práctica, ineficaz.

Los agentes públicos deben contar con formación mínima en:

- qué es la IA y cómo funciona;
- riesgos asociados;
- criterios de uso responsable;
- limitaciones de las herramientas.

La capacitación cumple una doble función:

- reduce riesgos;
- habilita un uso más efectivo de la tecnología.

Mecanismos de control y cumplimiento

Para que la regulación sea efectiva, deben existir mecanismos de seguimiento:

- lineamientos institucionales claros y accesibles;
- supervisión por parte de superiores jerárquicos;
- auditorías internas en casos relevantes;
- canales de consulta para dudas o situaciones no previstas.

No se trata de controlar cada uso individual, sino de establecer un entorno institucional que promueva el cumplimiento.

Riesgos de no regular el uso interno

La ausencia de regulación genera múltiples riesgos:

- filtración de datos personales;
- decisiones basadas en información incorrecta;
- pérdida de trazabilidad administrativa;
- responsabilidad difusa;
- deterioro de la calidad institucional.

En muchos casos, estos riesgos son más probables que los derivados de sistemas formales.

Enfoque progresivo

La regulación del uso interno debe ser gradual.

Se recomienda:

1. establecer reglas básicas;
2. capacitar a los agentes;
3. ajustar en función de la experiencia;
4. incorporar herramientas institucionales más seguras.

Este enfoque permite acompañar la evolución tecnológica sin generar fricciones innecesarias.

Conclusión sobre uso interno de IA

El uso interno de IA es el punto donde la política pública se encuentra con la práctica cotidiana.

Cuando está regulado:

- se reducen riesgos;
- se mejora la calidad del trabajo;
- se alinea la organización.

Cuando no lo está:

- la IA se usa de manera informal;
- los riesgos se multiplican;
- y la política pierde coherencia.

En definitiva, regular el uso interno no es restringir la innovación, sino **integrarla de manera responsable en el funcionamiento del Estado**.

Transparencia y legitimidad

La transparencia en el uso de inteligencia artificial no es un complemento comunicacional, sino un **mecanismo estructural de gobernanza**. Su función principal es asegurar que la adopción de IA por parte del Estado sea **comprensible, controlable y legítima** para la ciudadanía.

En ausencia de transparencia, incluso sistemas técnicamente correctos pueden generar desconfianza, cuestionamientos políticos y conflictos jurídicos. Por el contrario, una política de IA transparente no solo reduce riesgos, sino que **construye licencia social para innovar**.

La incorporación de IA en la gestión pública introduce una tensión estructural:

- por un lado, aumenta la capacidad del Estado para procesar información y tomar decisiones;

- por otro, puede volver opacos esos procesos para la ciudadanía.

Esto genera tres riesgos principales:

- **asimetría de información**: el Estado sabe cómo funcionan los sistemas, la ciudadanía no;
- **desconfianza**: percepción de decisiones “automatizadas” sin control;
- **déficit de rendición de cuentas**: dificultad para cuestionar decisiones.

La transparencia busca equilibrar esta relación, asegurando que el uso de IA sea **visible, explicable y sujeto a control**.

Transparencia como principio operativo, no declarativo

Muchas ordenanzas incluyen la transparencia como principio, pero no la traducen en mecanismos concretos.

Para que sea efectiva, la transparencia debe ser:

- **activa**: no depender de solicitudes de información;
- **estructurada**: basada en instrumentos definidos;
- **proporcional**: adaptada al nivel de riesgo del sistema;
- **operativa**: integrada en los procesos administrativos.

En otras palabras, la transparencia debe diseñarse como parte del sistema, no como una obligación genérica.

Registro público de sistemas de IA

El instrumento central de transparencia es el **registro público de sistemas de IA**.

Este registro permite que la ciudadanía conozca qué sistemas utiliza el municipio y con qué finalidad.

Contenido mínimo

- nombre del sistema;
- área responsable;
- finalidad;
- tipo de sistema (apoyo, recomendación, decisión);
- datos utilizados (de forma general);
- nivel de riesgo;
- estado (piloto, implementado).

Función

- habilitar control ciudadano;
- ordenar la información institucional;
- facilitar auditorías y evaluaciones.

No se trata de publicar detalles técnicos complejos, sino de garantizar **visibilidad básica y comprensible**.

Derecho a la información en procesos asistidos por IA

La transparencia debe materializarse también en el vínculo con el ciudadano.

Cuando un proceso administrativo involucra IA, debe garantizarse que la persona:

- sea informada de que se utilizó IA;
- conozca la finalidad del sistema;
- pueda entender, en términos generales, cómo se tomó la decisión;
- tenga acceso a mecanismos de revisión.

Este enfoque se alinea con principios de debido proceso y evita la “automatización invisible” de decisiones públicas.

Explicabilidad: límites y alcance

Uno de los desafíos centrales es la explicabilidad.

No todos los sistemas de IA son plenamente interpretables, pero esto no exime al Estado de su obligación de explicar.

La regulación debe adoptar un enfoque pragmático:

- no exigir explicaciones técnicas complejas;
- sí exigir **explicaciones funcionales comprensibles**.

Por ejemplo:

- qué variables influyeron;
- qué tipo de decisión se tomó;
- qué margen de intervención humana existe.

La explicabilidad debe ser suficiente para que el ciudadano pueda **comprender y eventualmente cuestionar** la decisión.

Identificación del uso de IA en actos administrativos

Un mecanismo clave es la identificación explícita del uso de IA.

Esto puede implicar:

- incluir leyendas en documentos generados con asistencia de IA;
- marcar procesos automatizados en sistemas digitales;
- diferenciar decisiones plenamente humanas de aquellas asistidas.

Este tipo de señalización cumple dos funciones:

- transparencia interna (dentro del municipio);
- transparencia externa (hacia la ciudadanía).

Transparencia y protección de datos: equilibrio necesario

La transparencia no es absoluta. Debe equilibrarse con:

- protección de datos personales;
- seguridad de la información;
- confidencialidad de ciertos procesos.

Esto implica que:

- no todos los datos pueden publicarse;
- no todos los algoritmos deben exponerse completamente;
- debe evitarse generar nuevos riesgos a partir de la transparencia.

El desafío es encontrar un punto de equilibrio entre **apertura y protección**.

Transparencia como mecanismo de control social

La transparencia habilita formas de control más amplias:

- control ciudadano;
- control de organizaciones de la sociedad civil;
- control académico;
- control mediático.

Este ecosistema de control externo contribuye a:

- detectar errores;
- identificar sesgos;
- mejorar la calidad de los sistemas.

En este sentido, la transparencia no es solo un deber, sino un **activo institucional**.

Relación entre transparencia y legitimidad

La legitimidad del uso de IA no depende únicamente de su eficacia, sino de su aceptación social.

La transparencia cumple un rol central en esta construcción:

- reduce incertidumbre;
- genera confianza;
- facilita la comprensión;
- habilita la participación.

Un sistema puede ser técnicamente correcto, pero si es percibido como opaco o injusto, pierde legitimidad.

Estrategia de comunicación pública

La transparencia debe complementarse con una estrategia de comunicación.

Esto implica:

- explicar de manera accesible qué es la IA y cómo se usa;
- comunicar casos de uso concretos;
- mostrar beneficios y límites;
- evitar lenguaje técnico innecesario.

La comunicación no reemplaza la transparencia, pero la hace **comprensible y efectiva**.

Transparencia interna

Además de la dimensión externa, es clave la transparencia dentro del propio municipio.

Los agentes públicos deben:

- conocer qué sistemas existen;
- entender cómo funcionan;
- saber cuándo se utilizan;
- tener acceso a lineamientos claros.

Esto mejora la coordinación, reduce errores y fortalece la gobernanza.

Riesgos de una mala gestión de la transparencia

Una transparencia mal diseñada puede generar:

- sobreexposición de información sensible;
- confusión en la ciudadanía;
- burocratización excesiva;
- desincentivo a la innovación.

Por ello, la transparencia debe ser **estratégica y proporcionada**, no meramente formal.

Conclusión sobre Transparencia

La transparencia es el puente entre la innovación tecnológica y la legitimidad democrática.

Cuando está bien implementada:

- fortalece la confianza;
- mejora la calidad institucional;
- habilita control y aprendizaje.

Cuando no lo está:

- genera desconfianza;
- expone al municipio a conflictos;
- limita la sostenibilidad de la política.

En definitiva, la transparencia no es solo una obligación normativa, sino la condición que permite que la IA sea **aceptada, comprendida y sostenida en el tiempo por la sociedad**.

Evaluación y medición de impacto

La evaluación y medición de impacto es el componente que cierra el ciclo de la política de IA. Mientras la priorización define qué hacer y la implementación ejecuta, la evaluación responde la pregunta clave: **¿la IA está generando valor público real?**

Sin este componente, la política corre el riesgo de convertirse en una sucesión de proyectos tecnológicos sin evidencia de efectividad, lo que debilita su sostenibilidad política, presupuestaria e institucional.

En ausencia de evaluación sistemática, los municipios enfrentan tres problemas recurrentes:

- **opacidad de resultados**: no se sabe si la IA mejora efectivamente la gestión;
- **dificultad para escalar**: no hay evidencia para justificar inversión o expansión;
- **riesgo de "innovación simbólica"**: proyectos que existen, pero no generan impacto.

La evaluación introduce una lógica de **gestión basada en evidencia**, alineando la política de IA con estándares modernos de administración pública.

Qué se entiende por impacto en IA pública

El impacto no debe medirse en términos tecnológicos (uso de algoritmos, cantidad de sistemas), sino en términos de **resultados en la gestión pública y en la vida de la ciudadanía**.

En este sentido, el impacto puede analizarse en al menos cuatro niveles:

a) Impacto operativo

- reducción de tiempos de trámite;
- automatización de tareas;
- disminución de errores administrativos.

b) Impacto en la calidad del servicio

- mejora en la atención al ciudadano;
- mayor precisión en respuestas;

- reducción de reclamos.

c) Impacto en eficiencia

- ahorro de costos;
- mejor asignación de recursos;
- optimización de procesos.

d) Impacto institucional

- fortalecimiento de capacidades internas;
- mejora en la toma de decisiones;
- mayor coordinación interáreas.

Diseño de indicadores: de la intuición a la medición

La evaluación requiere definir **indicadores claros desde el inicio**, idealmente en la etapa de diseño del piloto o proyecto.

Características de los indicadores

- relevantes para el problema abordado;
- medibles con datos disponibles;
- comparables en el tiempo;
- comprensibles para decisores políticos.

Tipos de indicadores

- **de proceso**: miden ejecución (ej. cantidad de trámites procesados).
- **de resultado**: miden efectos directos (ej. tiempo promedio de resolución).
- **de impacto**: miden cambios estructurales (ej. mejora en satisfacción ciudadana).

Un error frecuente es limitarse a indicadores de proceso, sin medir resultados reales.

Línea de base: condición necesaria

No es posible medir impacto sin un punto de comparación.

Por ello, todo proyecto de IA debe partir de una **línea de base**, que refleje cómo funciona el proceso antes de la intervención.

Esto permite responder preguntas como:

- ¿cuánto se redujo el tiempo?
- ¿cuánto mejoró la eficiencia?
- ¿cuánto cambió la calidad del servicio?

Sin línea de base, la evaluación se vuelve subjetiva.

Evaluación de pilotos: primera instancia crítica

Los pilotos son el primer momento formal de evaluación.

La evaluación de un piloto debe ser estructurada y documentada, abordando al menos tres dimensiones:

a) Técnica

- desempeño del sistema;
- estabilidad;
- calidad de resultados.

b) Operativa

- integración con procesos existentes;
- aceptación por parte de los agentes;
- impacto en la carga de trabajo.

c) Jurídica y de riesgo

- cumplimiento normativo;
- aparición de riesgos no previstos;
- necesidad de ajustes regulatorios.

El objetivo no es solo validar la tecnología, sino determinar si es **apropiada para el contexto institucional**.

Evaluación continua: más allá del piloto

La evaluación no termina con la implementación.

Los sistemas de IA deben ser objeto de **monitoreo continuo**, porque:

- los modelos pueden degradarse con el tiempo;
- los datos pueden cambiar;
- los efectos pueden variar según el contexto.

Esto implica establecer:

- indicadores periódicos;
- revisiones programadas;
- mecanismos de alerta ante desviaciones.

La evaluación debe ser un proceso permanente, no un evento puntual.

Integración con la toma de decisiones

La evaluación solo tiene valor si influye en decisiones.

Debe utilizarse para:

- escalar o discontinuar sistemas;
- reasignar recursos;
- redefinir prioridades;
- ajustar regulaciones.

Esto requiere que los resultados sean **accesibles y comprensibles para decisores políticos**, no solo para equipos técnicos.

Evaluación de riesgos e impactos no deseados

Además de medir beneficios, es fundamental evaluar efectos negativos o no previstos:

- aparición de sesgos;
- exclusión de ciertos grupos;
- dependencia tecnológica;
- impactos en el empleo público.

Este enfoque permite anticipar problemas y ajustar la política antes de que se consoliden.

Transparencia de resultados

La evaluación también cumple una función de transparencia.

Publicar resultados —de manera adecuada— permite:

- rendición de cuentas;
- legitimación de la política;
- aprendizaje colectivo.

Esto puede materializarse en:

- informes anuales;
- reportes de proyectos;
- dashboards de indicadores.

La transparencia en la evaluación refuerza la confianza institucional.

Capacidades para evaluar

La evaluación requiere capacidades específicas que no siempre están presentes en los municipios:

- análisis de datos;
- diseño de indicadores;
- interpretación de resultados;
- evaluación de impacto.

Por ello, es necesario:

- formar equipos internos;
- articular con universidades o centros de investigación;
- desarrollar herramientas de monitoreo.

Sin estas capacidades, la evaluación pierde rigor.

Riesgos de no evaluar

La ausencia de evaluación genera:

- continuidad de proyectos ineficientes;
- imposibilidad de justificar inversiones;
- pérdida de credibilidad;
- dificultad para escalar.

En el contexto de IA, donde los resultados pueden ser complejos, estos riesgos se amplifican.

Enfoque progresivo

La evaluación no necesita ser compleja desde el inicio.

Se recomienda:

1. comenzar con indicadores simples;
2. consolidar mecanismos de medición;
3. avanzar hacia evaluaciones más sofisticadas.

Este enfoque permite incorporar la evaluación como práctica institucional sin generar sobrecarga.

Conclusión sobre Evaluación e Impacto

La evaluación y medición de impacto es el mecanismo que conecta la innovación con el valor público.

Cuando está bien implementada:

- permite tomar decisiones informadas;
- mejora la eficiencia del gasto público;
- fortalece la legitimidad de la política.

Cuando no lo está:

- la IA se convierte en una apuesta incierta;
- los resultados no son verificables;
- y la política pierde sostenibilidad.

En definitiva, evaluar no es un ejercicio técnico aislado. Es la condición para que la inteligencia artificial deje de ser una promesa y se convierta en **una herramienta efectiva de mejora de la gestión pública**.