

Inteligencia Artificial y seguridad urbana: desafíos de gobernanza de datos y ciberseguridad en gobiernos locales

Por Victoria Anahí Rosas y Luz Quintana Becerro



OBSERVATORIO DE SEGURIDAD
Y CIBERSEGURIDAD



OBSERVATORIO DE
POLÍTICAS PÚBLICAS

Junio 2026



Inteligencia Artificial y seguridad urbana: desafíos de gobernanza de datos y ciberseguridad en gobiernos locales

1. Introducción.....	2
2. Escenario actual.....	3
2.1 Iniciativas locales y tecnologías aplicadas a la seguridad urbana.....	4
3. IA y seguridad urbana.....	4
4. Gobernanza de datos.....	6
4.1 Producción y circulación de datos.....	6
4.2 Vacíos regulatorios y desafíos normativos.....	7
4.3 Dependencia tecnológica, transparencia y rendición de cuentas.....	7
5. Capacidades estatales y desigualdades territoriales.....	8
6. Líneas de acción: hacia una estrategia de uso seguro y ético.....	9
6.1 Fortalecimiento institucional de la gobernanza de datos.....	9
6.2 Actualización normativa y protocolos de uso de datos.....	9
6.3 Fortalecimiento de capacidades estatales.....	10
6.4 Estrategias integrales de ciberseguridad.....	10
6.5 Transparencia y rendición de cuentas.....	10
7. Reflexiones finales.....	11
8. Referencias.....	13

¿Cómo citar este documento?

Rosas, V. A.; Quintana Becerro, L. (2026). *Inteligencia Artificial y seguridad urbana: desafíos de gobernanza de datos y ciberseguridad en gobiernos locales*. Fundación Metropolitana.



1. Introducción

En los últimos años, la expansión del uso de la inteligencia artificial (IA) en casi todos los ámbitos de la vida social se ha vuelto cada vez más visible. Desde los sistemas de recomendación que organizan los contenidos que consumimos en plataformas digitales, hasta los asistentes virtuales, los algoritmos de navegación, las herramientas de traducción automática o los sistemas de reconocimiento facial presentes en dispositivos móviles y espacios públicos, la IA se ha incorporado de manera progresiva a la vida cotidiana. Este proceso no sólo da cuenta de una creciente disponibilidad tecnológica, sino también de una transformación más profunda en la forma en que se producen, gestionan y utilizan los datos en múltiples esferas.

En este contexto de expansión generalizada, el sector público -y en particular los gobiernos locales- no ha permanecido ajeno a estas dinámicas. En América Latina, la adopción de sistemas basados en datos y herramientas de inteligencia artificial se inscribe en procesos más amplios de modernización estatal, orientados a mejorar la eficiencia administrativa, optimizar la toma de decisiones y fortalecer la relación con la ciudadanía. A nivel municipal, estas tecnologías comienzan a utilizarse en una variedad de áreas que incluyen la gestión de servicios urbanos, la automatización de trámites, el análisis predictivo y la administración de información en tiempo real (Villea Condori, 2025).

La literatura reciente señala que esta incorporación de la IA en la gestión pública local no solo implica la introducción de nuevas herramientas, sino también transformaciones en los modos de gestión, coordinación institucional y producción de información pública (Ariza y Bibiana Ruiz, 2025). No es solo un problema tecnológico, sino de gobernanza de datos y capacidades estatales. En efecto, el uso intensivo de datos y algoritmos habilita nuevas formas de intervención pública, pero al mismo tiempo plantea desafíos vinculados con la disponibilidad y calidad de los datos, la formación de los recursos humanos, la dependencia de proveedores tecnológicos y la necesidad de marcos regulatorios adecuados (Villea Condori, 2025; Ariza y Bibiana Ruiz, 2025).

El uso intensivo de datos y algoritmos también introduce nuevos desafíos vinculados con la protección de información sensible, la transparencia de los sistemas automatizados, la dependencia tecnológica y la capacidad de los gobiernos para supervisar herramientas cada vez más complejas. Estos, adquieren particular relevancia en contextos atravesados por desigualdades estructurales y brechas digitales persistentes. Estos aspectos resultan especialmente críticos en el nivel local, donde la proximidad con la ciudadanía y la gestión directa de políticas públicas intensifican tanto las oportunidades como los riesgos asociados a estas tecnologías.

A partir de este escenario, el presente trabajo se propone analizar la expansión del uso de inteligencia artificial y sistemas basados en datos para gobiernos locales de América Latina, con especial atención a los desafíos que esta tendencia plantea en



términos de gobernanza de datos, capacidades institucionales y regulación. De este modo, se busca aportar a la comprensión de un proceso en desarrollo que está redefiniendo las formas de acción estatal en el territorio y abriendo nuevas preguntas sobre el futuro de la gestión pública local.

2. Escenario actual

En América Latina, el desarrollo de la inteligencia artificial presenta fuertes asimetrías entre países. Mientras algunos avanzaron en estrategias nacionales consolidadas, inversiones sostenidas e infraestructura tecnológica robusta, otros continúan atravesando etapas más incipientes de adopción y regulación. Dentro de este escenario, Argentina ocupa una posición intermedia. El Índice Latinoamericano de Inteligencia Artificial (ILIA) es un índice elaborado por el Centro Nacional de Inteligencia Artificial (CENIA) de Chile, constituye uno de los principales instrumentos de referencia para evaluar el nivel de preparación y desarrollo de los países de la región en materia de inteligencia artificial. El índice analiza dimensiones vinculadas con factores habilitantes, investigación y desarrollo, gobernanza y adopción tecnológica, permitiendo comparar capacidades nacionales y monitorear la evolución de los ecosistemas de IA en América Latina. A partir de indicadores asociados a infraestructura digital, disponibilidad de talento especializado, producción científica, marcos regulatorios y capacidades de innovación, el ILIA clasifica a los países en distintos niveles de desarrollo y destaca las principales fortalezas y debilidades de cada caso.

Acorde a la última edición de este índice, Argentina se ubica dentro del grupo de “adoptantes”, es decir, aquellos Estados que cuentan con capacidades relevantes para incorporar tecnologías basadas en IA, aunque sin posicionarse entre los principales líderes regionales. Los principales diagnósticos sobre inteligencia artificial identifican una serie de factores habilitantes para evaluar la competitividad de un país en la materia: infraestructura digital, conectividad, capacidad de procesamiento de datos, talento especializado, ecosistema científico-tecnológico y marcos regulatorios. En el caso argentino, existen fortalezas importantes en recursos humanos y capacidades técnicas, aunque todavía insuficientes para consolidar un liderazgo regional sostenido.

Particularmente, uno de los principales desafíos identificados se vincula con la disponibilidad, calidad y gobernanza de los datos, elemento considerado central para el desarrollo de soluciones basadas en inteligencia artificial. La expansión de estas tecnologías depende no solo de la capacidad de generar grandes volúmenes de información, sino también de la existencia de mecanismos institucionales que permitan organizar, integrar, compartir y proteger esos datos de manera eficiente y segura. En América Latina, diversos estudios advierten que, si bien existe una creciente producción de datos por parte de organismos públicos y privados, gran parte de esa información permanece fragmentada, subutilizada o inaccesible para el desarrollo de políticas públicas y sistemas de IA.



A ello se suma la existencia de debilidades regulatorias e institucionales. Si bien Argentina avanzó en iniciativas vinculadas con transformación digital y estrategias nacionales de inteligencia artificial, estas políticas muestran dificultades de implementación sostenida, escasa articulación entre niveles de gobierno y limitaciones en términos de capacidades técnicas. Esta situación adquiere especial relevancia frente a problemáticas emergentes como la ciberdelincuencia, la protección de infraestructuras críticas y la gestión segura de información pública sensible, áreas donde las capacidades estatales todavía presentan importantes desafíos.

2.1 Iniciativas locales y tecnologías aplicadas a la seguridad urbana

En este marco, los gobiernos locales comenzaron a incorporar progresivamente tecnologías basadas en datos en distintas áreas de gestión. En la provincia de Buenos Aires, municipios como Tigre, San Isidro y La Plata desarrollaron centros de monitoreo urbano con sistemas de cámaras interconectadas, lectura automática de patentes, anillos digitales y herramientas de análisis en tiempo real orientadas a fortalecer tareas de prevención y respuesta frente al delito.

En muchos casos, estas iniciativas forman parte de procesos más amplios de modernización de la gestión local, orientados a mejorar capacidades operativas y ampliar la coordinación entre áreas estatales, fuerzas de seguridad y diversos gobiernos. Estas iniciativas permiten aumentar la capacidad de procesamiento y circulación de datos vinculados con eventos urbanos y dinámicas delictivas, buscando optimizar la asignación de recursos y reducir tiempos de respuesta.

No obstante, esta expansión tecnológica avanza sobre escenarios institucionales profundamente heterogéneos. Mientras ciertos municipios cuentan con mayores capacidades presupuestarias, infraestructura tecnológica y equipos técnicos especializados, otros presentan niveles limitados de digitalización y fuertes restricciones operativas. Como resultado, la incorporación de inteligencia artificial y sistemas basados en datos en seguridad urbana se desarrolla de manera desigual, generando brechas territoriales en términos de capacidades estatales, niveles de protección de datos y posibilidades de supervisión de los sistemas implementados.

3. IA y seguridad urbana

La incorporación de inteligencia artificial y sistemas basados en datos en políticas de seguridad urbana expresa una doble dinámica. Por un lado, estas herramientas permiten fortalecer capacidades estatales de prevención, monitoreo y respuesta frente al delito. Por otro lado, la literatura advierte que su implementación introduce nuevos riesgos vinculados con la ciberseguridad, la vigilancia, la opacidad algorítmica y la afectación de derechos.

En este marco, la IA aparece como un instrumento relevante para adaptar el funcionamiento policial a entornos sociales y delictivos cada vez más complejos. Su utilización puede contribuir a mejorar tiempos de respuesta, optimizar la asignación



de recursos y focalizar intervenciones en función de información procesada en tiempo real. Asimismo, distintas investigaciones destacan su utilidad para el análisis de datos provenientes de cámaras de seguridad, redes sociales, denuncias o registros administrativos, así como para fortalecer procesos de coordinación institucional y formación interna de las fuerzas de seguridad (Garzón Santos et al., 2025).

No obstante, en muchos casos no se trata de una “inteligencia artificial” autónoma en sentido estricto, sino de métodos estadísticos avanzados aplicados sobre grandes volúmenes de datos. Uno de los ejemplos más conocidos es la llamada policía predictiva, entendida como el uso de información histórica para anticipar dónde y cuándo podrían ocurrir determinados delitos. Estos sistemas utilizan patrones espaciales y temporales con el objetivo de orientar de manera más eficiente la distribución de patrullajes y recursos policiales (Berk, 2021).

El problema es que estos modelos dependen de datos producidos por prácticas policiales previas. En consecuencia, si esos datos reflejan sesgos históricos o desigualdades territoriales, los algoritmos pueden reproducir e incluso amplificar esas diferencias bajo una apariencia de neutralidad técnica (Berk, 2021). Diversos estudios advierten que ciertos sistemas de policía predictiva tienden a concentrar vigilancia sobre barrios o grupos sociales previamente sobrerrepresentados en controles y arrestos. Experiencias como la de Chicago muestran cómo algunos algoritmos terminan identificando sistemáticamente como “zonas de riesgo” a territorios históricamente más vigilados, reforzando circuitos de control selectivo (Hung y Yen, 2023).

Además de los sistemas de policía predictiva, otra área de expansión de la IA en seguridad corresponde a las herramientas de evaluación de riesgo, utilizadas para estimar probabilidades de reincidencia, incumplimiento de medidas judiciales o comisión de nuevos delitos. Estas aplicaciones pueden contribuir a decisiones más consistentes y reducir encarcelamientos innecesarios en casos de bajo riesgo, pero también presentan limitaciones importantes vinculadas con errores predictivos, falta de transparencia y potenciales efectos discriminatorios (Berk, 2021).

A partir de estos casos, Berk (2021) identifica tres debates centrales en torno al uso de IA en seguridad: la precisión de los modelos, los problemas de equidad entre distintos grupos sociales y la dificultad para auditar algoritmos utilizados por organismos públicos. En la práctica, no existe una solución técnica perfecta: mejorar precisión puede afectar criterios de equidad, mientras que aumentar transparencia puede reducir la capacidad predictiva. Por ello, la efectividad de estas herramientas depende menos de su sofisticación técnica que de la existencia de mecanismos adecuados de supervisión, control y protección de derechos.

En este sentido, la inteligencia artificial puede mejorar determinados procesos vinculados con la prevención y gestión de la seguridad, pero sus resultados dependen en gran medida de la calidad de los datos utilizados, los criterios de diseño de los algoritmos y los mecanismos de supervisión implementados. Por ello, evaluar sus



efectos sobre la equidad, la transparencia y el respeto de derechos constituye una condición indispensable para su utilización en funciones sensibles del Estado.

Más allá de estas herramientas, la expansión tecnológica también está modificando el propio significado de la seguridad urbana. Si históricamente las políticas locales se centraron en amenazas físicas, hoy una parte creciente del funcionamiento urbano depende de sistemas digitales que administran información crítica y sostienen servicios esenciales (Hossain et al., 2025). En este contexto, la seguridad urbana ya no puede comprenderse únicamente en términos físicos, sino también como la capacidad de proteger infraestructuras tecnológicas, redes de datos y servicios digitales frente a amenazas cibernéticas. Sistemas de videovigilancia, centros de monitoreo, bases de datos ciudadanas, redes de salud, expedientes electrónicos o plataformas de atención municipal forman parte de una infraestructura cuya interrupción o vulneración puede afectar directamente la vida urbana.

Un ataque informático que paraliza cámaras, bloquea sistemas de emergencia o compromete bases de datos no genera solo un problema técnico: también debilita la capacidad estatal de prevenir riesgos, responder ante incidentes y garantizar servicios esenciales. Desde esta perspectiva, la ciberseguridad no constituye un campo separado de la seguridad pública local, sino una condición necesaria para su funcionamiento en ciudades crecientemente digitalizadas.

4. Gobernanza de datos

La creciente incorporación de inteligencia artificial y sistemas basados en datos en las políticas de seguridad urbana otorga centralidad a la cuestión de la gobernanza de la información. En estos entornos, los datos no constituyen únicamente un insumo técnico, sino también un recurso estratégico que organiza la toma de decisiones públicas, orienta la intervención estatal y redefine las relaciones entre actores públicos y privados. Por ello, el análisis no debe limitarse a la disponibilidad de información, sino también a las condiciones bajo las cuales los datos son producidos, gestionados, almacenados, procesados y utilizados.

4.1 Producción y circulación de datos

La digitalización de la seguridad urbana ha dado lugar a una expansión sostenida en la producción de datos. Sistemas de videovigilancia, tecnologías de reconocimiento facial, plataformas digitales de denuncia, registros administrativos y sensores urbanos generan de manera continua grandes volúmenes de información sobre dinámicas territoriales, circulación de personas y eventos vinculados con la seguridad. Estos flujos configuran ecosistemas de datos urbanos en los que la información circula entre distintas dependencias estatales y, en algunos casos, entre diferentes niveles de gobierno.

Sin embargo, esta circulación no siempre se desarrolla bajo criterios claros de interoperabilidad, estandarización o calidad. En numerosos gobiernos locales, los sistemas de información permanecen fragmentados, respondiendo a estructuras



institucionales diferenciadas o a implementaciones tecnológicas no integradas. Como resultado, los datos suelen encontrarse dispersos en múltiples bases, con formatos heterogéneos y distintos niveles de actualización y confiabilidad, lo que limita su capacidad analítica y dificulta la elaboración de diagnósticos integrales y respuestas coordinadas.

A ello se suma que el acceso a esta información suele estar restringido sin criterios transparentes ni protocolos formalizados que definan quién puede utilizar los datos, con qué objetivos y bajo qué condiciones. Esta falta de trazabilidad debilita los mecanismos de control institucional y amplía el margen para usos discrecionales de información sensible, particularmente relevante en materia de seguridad, donde se procesan datos personales, patrones de comportamiento y registros de circulación en el espacio público.

4.2 Vacíos regulatorios y desafíos normativos

El desarrollo de sistemas basados en inteligencia artificial en el ámbito de la seguridad urbana plantea desafíos que exceden los marcos regulatorios tradicionales. En Argentina, la protección de datos personales se encuentra regulada principalmente por la Ley 25.326 y por la Agencia de Acceso a la Información Pública, que establecen principios generales para el tratamiento de información personal. Sin embargo, este marco fue diseñado en un contexto previo a la expansión de tecnologías basadas en grandes volúmenes de datos y sistemas automatizados de decisión, lo que reduce su capacidad para responder a problemáticas emergentes vinculadas con la inteligencia artificial.

En particular, persisten vacíos regulatorios respecto del uso de algoritmos en funciones de seguridad pública, la implementación de tecnologías de reconocimiento facial, la utilización de modelos predictivos y los mecanismos de auditoría y supervisión de sistemas automatizados. Tampoco existen lineamientos específicos que regulen de manera integral la gobernanza de datos en gobiernos locales, generando escenarios heterogéneos en términos de regulación, capacidades institucionales y protección de derechos.

A nivel municipal, esta situación se traduce en la incorporación de tecnologías digitales sin protocolos claros sobre almacenamiento, intercambio, uso o eliminación de datos. De este modo, la velocidad de adopción tecnológica tiende a superar la capacidad regulatoria del Estado. En otras palabras, la rápida expansión de estas tecnologías suele avanzar más rápido que los procesos legislativos y las capacidades regulatorias estatales, ampliando zonas de incertidumbre jurídica y debilitando los mecanismos de protección frente a posibles abusos o errores.

4.3 Dependencia tecnológica, transparencia y rendición de cuentas

Un rasgo estructural de la digitalización de la seguridad urbana es la fuerte dependencia de proveedores privados para el diseño, implementación y mantenimiento de los sistemas. En muchos casos, los gobiernos locales adquieren



soluciones tecnológicas “llave en mano”, que incluyen infraestructura, software y soporte técnico, lo que facilita su adopción pero reduce la autonomía estatal sobre herramientas que cumplen funciones sensibles.

El uso de sistemas propietarios o de funcionamiento opaco limita la posibilidad de auditar algoritmos, conocer los criterios de procesamiento de datos y evaluar sus impactos sobre la toma de decisiones públicas. Esta opacidad resulta especialmente problemática en el ámbito de la seguridad, donde decisiones basadas en datos pueden afectar derechos fundamentales como la privacidad, la no discriminación o la libertad de circulación. Además, la falta de transparencia dificulta la detección de sesgos, errores y usos indebidos de la información.

Frente a estos desafíos, resulta fundamental fortalecer los mecanismos de auditoría, trazabilidad y control sobre los sistemas utilizados en seguridad urbana. La posibilidad de conocer cómo se procesan los datos, bajo qué criterios operan los algoritmos y qué actores intervienen en su gestión constituye una condición necesaria para reducir riesgos asociados a la opacidad tecnológica y a la dependencia de proveedores externos.

5. Capacidades estatales y desigualdades territoriales

La incorporación de tecnologías digitales en la gestión pública local no se desarrolla sobre un terreno homogéneo. Los gobiernos municipales presentan capacidades estatales desiguales en términos de recursos financieros, infraestructura tecnológica, personal especializado y capacidad de planificación, lo que condiciona las posibilidades de implementar, sostener y supervisar sistemas basados en datos e inteligencia artificial.

La creciente dependencia tecnológica amplía las capacidades potenciales de los gobiernos locales, pero también incrementa su exposición frente a fallas técnicas, vulnerabilidades de seguridad y problemas de coordinación institucional (Hossain et al., 2024). La literatura especializada identifica entre los principales obstáculos para sostener estos procesos: las restricciones presupuestarias, infraestructuras tecnológicas obsoletas, escasez de personal especializado y marcos regulatorios fragmentados o insuficientes (Hossain et al., 2025). Estas limitaciones no sólo afectan la eficacia de las políticas tecnológicas, sino que también condicionan la capacidad estatal para supervisar, auditar y gobernar de manera autónoma los sistemas digitales incorporados a la gestión pública.

En Argentina, estas diferencias se reflejan en los niveles de digitalización municipal. Estudios recientes muestran que los gobiernos locales presentan perfiles muy heterogéneos en infraestructura tecnológica, recursos humanos y capacidades de gestión. Los municipios de la región Pampeana, Patagonia y Gran Buenos Aires concentran los niveles más altos de desarrollo digital, mientras que aquellos ubicados en el Noroeste, Noreste y Cuyo exhiben desempeños relativamente más bajos. La región Centro presenta situaciones intermedias y variables según la dimensión



analizada (Grandinetti et al., 2023). A su vez, investigaciones sobre capacidades municipales señalan que estas brechas tecnológicas se encuentran asociadas a desigualdades más amplias en materia burocrática, organizacional y de provisión de servicios públicos (Cao et al., 2023).

En la provincia de Buenos Aires, estas diferencias también se observan entre municipios metropolitanos y del interior, especialmente en términos de capacidades técnicas, planificación territorial y disponibilidad de recursos institucionales (Ríos, 2019). Los municipios de menor escala demográfica o con mayores restricciones presupuestarias suelen enfrentar mayores dificultades para desarrollar estrategias sostenidas de transformación digital y ciberseguridad.

Estas limitaciones adquieren particular relevancia en áreas como la ciberseguridad, la administración de datos sensibles y el mantenimiento de infraestructuras digitales complejas, donde la falta de recursos especializados puede afectar tanto la continuidad operativa como la capacidad de respuesta ante incidentes.

6. Líneas de acción: hacia una estrategia de uso seguro y ético

El diagnóstico desarrollado a lo largo del informe muestra que la incorporación de inteligencia artificial y sistemas basados en datos en la seguridad urbana de los gobiernos locales avanza en un contexto atravesado por brechas de capacidades, vacíos regulatorios y debilidades en la gobernanza de la información. Las debilidades identificadas en materia de regulación, capacidades estatales y gobernanza de datos requieren una agenda de acción orientada a fortalecer las condiciones de implementación de estas tecnologías. En este marco, es posible identificar cinco líneas prioritarias de acción orientadas a fortalecer la gobernanza de datos y las capacidades estatales en materia de seguridad urbana digital.

6.1 Fortalecimiento institucional de la gobernanza de datos

Una primera línea de acción consiste en consolidar estructuras institucionales claras para la gestión de datos en el ámbito local. La expansión de sistemas basados en inteligencia artificial requiere definir autoridades responsables, competencias específicas y mecanismos de coordinación que permitan ordenar la producción, almacenamiento, circulación y uso de información sensible dentro de las administraciones municipales. En numerosos gobiernos locales, la gestión de datos continúa fragmentada entre distintas áreas, sin protocolos comunes ni criterios homogéneos. Frente a ello, resulta necesario avanzar en esquemas de gobernanza que establezcan estándares compartidos, definan responsabilidades institucionales y fortalezcan la articulación entre municipios, provincias y organismos nacionales. Esto permitiría mejorar la interoperabilidad, reducir superposiciones y fortalecer la capacidad estatal para gestionar de manera más integrada los sistemas basados en datos.



6.2 Actualización normativa y protocolos de uso de datos

Un segundo eje se vincula con la necesidad de adecuar los marcos regulatorios a la expansión de tecnologías basadas en inteligencia artificial. Si bien Argentina cuenta con normas sobre protección de datos personales y acceso a la información pública, gran parte de este marco fue diseñado en contextos previos a la actual masificación de sistemas automatizados y análisis predictivo. En este sentido, resulta necesario desarrollar regulaciones específicas para el uso de inteligencia artificial en seguridad urbana, incorporando criterios claros sobre recolección, almacenamiento, intercambio y eliminación de datos. Asimismo, se vuelve relevante establecer protocolos de uso para tecnologías como videovigilancia inteligente, reconocimiento facial y herramientas predictivas, así como incorporar evaluaciones de impacto algorítmico que permitan anticipar riesgos vinculados con sesgos, discriminación o afectación de derechos.

6.3 Fortalecimiento de capacidades estatales

La transformación del Estado requiere capacidades institucionales capaces de implementar, supervisar y sostener estos procesos en el tiempo. Sin embargo, muchos gobiernos locales enfrentan restricciones vinculadas con la escasez de personal especializado, dificultades de capacitación y limitada disponibilidad de recursos técnicos. Frente a ello, resulta prioritario promover programas de formación continua en análisis de datos, inteligencia artificial, ciberseguridad y gestión de información pública, así como incorporar perfiles técnicos especializados dentro de las estructuras estatales. Estas medidas no sólo permitirían mejorar el funcionamiento de las herramientas implementadas, sino también reducir la dependencia de proveedores privados y fortalecer la autonomía pública en la gestión de sistemas complejos.

6.4 Estrategias integrales de ciberseguridad

La creciente dependencia de infraestructuras digitales vuelve indispensable incorporar estrategias integrales de ciberseguridad como parte constitutiva de las políticas de seguridad urbana. La protección de redes, sistemas y bases de datos municipales constituye una condición necesaria para garantizar la continuidad de servicios esenciales y resguardar información sensible de la ciudadanía.

En este marco, resulta necesario desarrollar políticas preventivas orientadas a reducir vulnerabilidades, fortalecer estándares de seguridad informática y establecer protocolos claros de respuesta frente a incidentes. Esto incluye auditorías periódicas, monitoreo continuo, actualización de sistemas críticos y planes de contingencia ante ataques o filtraciones de datos. Al mismo tiempo, la ciberseguridad requiere una mirada transversal que incorpore aspectos técnicos, organizacionales y de capacitación interna, fortaleciendo la resiliencia digital municipal.



6.5 Transparencia y rendición de cuentas

Finalmente, la expansión del uso de inteligencia artificial en seguridad urbana requiere fortalecer mecanismos de transparencia y rendición de cuentas que permitan supervisar el funcionamiento de los sistemas implementados y garantizar el respeto de derechos ciudadanos.

En muchos casos, la opacidad de los sistemas algorítmicos dificulta conocer qué datos se utilizan, cómo se procesan y bajo qué criterios operan determinadas herramientas. Frente a ello, resulta necesario promover políticas de transparencia activa, auditorías independientes y mecanismos de acceso a la información pública que fortalezcan el control democrático sobre tecnologías que impactan directamente en la vida cotidiana. Asimismo, la participación ciudadana puede contribuir a mejorar la legitimidad y el control social sobre estos procesos.

7. Reflexiones finales

La incorporación de inteligencia artificial y sistemas basados en datos en políticas de seguridad urbana constituye uno de los procesos más relevantes de la transformación digital contemporánea del Estado. En los gobiernos locales, estas tecnologías comenzaron a modificar las formas de producir información, gestionar riesgos y coordinar respuestas frente a problemáticas urbanas cada vez más complejas. La expansión de sistemas de monitoreo en tiempo real, análisis predictivo, automatización de procesos y procesamiento masivo de datos expresa una tendencia más amplia hacia formas de gestión pública crecientemente apoyadas en infraestructuras digitales.

Sin embargo, la expansión de estas tecnologías también introduce nuevos desafíos asociados a la protección de datos, la ciberseguridad, la transparencia de los sistemas automatizados y la supervisión de decisiones basadas en algoritmos. A medida que las funciones públicas dependen cada vez más de infraestructuras digitales complejas, la capacidad de gestionar estos riesgos adquiere una relevancia creciente para los gobiernos locales.

A su vez, el caso argentino refleja tensiones propias de los procesos de modernización tecnológica en contextos de desigualdad territorial y capacidades estatales heterogéneas. Mientras algunos municipios avanzan en estrategias relativamente consolidadas de digitalización e innovación pública, otros enfrentan limitaciones presupuestarias, debilidades técnicas y marcos regulatorios insuficientes. Estas diferencias condicionan las posibilidades de implementación y supervisión, generando escenarios profundamente desiguales.

Asimismo, uno de los principales desafíos radica en la velocidad del cambio tecnológico. La evolución acelerada de la inteligencia artificial y de los ecosistemas digitales contrasta con los tiempos más lentos de adaptación institucional, regulación estatal y construcción de capacidades públicas. En muchos casos, las tecnologías se incorporan más rápido de lo que los marcos regulatorios logran actualizarse,



generando zonas de incertidumbre jurídica y vacíos de supervisión. Esta brecha entre innovación tecnológica y capacidad regulatoria probablemente continúe ampliándose en los próximos años.

Frente a ello, resulta necesario desarrollar marcos institucionales capaces de adaptarse a tecnologías en constante evolución, incorporando mecanismos de evaluación, actualización y aprendizaje que permitan responder a escenarios de cambio permanente. Más que regular herramientas concretas cuyo funcionamiento puede modificarse rápidamente, el desafío consiste en consolidar principios de transparencia, rendición de cuentas, protección de derechos y supervisión pública que orienten el uso de datos y sistemas automatizados. La forma en que los gobiernos locales administren esta transformación será determinante para definir su impacto sobre la seguridad urbana y la calidad democrática de la gestión pública.

En definitiva, la expansión de la inteligencia artificial en la seguridad urbana abre interrogantes sobre cómo compatibilizar innovación tecnológica, protección de derechos y control democrático en ciudades cada vez más mediadas por infraestructuras digitales.



8. Referencias

- Agencia de Acceso a la Información Pública (AAIP). (s. f.). Protección de datos personales. Argentina.gob.ar
- Agencia de Acceso a la Información Pública (AAIP). (s. f.). Sitio oficial. Argentina.gob.ar
- Argentina. (2000). *Ley N.º 25.326 de Protección de los Datos Personales*. Boletín Oficial de la República Argentina, 2 de noviembre de 2000. <https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790>
- Ariza, L., & Bibiana Ruiz, C. (2025). Inteligencia Artificial en el sector público. Enfoques teóricos y propuestas para una gestión innovadora para América Latina. *Gobierno y administración pública*, (10), 119-134. <https://doi.org/10.29393/GP10-9SPLA20009>
- Berk, R. A. (2021). Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement. *Annual Review of Criminology*, 4, 209-237. <https://doi.org/10.1146/annurev-criminol-051520-012342>
- Cao, H. et. al. (2023). Las capacidades estatales con las que los gobiernos locales afrontaron la pandemia de la COVID-19. *Documentos y Aportes en Administración Pública y Gestión Estatal*, 23(40). <https://doi.org/10.14409/daapge.2023.40.e0039>
- Centro Nacional de Inteligencia Artificial (CENIA). (2025). *Índice Latinoamericano de Inteligencia Artificial (ILIA) 2025*. Santiago de Chile: CENIA.
- Garzón Santos, J. L., et al. (2025). Importancia de la inteligencia artificial para los cuerpos de policía: un análisis bibliométrico. *Revista Logos Ciencia & Tecnología*, 17(1). <https://revistalogos.policia.edu.co:8443/index.php/rlct/article/view/2009>
- Grandinetti, R. et al. (2023). Los perfiles de digitalización de los gobiernos locales argentinos en la pandemia del COVID-19. *Documentos Y Aportes En Administración Pública Y Gestión Estatal*, 23(40). <https://doi.org/10.14409/daapge.2023.40.e0040>
- Hossain, S. et al. (2024). Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. *Applied Sciences*, 14(13). <https://doi.org/10.3390/app14135501>
- Hossain, S. et al. (2025). Cybersecurity in local governments: A systematic review and framework of key challenges. *Urban Governance*, 5(1). <https://www.sciencedirect.com/science/article/pii/S2664328624000792?>



[via%3Dihub](#)

- Hung, T. W. & Yen, C. P. (2023). Predictive policing and algorithmic fairness. *Synthese*, 201(206). <https://doi.org/10.1007/s11229-023-04189-0>
- Ríos, L. V. (2019). *Capacidades estatales para la planificación y gestión de las políticas territoriales en la provincia de Buenos Aires: municipios metropolitanos y del interior en el contexto posneoliberal (2004-2015)*. Ponencia en Actas del IV Congreso Latinoamericano de Estudios Urbanos, Universidad Nacional de General Sarmiento, 2236-2262. <https://sedici.unlp.edu.ar/handle/10915/120194>
- Villea Condori, H. F. (2025). Inteligencia artificial y gestión pública: abordaje en gobiernos locales. *Revista El Tribunal*, 5(12), 567-580. <https://revistatribunal.org/index.php/tribunal/article/view/613/1202>