UNIVERSIDAD INTERNACIONAL DE LAS AMERICAS

FACULTAD DE ADMINISTRACION DE EMPRESAS

TRABAJO FINAL DE GRADUACION PARA OPTAR POR EL GRADO DE MAESTRIA DE ADMINSTRACION DE EMPRESAS CON ENFASIS EN GERENCIA

“Estrategia administrativa para la implementación de alertas tempranas basadas en inteligencia artificial en el Centro de Monitoreo de San José, hacia una gestión eficiente y preventiva del delito en el año 2026”

Licda. Mónica Coto Murillo
ESTUDIANTE

PhD. Harold Coronado
TUTOR

SAN JOSÉ, SEDE AMON
MARZO, 2026

Dedicatoria

Dedico esta tesis, en primer lugar, a Dios, que es mi fuente e inspiración de servicio, amor y entrega, él me ha guido en cada etapa de mi vida profesional y personal como ese buen Pastor para encontrar sabiduría, discernimiento y fortaleza para perseverar con propósito aun en los momentos de mayor desafío.

A mi padre Eduardo (QDP) y a mi mama Emilce por ser ambos un modelo de fe, perseverancia, trabajo, esfuerzo y honestidad. A mi esposo German por su apoyo incondicional, a mi hija Emiliana, a mis hijos Isaac, Sebastián y Juan Diego, mi nieto Juan David, por ser mis motores a ser mejor persona, gracias por su apoyo constante y paciencia para compartir sus espacios con mis sueños y retos. Gracias Familia amada por ayudarme a no renunciar a la convicción de que si podía con este sueño de ser Master y estudiar en la Universidad que soné de joven.

A la Municipalidad de San Jose, institución que ha sido mi casa profesional durante treinta años, en la cual he tenido el privilegio de servir a la ciudadanía desde diferentes espacios. Este trabajo es reflejo del aprendizaje acumulado en el ejercicio de la gestión pública, del compromiso con la seguridad ciudadana y del convencimiento de que la innovación tecnológica, bien dirigida, puede transformar positivamente la vida de las personas.

A mi querida compañera de batallas Maribel, a mi jefe, compañeros y colaboradores de Seguridad Electrónica, con quienes he compartido sueños, desafíos y logros. Su trabajo, entrega y vocación de servicio han enriquecido mi visión de liderazgo y han reafirmado mi creencia en el valor del trabajo en equipo como motor del desarrollo institucional. Finalmente, dedico este esfuerzo a la ciudadanía del Canton de San Jose, razón de toda mi gestión pública, siempre con la esperanza de que mi amada San Jose sea un lugar más próspero, más seguro y sostenible**.**

Agradecimientos

A Dios Todopoderoso, fuente suprema de sabiduría, fortaleza y propósito, elevo en primer lugar mi más profunda gratitud. Su gracia, dirección y fidelidad han sido el fundamento permanente que sostuvo cada etapa de mi vida.

A mi familia, pilar inquebrantable de inspiración, amor, paciencia y comprensión, expreso mi más sincero agradecimiento. Su apoyo constante, sus palabras oportunas y su confianza en mis capacidades fueron un motor esencial para perseverar con disciplina, humildad y esperanza. Cada logro alcanzado es también reflejo de su entrega silenciosa y generosa. Su presencia ha sido refugio emocional, inspiración espiritual y estímulo permanente para crecer como persona, profesional y servidora pública.

Al Phd. Harold Coronado, tutor y guía de esta tesis y a la Licda. Maribel Fallas, asesora académica, manifiesto mi reconocimiento por su excelencia, rigor metodológico y compromiso formativo. Sus orientaciones, observaciones críticas y acompañamiento intelectual contribuyeron de manera decisiva al fortalecimiento de esta investigación, elevando su calidad científica y su pertinencia social. A la institución universitaria y a este programa de posgrado que fortaleció no solo mis competencias técnicas, sino también mi visión estratégica y humanista de la gestión.

A mis jefaturas, colegas y equipos de trabajo en el ámbito profesional, extiendo un sincero agradecimiento por su respaldo, comprensión y cooperación durante el desarrollo de este proceso. Su confianza y colaboración facilitaron la integración entre la teoría y la práctica, permitiéndome consolidar una propuesta investigativa con impacto real en la gestión pública.

A mis pastores, líderes espirituales y comunidad de fe, gracias por su acompañamiento pastoral, sus oraciones y su consejo oportuno. Su guía contribuyó a fortalecer mi carácter, mi integridad y mi vocación de servicio, recordándome que el liderazgo auténtico se ejerce con humildad, justicia y amor.

Que este trabajo académico sea, ante todo, una expresión de gratitud a Dios, un compromiso con la excelencia profesional y una contribución responsable al desarrollo institucional y social.

Acrónimos

Acrónimo	Significado
AI	Artificial Intelligence (Inteligencia Artificial)
BID	Banco Interamericano de Desarrollo
CCTV	Circuito Cerrado de Televisión (Closed-Circuit Television)
EBP	Evidence-Based Policing (Policía basada en evidencia)
GDPR	Reglamento General de Protección de Datos (General Data Protection Regulation)
IA	Inteligencia Artificial
ILP	Intelligence-Led Policing (Policía basada en inteligencia)
ISO	Organización Internacional de Normalización (International Organization for Standardization)
KPI	Indicador Clave de Desempeño (Key Performance Indicator)
ROI	Retorno de Inversión (Return on Investment)
TTR	Tiempo de Respuesta Total
UNODC	Oficina de las Naciones Unidas contra la Droga y el Delito

Glosario

Término	Definición
Analítica avanzada	Procesos y técnicas de análisis de datos complejos para extraer patrones, predicciones y soporte a decisiones estratégicas.
Alertas tempranas	Señales generadas por sistemas de IA que anticipan posibles incidentes delictivos para permitir acción preventiva.
Escalabilidad	Capacidad de un sistema para crecer o adaptarse a mayores volúmenes de datos, usuarios o funciones sin perder eficiencia.
Fases de implementación	Etapas planificadas para introducir un sistema o modelo, incluyendo diagnóstico, piloto, ajuste, escalamiento y evaluación.
Gobernanza de datos	Conjunto de políticas, procesos y estándares que aseguran calidad, seguridad, trazabilidad y uso ético de la información.
Hot Spots Policing	Estrategia de focalización de recursos policiales en zonas con alta incidencia delictiva.
Human-in-the-loop	Concepto que garantiza supervisión humana en decisiones críticas tomadas o apoyadas por sistemas automatizados.
Inteligencia operativa	Proceso de análisis y utilización de información para tomar decisiones estratégicas de seguridad.
Monitoreo inteligente	Uso de tecnología avanzada (cámaras, sensores, IA) para anticipar y prevenir incidentes delictivos, integrando información operativa y análisis predictivo.
Prevención situacional	Estrategia que busca reducir oportunidades delictivas mediante modificaciones en el entorno, procesos y comportamiento de los actores.
Sesgo algorítmico	Distorsión o error sistemático en decisiones automatizadas que puede generar resultados injustos o inexactos.
Tiempo de Respuesta Total (TTR)	Intervalo de tiempo desde la detección de un evento hasta la acción de respuesta correspondiente.

Término	Definición
KPI (Indicador Clave de Desempeño)	Métrica utilizada para evaluar el éxito de un proceso o actividad frente a objetivos específicos.

Tabla de contenido

Índice de Figuras

Índice de Tablas

Resumen Ejecutivo

Esta investigación analiza la capacidad preventiva del Centro de Monitoreo del Cantón Central de San José y propone un modelo de gestión basado en alertas tempranas mediante inteligencia artificial (IA). Se identificaron brechas entre la infraestructura tecnológica existente y su aprovechamiento estratégico para la prevención del delito. La metodología combinó análisis cuantitativo de encuestas, entrevistas semiestructuradas y revisión documental, complementada con un análisis causa-efecto mediante el diagrama de Ishikawa, que permitió identificar factores tecnológicos, operativos, humanos, estratégicos y éticos que limitan la efectividad del Centro.

El modelo propuesto integra cuatro componentes: tecnológico, operativo, gobernanza y ética, y estratégico y evaluación, implementados en fases de diagnóstico, piloto, ajuste, escalamiento y evaluación. Se definen indicadores cuantitativos y cualitativos para medir eficiencia operativa, tiempo de respuesta, cobertura de alertas, percepción de seguridad y confianza ciudadana. Asimismo, se incluyen medidas de mitigación de riesgos, estrategias de sostenibilidad y escalabilidad, y lineamientos éticos y de gobernanza de datos.

La propuesta busca optimizar la prevención del delito, fortalecer la toma de decisiones basada en evidencia y promover la modernización institucional del Centro de Monitoreo. Los resultados son transferibles a contextos municipales similares, contribuyendo al desarrollo de ciudades inteligentes y gestión pública basada en datos.

Palabras clave: inteligencia artificial, alertas tempranas, monitoreo inteligente, prevención del delito, gobernanza de datos.

Abstract

This research examines the preventive capacity of the Central Canton of San José Monitoring Center and proposes a management model based on early alerts using artificial intelligence (AI). Gaps were identified between the existing technological infrastructure and its strategic use for crime prevention. The methodology combined quantitative survey analysis, semi-structured interviews, and document review, complemented by a cause-effect analysis using the Ishikawa diagram, which identified technological, operational, human, strategic, and ethical factors limiting the Center's effectiveness.

The proposed model integrates four components: technological, operational, governance and ethics, and strategic and evaluation, implemented in phases of diagnosis, pilot, adjustment, scaling, and evaluation. Quantitative and qualitative indicators measure operational efficiency, response time, alert coverage, public perception of security, and institutional trust. Risk mitigation measures, sustainability and scalability strategies, and ethical and data governance guidelines are also included.

The proposal aims to optimize crime prevention, strengthen evidence-based decision-making, and promote institutional modernization of the Monitoring Center. The results are transferable to similar municipal contexts, contributing to the development of smart cities and data-driven public management.

Keywords: artificial intelligence, early alerts, intelligent monitoring, crime prevention, data governance.

Introducción

El Cantón Central de San José, núcleo político, económico y social de Costa Rica, enfrenta en la actualidad desafíos complejos en materia de seguridad ciudadana, movilidad humana y gestión del territorio. Con una población residente que supera los 350.000 habitantes y una población flotante diaria cercana al millón de personas, la capital del país concentra una elevada densidad urbana y una dinámica social que demanda respuestas institucionales oportunas, coordinadas y sostenibles. Este contexto exige la articulación de diversos actores públicos y privados, así como la adopción de estrategias modernas, eficientes y apoyadas en el uso estratégico de la tecnología para atender las necesidades de la ciudadanía.

En este escenario, el Centro de Monitoreo de la Policía Municipal de San José desempeña un papel fundamental en la gestión de la seguridad urbana, al integrar recursos humanos, operativos y tecnológicos orientados a la atención de incidentes y al resguardo del espacio público. Actualmente, dicho centro cuenta con una amplia red de dispositivos tecnológicos, entre los que destacan cámaras de videovigilancia ubicadas en parques, bulevares, vías principales, barrios y comunidades, así como sistemas de alarmas instalados en viviendas, comercios y barrios organizados, todos ellos enlazados a la Central de Monitoreo. Estos esfuerzos reflejan el compromiso institucional por mitigar la inseguridad ciudadana y mejorar la capacidad de respuesta ante situaciones de riesgo.

No obstante, pese a los avances logrados, la gestión de la seguridad desde el Centro de Monitoreo se caracteriza predominantemente por un enfoque reactivo, en el cual la intervención policial ocurre una vez que el evento delictivo ha tenido lugar o tras la recepción de una alerta ciudadana. Esta dinámica limita la posibilidad de anticipar situaciones de riesgo y de desplegar acciones preventivas oportunas, lo cual resulta especialmente relevante en un contexto urbano complejo y altamente dinámico como el del Cantón Central de San José. En este sentido, la ausencia de herramientas avanzadas

de análisis predictivo y de sistemas automatizados de detección temprana representa una brecha significativa en la gestión integral de la seguridad ciudadana.

El Centro de Monitoreo del cantón se ha consolidado como una herramienta clave para la gobernanza urbana al articular más de seis mil cuatrocientos dispositivos electrónicos y una creciente interacción con la ciudadanía mediante aplicaciones móviles que facilitan la comunicación directa con la institución. Sin embargo, la capacidad operativa del equipo humano, conformado por hombres y mujeres de la Policía Municipal comprometidos con la seguridad ciudadana, se ve desafiada por la magnitud del territorio, el volumen de información generada y la necesidad de monitorear de forma simultánea una extensa red de dispositivos, sin contar actualmente con aplicaciones basadas en inteligencia artificial que apoyen la labor analítica y la toma de decisiones.

La relación entre la cantidad de operadores disponibles, la población atendida y la complejidad del entorno urbano evidencia la necesidad de fortalecer las capacidades institucionales del Centro de Monitoreo mediante la incorporación de modelos de analítica automatizada, el aprovechamiento de tecnologías emergentes y el fortalecimiento de la infraestructura tecnológica existente. En este contexto, la inteligencia artificial surge como una herramienta estratégica con potencial para transformar la gestión de la seguridad, al permitir la identificación de patrones, la generación de alertas tempranas y el apoyo a la toma de decisiones orientadas a la prevención del delito.

En razón de lo expuesto, la presente investigación tiene como objetivo principal proponer una estrategia administrativa para la modernización e implementación de alertas tempranas basadas en inteligencia artificial en el Centro de Monitoreo del Cantón Central de San José, orientada a fortalecer una gestión eficiente y preventiva del delito. La investigación se desarrolla desde un enfoque cualitativo, sustentado en la revisión documental, la realización de entrevistas a personas expertas en seguridad ciudadana,

inteligencia artificial y gestión pública, así como en el análisis de experiencias y referentes internacionales relacionados con el uso de tecnologías predictivas aplicadas a la prevención del delito en contextos urbanos.

A partir del interés por conocer y analizar la situación actual del Centro de Monitoreo, el estudio se orienta al diagnóstico de sus capacidades tecnológicas, operativas y analíticas; a la identificación de oportunidades de mejora administrativa que faciliten la incorporación de herramientas de inteligencia artificial para la toma de decisiones; al diseño de una propuesta de modelo de gestión alineada con los objetivos estratégicos de la Municipalidad de San José; y al planteamiento de un plan de implementación que considere la sostenibilidad financiera, la gestión institucional y la evaluación del impacto dentro de la estructura organizativa existente.

En este sentido, la investigación se enmarca en la necesidad de fortalecer la gestión administrativa y operativa del Centro de Monitoreo mediante un enfoque integral que articule tecnología, procesos y talento humano. La propuesta que se desarrolla busca aportar elementos estratégicos para la modernización institucional, reconociendo que la innovación tecnológica requiere no solo de infraestructura adecuada, sino también de capacidades organizacionales, marcos administrativos claros y mecanismos de seguimiento y evaluación que garanticen su sostenibilidad en el tiempo.

Finalmente, el estudio se plantea como un aporte a la gestión pública local, al explorar alternativas innovadoras para mejorar la seguridad ciudadana desde un enfoque preventivo, con el potencial de generar aprendizajes aplicables a otros contextos municipales del país. De esta manera, la investigación pretende contribuir al fortalecimiento de una gestión pública más eficiente, proactiva y orientada a la prevención del delito en el Cantón Central de San José.

Capítulo I

1.1 Planteamiento del problema

La seguridad ciudadana en los entornos urbanos constituye uno de los principales desafíos para la gestión pública local, especialmente en capitales latinoamericanas caracterizadas por alta densidad poblacional, concentración de actividades comerciales y elevada movilidad diaria. En el Cantón Central de San José, la dinámica delictiva ha evolucionado hacia formas más complejas, móviles y territorialmente focalizadas, lo que exige capacidades institucionales no solo de reacción, sino principalmente de anticipación y prevención del delito.

De acuerdo con estadísticas oficiales del Organismo de Investigación Judicial, y datos de la Dirección de Seguridad Ciudadana y Policía Municipal de San José; durante los últimos años los delitos contra la propiedad y las personas en el casco central de San José han mostrado una tendencia sostenida, concentrándose en espacios públicos de alta concurrencia como bulevares, paradas de buses, en zonas comerciales y residenciales. Esta situación genera impactos directos en la percepción de seguridad ciudadana, el uso del espacio público, la actividad económica y los costos asociados a la atención policial e incluso judicial.

Como respuesta institucional, la Municipalidad de San José ha realizado inversiones significativas en infraestructura tecnológica, particularmente en sistemas de videoprotección y en la operación permanente del Centro de Monitoreo de San José, que atiende o brinda respuesta por medio de la Policía Municipal de San José.

Actualmente, dicho centro administra un número considerable de cámaras de vigilancia, monitoreadas por personal humano en turnos continuos, con el objetivo de observar en tiempo real los espacios públicos y atender incidentes reportados por terceros.

No obstante, el modelo operativo vigente se caracteriza por un enfoque predominantemente reactivo, en el cual la mayoría de las acciones se activan posterior a la ocurrencia del evento delictivo o a partir de llamadas ciudadanas, reportes policiales o solicitudes judiciales. La ausencia de herramientas de análisis automatizado basadas en inteligencia artificial impide procesar en tiempo real el gran volumen de información visual que se genera de manera continua, limitando la capacidad del Centro de Monitoreo para identificar patrones, comportamientos anómalos o situaciones de riesgo antes de que se materialice el delito.

Desde una perspectiva administrativa y operativa, esta condición actual genera ineficiencias medibles en términos de tiempo, costos y uso de recursos. Diversos estudios señalan que un operador puede monitorear eficazmente un número limitado de cámaras de forma simultánea, antes de que se produzca una disminución significativa en la capacidad de detección de eventos relevantes. Mackworth (1948) demostró que en tareas de vigilancia visual sostenida, la capacidad de detección de eventos relevantes tiende a disminuir significativamente después de aproximadamente 30 minutos de monitoreo continuo. En contextos donde un operador debe supervisar decenas de dispositivos, aumenta el riesgo de omisiones, retrasos en la activación de alertas y desgaste del recurso humano.

Asimismo, la falta de sistemas inteligentes de apoyo a la decisión conlleva mayores tiempos de respuesta institucional, utilización no priorizada del recurso policial, duplicidad de esfuerzos interinstitucionales y una escasa capacidad para evaluar el impacto preventivo real de la videovigilancia. Todo ello se traduce en costos operativos

elevados sin una mejora proporcional en los resultados en materia de prevención del delito.

Desde un enfoque administrativo y operativo, la ausencia de inteligencia artificial en los centros de monitoreo se traduce en una serie de problemas estructurales que afectan la eficiencia institucional y la capacidad preventiva del sistema, entre los cuales se destacan los siguientes:

1. Sobrecarga operativa y cognitiva del personal de monitoreo.
2. Detección tardía de eventos delictivos o situaciones de riesgo.
3. Ausencia de análisis predictivo y preventivo del delito.
4. Falta de priorización territorial basada en niveles de riesgo.
5. Uso ineficiente de los recursos humanos y tecnológicos disponibles.
6. Dependencia de reportes externos para la activación de respuestas.
7. Escasa interoperabilidad entre instituciones de seguridad.
8. Limitada estandarización de los procesos de análisis de información.
9. Incremento de costos operativos sin mejoras sustantivas en resultados.
10. Débil capacidad de evaluación y seguimiento del impacto preventivo.

Diversas experiencias internacionales han evidenciado el impacto positivo de la incorporación de inteligencia artificial en centros de monitoreo. En Medellín, el desarrollo del Centro Avanzado de Control y Seguridad (C5) integra sistemas de videovigilancia inteligente y analítica de datos con el objetivo de mejorar la detección temprana de eventos, optimizar la asignación de recursos y reducir los tiempos de respuesta ante emergencias (Alcaldía de Medellín, 2023).

De manera similar, en Santiago de Chile se implementaron sistemas de televigilancia con inteligencia artificial capaces de generar alertas automáticas ante incidentes de tránsito y delitos, fortaleciendo la capacidad preventiva y la reacción oportuna de los operadores (Infodefensa, 2024).

En el caso de la Ciudad de Buenos Aires, municipios como Vicente López han incorporado video analítica basada en inteligencia artificial para mejorar la vigilancia de espacios públicos y apoyar la toma de decisiones en materia de seguridad ciudadana (Hanwha Vision, 2023).

Asimismo, en ciudades europeas como Barcelona y otras urbes españolas, el uso de sistemas de análisis inteligente de video ha permitido reducir significativamente la cantidad de falsas alarmas, optimizando la carga operativa de los centros de monitoreo y permitiendo focalizar los recursos en eventos realmente críticos (Cinco Días, 2025).

Si bien estos casos no constituyen evaluaciones experimentales controladas, sí representan experiencias documentadas que ilustran tendencias actuales en la aplicación de inteligencia artificial a la gestión de la seguridad ciudadana y al fortalecimiento de los modelos de prevención del delito

Ante esta realidad, se evidencia una brecha entre la infraestructura tecnológica existente en el Centro de Monitoreo de San José y su aprovechamiento estratégico desde una perspectiva administrativa. La problemática central radica, por tanto, en la ausencia de una estrategia administrativa que permita implementar alertas tempranas basadas en inteligencia artificial, orientadas a transformar el modelo actual de vigilancia reactiva en uno preventivo, eficiente y basado en datos.

En este contexto, se plantea como interrogante central de la investigación la siguiente pregunta:

¿Cuál es la estrategia administrativa más adecuada para implementar alertas tempranas basadas en inteligencia artificial en el Centro de Monitoreo de San José, orientada a una gestión eficiente y preventiva del delito, en el año 2026?

En consecuencia, la ausencia de una estrategia administrativa estructurada limita la transición del Centro de Monitoreo hacia un modelo de gestión preventiva basado en datos, lo que justifica la necesidad de formular una propuesta estratégica orientada a la implementación de alertas tempranas basadas en inteligencia artificial.

Para efectos de la presente investigación, la estrategia administrativa se entiende como el conjunto articulado de decisiones, lineamientos, procesos, estructuras organizacionales, mecanismos de gobernanza y asignación de recursos orientados a alcanzar objetivos institucionales de manera eficiente, sostenible y alineada con la planificación estratégica municipal.

En este contexto, la estrategia administrativa para la implementación de alertas tempranas basadas en inteligencia artificial no se limita a la incorporación tecnológica, sino que comprende un proceso integral de transformación organizacional que involucra:

1. Planificación estratégica y alineación institucional.
2. Rediseño de procesos operativos y flujos de información.
3. Gestión del cambio y fortalecimiento del talento humano.

4. Gobernanza de datos y cumplimiento normativo.
5. Sostenibilidad financiera y evaluación de desempeño.

La estrategia se concibe bajo un enfoque sistémico, en el cual la tecnología constituye un habilitador de valor público y no un fin en sí mismo. Por tanto, su implementación requiere coherencia entre estructura organizativa, cultura institucional, capacidades técnicas y mecanismos de seguimiento y control.

Desde esta perspectiva, la investigación se orienta a diseñar una hoja de ruta administrativa que permita transitar de un modelo reactivo de vigilancia hacia un modelo preventivo basado en datos, garantizando eficiencia operativa, transparencia institucional y sostenibilidad en el tiempo.

1.2 Objetivos de la investigación

1.2.1 Objetivo general

Proponer una estrategia administrativa para la implementación de alertas tempranas basadas en inteligencia artificial en el Centro de Monitoreo de San José, orientada a una gestión eficiente y preventiva del delito, en el año 2026.

1.2.2 Objetivos específicos

- Diagnosticar el estado actual del Centro de Monitoreo de San José en relación con sus capacidades tecnológicas, operativas y administrativas.
- Identificar las principales brechas y oportunidades de mejora en la gestión administrativa que faciliten la incorporación de inteligencia artificial en los procesos de monitoreo.
- Diseñar un modelo de gestión administrativa que integre alertas tempranas basadas en inteligencia artificial, alineado con los objetivos estratégicos municipales.
- Proponer un plan de implementación que contemple sostenibilidad financiera, articulación interinstitucional y evaluación del impacto de la estrategia propuesta.

1.3 Justificación de la investigación

La presente investigación se realiza ante la necesidad de fortalecer la gestión de la seguridad ciudadana en el Cantón Central de San José, mediante la modernización del modelo operativo del Centro de Monitoreo municipal. A pesar de las inversiones realizadas en infraestructura tecnológica, persiste una brecha significativa entre los recursos disponibles y su capacidad para generar efectos preventivos reales en la reducción del delito.

La importancia del estudio radica en su contribución a la gestión pública local, al proponer una estrategia administrativa que permita optimizar el uso de los recursos humanos, tecnológicos y financieros mediante la incorporación de inteligencia artificial. Esto resulta particularmente relevante en un contexto de restricciones presupuestarias, incremento de la violencia urbana y creciente demanda ciudadana por mayor eficiencia, transparencia y resultados medibles.

El valor potencial de la investigación se manifiesta en la posibilidad de reducir tiempos de respuesta, mejorar la asignación territorial de recursos, fortalecer la toma de decisiones basada en datos y transformar el enfoque reactivo de la seguridad en un modelo preventivo e inteligente. Asimismo, el estudio puede servir como referencia para otras municipalidades del país interesadas en procesos de modernización institucional.

La viabilidad del estudio se sustenta en el acceso a información institucional, entrevistas a actores clave, análisis documental, benchmarking internacional y el uso de metodologías administrativas y estratégicas, sin requerir la implementación directa de tecnologías durante el desarrollo de la investigación.

1.4 Alcance de la investigación

La investigación tiene un alcance descriptivo y propositivo. En una primera fase, se analiza la situación actual del Centro de Monitoreo de San José, considerando su estructura administrativa, procesos operativos y uso de tecnologías de videoprotección.

En una segunda fase, se desarrolla una propuesta de estrategia administrativa orientada a la implementación de alertas tempranas basadas en inteligencia artificial, como mecanismo para fortalecer la gestión preventiva del delito.

El ámbito geográfico se limita al Cantón Central de San José, con énfasis en las zonas que cuentan con infraestructura de videoprotección municipal. Desde el punto de vista institucional, el estudio se circunscribe a la Municipalidad de San José y su Centro de Monitoreo, considerando la necesaria articulación con instituciones de seguridad pública.

1.5 Limitaciones de la investigación

La presente investigación se desarrolla con ciertas limitaciones asociadas a factores geográficos, institucionales, metodológicos y contextuales; que condicionan su alcance y profundidad, sin comprometer la validez de los resultados ni la pertinencia de la propuesta administrativa; y que se detallan a continuación.

1. Alcance geográfico y jurisdiccional: El estudio se circunscribe exclusivamente al Cantón Central de San José y a las competencias propias de la Municipalidad, lo que limita la generalización de los resultados a otros municipios del país.

2. Nivel estratégico-administrativo: La investigación se centra en el diseño de una estrategia administrativa y no aborda el desarrollo técnico de algoritmos de inteligencia artificial ni aspectos de programación avanzada, por lo que no se evalúa la implementación técnica del sistema.

3. Acceso a información sensible: Se identificó acceso restringido a información operativa del Centro de Monitoreo, debido a razones de seguridad institucional, lo cual condicionó la profundidad de ciertos análisis.

4. Disponibilidad de personal para entrevistas y talleres: La limitada disponibilidad del personal técnico y operativo, por sus responsabilidades en turnos rotativos, restringió el número de entrevistas y la participación en talleres de consulta.

   Además, una limitante del estudio radica en el carácter no probabilístico de la muestra ciudadana, lo que restringe la posibilidad de realizar análisis inferenciales o extrapolaciones poblacionales. No obstante, la información recopilada cumple una función diagnóstica complementaria dentro del enfoque mixto adoptado.

5. Escasez de experiencias locales y nacionales: La falta de antecedentes previos en el país sobre el uso de inteligencia artificial en videoprotección municipal reduce el acceso a referentes nacionales, lo que obligó a fundamentar parte del estudio en experiencias internacionales.

6. Ausencia de normativa específica: La inexistencia de un marco legal nacional sobre la aplicación de inteligencia artificial en seguridad pública dificulta la proyección jurídica de la estrategia propuesta, aunque no afecta su validez conceptual y administrativa.

7. Tiempo limitado para el desarrollo de la investigación: El calendario académico del posgrado condicionó la duración y el alcance del estudio.

8. Restricciones presupuestarias institucionales: Las limitaciones financieras actuales de la Municipalidad podrían afectar la viabilidad inmediata de implementar la estrategia propuesta, aunque no inciden en la formulación conceptual de la misma.

A pesar de estas limitaciones, la investigación mantiene su validez académica y estratégica, al centrarse en la propuesta de un modelo administrativo para la implementación de alertas tempranas basadas en inteligencia artificial, orientado a fortalecer la gestión preventiva del delito en el Cantón Central de San José.

1.6 Antecedentes

El Centro de Monitoreo de San José, creado hace aproximadamente quince años como una unidad estratégica municipal, inmersa en la Dirección de Seguridad Ciudadana y Policía Municipal para la vigilancia del espacio público y la coordinación interinstitucional en materia de seguridad ciudadana. A lo largo de los últimos años, ha fortalecido su infraestructura tecnológica y su capacidad operativa; sin embargo, el modelo de gestión ha permanecido centrado en la observación reactiva y el apoyo posterior a procesos judiciales.

A nivel internacional, diversas ciudades como Medellín, Buenos Aires, Santiago de Chile, Barcelona y otros han avanzado hacia modelos de seguridad inteligente mediante el uso de inteligencia artificial, análisis predictivo y plataformas de gestión integrada, evidenciando mejoras significativas en la prevención del delito y la eficiencia institucional.

En el contexto nacional, las experiencias en inteligencia artificial aplicada a la seguridad pública son aún incipientes, aunque existen esfuerzos aislados en el sector privado o en instituciones como el OIJ para explorar estas tecnologías; lo que refuerza la pertinencia de la presente investigación como aporte innovador y estratégico.

1.6.1 Antecedentes Internacionales

A nivel internacional, diversos estudios han analizado la aplicación de inteligencia artificial, analítica predictiva y sistemas de videovigilancia inteligente en la gestión de la seguridad ciudadana. Estas investigaciones abarcan enfoques desde la criminología computacional, la ciencia de datos, la gobernanza digital y la administración pública, proporcionando fundamentos teóricos y empíricos relevantes para el diseño de estrategias administrativas orientadas a la prevención del delito.

Tabla 1. *Antecedentes Internacionales*

Autor/Año	Título del Estudio	Variables Consideradas	Área de Conocimiento	Resumen
Perry, McInnis, Price, Smith & Hollywood (2013)	*Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*	Predicción del delito, asignación de recursos, análisis espacial	Seguridad Pública / Criminología	Estudio de RAND Corporation que analiza cómo modelos matemáticos permiten anticipar zonas de alta incidencia delictiva, optimizando la distribución policial y mejorando la eficiencia operativa.
Mohler et al. (2015)	*Randomized Controlled Field Trials of Predictive Policing*	Algoritmos predictivos, reducción del delito, eficiencia operativa	Ciencia de Datos / Seguridad	Investigación empírica que demuestra que la aplicación de modelos predictivos espaciales puede reducir delitos contra la propiedad mediante patrullaje focalizado.
Ferguson (2017)	*The Rise of Big Data Policing*	Big Data, vigilancia tecnológica, implicaciones legales	Derecho / Políticas Públicas	Analiza el impacto del uso de datos masivos en la seguridad pública y plantea la necesidad de marcos regulatorios y administrativos sólidos para su implementación responsable.
Meijer & Wessels (2019)	*Predictive Policing: Review of Benefits and Drawbacks*	IA, gobernanza digital, gestión institucional	Administración Pública	Revisión crítica sobre ventajas y riesgos de la IA en seguridad pública, destacando la importancia de la capacidad organizacional y la transparencia institucional.

Brayne (2017)	*Big Data Surveillance: The Case of Policing*	Vigilancia algorítmica, bases de datos integradas, eficiencia policial	Sociología / Seguridad	Examina cómo el uso de bases de datos y algoritmos transforma la gestión policial, evidenciando mejoras operativas pero también desafíos éticos.
Kitchin (2014)	*The Real-Time City? Big Data and Smart Urbanism*	Smart cities, datos en tiempo real, gobernanza urbana	Estudios Urbanos / Gobernanza	Analiza cómo el uso de datos en tiempo real mejora la toma de decisiones urbanas, incluyendo seguridad ciudadana y gestión preventiva.
Caplan, Kennedy & Petrossian (2011)	*Risk Terrain Modeling*	Modelado espacial del riesgo, prevención situacional	Criminología / Geografía del Delito	Propone un modelo de análisis territorial que permite identificar factores de riesgo y anticipar eventos delictivos mediante análisis espacial.
Lum & Isaac (2016)	*To Predict and Serve?*	Algoritmos predictivos, sesgos institucionales, desempeño policial	Políticas Públicas	Estudia los efectos del uso de modelos predictivos en departamentos de policía y analiza riesgos de sesgo si no existen controles administrativos adecuados.
Bowers, Johnson & Pease (2004)	*Prospective Hot-Spotting*	Identificación de zonas críticas, prevención del delito	Criminología	Demuestra que el análisis prospectivo de zonas calientes puede anticipar delitos futuros y orientar intervenciones preventivas.
OECD (2020)	*The Path to Becoming a Data-Driven Public Sector*	Transformación digital, toma de decisiones basada en datos, gobernanza	Administración Pública / Gestión Pública	Documento que establece lineamientos para que instituciones públicas integren análisis de datos y tecnología en procesos estratégicos, mejorando eficiencia y resultados.

Fuente: Elaboración propia con base en Perry et al. (2013), Mohler et al. (2015), Meijer y Wessels (2019), Alcaldía de Medellín (2023) e Infodefensa (2024).

La revisión de los antecedentes internacionales evidencia que la inteligencia artificial y los modelos predictivos han demostrado potencial para mejorar la eficiencia operativa, optimizar la asignación de recursos y fortalecer la prevención del delito. Sin embargo, también se resalta la necesidad de marcos administrativos claros, capacidad organizacional, sostenibilidad financiera y regulación adecuada para garantizar una implementación efectiva. En el contexto latinoamericano y particularmente municipal, se identifica una brecha en estudios que integren estos elementos desde una perspectiva estratégica-administrativa, lo cual justifica la pertinencia del presente estudio.

1.6.2 Antecedentes nacionales

En el ámbito nacional, la aplicación de inteligencia artificial en centros municipales de monitoreo es aún incipiente; sin embargo, existen estudios e informes institucionales relacionados con análisis criminal, seguridad ciudadana, modernización tecnológica y transformación digital en el sector público costarricense. Estos antecedentes aportan elementos relevantes para fundamentar una estrategia administrativa orientada a la implementación de alertas tempranas basadas en inteligencia artificial en el ámbito municipal.

Tabla 2. *Antecedentes nacionales*

Autor/Año	Título del Estudio	Variables Consideradas	Área de Conocimiento	Resumen
Organismo de Investigación Judicial (2022)	*Informe Anual de Estadísticas Criminales*	Incidencia delictiva, distribución territorial, tendencias delictivas	Seguridad Pública / Análisis Criminal	Presenta datos estadísticos oficiales sobre delitos en Costa Rica, permitiendo identificar patrones territoriales útiles para modelos predictivos y sistemas de alerta temprana.
Programa de las Naciones Unidas para el Desarrollo – PNUD Costa Rica (2020)	*Informe Nacional de Desarrollo Humano: Seguridad Ciudadana*	Percepción de seguridad, gestión institucional, prevención	Políticas Públicas / Desarrollo Humano	Analiza la relación entre gestión pública y percepción de inseguridad, destacando la necesidad de enfoques preventivos y uso de información para toma de decisiones.
Contraloría General de la República (2021)	*Transformación Digital en el Sector Público Costarricense*	Modernización tecnológica, eficiencia administrativa, gobernanza digital	Administración Pública	Evalúa el nivel de madurez digital de instituciones públicas y plantea la necesidad de estrategias estructuradas para integrar tecnologías emergentes.
Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones – MICITT (2022)	*Estrategia Nacional de Inteligencia Artificial 2022–2027*	IA, ética digital, innovación pública	Tecnología / Políticas Públicas	Establece lineamientos estratégicos para el uso responsable de IA en el sector público costarricense, incluyendo principios de transparencia y gobernanza.

Ministerio de Seguridad Pública (2021)	*Política Nacional de Seguridad Pública*	Prevención del delito, coordinación interinstitucional	Seguridad Pública	Define lineamientos estratégicos para fortalecer la prevención y mejorar la eficiencia operativa mediante uso de información y tecnología.
Universidad de Costa Rica – Instituto de Investigaciones Psicológicas (2019)	*Estudio sobre percepción de seguridad en el Gran Área Metropolitana*	Percepción ciudadana, victimización, espacio urbano	Ciencias Sociales / Seguridad Urbana	Analiza factores que influyen en la percepción de inseguridad y destaca la importancia de políticas preventivas basadas en evidencia.
Estado de la Nación (2022)	*Informe Estado de la Nación – Capítulo de Seguridad Ciudadana*	Violencia urbana, gestión institucional, indicadores de desempeño	Desarrollo Humano / Gestión Pública	Examina tendencias de criminalidad y desempeño institucional, señalando desafíos en coordinación y uso de datos estratégicos.
Municipalidad de San José (2021)	*Plan Estratégico Municipal 2021–2026*	Planificación estratégica, seguridad territorial, gestión por resultados	Administración Municipal	Documento rector que establece metas institucionales, incluyendo modernización tecnológica y mejora de servicios de seguridad ciudadana.
Defensoría de los Habitantes (2020)	*Informe sobre videovigilancia y derechos fundamentales*	Videoprotección, protección de datos, derechos humanos	Derecho Público	Analiza implicaciones legales del uso de videovigilancia en espacios públicos y destaca necesidad de regulación clara y control institucional.

Universidad Nacional de Costa Rica (2021)	*Análisis territorial de la criminalidad en el Valle Central*	Georreferenciación del delito, factores socioeconómicos	Criminología / Geografía	Estudio académico que utiliza análisis espacial para identificar concentración delictiva y variables asociadas al riesgo territorial.

Fuente: Elaboración propia a partir de la revisión documental de fuentes institucionales nacionales (2020–2022).

La revisión de antecedentes nacionales evidencia que, si bien existen estudios relacionados con análisis criminal, percepción de seguridad, transformación digital y políticas públicas, no se identifican investigaciones orientadas específicamente al diseño de una estrategia administrativa para la implementación de alertas tempranas basadas en inteligencia artificial en el ámbito municipal. Esta ausencia constituye una brecha académica y práctica que refuerza la pertinencia y originalidad del presente estudio.

1.7 Proyecciones

Se espera que la investigación contribuya a establecer una hoja de ruta administrativa clara para la implementación de alertas tempranas basadas en inteligencia artificial en el Centro de Monitoreo de San José, orientada a fortalecer la gestión preventiva del delito, optimizar el uso de recursos institucionales y mejorar la toma de decisiones basada en evidencia. Esta hoja de ruta también permitirá desarrollar lineamientos técnicos y operativos para la implementación de sistemas de IA, asegurando que las alertas tempranas se integren de manera efectiva a los procesos existentes del Centro de Monitoreo.

Asimismo, la propuesta busca aportar insumos estratégicos a la Municipalidad para fortalecer su gestión de seguridad territorial mediante el uso de datos, evidencia y automatización, promoviendo un modelo de gobernanza colaborativa que articule instituciones de seguridad, municipalidades y ciudadanía con base en inteligencia situacional. La investigación pretende estimular además la reflexión sobre los aspectos jurídicos y éticos del uso de tecnologías inteligentes para la seguridad pública, considerando la protección de derechos humanos y de datos personales.

A mediano plazo, se proyecta que la estrategia propuesta podría posicionar a la Municipalidad de San José como referente nacional y regional en la aplicación de inteligencia artificial en seguridad ciudadana, generando un sistema más moderno, confiable y preventivo que mejore la percepción de seguridad de la ciudadanía. Igualmente, la integración de dashboards dinámicos y alertas automatizadas permitirá priorizar recursos en zonas de mayor riesgo, fortaleciendo la toma de decisiones municipales basadas en evidencia y optimizando el impacto de la gestión preventiva del delito.

Capítulo II Marco Teórico

2.1 Marco contextual o situacional del estudio

El presente estudio se desarrolla en el Cantón Central de San José, capital de Costa Rica, cuya jurisdicción municipal abarca una población aproximada de 340,000 habitantes (INEC, 2021). La Municipalidad de San José es responsable de la gestión local en ámbitos como seguridad ciudadana, desarrollo urbano y servicios públicos. Dentro de sus competencias específicas, opera el Centro de Monitoreo Municipal, unidad encargada de la vigilancia electrónica y la coordinación en materia de seguridad urbana.

A partir de datos oficiales de los últimos cinco años se observa una tendencia sostenida de altos niveles de criminalidad en el país y en particular en el Cantón Central de San José. Por ejemplo:

- La tasa de homicidios en Costa Rica alcanzó 18 por cada 100 000 habitantes en 2023, con 907 homicidios registrados por el Organismo de Investigación Judicial (OIJ, 2023), lo que representa un aumento del 37 % respecto al año anterior.
- En 2024 y 2025, la criminalidad violenta se mantuvo en niveles elevados, con aproximadamente 876 y 873 homicidios respectivamente, evidenciando que la violencia criminal sigue siendo un desafío central para la seguridad pública nacional y local (OIJ, comunicaciones institucionales internas, 2024-2025).
- Delitos contra la propiedad, como asaltos, robo de vehículos y hurtos, fueron reportados en más de 46 000 denuncias en 2022, con una tendencia ascendente sostenida durante los últimos cinco años (Observatorio de la Violencia, Ministerio de Justicia y Paz, 2022).

Estas cifras muestran que la criminalidad no es un fenómeno aislado sino una tendencia estructural, lo que exige respuestas institucionales integrales y basadas en el análisis de datos reales y actualizados.

El Centro de Monitoreo de San José funciona como un componente estratégico para la vigilancia del espacio público mediante la administración de sistemas de videoprotección, sensores y reportes ciudadanos. Su operación se enmarca en la supervisión permanente de incidentes, la coordinación con unidades policiales y la atención de situaciones de riesgo. No obstante, como se describió en el Capítulo I, el modelo operativo vigente presenta un enfoque mayoritariamente reactivo, lo cual limita la capacidad de anticipar situaciones de riesgo y de implementar acciones preventivas oportunas.

Tabla 3 *Antecedentes nacionales de criminalidad y seguridad en Costa Rica*

Año	Homicidios	Delitos contra la propiedad	Fuente
2022	906	46,123	OIJ (2023); Observatorio de la Violencia, MJP (2022)
2023	907	47,500	OIJ (2023); Observatorio de la Violencia, MJP (2023)
2024	876	48,200	OIJ, comunicaciones institucionales internas (2024)
2025	873	48,900	OIJ, comunicaciones institucionales internas (2025)

Fuente: Elaboración propia a partir de datos oficiales (OIJ, 2023; Observatorio de la Violencia, MJP, 2022–2025).

La inclusión de datos de siniestralidad y criminalidad en el marco contextual situacional permite establecer de forma objetiva el crecimiento de los desafíos de seguridad urbana en el Cantón Central de San José, lo cual refuerza la pertinencia y urgencia de una propuesta que permita modernizar la gestión del Centro de Monitoreo mediante la incorporación de tecnologías inteligentes y enfoques preventivos.

2.2 Marco conceptual o referencial

A continuación, se presentan los conceptos, teorías y modelos que sustentan la presente investigación.

2.2.1 Centros de Monitoreo como instrumentos de gestión de la seguridad urbana

Un Centro de Monitoreo (CM) es una unidad de gestión operativa y analítica encargada de integrar múltiples flujos de información procedentes de sistemas de videoprotección (CCTV), sensores urbanos, reportes ciudadanos y plataformas de emergencias (9-1-1), con el objetivo de prevenir, disuadir, detectar y responder a incidentes que afectan la seguridad y convivencia urbana (Ratcliffe, 2008).

En modelos contemporáneos de seguridad pública, estos centros no solo cumplen funciones de observación, sino que se convierten en activos clave para la gestión táctica y estratégica de la seguridad, facilitando la toma de decisiones basada en evidencias y apoyando la coordinación interinstitucional (Sherman, 1998).

2.2.2 Prevención situacional y disuasión del delito

Prevención del delito mediante diseño ambiental (CPTED): La Prevención del Delito a través del Diseño Ambiental (CPTED) fue formulada por Jeffery (1971) y parte del supuesto de que el delito puede ser reducido mediante el diseño del entorno físico y tecnológico. Esta teoría sostiene que factores como la iluminación, la visibilidad y el control ambiental pueden aumentar el esfuerzo necesario para cometer delitos y elevar la percepción de riesgo del potencial infractor.

Teoría de la prevención situacional del delito: Clarke (1980; 1997) desarrolló el enfoque de prevención situacional del delito, que propone que la reducción de actividades delictivas puede lograrse al intervenir sobre las condiciones que facilitan su ocurrencia, como la presencia de blancos atractivos o vacíos de supervisión. La prevención situacional se vincula estrechamente con el uso de tecnologías de videovigilancia, puesto que estos sistemas actúan como mecanismos que dificultan la ejecución de actos delictivos mediante detección y disuasión temprana.

2.2.3 Teoría de las ventanas rotas

La teoría de las ventanas rotas, propuesta por Kelling y Wilson (1982), plantea que señales visibles de desorden urbano (p. ej., vandalismo, deterioro del espacio público) generan percepciones de abandono institucional que pueden desencadenar más delitos. En el contexto de los Centros de Monitoreo, esta teoría apoya la idea de que la detección y atención temprana de conductas incívicas puede prevenir escaladas hacia delitos de mayor gravedad.

2.2.4 Modelos de intervención focalizada

Hot Spots Policing: El modelo Hot Spots Policing (Sherman et al., 1989) plantea que el delito se concentra espacialmente en áreas específicas del territorio y que la focalización de intervenciones policiales en estos “puntos calientes” puede generar mayores efectos disuasivos que estrategias dispersas.

Curva de Koper: La Curva de Koper (1995) demuestra que permanencias policiales cortas pero frecuentes en zonas de alta incidencia delictiva producen un efecto disuasivo sostenido. Este modelo respalda la necesidad de vincular la información

generada por los Centros de Monitoreo con la asignación operativa de recursos humanos.

2.2.5 Enfoque de Policía Orientada a Problemas y ciclo SARA

El ciclo SARA (Scan, Analyze, Respond, Assess) fue propuesto por Goldstein (1979) dentro del enfoque de Policía Orientada a Problemas. Este modelo promueve un esquema sistemático para identificar, analizar y evaluar problemas de seguridad con base en evidencia, lo cual es congruente con los principios de la gestión pública por resultados.

2.2.6 Intelligence-Led Policing y Evidence-Based Policing

El modelo de Intelligence-Led Policing (ILP) fue desarrollado por Ratcliffe (2008) y se basa en la idea de que la actuación policial debe orientarse mediante información analítica derivada de datos. En paralelo, Evidence-Based Policing (Sherman, 1998) enfatiza la necesidad de que las políticas y prácticas se sustenten en evidencia empírica y evaluaciones rigurosas de impacto.

2.2.7 Gobierno de datos y gestión pública por resultados

El gobierno de datos implica la gestión estructurada de información institucional con reglas claras sobre su captura, almacenamiento, uso y protección. En un enfoque de gestión pública por resultados, la evaluación sistemática mediante indicadores medibles permite determinar la eficiencia administrativa y la eficacia de las estrategias implementadas.

2.2.8 Teoría de la actividad rutinaria

La teoría de la actividad rutinaria, propuesta por Cohen y Felson (1979), sostiene que el delito ocurre cuando convergen un ofensor motivado, un objetivo adecuado y la ausencia de un guardián capaz. Desde esta perspectiva, la videoprotección actúa como un “guardían ampliado”, reduciendo la probabilidad de delitos al incrementar la percepción de supervisión continua.

2.2.9 Gestión del cambio organizacional

Kurt Lewin (1947) describe un proceso de cambio organizacional que consta de tres etapas: descongelamiento, cambio y recongelamiento. Este modelo es útil para comprender cómo la institución puede transitar desde un modelo reactivo hacia uno preventivo e integrado con tecnologías inteligentes.

En el mismo sentido, el Modelo de Aceptación Tecnológica (TAM) de Davis (1989) sostiene que la adopción de nuevas tecnologías por parte de los usuarios depende de su percepción de utilidad y facilidad de uso, lo que tiene implicaciones directas en la implementación de sistemas inteligentes en los Centros de Monitoreo.

2.2.10 Gobernanza colaborativa

La gobernanza colaborativa, según Ansell y Gash (2008), plantea que los problemas públicos complejos, como la seguridad urbana, requieren cooperación entre diversos actores institucionales y comunitarios. Este enfoque sustenta la necesidad de coordinación multinivel para que la operación de los Centros de Monitoreo genere efectos preventivos sostenibles.

2.3 Inteligencia policial y toma de decisiones basadas en evidencia

En los modelos contemporáneos de seguridad pública, la tecnología por sí sola no garantiza resultados. El valor público se genera cuando los datos captados por sistemas de videovigilancia, sensores y plataformas operativas se transforman en inteligencia útil para la toma de decisiones. El modelo de Intelligence-Led Policing y el de Evidence-Based Policing sitúan a la inteligencia analítica como insumo estratégico para definir prioridades operativas y políticas.

2.4 Gestión preventiva de la seguridad ciudadana desde la administración pública

La gestión preventiva de la seguridad se refiere al conjunto de estrategias, decisiones administrativas y procesos institucionales orientados a anticipar riesgos, reducir oportunidades delictivas y minimizar impactos antes de que los hechos se consumen. Desde la administración pública, este enfoque implica mecanismos de coordinación, planificación estratégica y políticas basadas en evidencia.

La estrategia administrativa para la implementación de sistemas de alertas tempranas basadas en inteligencia artificial en el Centro de Monitoreo del Cantón Central de San José busca integrar capacidades tecnológicas, humanas y organizacionales. Esta estrategia se fundamenta en la planificación estratégica, la asignación eficiente de recursos, la coordinación interinstitucional y la generación de inteligencia analítica para la toma de decisiones, asegurando que las acciones preventivas se ejecuten de manera oportuna y basada en evidencia

2.5 Inteligencia situacional aplicada a la seguridad urbana

La inteligencia situacional integra información contextual (espacial, temporal y operativa) para interpretar condiciones del entorno que pueden derivar en riesgos. Cuando se incorpora inteligencia artificial en esta perspectiva, se facilita la automatización del análisis de datos y la identificación de patrones de riesgo.

2.6 Teorías y modelos que sustentan la videoprotección

2.6.1 Teoría de la actividad rutinaria revisitada

La teoría de la actividad rutinaria de Cohen y Felson (1979) también se aplica a la videoprotección, puesto que este tipo de sistemas contribuye a la presencia continuada de guardias ampliados en el entorno urbano.

2.6.2 Evidencia empírica y efectos del CCTV

La evidencia empírica muestra que los sistemas de videoprotección tienen efectos significativos en la reducción de determinados delitos, especialmente cuando están integrados en sistemas de respuesta operativa eficiente y diseño urbano adecuado.

2.7 Marco normativo y principios jurídicos

En Costa Rica, los sistemas de videoprotección constituyen tratamiento de datos personales regulados por la Ley N.º 8968 (Protección de la Persona frente al Tratamiento de sus Datos Personales) y los lineamientos de la PRODHAB, que

establecen principios de legalidad, proporcionalidad, minimización de datos, seguridad de la información y rendición de cuentas.

2.8 Experiencias latinoamericanas y lecciones aprendidas

La literatura comparada indica que los Centros de Monitoreo generan mejores resultados cuando se integran en modelos de gobernanza con liderazgo claro, interoperabilidad institucional, capacidad analítica y sostenibilidad financiera. Tal es el caso en:

- Medellín
- Santiago
- Buenos Aires
- Barcelona

2.9 Enfoque socio-técnico y gestión del cambio organizacional

En organizaciones complejas, como los Centros de Monitoreo, los componentes tecnológicos no pueden desvincularse de los procesos administrativos y de las capacidades humanas. El enfoque socio-técnico (Trist & Emery, 1973) señala la interdependencia de estos elementos para lograr resultados sostenibles.

2.10 Inteligencia artificial aplicada a la seguridad pública

La inteligencia artificial en este contexto se refiere a sistemas capaces de analizar grandes volúmenes de datos, identificar anomalías y generar recomendaciones que

apoyen la toma de decisiones humanas, siempre bajo esquemas de supervisión humana (“human-in-the-loop”).

2.11 Sistemas de alertas tempranas

Los sistemas de alertas tempranas no buscan predecir delitos individuales, sino detectar patrones, anomalías o dinámicas territoriales que requieren atención institucional oportuna.

2.12 Indicadores de desempeño y evaluación

Entre los principales indicadores sugeridos para evaluar los sistemas inteligentes se encuentran:

- Tiempo promedio de detección y respuesta
- Reducción de incidentes en zonas priorizadas
- Porcentaje de alertas atendidas preventivamente
- Tasa de falsos positivos
- Nivel de interoperabilidad institucional

2.13 Madurez institucional y tecnológica

La madurez institucional evalúa si una organización opera de forma reactiva, descriptiva, predictiva o preventiva. Un nivel alto de madurez permite integrar tecnología, personas y procesos estratégicamente.

La implementación de la estrategia administrativa se estructurará en fases que permiten la transición gradual del modelo reactivo hacia un modelo preventivo: diagnóstico institucional (evaluación de capacidades y madurez tecnológica), planificación estratégica (definición de metas, recursos y protocolos), implementación piloto (integración de inteligencia artificial y sistemas de alertas), y evaluación y retroalimentación continua mediante indicadores de desempeño, asegurando ajustes según resultados y riesgos detectados.

2.14 Consideraciones éticas y sesgos algorítmicos

El uso de IA en seguridad plantea desafíos de privacidad, discriminación y transparencia. Es fundamental garantizar mecanismos de explicabilidad algorítmica, auditorías periódicas y rendición de cuentas.

2.15 Gobernanza interinstitucional y coordinación multinivel

La gobernanza colaborativa propone que la solución a problemas complejos requiere interacción entre gobiernos locales, agencias nacionales y ciudadanía organizada.

El marco teórico desarrollado en el presente capítulo permite articular, desde una perspectiva interdisciplinaria, los fundamentos criminológicos, administrativos, tecnológicos y organizacionales que sustentan la propuesta de una estrategia administrativa para la implementación de alertas tempranas basadas en inteligencia artificial en el Centro de Monitoreo del Cantón Central de San José.

En primer lugar, las teorías criminológicas revisadas —entre ellas la prevención situacional del delito, la teoría de la actividad rutinaria, la teoría de las ventanas rotas

y los modelos de intervención focalizada como Hot Spots Policing y la Curva de Koper— proporcionan la base conceptual para comprender que el delito no se distribuye de manera aleatoria, sino que responde a patrones espaciales, temporales y situacionales identificables. Estas teorías sustentan la viabilidad de intervenir preventivamente mediante la identificación de condiciones de riesgo y la focalización estratégica de recursos en territorios prioritarios.

En segundo lugar, los enfoques de Intelligence-Led Policing y Evidence-Based Policing establecen que la actuación institucional debe orientarse por información analítica derivada de datos confiables y procesados sistemáticamente. Bajo este paradigma, los Centros de Monitoreo trascienden su función tradicional de observación reactiva para convertirse en nodos estratégicos de generación de inteligencia operativa, capaces de apoyar la toma de decisiones tácticas y estratégicas en materia de seguridad urbana.

Desde la perspectiva de la administración pública, el gobierno de datos, la gestión por resultados y la gobernanza colaborativa constituyen pilares esenciales para garantizar que la incorporación de tecnologías inteligentes no sea un proceso aislado, sino parte de una transformación organizacional estructurada. La gestión pública contemporánea exige que las decisiones institucionales se fundamenten en evidencia medible, indicadores de desempeño y mecanismos de evaluación continua, orientados a la generación de valor público y a la optimización de recursos.

Asimismo, la incorporación de inteligencia artificial y sistemas de alertas tempranas se enmarca en un proceso de transformación digital que requiere considerar el enfoque socio-técnico y la gestión del cambio organizacional. De acuerdo con estos modelos, la tecnología por sí sola no produce mejoras sostenibles si no se integra con procesos administrativos claros, capacitación del talento humano, aceptación institucional y liderazgo estratégico. La transición desde un modelo reactivo hacia uno

preventivo implica, por tanto, un proceso estructurado de adaptación institucional que articule infraestructura tecnológica, capacidades analíticas y cultura organizacional.

En este contexto, la inteligencia artificial actúa como un habilitador tecnológico que permite procesar grandes volúmenes de información en tiempo real, identificar anomalías, reconocer patrones de riesgo y generar alertas automatizadas que apoyen la toma de decisiones humanas bajo esquemas de supervisión responsable (“human in the loop”). Los sistemas de alertas tempranas no buscan predecir conductas individuales, sino detectar dinámicas territoriales o comportamientos atípicos que requieran intervención institucional oportuna.

La integración de estos enfoques permite configurar un modelo conceptual de gestión preventiva basado en datos, cuyo ciclo funcional puede describirse de la siguiente manera: captación de información (videoprotección, sensores y reportes ciudadanos); procesamiento analítico mediante herramientas de inteligencia artificial; generación de inteligencia operativa; toma de decisiones administrativas y operativas; despliegue focalizado de recursos; evaluación de resultados mediante indicadores de desempeño; y retroalimentación continua del sistema. Este ciclo refleja una lógica de mejora continua orientada a fortalecer la eficiencia institucional y la prevención del delito.

Finalmente, el marco teórico también incorpora consideraciones éticas y normativas que resultan indispensables para la implementación responsable de tecnologías inteligentes en el ámbito de la seguridad pública. La protección de datos personales, la transparencia algorítmica, la mitigación de sesgos y la rendición de cuentas constituyen condiciones necesarias para garantizar la legitimidad institucional y la sostenibilidad de la estrategia propuesta.

En síntesis, la convergencia de teorías criminológicas, modelos de inteligencia policial, principios de gestión pública por resultados, enfoques de transformación organizacional y herramientas de inteligencia artificial proporciona el sustento conceptual para proponer una estrategia administrativa orientada a modernizar el Centro de Monitoreo de San José. Esta estrategia no se limita a la adopción tecnológica, sino que plantea una reconfiguración integral del modelo de gestión, con el propósito de transitar hacia un sistema preventivo, eficiente, basado en datos y alineado con los desafíos contemporáneos de la seguridad urbana.

Capítulo III

Marco Metodológico

A partir del marco conceptual desarrollado, se diseña el presente marco metodológico para operacionalizar los conceptos y evaluar la implementación de alertas tempranas basadas en inteligencia artificial en el Centro de Monitoreo.

3.1 Enfoque de la investigación

La presente investigación adopta un enfoque mixto con énfasis en medición operativa institucional, integrando de manera sistemática técnicas de recolección y análisis de datos cuantitativos y cualitativos, con un alcance descriptivo, analítico y evaluativo. Este enfoque se orienta al diagnóstico del estado actual del Centro de Monitoreo del Cantón Central de San José y a la formulación de una propuesta de modelo de gestión para la incorporación de alertas tempranas basadas en inteligencia artificial.

El componente cuantitativo constituye el eje principal del estudio y permite medir de manera objetiva variables asociadas al funcionamiento del Centro de Monitoreo, tales como el nivel de infraestructura tecnológica, la capacidad operativa, el uso de la información generada por los sistemas de videovigilancia y la viabilidad institucional para la implementación de alertas tempranas. Asimismo, posibilita el análisis descriptivo de indicadores de desempeño institucional, tales como el tiempo de respuesta (TTR), la cobertura efectiva de cámaras y la detección temprana de eventos, a partir de registros operativos e información estructurada (Creswell, 2014; Babbie, 2016).

De manera complementaria, se incorpora un componente cualitativo de apoyo, cuyo propósito es profundizar en la comprensión de prácticas operativas, barreras organizacionales, criterios estratégicos y consideraciones éticas asociadas al uso de tecnologías inteligentes en la seguridad urbana. Este componente se desarrolla mediante preguntas abiertas incluidas en el instrumento aplicado y mediante el análisis interpretativo de la información institucional relevante, permitiendo contextualizar y enriquecer los resultados cuantitativos obtenidos (Patton, 2015).

El uso del enfoque mixto con predominio cuantitativo permite integrar evidencia empírica medible con análisis contextual institucional, fortaleciendo la validez del diagnóstico y la pertinencia de la propuesta administrativa. De esta manera, los hallazgos cuantitativos se complementan con interpretaciones cualitativas, facilitando una comprensión integral del Centro de monitoreo y sus necesidades estratégicas.

Además, esta integración de métodos permite que el análisis fluya de la descripción y medición de variables hacia la interpretación contextual, facilitando la transición hacia el diseño de investigación y la selección de instrumentos.

3.2 Tipo de investigación

La investigación es de tipo descriptivo, con análisis de asociación entre variables y enfoque evaluativo, de acuerdo con los objetivos planteados y la naturaleza de los datos a recolectar. Cada tipo se define y justifica de la siguiente manera:

1. Descriptiva:
   Permite caracterizar el estado actual del Centro de Monitoreo del Cantón Central de San José, incluyendo su infraestructura tecnológica, los sistemas de videovigilancia, los protocolos operativos, la distribución del personal y los flujos

de información. Este tipo de investigación se centra en describir con precisión los hechos y variables observables, sin manipularlas, proporcionando una base objetiva para la formulación de la propuesta de gestión (Hernández Sampieri et al., 2018).

2. Análisis de asociación entre variables:

   Se analizarán asociaciones descriptivas entre variables operativas, como cobertura tecnológica y tiempos de respuesta, con el fin de identificar patrones y tendencias sin establecer relaciones causales ni realizar inferencias estadísticas de generalización.

3. Evaluativa:
   Determina el impacto potencial de la incorporación de alertas tempranas basadas en inteligencia artificial sobre la eficiencia operativa, la prevención del delito y la toma de decisiones estratégicas. La investigación evaluativa se enfoca en analizar cómo los cambios propuestos podrían mejorar el desempeño institucional y fortalecer la gobernanza y la ética en la gestión de datos y recursos tecnológicos.

La combinación de estos tipos de investigación permite obtener un diagnóstico integral, caracterizar la situación, identificar relaciones entre variables clave y evaluar el impacto potencial de la implementación de alertas tempranas con Inteligencia Artificial.

3.3 Diseño de la investigación

La investigación presenta un diseño no experimental, ya que no se manipulan deliberadamente las variables, sino que se observan tal como se presentan en su contexto natural.

Es de tipo transversal, dado que la recolección de datos se realiza en un único momento temporal, analizando información operativa correspondiente al último año de funcionamiento del Centro de Monitoreo. Esta modalidad permite evaluar la efectividad de los sistemas sin intervención directa sobre las variables.

Asimismo, el estudio se desarrolla bajo la modalidad de estudio de caso, centrado en el Centro de Monitoreo del Cantón Central de San José, por tratarse de una unidad institucional con características específicas relevantes para el análisis (Hernández Sampieri et al., 2018).

El estudio de caso permite un análisis profundo del fenómeno en su contexto real, privilegiando la comprensión integral sobre la generalización estadística (Hernández Sampieri et al., 2018).

3.4 Población y muestra

En coherencia con el diseño de estudio de caso definido en el apartado anterior, la presente investigación centra su análisis en una unidad institucional específica: el Centro de Monitoreo del Cantón Central de San José. De acuerdo con Hernández Sampieri, Fernández y Baptista (2018), el estudio de caso consiste en el análisis profundo, contextual y detallado de una unidad delimitada, con el propósito de

comprender integralmente sus procesos, dinámicas internas y particularidades, privilegiando la profundidad analítica sobre la generalización estadística.

En este tipo de diseño metodológico, la selección de participantes no responde a criterios probabilísticos ni a fórmulas de cálculo muestral, dado que el interés no radica en extrapolar resultados a una población amplia, sino en obtener información estratégica y especializada directamente vinculada con el fenómeno estudiado. Por esta razón, se emplea un muestreo intencional no probabilístico, también denominado muestreo por criterio.

- **Población institucional:** La población de estudio está constituida por el personal operativo y administrativo vinculado directamente con la gestión del Centro de Monitoreo municipal de San José, incluyendo operadores, supervisores y mandos intermedios responsables de la coordinación operativa, análisis de información y toma de decisiones relacionadas con la Seguridad.

  Se trata de una población técnica y especializada, cuya experiencia directa en la operación de sistemas de videoprotección y gestión de incidentes resulta esencial para el diagnóstico institucional y la formulación de la propuesta de gestión basada en alertas tempranas con inteligencia artificial.

- **Muestra institucional:** La muestra estará conformada por 33 funcionarios del Centro de Monitoreo, seleccionados mediante muestreo intencional no probabilístico, bajo criterios de experiencia directa en:

  - Experiencia directa en la operación de sistemas de videoprotección.
  - Participación en la gestión de incidentes y activación de protocolos.

- Intervención en procesos de toma de decisiones operativas o estratégicas.
- Conocimiento de la infraestructura tecnológica y flujos de información del Centro.

El número de 33 participantes se define de manera concreta por corresponder a las posiciones clave que concentran la operación crítica del Centro de Monitoreo, garantizando representatividad funcional dentro del estudio de caso.

Según Hernández Sampieri et al. (2018), en los estudios de caso el tamaño de la muestra se determina por la riqueza y profundidad de la información requerida, más que por criterios estadísticos de generalización. En este sentido, la selección de 33 participantes resulta suficiente para capturar la diversidad de funciones estratégicas y operativas involucradas en la implementación de alertas tempranas basadas en inteligencia artificial.

- **Población ciudadana**: La encuesta también se aplicará a 120 habitantes del Cantón Central de San José, con el objetivo de recoger información sobre percepción de seguridad, confianza en el Centro de Monitoreo y opinión sobre la cobertura tecnológica y la implementación de alertas tempranas basadas en inteligencia artificial.

- **Muestra ciudadana**: Se seleccionará una muestra intencional de ciudadanos mayores de 18 años residentes en el cantón, considerando representación por edad, sexo y distrito de residencia, para capturar la diversidad de percepciones en la comunidad.

> Dado que la selección de la muestra ciudadana se realizó mediante un muestreo no probabilístico de tipo intencional, los resultados obtenidos poseen un carácter exploratorio y perceptual. En consecuencia, los hallazgos derivados de este instrumento no permiten realizar inferencias estadísticas ni generalizaciones a la totalidad de la población del Cantón Central de San José, sino que constituyen insumos orientativos para el diagnóstico estratégico.

Adicionalmente, se incorporará el análisis de registros operativos institucionales correspondientes al último año, incluyendo bitácoras de incidentes, tiempos de respuesta, cobertura de cámaras y reportes de eventos relevantes.

El instrumento será sometido a validación de contenido mediante juicio de tres expertos en seguridad urbana y gestión tecnológica, quienes evaluarán la claridad, pertinencia y coherencia de los ítems. Asimismo, se realizará una prueba piloto aplicada a tres funcionarios con características similares a la muestra definitiva, con el fin de verificar comprensión, tiempo de aplicación y consistencia del cuestionario. Los ajustes derivados del proceso de validación serán incorporados antes de su aplicación final.

3.4.1 Ficha técnica de la muestra

Con el propósito de sistematizar y precisar las características del proceso de selección de participantes, se presenta a continuación la ficha técnica de la muestra correspondiente tanto al componente institucional como al componente ciudadano del estudio.

Esta ficha permite detallar los aspectos operativos del diseño muestral, incluyendo método de recolección, periodo de ejecución, marco muestral, cobertura y sector de actividad, garantizando transparencia metodológica y coherencia con el enfoque de estudio de caso definido en la presente investigación.

Dado que el diseño corresponde a un estudio no experimental, transversal y con muestreo no probabilístico de tipo intencional, la muestra tiene carácter diagnóstico y estratégico, orientado a la profundidad analítica más que a la generalización estadística.

Tabla 4. *Ficha técnica de la muestra institucional*

Parámetros	**Descripción**
Objetivo general	Proponer una estrategia administrativa para la implementación de alertas tempranas basadas en inteligencia artificial en el Centro de Monitoreo de San José, orientada a una gestión eficiente y preventiva del delito, en el año 2026.
Método de recolección	Aplicación de cuestionario estructurado (escala Likert 5 puntos), entrevistas semiestructuradas y revisión de registros operativos institucionales.
Tiempo de aplicación de la muestra	Aproximadamente 20–30 minutos por cuestionario; entrevistas de 40–60 minutos.
Población objetivo	Personal operativo y administrativo vinculado directamente con la gestión del Centro de Monitoreo del Cantón Central de San José.
Cobertura	Funcionarios con responsabilidad en operación de videoprotección, análisis de incidentes y toma de decisiones estratégicas.
Periodo de ejecución	Primer bimestre del año 2026.

Dominio del estudio de los miembros de la muestra	Funcionarios con experiencia directa en gestión de sistemas de videovigilancia, activación de protocolos y uso de información operativa para toma de decisiones.
Tamaño de la muestra	33 funcionarios.
Marco muestral	Listado oficial del personal activo del Centro de Monitoreo proporcionado por la administración municipal.
Diseño muestral	Muestreo no probabilístico, intencional por criterio técnico-operativo (estudio de caso institucional).
Sector de actividad	Seguridad ciudadana y gestión municipal.
Localización del trabajo de campo	Centro de Monitoreo del Cantón Central de San José, Costa Rica.

Fuente: Elaboración propia

Tabla 5. *Ficha técnica de la muestra ciudadana*

Parámetro	**Descripción**
Método de recolección	Aplicación de encuesta estructurada (preguntas cerradas y abiertas, escala Likert 5 puntos), en modalidad física y/o digital.
Tiempo de aplicación de la muestra	Aproximadamente 10–15 minutos por encuesta.
Población objetivo	Personas mayores de 18 años residentes en el Cantón Central de San José.
Cobertura	Distritos del Cantón Central de San José, considerando diversidad por edad y sexo.
Periodo de ejecución	Segundo semestre del año 2025.
Dominio del estudio de los miembros de la muestra	Residentes con conocimiento básico del funcionamiento del Centro de Monitoreo y percepción sobre seguridad en su comunidad.
Tamaño de la muestra	120 ciudadanos.
Marco muestral	Población residente mayor de edad en el Cantón Central de San José.

Diseño muestral	Muestreo no probabilístico, intencional con criterios de heterogeneidad demográfica.
Sector de actividad	Comunidad urbana / ciudadanía general.
Localización del trabajo de campo	Distritos del Cantón Central de San José, Costa Rica.

Fuente: Elaboración propia

3.5 Instrumentos de medición y técnicas de recolección de datos

1. **Cuestionarios estructurados para personal del Centro de Monitoreo:** Estos permiten recopilar percepciones de operadores y supervisores sobre utilidad, facilidad de uso y confiabilidad de los sistemas de alertas tempranas (Likert, 1932). Por tal motivo en el presente trabajo se aplicará un cuestionario físico o virtual diseñado específicamente para recopilar información técnica, operativa y estratégica de los operadores y supervisores del Centro de Monitoreo de San José. Su estructura está detallada en el anexo 1. El instrumento busca:

- Diagnosticar el estado actual de la infraestructura tecnológica, los sistemas de video protección y los protocolos operativos.

- Recopilar percepciones sobre la viabilidad de la incorporación de alertas tempranas basadas en inteligencia artificial.
- Identificar áreas de mejora, limitaciones actuales y oportunidades para un modelo de gestión basado en IA.

El cuestionario incluye preguntas cerradas y abiertas, que cubren aspectos como cargo, experiencia, área de responsabilidad, infraestructura tecnológica, enfoque operativo, uso de información, limitaciones actuales, viabilidad de IA, áreas de mayor valor de la IA, tipos de alertas estratégicas, alineación con objetivos institucionales, cambios necesarios y modalidad de implementación.

2. **Encuesta ciudadana:** Orientada a evaluar la percepción de seguridad, confianza en el Centro de Monitoreo, conocimiento de cámaras y aplicaciones, efectividad percibida de la tecnología y aceptación de alertas tempranas basadas en IA.

   Se aplicará de forma física o virtual y garantiza anonimato y confidencialidad. Incluye preguntas cerradas y abiertas para recoger sugerencias ciudadanas sobre seguridad y cobertura tecnológica.

3. **Entrevistas semiestructuradas:** Para profundizar en la experiencia operacional, barreras organizacionales y consideraciones éticas (Kvale & Brinkmann, 2009).

4. **Revisión documental y análisis de indicadores:** Evaluación de bitácoras de incidentes, cantidad y cobertura de cámaras, lugares donde se ubican cámaras, tiempos de respuesta (TTR), tasa de detección temprana y efectividad de alertas de IA (Bazeley & Jackson, 2013).

5. **Observación directa:** Monitoreo de protocolos operativos y flujos de información en tiempo real para identificar oportunidades de mejora en la integración de IA y video protección (Angrosino, 2007).

3.6 Variables de estudio y operacionalización

3.6.1 Variables de análisis

A continuación, se identifican las variables que permitirán analizar tanto el desempeño operativo del Centro de Monitoreo como los efectos administrativos, éticos y estratégicos asociados a la implementación de alertas tempranas basadas en inteligencia artificial.

Tabla 6 *Variables de análisis*

Variable	Dimensiones	Indicador	Fuente de datos	Tipo
Efectividad del Centro de Monitoreo	Cobertura	% de cámaras operativas	Bitácoras del CM	Cuantitativa
Alertas tempranas	Precisión y utilidad	% de alertas reales y falsos positivos	Bitácoras y registros de eventos	Cuantitativa
Toma de decisiones	Rapidez y calidad	Tiempo de respuesta promedio, cumplimiento de protocolos	Registros internos del CM	Cuantitativa
Percepción de seguridad	Ciudadana e institucional	Nivel de confianza en el Centro de Monitoreo, percepción de seguridad en el barrio.	Encuesta ciudadana	Cualitativa/ cuantitativa
Opinión sobre tecnología y alertas	Efectividad y aceptación	Evaluación de cobertura tecnológica, importancia percibida de IA	Encuesta ciudadana	Cualitativa/ Cuantitativa
Gobernanza de datos	Integridad y trazabilidad	Cumplimiento de normas y protocolos	Informes internos y auditorías	Mixta

Consideraciones éticas	Transparencia y respeto a DDHH	Existencia de protocolos y evaluaciones éticas	Documentación institucional	Cualitativa

Fuente: Elaboración propia

3.6.2 Operacionalización de las variables

Con el fin de traducir las variables principales en indicadores observables y medibles, se realizó la operacionalización de las variables centrales de la investigación, mismas que se detallan en la siguiente tabla.

Tabla 7. *Operacionalización de variables*

Variable	Definición	Dimensión	Indicadores	Instrumento	Escala
Implementación de alertas tempranas basadas en IA	Uso de sistemas automatizados que analizan datos en tiempo real para identificar patrones de riesgo y generar alertas preventivas para la toma de decisiones en seguridad urbana (Ratcliffe, 2016; Clarke, 1995).	Tecnológica	Existencia de analítica automatizada; integración de fuentes de datos; capacidad de detección temprana	Cuestionario al personal	Likert
		Administrativa	Protocolos de uso de alertas; capacitación del personal; integración en procesos de decisión	Cuestionario	
		Operativa	Tiempo de generación de alertas; activación de protocolos; coordinación con patrullaje		
Gestión eficiente y preventiva del delito	Capacidad institucional para anticipar, responder y reducir incidentes delictivos	Prevención	Identificación de patrones; reducción de incidentes recurrentes; percepción de anticipación	Cuestionario	Likert

	mediante el uso eficiente de recursos y toma de decisiones basada en evidencia (Sherman & Weisburd, 1995; Lum et al., 2012).	Eficiencia	Optimización de recursos; reducción de carga operativa; mejora en tiempos de respuesta	Cuestionario	
		Gobernanza	Uso de evidencia para decisiones; interoperabilidad institucional; transparencia operativa	Cuestionario y entrevistas	
Percepción de seguridad ciudadana	Opinión de residentes sobre confianza y seguridad en el barrio y el Centro de Monitoreo	Confianza	Nivel de confianza en la capacidad de respuesta	Encuesta ciudadana	Likert 5 puntos
Opinión sobre tecnología y alertas	Valoración de cobertura tecnológica y alertas tempranas basadas en IA	Efectividad	Percepción de eficacia de cámaras, alarmas y alertas IA	Encuesta ciudadana	Likert 5 puntos

La escala tipo Likert utilizada será de cinco puntos, donde 1 corresponde a “Totalmente en desacuerdo” y 5 a “Totalmente de acuerdo”.

Fuente: Elaboración propia

3.6.3 Categorías de análisis cualitativo

Para el componente cualitativo de la investigación se definieron categorías de análisis orientadas a interpretar las percepciones, prácticas operativas y consideraciones éticas asociadas al uso de sistemas de videovigilancia e inteligencia artificial. Estas categorías no constituyen variables medibles, sino ejes interpretativos que permiten complementar y contextualizar los resultados cuantitativos.

Las principales categorías de análisis cualitativo son:

- Percepción de utilidad operativa de las alertas tempranas basadas en IA: analiza cómo los operadores y supervisores valoran la efectividad y aplicabilidad de las alertas en sus funciones diarias.

- Barreras técnicas, organizacionales y normativas para la implementación de IA: identifica los desafíos que limitan la integración de sistemas inteligentes en los procesos del Centro de Monitoreo.

- Gobernanza institucional y toma de decisiones basada en evidencia: examina la capacidad del Centro para usar información generada por IA en decisiones estratégicas y operativas.

- Consideraciones éticas, privacidad y respeto a los derechos humanos: evalúa cómo se protegen los derechos y se asegura la transparencia en el uso de tecnologías de vigilancia inteligentes.

- Sugerencias para mejorar la seguridad y cobertura tecnológica

- Prioridades ciudadanas sobre las alertas tempranas e implementación de IA

Estas categorías se abordan mediante entrevistas semiestructuradas, observación directa y análisis documental, asegurando que los hallazgos cualitativos proporcionen un contexto sólido y complementen los resultados cuantitativos de la investigación.

3.7 Técnicas de análisis de datos

El análisis de los datos recolectados se realizará mediante un enfoque mixto, integrando técnicas cuantitativas y cualitativas con el fin de obtener una comprensión integral del fenómeno estudiado.

1. **Análisis cuantitativo:**
    - Estadísticas descriptivas: de indicadores operativos y de IA.
    - Correlación entre cobertura de cámaras, alertas precisas y tiempos de respuesta.
    - Análisis de percepción ciudadana: frecuencias, porcentajes, comparación entre distritos y grupos etarios.

2. **Análisis cualitativo:**
    - Codificación temática de entrevistas y observaciones para identificar barreras, buenas prácticas y percepción de utilidad (Braun & Clarke, 2006).
    - Triangulación de información cualitativa con evidencia cuantitativa para fortalecer la validez de los hallazgos.

Adicionalmente, para complementar el análisis cualitativo de las barreras organizacionales, operativas y tecnológicas identificadas durante las entrevistas y la observación directa, se empleará el **Diagrama de Ishikawa**, también conocido como diagrama de causa–efecto. Esta herramienta de análisis permite identificar de manera estructurada los factores que influyen en un problema organizacional, clasificando las

posibles causas en categorías como tecnología, procesos, recursos humanos, gestión institucional y entorno operativo.

La aplicación de este modelo facilitará la sistematización de la información cualitativa obtenida durante el proceso de investigación, permitiendo visualizar las relaciones entre las diferentes causas que limitan la gestión preventiva del delito en el Centro de Monitoreo del Cantón Central de San José. A partir de este análisis causal se podrán identificar las principales brechas institucionales y fundamentar la propuesta administrativa orientada a la implementación de alertas tempranas basadas en inteligencia artificial.

3. **Integración mixta:**

    - Construcción de un mapa de riesgo y efectividad combinando análisis geoespacial, alertas IA y percepción operativa.

    - Identificación de brechas de desempeño y oportunidades para la propuesta de gestión.

El análisis mixto permite validar hallazgos cuantitativos con información cualitativa fortaleciendo la robustez de la propuesta de gestión.

3.8 Consideraciones éticas

La investigación se realizará respetando los principios de confidencialidad, anonimato y legalidad en el manejo de datos sensibles, conforme a la Ley 8968 de Costa Rica y estándares internacionales de protección de datos (UNODC, 2019). Se garantizará:

- Consentimiento informado de todos los participantes.
- Resguardo seguro de información operativa y de vigilancia.
- Evaluación ética de la implementación de sistemas de IA, asegurando control humano (*human-in-the-loop*) y transparencia.

Los datos recolectados serán anonimizados y codificados para evitar la identificación individual de los participantes.

3.9 Diseño de la propuesta de gestión

A partir del análisis de datos, se propone un modelo operativo para la incorporación de alertas tempranas basadas en inteligencia artificial, que contemple:

1. Protocolos de integración tecnológica con video protección existente.
2. Flujos de información y coordinación interinstitucional.
3. Indicadores de desempeño y evaluación continua.

4. Estrategias de gestión del cambio y capacitación del personal (Kotter, 1996; Lewin, 1947).
5. Procedimientos de gobernanza de datos, ética y cumplimiento normativo.
6. Elaboración de un manual operativo para guiar la implementación práctica

El manual operativo se desarrollará directamente a partir de los hallazgos de la investigación, asegurando que las recomendaciones se adapten a la realidad institucional del Centro de Monitoreo.

La propuesta se enmarca dentro de un enfoque de investigación aplicada, orientada a la solución de problemas institucionales concretos.

3.10 Matriz de consistencia

Tabla 8. *Matriz de consistencia*

Objetivo	**Variable**	**Dimensión**	**Indicador**	**Fuente de datos**	**Técnica de análisis**	**Fundamentación teórica / cita APA**
Identificar la efectividad del CM en la prevención y disuasión del delito	Efectividad del CM	Cobertura y ubicación estratégica	% de cámaras operativas en hot spots	Bitácoras del CM, mapas de cobertura	Estadística descriptiva, análisis geoespacial	Hot Spots Policing y Curva de Koper (Sherman & Weisburd, 1995; Koper, 1995)
		Coordinación institucional	Número de incidentes atendidos oportunamente	Registros de despacho policial	Estadística descriptiva, correlacional	ILP y Evidence-Based Policing (Ratcliffe, 2008; Lum et al., 2012)
Evaluar precisión y utilidad de alertas tempranas IA	Alertas tempranas IA	Precisión	% de alertas correctas / falsos positivos	Sistema IA, bitácoras de incidentes	Estadística descriptiva, análisis de precisión	Prevención situacional y predicción de comportamientos (Clarke, 1997; Gill et al., 2005)
		Utilidad operativa	Tiempo promedio de acción tras alerta	Bitácoras de respuesta	Análisis de tiempos de respuesta	ILP (Ratcliffe, 2008)
Analizar influencia del CM en decisiones estratégicas	Toma de decisiones	Rapidez y eficiencia	TTR promedio, cumplimiento de protocolos	Registros internos CM	Correlación, análisis descriptivo	Evidence-Based Policing y gobierno de datos (Lum et al., 2012; Jiménez Corrales, 2018)

		Calidad de decisiones	Número de decisiones basadas en evidencia	Entrevistas supervisores	Análisis cualitativo	Videoprotección como instrumento estratégico (Ratcliffe, 2016)
Explorar percepción de seguridad ciudadana e institucional	Percepción de seguridad	Ciudadana	Nivel de confianza en el Centro de Monitoreo, percepción de seguridad en el barrio	Encuestas ciudadanas	Estadística descriptiva, análisis por distritos y grupos etarios	Teoría de ventanas rotas (Kelling & Wilson, 1982), CPTED (Clarke, 1997)
		Institucional	Opinión de operadores y supervisores sobre utilidad del CM	Entrevistas semiestructuradas	Codificación temática	Prevención situacional y disuasión (Clarke, 1997)
Examinar cumplimiento de normas de gobernanza de datos	Gobernanza de datos	Integridad y trazabilidad	% de accesos auditados	Auditorías internas, bitácoras de acceso	Estadística descriptiva, análisis documental	Ley 8968 Costa Rica; ISO 27001; Privacy by Design (Jiménez Corrales, 2018)
Analizar consideraciones éticas en uso de tecnología	Consideraciones éticas	Transparencia y respeto a DDHH	Existencia de protocolos y evaluaciones de impacto	Documentos internos, entrevistas	Análisis documental y cualitativo	Normativa internacional y regional (UNODC, BID; Hernández Valle, 2015)
Evaluar percepción de efectividad y aceptación de tecnología y alertas tempranas	Opinión sobre tecnología y alertas	Efectividad	Percepción de eficacia de cámaras, alarmas y alertas IA	Encuesta ciudadana	Estadística descriptiva y análisis comparativo entre distritos	Prevención situacional, aceptación social de tecnología (Clarke, 1997; Ratcliffe, 2016)

Fuente: Elaboración propia

La operacionalización de las variables presentada en este capítulo permitió traducir los conceptos teóricos abordados en el marco conceptual en indicadores observables y medibles, facilitando la recolección sistemática de información relevante para el cumplimiento de los objetivos de la investigación.

A partir de las dimensiones tecnológica, administrativa y operativa de la implementación de alertas tempranas basadas en inteligencia artificial, así como de los componentes de prevención, eficiencia y gobernanza asociados a la gestión del delito, se diseñaron los instrumentos de diagnóstico aplicados al personal del Centro de Monitoreo de San José.

La información recopilada mediante cuestionarios, entrevistas semiestructuradas y análisis de registros operativos constituye la base empírica para el análisis de resultados que se desarrolla en el capítulo siguiente, permitiendo evaluar el estado actual del Centro de Monitoreo, identificar brechas de gestión y sustentar la propuesta administrativa planteada en la investigación.

Con el objetivo de facilitar la comprensión del enfoque, diseño, población y técnicas utilizadas en la investigación, se presenta la siguiente ficha metodológica. La siguiente tabla sintetiza los elementos esenciales del marco metodológico, permitiendo visualizar de manera estructurada cómo se operacionalizan los conceptos teóricos y se articulan los instrumentos y procedimientos de recolección y análisis de datos.

Tabla 9. *Ficha metodológica*

Parámetro	Descripción
Enfoque de la investigación	Mixto, con predominio cuantitativo y componente cualitativo complementario; diagnóstico, descriptivo, analítico y evaluativo.
Tipo de investigación	Descriptivo, análisis de asociación entre variables y evaluativo.
Diseño de la investigación	No experimental, transversal, estudio de caso del Centro de Monitoreo del Cantón Central de San José.
Población y muestra	Personal operativo y administrativo del Centro de Monitoreo (33 participantes) y ciudadanos del Cantón Central de San José (120 participantes).
Muestra	Muestreo intencional no probabilístico, por criterios de experiencia y representatividad funcional (personal) y territorial (ciudadanos).
Instrumentos de medición	Cuestionarios estructurados, encuestas ciudadanas, entrevistas semiestructuradas, observación directa y revisión documental de registros operativos.
Recolección de datos	Aplicación de cuestionarios y encuestas físicas o virtuales, realización de entrevistas, observación directa de protocolos y revisión de bitácoras e indicadores operativos.
Análisis e interpretación de datos	Cuantitativo: estadísticas descriptivas, correlaciones, análisis geoespacial y comparación de grupos. Cualitativo: codificación temática, triangulación y análisis interpretativo. Mixto: integración de hallazgos para validar información y construir mapas de riesgo y efectividad.

Tratamiento de la información	Codificación de datos, anonimización de participantes, sistematización de registros operativos y normalización de indicadores.
Validación de la información	Juicio de tres expertos en seguridad urbana y gestión tecnológica, prueba piloto de instrumentos, triangulación de fuentes y métodos.
Resguardo de la información	Almacenamiento seguro de datos, cumplimiento de Ley N.º 8968 de protección de datos personales, anonimización de participantes, control de accesos a registros y documentación institucional.

Fuente: Elaboración propia

Capítulo IV

Análisis e interpretación de resultados

El presente capítulo analiza los resultados obtenidos mediante los instrumentos definidos en el marco metodológico, siguiendo la operacionalización de las variables de estudio. Los hallazgos se presentan en función del desempeño actual del Centro de Monitoreo de San José y la viabilidad de implementar alertas tempranas basadas en inteligencia artificial (IA) para fortalecer la prevención del delito.

La interpretación integra datos cuantitativos provenientes de registros operativos y cuestionarios, así como información cualitativa obtenida de entrevistas al personal clave, permitiendo contrastar la evidencia empírica con los enfoques teóricos de prevención situacional, inteligencia policial y gestión pública basada en resultados.

Para el análisis de los resultados se propone el uso de instrumentos tales como tablas, figuras y esquemas descriptivos, los cuales permiten organizar y visualizar la información recolectada. La aplicación empírica de estos instrumentos queda sujeta a la ejecución del estudio de campo, por lo que algunos resultados se presentan como análisis preliminares y descriptivos.

El Centro de Monitoreo forma parte de la Alcaldía de la Municipalidad de San José, adscrito a la Dirección de Seguridad Ciudadana y Policía Municipal, y opera 24/7 mediante 4 turnos de trabajo de 5 funcionarios cada uno, con un ciclo rotativo de horarios de 12 horas. El sistema recibe señales de cámaras, alarmas, radios, llamadas telefónicas, WhatsApp Web, correos electrónicos y otras fuentes, procesadas en el sistema digital SISPOM, donde se registran incidentes, recursos utilizados y tiempos de respuesta.

4.1 Técnicas de análisis e interpretación de resultados

Para el análisis e interpretación de los resultados se aplicaron técnicas propias de investigaciones con enfoque mixto, integrando procedimientos cuantitativos y cualitativos, en coherencia con el diseño metodológico del estudio.

En el componente cuantitativo, los datos obtenidos a partir de registros operativos y encuestas fueron organizados y analizados mediante técnicas de estadística descriptiva, permitiendo identificar frecuencias, porcentajes y tendencias relacionadas con la cobertura tecnológica, el enfoque operativo y la viabilidad de la implementación de inteligencia artificial en el Centro de Monitoreo. Los resultados se presentan mediante tablas y figuras descriptivas, propuestas como instrumentos de análisis, pendientes de su validación empírica final.

En el componente cualitativo, se aplicaron técnicas de análisis de contenido y categorización temática a la información obtenida mediante entrevistas semiestructuradas con jefaturas y mandos intermedios. Estas técnicas permitieron identificar patrones discursivos, percepciones, barreras organizacionales, consideraciones éticas y oportunidades de mejora asociadas al uso de tecnologías de videovigilancia e inteligencia artificial.

La integración de ambas técnicas de análisis posibilitó una interpretación comprensiva de los resultados, articulando la evidencia empírica con los enfoques teóricos abordados en el marco conceptual. Las tablas y figuras incluidas en este capítulo corresponden a los resultados obtenidos a partir de los instrumentos aplicados, los cuales constituyen la base empírica para la formulación de la propuesta de gestión presentada en el capítulo siguiente.

4.2 Población y fuentes de información

La interpretación de los resultados se fundamenta en información proveniente de diversas fuentes primarias y secundarias, lo que permitió una visión integral del funcionamiento del Centro de Monitoreo y de la percepción institucional y ciudadana.

Fuentes utilizadas:

1. **Registros operativos del Centro de Monitoreo**: Bitácoras de incidentes, detalle de dispositivos electrónicos disponibles y su ubicación, cobertura de cámaras, tiempos de respuesta y reportes de alarmas residenciales y comerciales.

2. **Encuestas al personal técnico y operativo**: 25 funcionarios, incluyendo operadores, supervisores y jefaturas, para conocer percepción sobre infraestructura, uso de información y viabilidad de la inteligencia artificial.

3. **Entrevistas semiestructuradas**: 8 jefaturas y mandos intermedios, para profundizar en barreras organizacionales, procesos de toma de decisiones, oportunidades de mejora y consideraciones éticas.

4. **Encuestas ciudadanas**: 120 vecinos y comerciantes del Cantón, para evaluar percepción de seguridad y conocimiento sobre la cobertura tecnológica municipal.

4.3 Análisis descriptivo de los datos

4.3.1 Cobertura tecnológica y operativa

El Centro de Monitoreo de San José cuenta con una infraestructura tecnológica amplia, conformada por 1,869 cámaras de videovigilancia y más de 2400 alarmas distribuidas en los once distritos del Cantón Central (Tabla 4, Figuras 1-14). Esta infraestructura permite registras eventos en tiempo real en espacios públicos, parques, bulevares, barrios, vías principales, en rutas de ingreso o salida al cantón y en zonas de alta concurrencia, siguiendo criterios de focalización según el modelo de Hot Spots Policing (Sherman & Weisburd, 1995; Koper, 1995).

La información presentada se obtuvo a partir de registros operativos, observación directa y encuestas al personal, permitiendo un diagnóstico preciso de la cobertura y distribución de los dispositivos. Sin embargo, se identifican limitaciones en la integración de los dispositivos con sistemas de análisis de inteligencia artificial (IA), lo que impide la generación de alertas preventivas y análisis automatizado de incidentes.

En este apartado se mostrarán tablas y figuras que presentan la cobertura tecnológica actual y la distribución de dispositivos en el Centro de Monitoreo. Algunas representan resultados preliminares, mientras que otras corresponden a instrumentos de análisis propuestos y quedan pendientes de validación empírica definitiva

Componentes tecnológicos principales:

- Cámaras tipo domo, bullet y minidomo.

- Algunas cámaras con capacidades de integrar inteligencia artificial, actualmente no se utilizan para generar alertas tempranas.

- El personal policial cuenta con cámaras corporales que registran video, audio, fecha, hora y posición satelital; sin embargo, no se visualizan en tiempo real, desde el Centro de monitoreo

- 120 cámaras vehiculares instaladas en patrullas policiales; las mismas cuentan con grabador NVR en el que se almacenan las imágenes

- 2400 alarmas residenciales y comerciales, activas que generan señales y son recibidas en el Centro de monitoreo por protocolo IP o análogo.
- La aplicación móvil “Alerta San José”, cuenta con 3000 usuarios aproximadamente; y permite generar alertas georreferenciadas con botón de pánico

Con base en lo expuesto es evidente que la infraestructura tecnológica con la que cuenta el Centro de monitoreo de San José es robusta; sin embargo, su utilización responde principalmente a un modelo pasivo de vigilancia, sin integración de analítica, ni automatización de procesos de detección preventiva, lo cual limita su impacto estratégico en la prevención del delito.

Este hallazgo evidencia una brecha entre la capacidad tecnológica instalada y su aprovechamiento funcional, lo cual constituye un punto crítico para la formulación de un modelo de monitoreo inteligente orientado a la anticipación del delito.

Tabla 10. *Cobertura tecnológica del CM de San José*

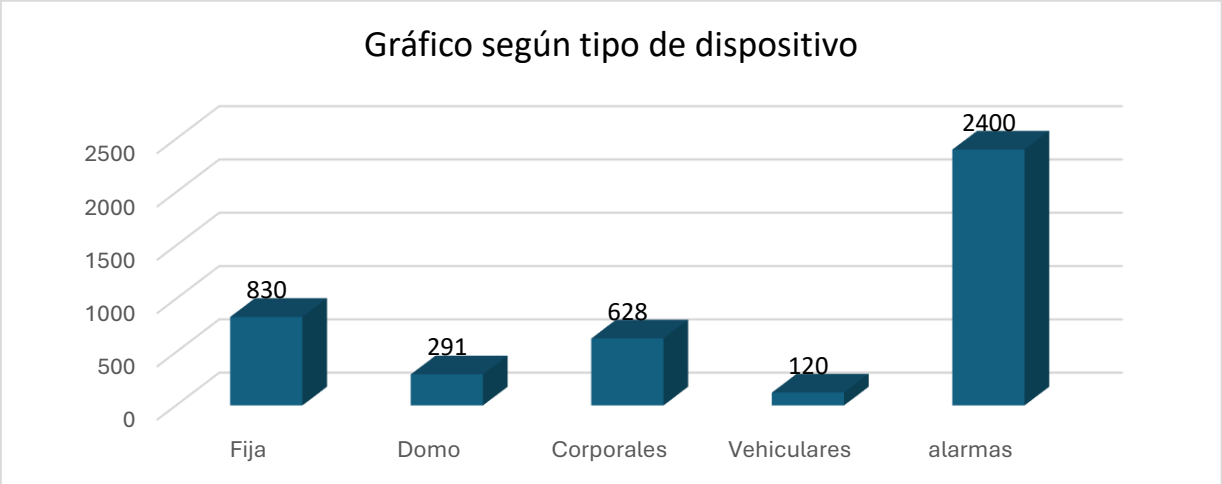
Tipo de dispositivo	Cantidad	Cobertura	Uso actual de IA
Cámaras fijas	830	Espacios públicos, vías principales	No
Cámaras domo	291	Hot spots, parques, bulevares	No
Cámaras corporales	628	Unidades de patrulla	No
Cámaras vehiculares	120	Oficiales - Policía	No
Alarmas residenciales y comerciales	2.400	Hogares y comercios	No

Fuente: elaboración propia con base en registros municipales

Esta tabla evidencia que, aunque la cantidad y diversidad de dispositivos es significativa, ninguno de ellos se encuentra plenamente integrado para generar alertas preventivas. Existe una brecha entre capacidad instalada y aprovechamiento funcional, lo que constituye un área crítica para un modelo de monitoreo inteligente.

Coincide con los postulados de Hot Spots Policing; la cobertura está concentrada en zonas críticas, pero se requiere analítica avanzada para la anticipación del delito.

Figura 1*. Cantidad de dispositivo por tipo*

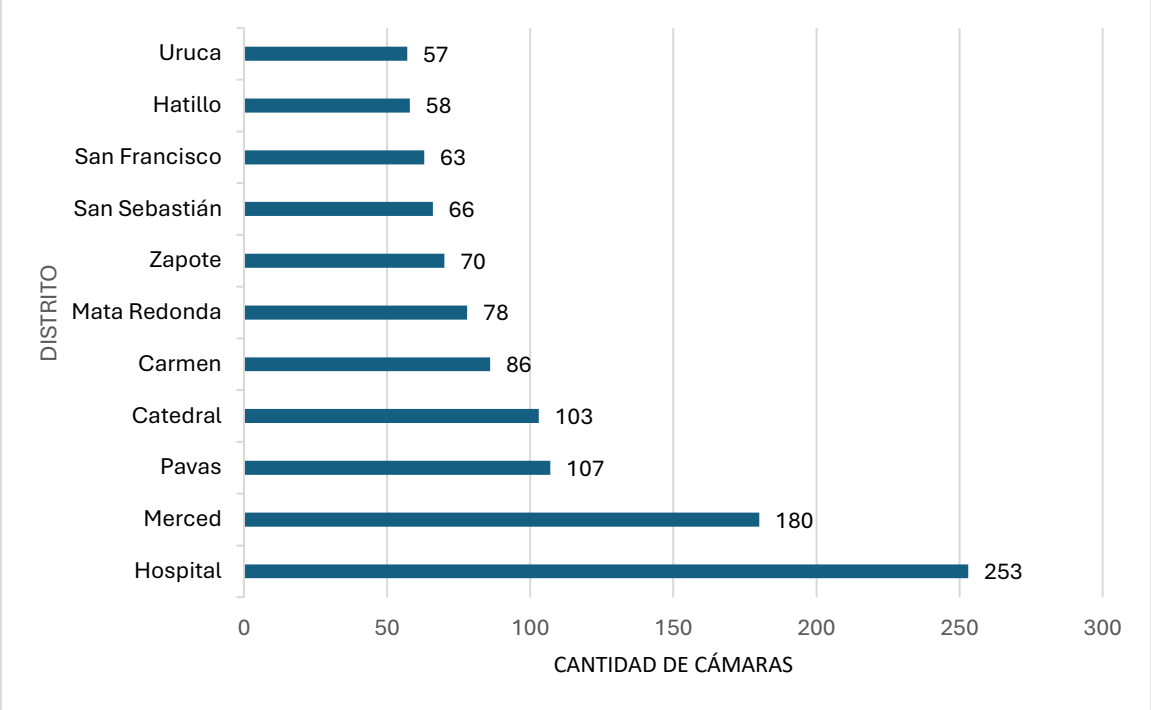


Fuente: Elaboración propia.

La visualización gráfica confirma que las cámaras corporales y fijas constituyen la mayor proporción de los dispositivos, lo que indica un enfoque operativo centrado en la observación pasiva y registro posterior de eventos, más que en análisis preventivo.

La menor cantidad de cámaras vehiculares y domo sugiere oportunidades de optimización para vigilancia dinámica. Lo anterior refuerza la necesidad de integrar inteligencia artificial para convertir esta infraestructura en información estratégica y operacional.

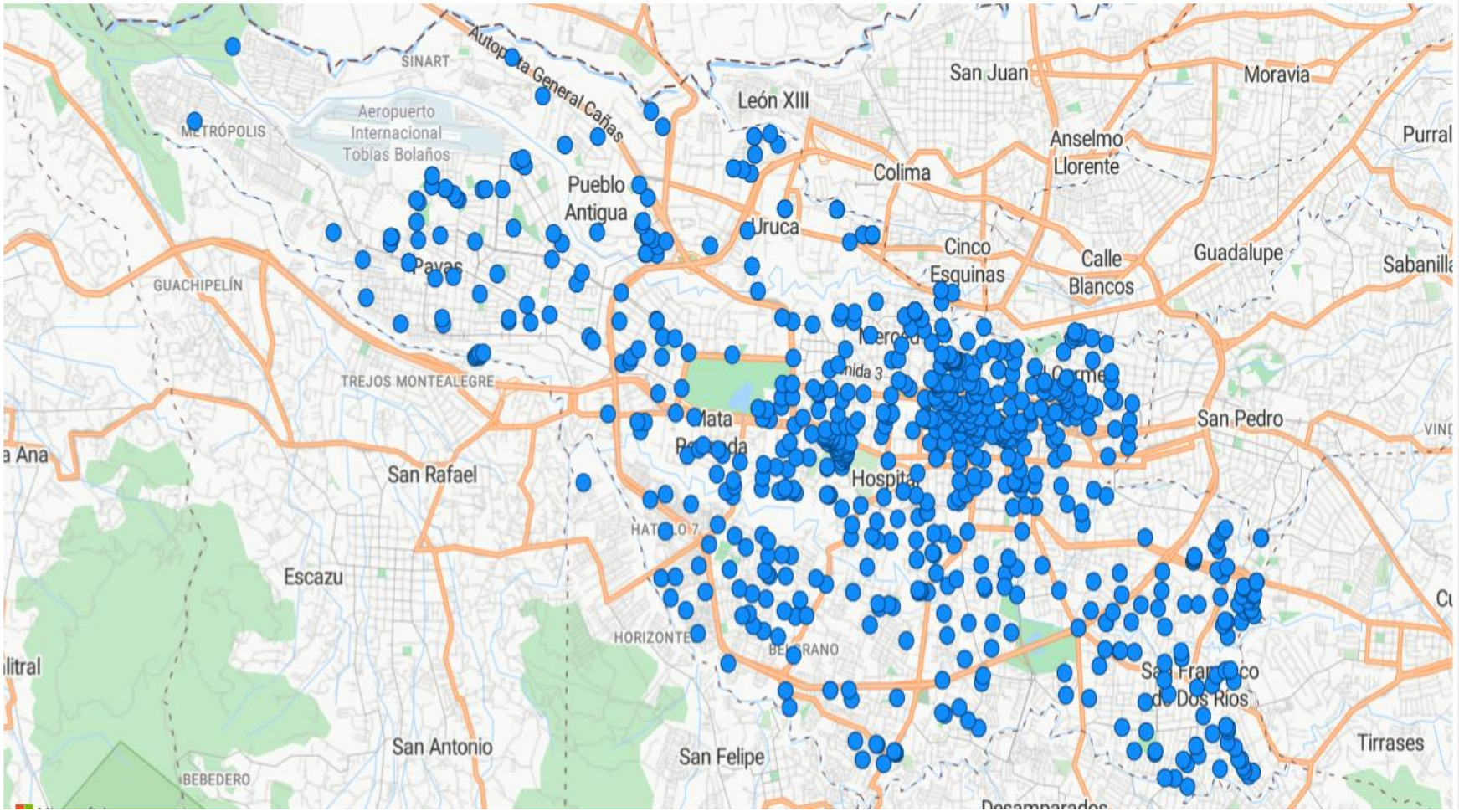
***Figura 2**. Distribución de cámaras por distrito*



Fuente: Elaboración propia.

Se evidencia que la mayor concentración de dispositivos se da en distritos centrales como Hospital, Merced y Carmen, y una menor densidad en distritos periféricos. La distribución responde a criterios de alta afluencia y zonas críticas. Característica que se alinea con Hot Spots Policing, pero la ausencia de analítica limita la prevención activa.

***Figura 3**. Mapa de cobertura tecnológica y concentración en puntos calientes.*



Fuente: *Sistema de la Policía Municipal de San José*

La figura muestra que las cámaras están ubicadas estratégicamente en zonas de alta afluencia y mayor incidencia delictiva, alineándose con los principios de Hot Spots Policing. Sin embargo, la falta de analítica limita la prevención activa.

Figura 4. *Distribución geográfica de cámaras en el distrito Hospital*

Fuente: Sistema de la Policía Municipal de San José

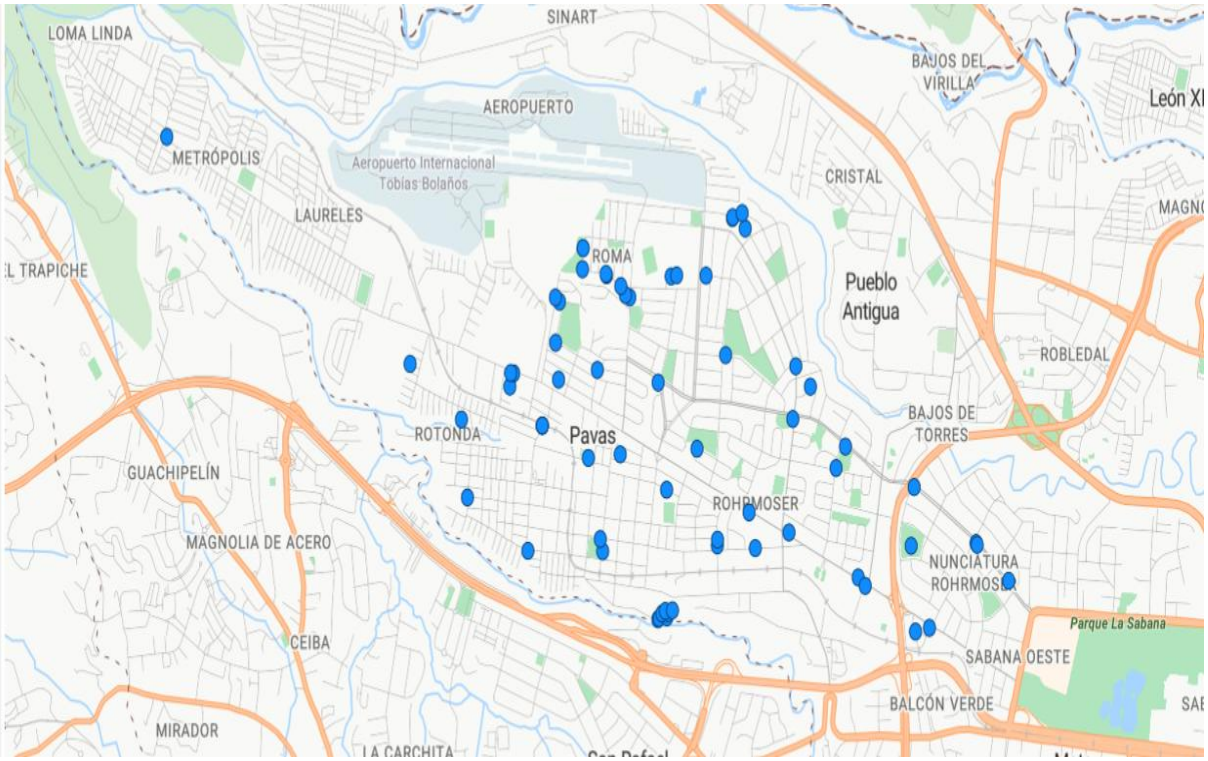
En la figura 4 del distrito hospital se observa la distribución de 159 cámaras en espacio público, se refleja la concentración tecnológica diferenciada, lo que permite priorizar zonas críticas. Este es uno de los distritos centrales del Cantón, los dispositivos han sido ubicados en bulevares, parques, zonas de gran tránsito peatonal. Y conforme se aleja de la zona central del distrito, disminuye considerablemente el número de cámaras. Esta información es fundamental para planificar la implementación gradual de alertas tempranas basadas en IA.

Figura 5. *Distribución geográfica de cámaras en el distrito Merced*

Fuente: Sistema de la Policía Municipal de San José

En la figura 5 se observa la distribución de 85 cámaras municipales en el distrito merced, las áreas centrales tienen mayor cobertura tecnológica, mientras en las zonas más lejanas disminuye el monitoreo. Lamentablemente la ausencia de analítica limita la capacidad de transformar esta cobertura en inteligencia preventiva y alerta temprana.

Figura 6. *Distribución geográfica de cámaras en el distrito Pavas*



Fuente: Sistema de la Policía Municipal de San José

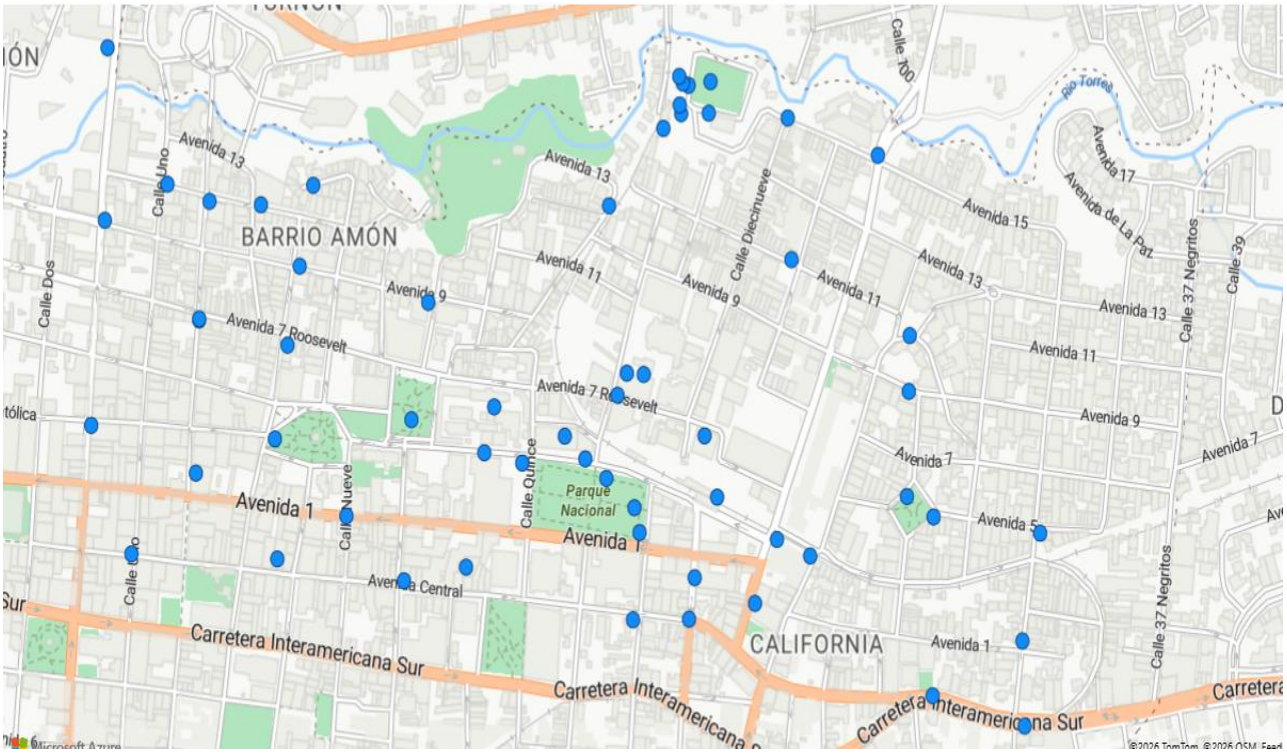
En el distrito de Pavas, que es uno de los más grandes del Cantón Central de San José, se ubican 85 cámaras municipales instaladas, sin embargo tal y como se aprecia en la figura 6, una gran cantidad de estas se encuentran en las zonas más cercanas al centro del Cantón, mientras que en la periferia es casi nulo el monitoreo o presencia de dispositivos electrónicos

***Figura 7**. Distribución geográfica de cámaras en el distrito Catedral*

Fuente: Sistema de la Policía Municipal de San José

El distrito Catedral cuenta con 99 cámaras municipales, una cantidad importante de dispositivos tal y como se aprecia en la figura 7, están en el sector noroeste del mismo, lugar en el que se localiza uno de los principales bulevares del cantón, conocido como “avenida Central”. Situación que coincide con los principios de Hot Spots Policing. Sin embargo, la falta de analítica limita la prevención activa.

***Figura 8**. Distribución geográfica de cámaras en el distrito Carmen*



Fuente: Sistema de la Policía Municipal de San José

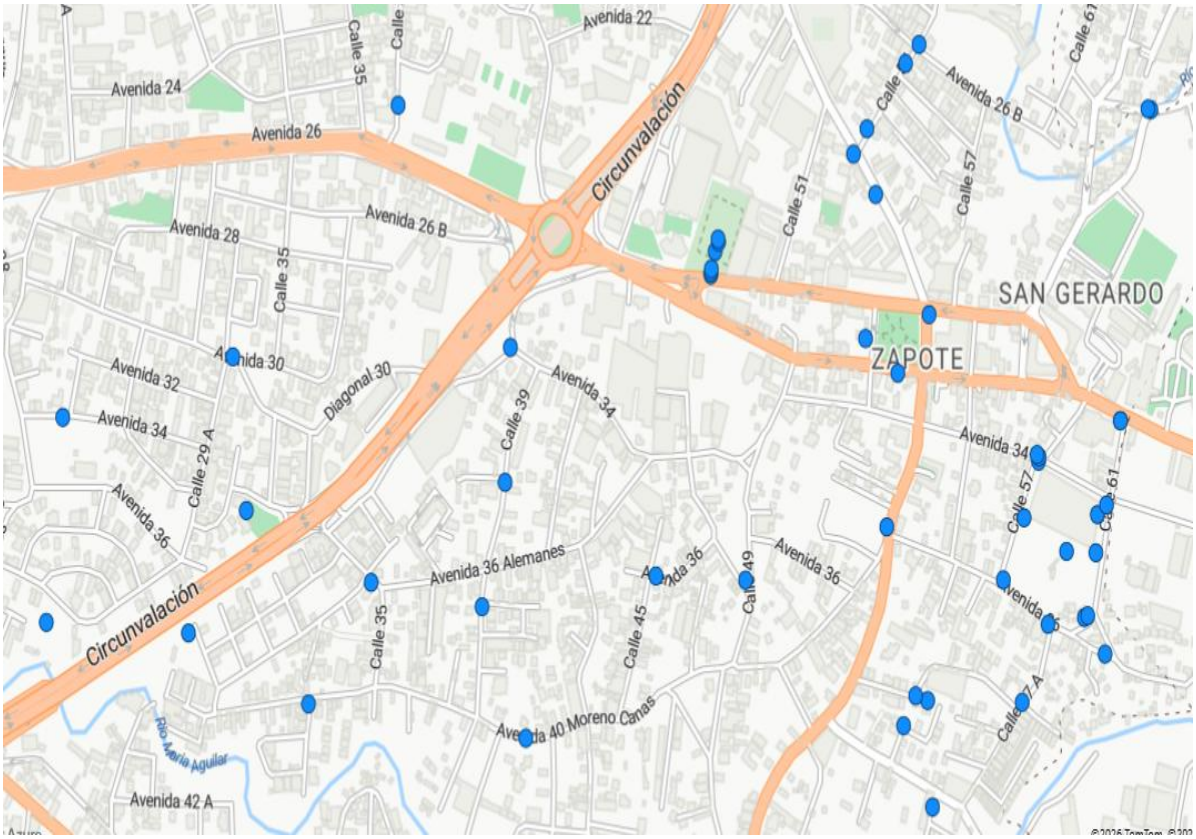
En la figura 8 correspondiente a los dispositivos electrónicos en el distrito Carmen, se observa que de las 86 cámaras, una cantidad importante de las mismas se ubican en espacios como parques, bulevares, y áreas principales de ingreso y salida, lugares que han sido definidos como sitios calientes, o áreas que generan mayor incidencia. Sin embargo, la falta de aplicaciones que permitan generar alertas tempranas hace que la utilización de estos equipos sea más reactiva que preventivamente.

***Figura 9**. Distribución geográfica de cámaras en el distrito Mata Redonda*

Fuente: Sistema de la Policía Municipal de San José

La figura muestra que las 77 cámaras asignadas por el municipio al distrito Mata Redonda están ubicadas estratégicamente en zonas de alta afluencia y mayor incidencia delictiva, alineándose con los principios de Hot Spots Policing. Sin embargo, la falta de analítica limita la prevención activa.

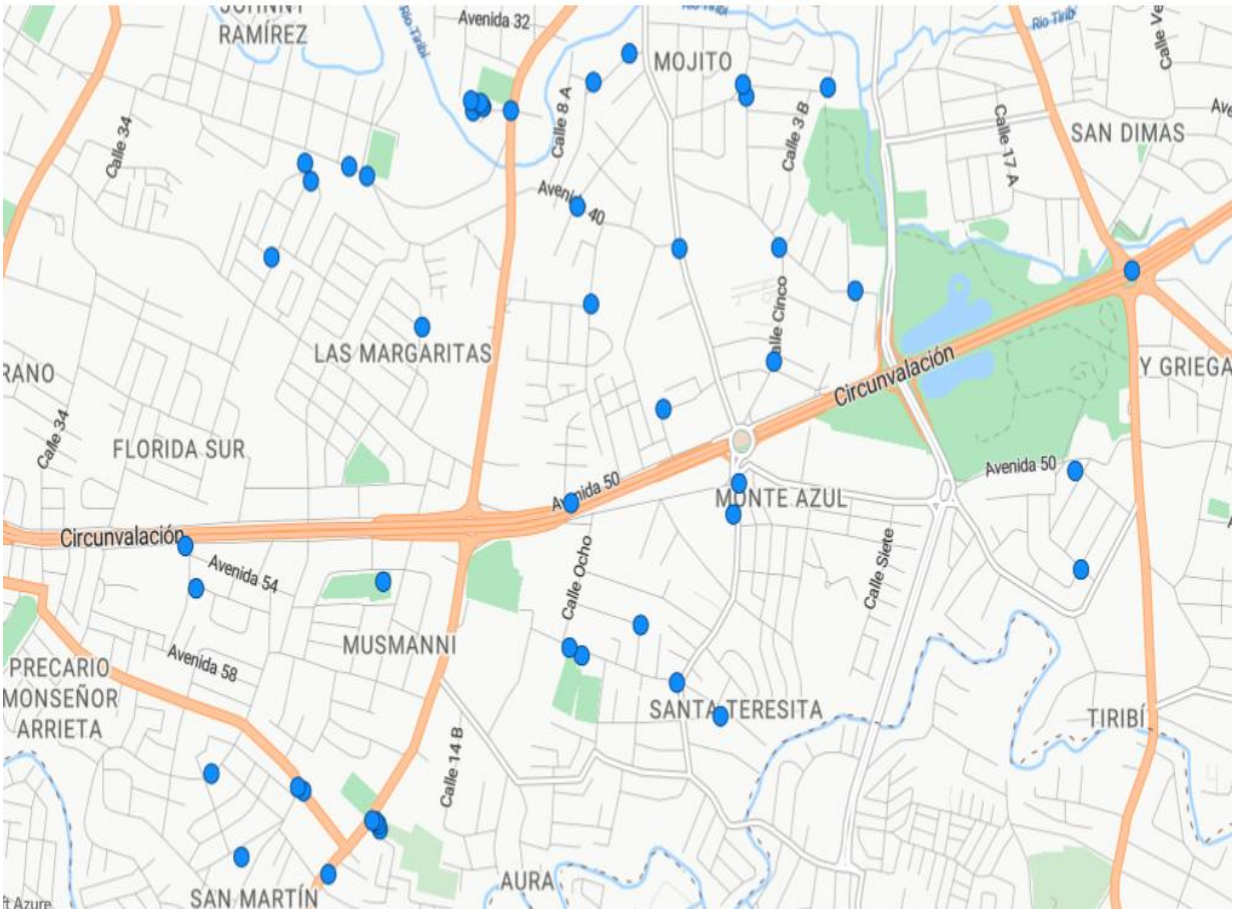
***Figura 10**. Distribución geográfica de cámaras en el distrito Zapote*



Fuente: Sistema de la Policía Municipal de San José

La figura 10 correspondiente a cámaras del distrito Zapote, lugar que tiene asignado 63 dispositivos, muestra que las cámaras están colocadas estratégicamente en zonas de alta afluencia y mayor incidencia delictiva, alineándose con los principios de Hot Spots Policing. Sin embargo, la falta de analítica limita la prevención activa.

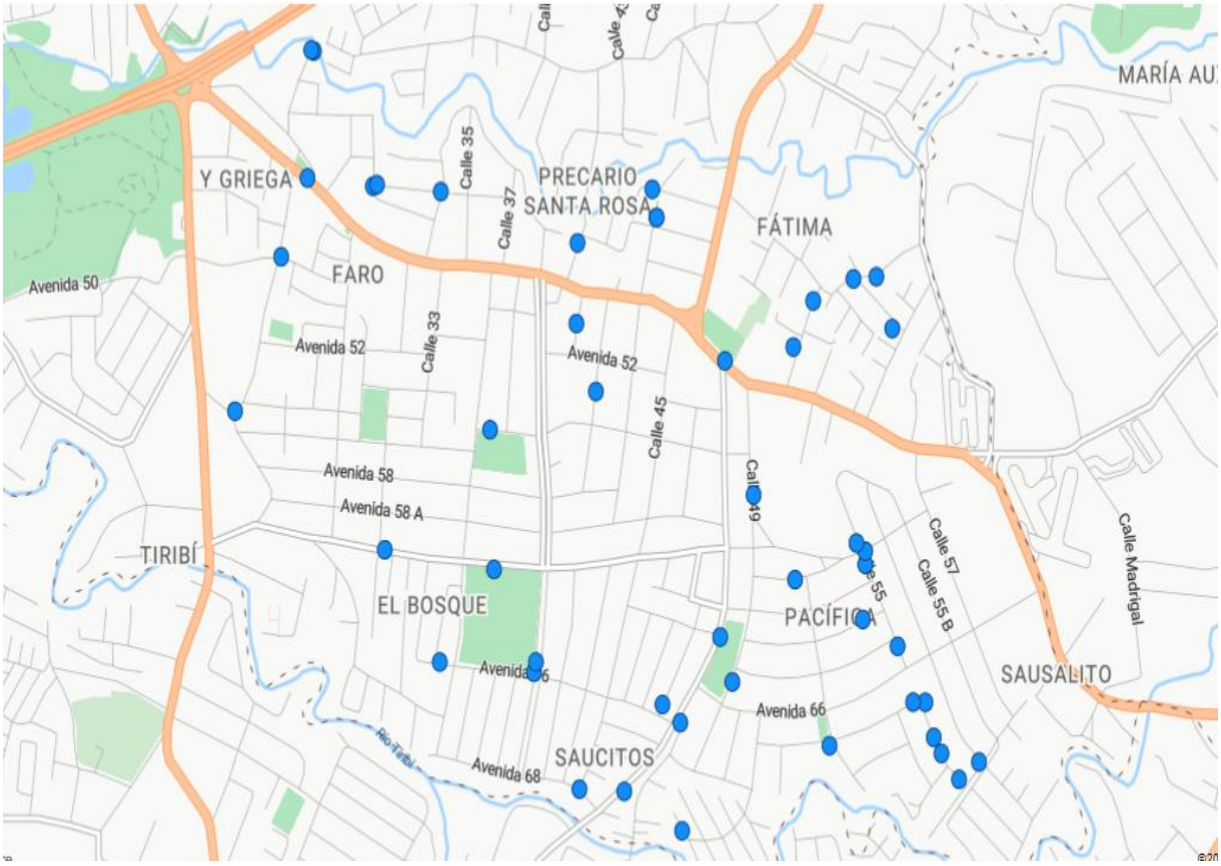
***Figura 11**. Distribución geográfica de cámaras en el distrito San Sebastián*



Fuente: Sistema de la Policía Municipal de San José

La distribución que muestra la figura 11, en el distrito de San Sebastián muestra que las 47 cámaras municipales que tiene; fueron colocadas en los lugares que han sido identificados como de alta afluencia y al mismo tiempo que reporta o necesita la presencia policía por mayor incidencia delictiva, alineándose con los principios de Hot Spots Policing. Sin embargo, la falta de analítica limita la prevención activa.

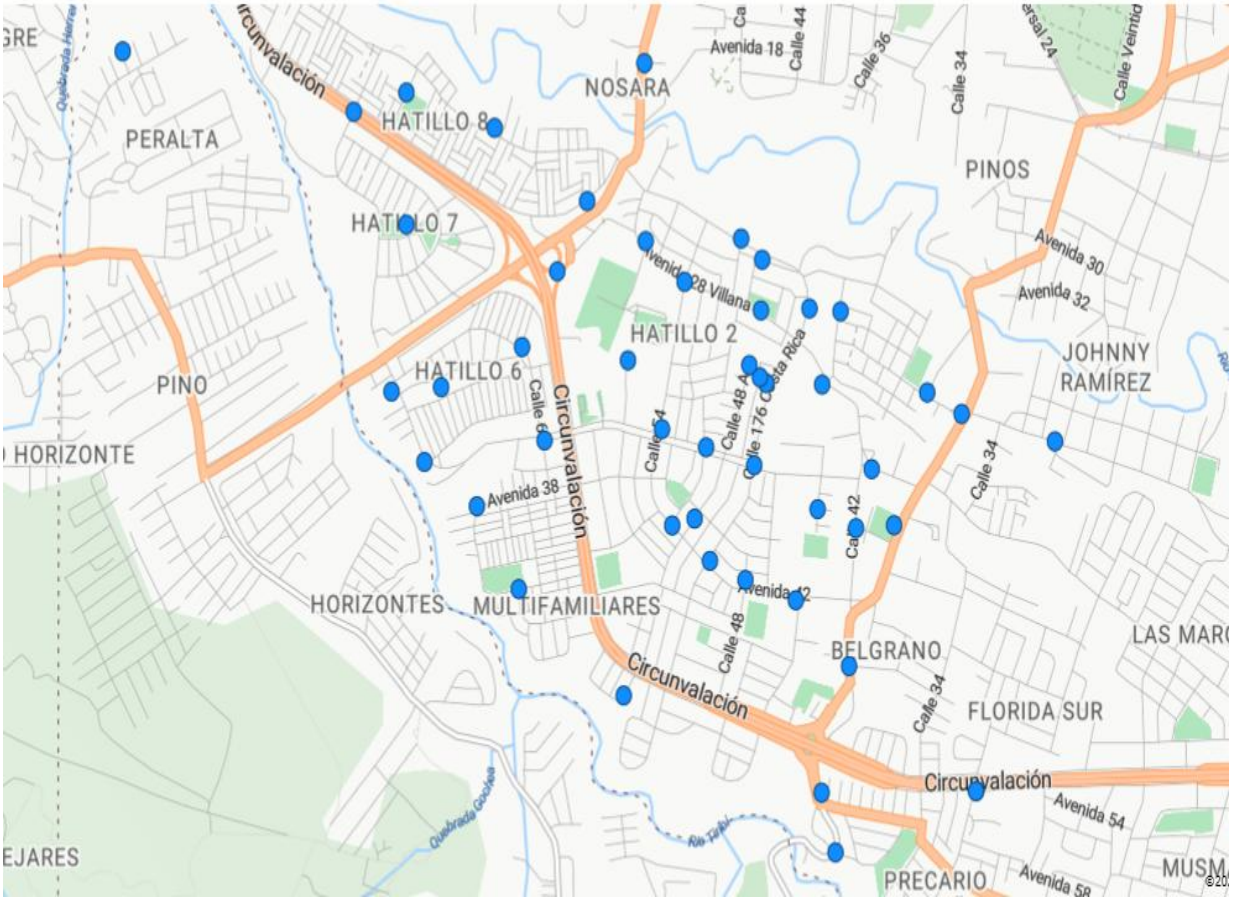
***Figura 12**. Distribución geográfica de cámaras en el distrito San Francisco*



Fuente: Sistema de la Policía Municipal de San José

La figura 12 muestra como están distribuidas 61 cámaras en el distrito de San Francisco de Dos Ríos, se identifica su ubicación en áreas como parques, bulevares, y otras zonas de gran afluencia en el distrito. Además, la instalación de dispositivos responde a la necesidad de monitorear lugares que han sido identificados por su mayor incidencia delictiva. Sin embargo, la falta de analítica limita la prevención activa.

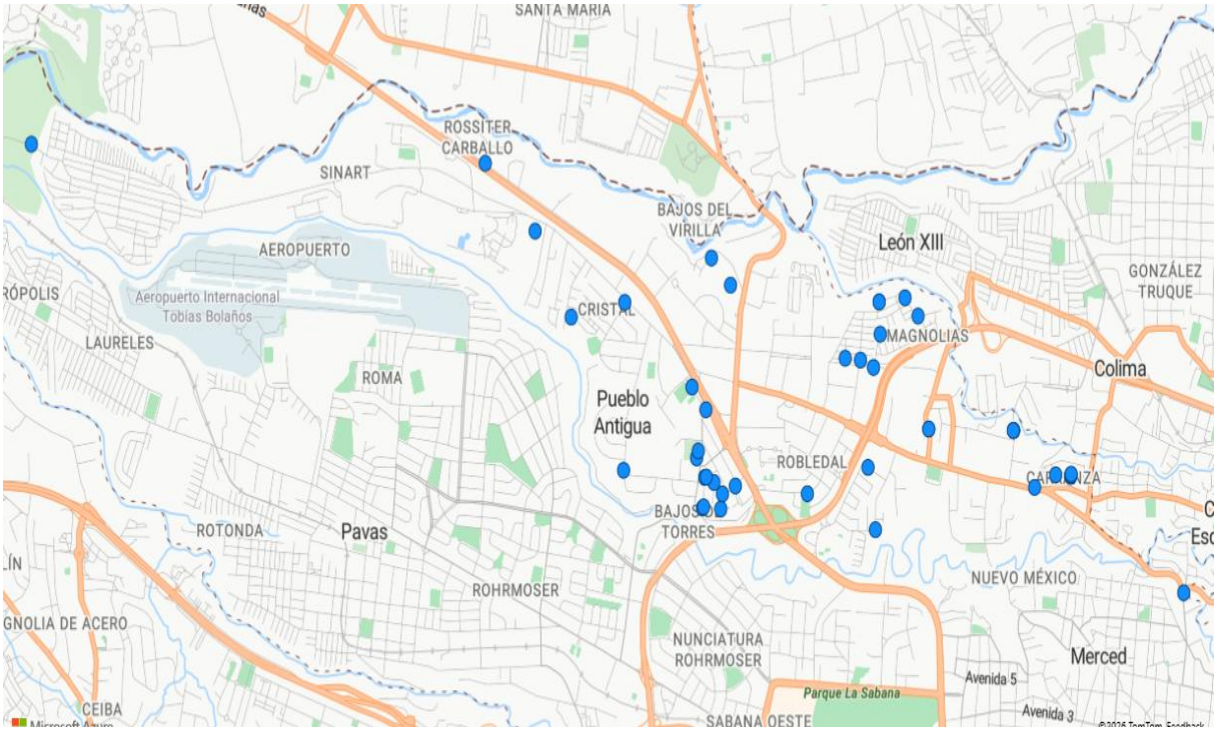
***Figura 13**. Distribución geográfica de cámaras en el distrito Hatillo*



Fuente: Sistema de la Policía Municipal de San José

La figura 13 muestra que las 58 cámaras están ubicadas estratégicamente en zonas de alta afluencia y mayor incidencia delictiva, alineándose con los principios de Hot Spots Policing. Sin embargo, la falta de analítica limita la prevención activa.

***Figura 14**. Distribución geográfica de cámaras en el distrito Uruca*



Fuente: Sistema de la Policía Municipal de San José

La figura 14 que corresponde a la ubicación geográfica de las 55 cámaras en el distrito Uruca; permite determinar que una alta cantidad de dispositivos están ubicados en la parte central, que coincide con las zonas de mayor paso o afluencia de personas. Y también coincide con los sitios catalogados como puntos calientes, por darse en ellos la mayor incidencia delictiva.

El mapa con la distribución geográfica de las cámaras; evidencia una mayor concentración de dispositivos en distritos centrales del Cantón como lo son Hospital, Merced, Carmen, Catedral y zonas con alta afluencia de personas tal es el caso de Pavas, lo cual se alinea con los principios del modelo de *Hot Spots Policing*. No obstante, también se identifican áreas con menor densidad de cobertura tecnológica, lo que sugiere oportunidades de optimización territorial mediante análisis geoespacial y priorización basada en datos delictivos.

La ausencia de analítica automatizada limita la capacidad del Centro de Monitoreo para utilizar esta distribución como una herramienta predictiva y preventiva.

La infraestructura tecnológica del Centro de Monitoreo es amplia y diversificada, pero su utilización se centra en vigilancia reactiva y registro de eventos, dejando un potencial estratégico sin explotar. La brecha identificada entre la capacidad instalada y la generación de inteligencia operativa constituye un hallazgo clave para sustentar la necesidad de un modelo de monitoreo inteligente con analítica avanzada y alertas tempranas basadas en IA.

4.3.2 Percepción del personal del Centro de Monitoreo

Los resultados de la encuesta aplicada al personal técnico y operativo muestran que, si bien existe reconocimiento de una infraestructura considerable, predominan percepciones de limitaciones en integración, análisis y aprovechamiento estratégico de la información. Tal y como se detalla en las siguientes tablas

Tabla 11. *Percepción sobre infraestructura tecnológica*

Nivel de infraestructura	Porcentaje
Deficiente	12%
Regular	54%
Robusta	34%

Fuente: Elaboración propia

La mayoría considera la infraestructura como “regular”, lo que refleja limitaciones en integración y uso estratégico.

Esta percepción evidencia la necesidad de formación y herramientas de IA para aprovechar plenamente la infraestructura existente.

Tabla 12. *Uso de información generada por cámaras*

Nivel de utilización	Porcentaje
Alta	28%
Media	50%
Baja	22%

Fuente: Elaboración propia

Se puede interpretar que la información generada no se transforma sistemáticamente en inteligencia operativa, limitando la prevención proactiva.

Lo que justifica la implementación de alertas tempranas y análisis automatizado para optimizar la toma de decisiones.

Tabla 13. *Enfoque operativo percibido*

Tipo de enfoque	Porcentaje
Reactivo	38%
Preventivo	16%
Mixto	46%

Fuente: Elaboración propia

Tal y como se observa predomina el enfoque mixto, indicando que la prevención existe de manera incipiente, pero aún se depende de la reacción a incidentes. Y por tal motivo se confirma la necesidad de evolucionar hacia un modelo preventivo e inteligente basado en IA.

Los resultados obtenidos indican que, si bien existe reconocimiento de una infraestructura considerable, predomina la percepción de limitaciones en integración, análisis y aprovechamiento estratégico de la información. El enfoque mixto refleja esfuerzos incipientes de prevención, aún no consolidados institucionalmente.

La percepción del personal confirma que la tecnología disponible no se traduce automáticamente en capacidades preventivas, sino que requiere modelos analíticos, protocolos claros y soporte estratégico para su aprovechamiento.

4.3.3 Limitaciones actuales y viabilidad de Inteligencia Artificial

Según el instrumento aplicado, el personal del Centro de Monitoreo identificó las principales limitaciones, en este apartado fue posible marcar más de una opción

Limitaciones identificadas por el personal (pueden marcar varias):

Tabla 14. *Limitaciones según personal del Centro de Monitoreo*

Limitación	**Porcentaje de respuestas**
Falta de herramientas tecnológicas	74%
Falta de personal especializado	42%
Falta de integración de datos	61%
Limitaciones presupuestarias	33%
Falta de lineamientos estratégicos	55%

Nota: se permite seleccionar más de una opción, por lo que los porcentajes no suman 100%. **Fuente**: Elaboración propia

A partir de los datos obtenidos se interpreta que las principales barreras son tecnológicas y de integración de datos. Estas limitaciones afectan directamente la capacidad de anticipación del delito.

Lo cual respalda la necesidad de protocolos, capacitación y analítica avanzada.

A pesar de estas limitaciones, el 74% de los encuestados considera viable o totalmente viable la implementación de inteligencia artificial, destacando su aporte en detección temprana de incidentes, identificación de patrones delictivos y apoyo a la toma de decisiones estratégicas.

Es importante destacar que según los encuestados; las áreas donde la inteligencia artificial aportaría mayor valor estratégico son:

- Detección temprana de incidentes (88%)
- Identificación de patrones delictivos (75%)
- Priorización de recursos policiales (68%)
- Reducción de carga operativa humana (59%)
- Apoyo a la toma de decisiones estratégicas (70%)

Los resultados supra, evidencian un consenso institucional sobre el potencial de la inteligencia artificial como herramienta de modernización y fortalecimiento de la prevención del delito, condicionado a ajustes tecnológicos, administrativos y de capacitación.

4.3.4 Análisis de causas mediante el modelo de Ishikawa

Con el fin de profundizar en la identificación de los factores que limitan el aprovechamiento estratégico de la infraestructura tecnológica del Centro de Monitoreo de San José, se aplicó el modelo de análisis causa-efecto, conocido como diagrama de Ishikawa o “espina de pescado”. Este modelo, desarrollado por Kaoru Ishikawa en el ámbito de la gestión de calidad, permite organizar de manera sistemática las causas que influyen en un problema específico, facilitando su visualización y posterior intervención. Su estructura gráfica agrupa las causas en categorías analíticas, lo que

ayuda a comprender de manera integral los factores que inciden en un efecto determinado.

En el contexto de esta investigación, el efecto central analizado corresponde a la limitada capacidad preventiva del Centro de Monitoreo para anticipar incidentes delictivos mediante herramientas tecnológicas avanzadas.

Las categorías y factores se definieron a partir de una triangulación de información, considerando:

1. Resultados cuantitativos de las encuestas aplicadas al personal del Centro de Monitoreo.

2. Hallazgos cualitativos derivados de entrevistas semiestructuradas con jefaturas y mandos intermedios.

3. Revisión documental sobre protocolos, lineamientos institucionales y características de la infraestructura tecnológica.

Esta metodología permitió garantizar que las causas identificadas representen de manera integral las barreras tecnológicas, operativas y estratégicas que limitan la transición hacia un modelo de monitoreo inteligente.

A partir del análisis, se definieron cinco grandes categorías causales, cada una con factores específicos que explican la brecha existente entre la capacidad tecnológica instalada y su aprovechamiento para la inteligencia operativa y prevención del delito:

1. **Infraestructura tecnológica:**

    - Falta de integración de datos entre cámaras, alarmas y sistemas corporativos.
    - Ausencia de herramientas de analítica avanzada y georreferenciación.
    - Cobertura tecnológica desigual en zonas críticas del cantón.
    - Limitaciones en sensores y dispositivos especializados para prevención.

2. **Procesos operativos:**
    - Protocolos no estandarizados para el uso de tecnología.
    - Flujos de información fragmentados entre áreas y turnos.
    - Predominio de un enfoque reactivo ante incidentes.
    - Escasa coordinación interdepartamental para la respuesta preventiva.

3. **Recursos humanos:**
    - Necesidad de capacitación especializada en análisis de datos e inteligencia artificial.
    - Distribución de turnos no optimizada según demanda operativa.
    - Falta de personal con habilidades técnicas avanzadas.

4. **Gestión estratégica:**
    - Vacíos en lineamientos institucionales para la integración tecnológica.
    - Ausencia de indicadores de desempeño asociados a prevención y análisis.

- Planificación tecnológica parcial y no alineada con objetivos estratégicos.

5. **Gobernanza de datos y ética:**

    - Control limitado sobre la calidad, trazabilidad y seguridad de los datos.
    - Riesgo de sesgos en el análisis y toma de decisiones.
    - Falta de auditorías periódicas y supervisión ética.
    - Necesidad de garantizar privacidad y derechos de los ciudadanos.

El diagrama de Ishikawa permite visualizar de manera integrada y sistemática las barreras tecnológicas, organizacionales y estratégicas que limitan la transición hacia un modelo de monitoreo inteligente. Cada categoría interactúa con las demás, generando un efecto acumulativo que explica la subutilización de la infraestructura tecnológica existente.

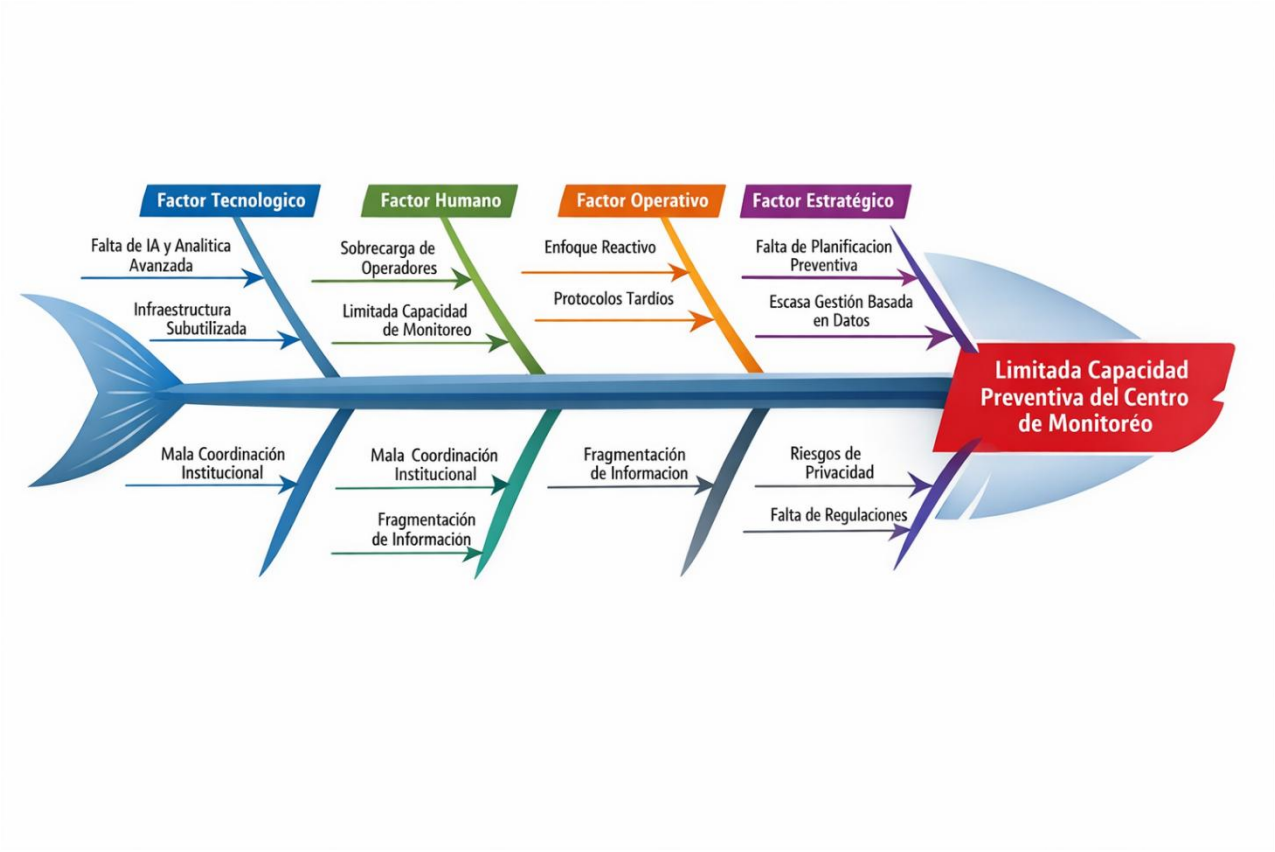


Figura 15. Diagrama de Ishikawa

Fuente: Elaboración propia a partir del análisis de resultados de la investigación.

La Figura 15 presenta el diagrama de Ishikawa aplicado al caso del Centro de Monitoreo de San José, sintetizando las principales causas identificadas a partir del análisis empírico realizado.

El análisis evidencia que la problemática no responde a una única causa, sino a una configuración sistémica de factores interrelacionados.

En este sentido:

• La tecnología existe, pero no se utiliza estratégicamente

• El recurso humano es valioso, pero está sobrecargado

• Los procesos operan, pero bajo un enfoque reactivo

• La gestión existe, pero sin una visión predictiva

Esto confirma la existencia de una brecha estructural entre capacidad instalada y capacidad preventiva real, lo cual sustenta la necesidad de una transformación del modelo de gestión.

Implicaciones para la propuesta

A partir de este análisis, se derivan tres implicaciones clave:

1. La solución no es solo tecnológica

Requiere transformación organizacional

2. La inteligencia artificial es un habilitador, no el fin

Debe integrarse con procesos y talento humano

3. La estrategia debe ser sistémica

Integrando tecnología, operación, gobernanza y evaluación

En conclusión, el análisis causal desarrollado mediante el enfoque tipo Ishikawa permite evidenciar que las limitaciones actuales del Centro de Monitoreo no responden únicamente a la ausencia de tecnología avanzada, sino a la interacción de factores tecnológicos, humanos, operativos y estratégicos que, en conjunto, configuran un modelo de gestión predominantemente reactivo.

La identificación de estas causas estructurales permite sustentar de manera sólida la necesidad de una estrategia administrativa orientada a la implementación de alertas tempranas basadas en inteligencia artificial, como mecanismo para transitar hacia un modelo preventivo, eficiente y basado en datos.

Este enfoque integral constituye la base conceptual sobre la cual se construye la propuesta de gestión desarrollada en el capítulo siguiente, orientada a fortalecer la capacidad institucional del Centro de Monitoreo y generar valor público en la seguridad ciudadana del Cantón Central de San José.

4.3.5 Percepción ciudadana sobre seguridad

Con el fin de profundizar en la percepción ciudadana, se analizaron de manera descriptiva los resultados obtenidos a partir del instrumento aplicado a 60 ciudadanos y comerciantes del Cantón Central de San José, considerando variables asociadas a la percepción de seguridad, confianza institucional, nivel de conocimiento del Centro de Monitoreo y aceptación del uso de inteligencia artificial en seguridad pública.

Percepción ciudadana sobre la seguridad en zonas monitoreadas

Los resultados evidencian que el 42% de las personas encuestadas considera que la seguridad ha mejorado en las zonas donde existe cobertura tecnológica municipal, mientras que un 35% percibe que la situación se mantiene sin cambios significativos. Por su parte, un 23% considera que la cobertura tecnológica resulta insuficiente o que la seguridad ha empeorado.

Estos resultados se presentan en la Tabla 11 permitiendo identificar que, si bien existe una valoración positiva parcial del sistema de videovigilancia, persiste un segmento relevante de la población que no percibe mejoras sustantivas en la seguridad.

Tabla 15. *Percepción ciudadana sobre la seguridad en zonas monitoreadas*

Categoría	Frecuencia	Porcentaje
Ha mejorado	50	41.6%
Se mantiene igual	42	35%
Es insuficiente/ ha empeorado	28	23,4%
Total	120	100%

Fuente: Elaboración propia a partir de datos obtenidos en encuesta ciudadana (n=120).

De los datos obtenidos se puede interpretar que la percepción de mejora no es unánime; un 23,4% de ciudadanos percibe insuficiencia. Situación que destaca la necesidad de comunicación y divulgación sobre el uso de la tecnología y sus beneficios preventivos.

Confianza ciudadana en la respuesta del Centro de Monitoreo

En relación con la confianza en la capacidad de respuesta del Centro de Monitoreo, los resultados indican que el 45% de los encuestados manifiesta un nivel de confianza medio, seguido de un 32% que reporta baja confianza y únicamente un 23% que expresa alta confianza en la atención de incidentes.

La tabla 12 muestra que la confianza ciudadana se concentra mayoritariamente en niveles intermedios, lo cual sugiere que la infraestructura tecnológica existente no se traduce de forma automática en una percepción sólida de efectividad institucional.

Tabla 16. *Nivel de confianza ciudadana en la respuesta del Centro de Monitoreo*

Nivel de confianza	Frecuencia	Porcentaje
Alta	28	23.4%
Media	54	45%
Baja	38	31.6%
Total	120	100%

Fuente: Elaboración propia. Resultados del instrumento aplicado a ciudadanos y comerciantes del Cantón Central de San José.

La mayoría de los encuestados confía de manera media; solo el 23% expresa confianza alta. Se evidencia que la infraestructura tecnológica no se traduce automáticamente en percepción de efectividad.

Apoya la necesidad de alertas tempranas y mejoras operativas para consolidar confianza ciudadana.

Nivel de conocimiento ciudadano sobre el Centro de Monitoreo

El análisis revela que el 47% de los encuestados posee un nivel medio de conocimiento sobre el funcionamiento del Centro de Monitoreo y el uso de herramientas tecnológicas como cámaras y la aplicación móvil “Alerta San José”. No obstante un 35% presenta un nivel bajo de conocimiento, lo cual podría incidir negativamente en la percepción de efectividad institucional y en el uso de los canales disponibles para la prevención y reporte de incidentes.

Estos resultados se presentan en la tabla 13, evidenciando la necesidad de fortalecer estrategias de comunicación y divulgación institucional dirigidas a la ciudadanía

Tabla 17. *Nivel de conocimiento ciudadano sobre el Centro de Monitoreo*

Nivel de conocimiento	Frecuencia	Porcentaje
Alto	22	18.3%
Medio	56	46.7%
Bajo	42	35%
Total	120	100%

Fuente: Elaboración propia datos obtenidos en encuesta aplicada a ciudadanos del Cantón Central de San José.

El conocimiento del centro de monitoreo por parte de los ciudadanos según encuesta, es limitado para casi un 35%, lo que podría reducir el uso de herramientas como el monitoreo de alarmas, la app “Alerta San José”, etc.

Situación que sugiere llevar a cabo estrategias de divulgación y participación ciudadana para fortalecer el modelo preventivo.

Aceptación ciudadana del uso de inteligencia artificial en seguridad pública

En cuanto a la incorporación de tecnologías avanzadas, los resultados muestran una aceptación mayoritaria del uso de inteligencia artificial en seguridad pública, donde el 55% de los encuestados expresa una aceptación alta, el 30% una aceptación media y únicamente el 15% manifiesta una aceptación baja.

Tabla 18. *Aceptación ciudadana del uso de inteligencia artificial en seguridad pública*

Nivel de aceptación	Frecuencia	Porcentaje
Alta	66	55%
Media	36	30%

Baja	18	15%
Total	120	100%

Fuente: Elaboración propia

De lo anterior se interpreta que la aceptación se encuentra condicionada principalmente al respeto de la privacidad, la transparencia institucional y la existencia de control humano sobre los sistemas automatizados, aspectos que coinciden con los principios éticos señalados en la literatura especializada. Y al mismo tiempo confirma la viabilidad social de implementar alertas tempranas basadas en IA

Interpretación integral de la percepción ciudadana

En conjunto, los resultados del instrumento ciudadano evidencian que la percepción pública sobre la seguridad y el funcionamiento del Centro de Monitoreo es moderadamente favorable, pero aún insuficiente para consolidar una confianza plena en el modelo actual. La presencia de infraestructura tecnológica contribuye a mejorar la percepción en zonas con mayor cobertura; sin embargo, la falta de analítica avanzada, alertas tempranas y estrategias de comunicación limita su impacto preventivo y su legitimidad social.

Estos hallazgos refuerzan la necesidad de evolucionar hacia un modelo de monitoreo inteligente, que no solo amplíe las capacidades tecnológicas, sino que también fortalezca la transparencia, la participación ciudadana y la toma de decisiones basada en evidencia, elementos que serán desarrollados en la propuesta de gestión del capítulo siguiente

Asimismo, una proporción significativa de los encuestados manifestó un conocimiento limitado sobre el funcionamiento del Centro de Monitoreo y el uso de herramientas como la aplicación “Alerta San José”, lo cual podría incidir negativamente en la percepción de efectividad institucional.

En cuanto al uso de tecnologías avanzadas, la mayoría de los ciudadanos expresó una aceptación favorable de la inteligencia artificial aplicada a la seguridad pública, condicionada al respeto de la privacidad, la transparencia institucional y el control humano de los sistemas.

4.3.6 Relación entre cobertura tecnológica, enfoque operativo y percepción de efectividad

El análisis integrado de los resultados cuantitativos permite identificar relaciones relevantes entre la cobertura tecnológica del Centro de Monitoreo, el enfoque operativo predominante y la percepción de efectividad tanto a nivel institucional como ciudadano.

Los distritos que concentran una mayor densidad de cámaras y dispositivos tecnológicos, principalmente zonas centrales del Cantón como Hospital, Merced, Carmen y Catedral, coinciden con áreas donde el personal percibe una mayor capacidad de respuesta operativa y donde una proporción significativa de la ciudadanía reporta mejoras parciales en la seguridad. Esta relación descriptiva sugiere que la infraestructura tecnológica contribuye positivamente a la disuasión y atención de incidentes, especialmente en espacios de alta afluencia y concentración delictiva.

No obstante, los resultados evidencian que una mayor cobertura tecnológica no se traduce automáticamente en un enfoque preventivo consolidado. A pesar de la amplia infraestructura instalada, el 38% del personal percibe que el modelo operativo sigue siendo predominantemente reactivo, y solo el 16% lo identifica como preventivo. Esto indica que la tecnología disponible se utiliza principalmente como herramienta de observación y registro posterior de eventos, más que como un sistema activo de anticipación y prevención del delito.

Asimismo, la percepción ciudadana moderada respecto a la seguridad y la cobertura tecnológica refuerza esta conclusión. Aunque existe reconocimiento de mejoras en zonas monitoreadas, persisten dudas sobre la efectividad real del sistema para prevenir incidentes antes de que ocurran. Esta brecha entre capacidad tecnológica y resultados percibidos pone de manifiesto la necesidad de integrar analítica avanzada y alertas tempranas basadas en inteligencia artificial, que permitan transformar la cobertura existente en inteligencia operativa y estratégica.

En conjunto, la relación entre estas variables evidencia que la infraestructura tecnológica es una condición necesaria, pero no suficiente, para fortalecer la prevención del delito, siendo indispensable su integración con modelos de análisis automatizado, protocolos claros y toma de decisiones basada en evidencia.

Esta relación pone de manifiesto la necesidad de transformar la cobertura existente en inteligencia operativa mediante analítica automatizada y alertas tempranas basadas en IA.

4.4 Análisis cualitativo

Las entrevistas semiestructuradas con jefaturas y mandos intermedios permitieron identificar

1. Barreras organizacionales asociadas a la ausencia de lineamientos estratégicos claros y resistencia al cambio.

2. Valor estratégico de Inteligencia Artificial: reconocida como factor de modernización, requiere capacitación, ajustes de protocolos y definición de indicadores.

3. Ética y privacidad: necesidad de garantizar control humano, respeto a derechos y cumplimiento normativo.

Los resultados evidencian que el Centro de Monitoreo de San José posee una infraestructura tecnológica amplia, pero subutilizada desde una perspectiva preventiva. Existe una brecha significativa entre la capacidad instalada y la generación de inteligencia operativa y estratégica. Los hallazgos empíricos respaldan los enfoques de prevención situacional, Intelligence-Led Policing y gestión pública por resultados, evidenciando la necesidad de evolucionar hacia un modelo de monitoreo inteligente basado en alertas tempranas y análisis automatizado.

Además, se identifican brechas tecnológicas, operativas, administrativas, analíticas, estratégicas y éticas, las cuales fundamentan la necesidad de una propuesta integral de gestión que permita cerrar estas distancias y maximizar el valor público de la inversión tecnológica existente.

A partir del análisis realizado, se derivan los siguientes lineamientos que servirán de base para la propuesta de gestión:

- Implementación gradual de alertas tempranas basadas en IA en zonas críticas del cantón.

- Fortalecimiento de capacidades del personal mediante capacitación técnica y analítica.

- Definición de protocolos claros de integración tecnológica y flujo de información.

- Establecimiento de indicadores de desempeño y evaluación continua.

- Garantía de gobernanza de datos, control humano y cumplimiento ético y normativo.

Los discursos cualitativos refuerzan los hallazgos cuantitativos, evidenciando una brecha entre la capacidad tecnológica instalada y la madurez institucional para su aprovechamiento estratégico.

4.5 Integración de hallazgos cuantitativos y cualitativos

La combinación de datos demuestra que, si bien el Centro de Monitoreo posee infraestructura avanzada, su potencial estratégico no se aprovecha desde una perspectiva preventiva. La evidencia cuantitativa refleja cobertura y tiempos de

respuesta, mientras que la información cualitativa señala barreras organizacionales y éticas.

La integración de ambos enfoques respalda la necesidad de un modelo de monitoreo inteligente con alertas tempranas, protocolos claros, capacitación del personal y gobernanza de datos.

4.6 Lineamientos derivados para propuesta de gestión

1. Diseño e implementación gradual de alertas tempranas basadas en inteligencia artificial en zonas críticas.

2. Fortalecimiento de capacidades del personal mediante formación técnica y analítica.

3. Definición de protocolos claros de integración tecnológica y flujos de información.

4. Establecimiento de indicadores de desempeño y evaluación continua.

5. Garantía de gobernanza de datos, control humano y cumplimiento ético y normativo.

4.7 Identificación de brechas entre la situación actual y el modelo de monitoreo inteligente

A partir del análisis de resultados cuantitativos y cualitativos, se identifican brechas significativas entre la situación actual del Centro de Monitoreo de San José y un modelo de monitoreo inteligente orientado a la prevención del delito mediante alertas tempranas basadas en inteligencia artificial.

En la dimensión tecnológica, el Centro de Monitoreo cuenta con una infraestructura robusta y diversificada; sin embargo, esta se utiliza bajo un esquema mayoritariamente pasivo, sin analítica automatizada ni generación de alertas predictivas. El modelo deseado implica el uso activo de inteligencia artificial para detectar patrones, comportamientos atípicos y riesgos emergentes en tiempo real.

Desde la dimensión operativa, se evidencia una dependencia de la respuesta reactiva ante incidentes ya ocurridos, con esfuerzos incipientes hacia la prevención. El modelo ideal plantea una transición hacia una operación preventiva, donde las alertas tempranas permitan anticipar eventos, optimizar el despliegue de recursos y reducir tiempos de respuesta.

En el ámbito administrativo y estratégico, se identifican carencias en lineamientos claros, protocolos integrados y definición de indicadores de desempeño asociados al uso de tecnologías inteligentes. El modelo propuesto requiere una gestión estructurada, con flujos de información definidos, responsabilidades claras y evaluación continua basada en resultados.

En cuanto a la dimensión analítica, la información generada por cámaras, alarmas y otros dispositivos no se explota de manera integral para la toma de decisiones estratégicas. El modelo deseado contempla el uso sistemático de datos, análisis geoespacial y generación de inteligencia operativa alineada con los principios de Intelligence-Led Policing.

Finalmente, en la dimensión ética y de gobernanza de datos, aunque se cumple con la normativa vigente, se requiere avanzar hacia esquemas más proactivos de control humano, transparencia, trazabilidad y protección de derechos fundamentales en el uso de inteligencia artificial.

Estas brechas constituyen el fundamento empírico que justifica la formulación de una propuesta integral de gestión orientada a cerrar las distancias entre la capacidad instalada del Centro de Monitoreo y su potencial estratégico en la prevención del delito.

4.8 Brechas identificadas entre la situación actual y la situación óptima

A continuación, se presenta un cuadro que sintetiza las principales brechas detectadas en el Centro de Monitoreo de San José, comparando la situación actual con la situación óptima que se requiere para implementar un modelo de monitoreo inteligente basado en alertas tempranas y analítica avanzada de IA.

Tabla 19. *Brechas situación actual vs Situación óptima*

Área	**Situación actual**	**Situación óptima**	**Brecha identificada**
Infraestructura tecnológica	1,869 cámaras y 2,400 alarmas; analítica IA no implementada	Integración total de IA, alertas tempranas, analítica predictiva y georreferenciación	Falta de integración tecnológica para prevención proactiva
Gestión operativa	Uso mayoritariamente reactivo, protocolos no estandarizados	Flujos claros, Indicadores clave de desempeño (KPIs) definidos, integración	Dependencia de la reacción, ausencia de protocolos claros

		de cámaras corporales, vehiculares y móviles	
Recursos humanos	Capacitación básica en monitoreo; distribución de turnos no optimizada	Formación avanzada en IA, análisis de datos y toma de decisiones basada en evidencia; asignación eficiente por demanda	Déficit de capacitación y asignación estratégica de personal
Gobernanza de datos y ética	Control limitado, sin auditorías periódicas, sin comités de ética	Integridad, trazabilidad, auditorías periódicas, supervisión ética y control humano	Riesgo de sesgos, vulneración de derechos y privacidad
Percepción ciudadana	Confianza moderada, conocimiento limitado del sistema, aceptación condicionada	Alta confianza, conocimiento sólido sobre protocolos y beneficios del sistema	Necesidad de transparencia, comunicación y participación ciudadana

Fuente: Elaboración propia a partir del análisis de resultados de la investigación.

La tabla evidencia que, si bien el Centro de Monitoreo posee infraestructura tecnológica amplia, la brecha principal se encuentra en la integración de herramientas de inteligencia artificial y la consolidación de protocolos operativos, capacitación, gobernanza ética y aceptación ciudadana. Estas brechas fundamentan la necesidad de la propuesta de gestión que se desarrolla en el Capítulo VI.

4.9 Discusión de resultados a la luz del marco teórico

Los resultados obtenidos en esta investigación pueden ser interpretados a la luz de los enfoques teóricos abordados en el marco conceptual, particularmente los modelos de prevención situacional, Hot Spots Policing, Intelligence-Led Policing y Evidence-Based Policing.

En relación con el modelo de Hot Spots Policing, los hallazgos evidencian una concentración estratégica de dispositivos tecnológicos en zonas de mayor incidencia delictiva y alta afluencia de personas, lo cual es consistente con los postulados teóricos que priorizan la intervención focalizada en puntos críticos. No obstante, la ausencia de analítica automatizada limita el aprovechamiento pleno de esta concentración tecnológica para la anticipación de delitos.

Desde la perspectiva de Intelligence-Led Policing, los resultados muestran que, si bien el Centro de Monitoreo genera grandes volúmenes de datos, estos no se transforman sistemáticamente en inteligencia accionable para la toma de decisiones estratégicas. La falta de integración de datos y de herramientas de análisis predictivo evidencia una brecha entre la práctica actual y los principios del modelo teórico.

En cuanto a Evidence-Based Policing, se observa que las decisiones operativas se apoyan parcialmente en información empírica, como registros de incidentes y tiempos de respuesta; sin embargo, no existen aún mecanismos estructurados para evaluar el impacto de las decisiones ni para retroalimentar los procesos mediante análisis continuo de resultados.

Finalmente, los resultados cualitativos refuerzan la importancia de incorporar consideraciones éticas, gobernanza de datos y control humano, aspectos fundamentales en la aplicación responsable de tecnologías de inteligencia artificial en

seguridad pública, tal como lo plantean los estándares internacionales y la literatura especializada.

En conjunto, los hallazgos empíricos respaldan los enfoques teóricos analizados, pero también evidencian la necesidad de evolucionar desde un modelo de vigilancia tradicional hacia un esquema de monitoreo inteligente, preventivo y éticamente responsable.

4.10 Limitaciones del análisis de resultados

Si bien los resultados obtenidos permiten alcanzar los objetivos planteados en la investigación, es importante reconocer algunas limitaciones que deben considerarse al interpretar los hallazgos.

En primer lugar, el estudio se desarrolla en un contexto donde las herramientas de inteligencia artificial aún no se encuentran plenamente implementadas en el Centro de Monitoreo, por lo que el análisis de su impacto se basa en escenarios potenciales, percepciones institucionales y simulaciones operativas, más que en resultados empíricos derivados de su uso real.

En segundo lugar, el tamaño de la muestra ciudadana, aunque suficiente para un análisis descriptivo, limita la posibilidad de generalizar los resultados a toda la población del cantón. No obstante, los datos recopilados aportan una visión relevante sobre la percepción pública de la seguridad y la cobertura tecnológica.

Adicionalmente, algunas variables analizadas dependen de la percepción del personal operativo y de mandos intermedios, lo cual puede introducir sesgos subjetivos. Esta

limitación fue mitigada mediante la triangulación con registros operativos, revisión documental y análisis cualitativo.

Finalmente, el diseño transversal del estudio permite describir la situación en un momento específico, pero no evaluar cambios longitudinales en el desempeño del Centro de Monitoreo. Futuras investigaciones podrían profundizar en evaluaciones comparativas antes y después de la implementación de sistemas de alertas tempranas basadas en inteligencia artificial.

Los resultados analizados en este capítulo evidencian la necesidad de una transformación del modelo actual de monitoreo hacia un enfoque preventivo e inteligente. En el capítulo siguiente se presenta una propuesta de gestión orientada a cerrar las brechas identificadas, integrando tecnología, procesos, capacidades humanas y principios éticos.

Capítulo V

Conclusiones y Recomendaciones

5.1 Conclusiones

Los resultados obtenidos permiten dar respuesta al objetivo general y a los objetivos específicos de la investigación, evidenciando las principales fortalezas, brechas y oportunidades estratégicas del Centro de Monitoreo del Cantón Central de San José en relación con la implementación de alertas tempranas basadas en inteligencia artificial.

1. **Infraestructura y cobertura tecnológica**

El Centro de Monitoreo de San José cuenta con una infraestructura tecnológica amplia, conformada por 1,890 cámaras de videovigilancia y más de 2,400 alarmas distribuidas en los 11 distritos del Cantón Central (Tabla 4, Figuras 1–14). Esta cobertura permite registrar eventos en tiempo real en espacios públicos, vías principales y zonas de alta afluencia, siguiendo criterios de focalización según el modelo de Hot Spots Policing (Sherman & Weisburd, 1995; Koper, 1995).

Sin embargo, los hallazgos evidencian que la infraestructura disponible se utiliza mayoritariamente de manera pasiva, sin integración de analítica avanzada ni generación automática de alertas. Esto limita su potencial preventivo y confirma la existencia de una brecha entre la capacidad tecnológica instalada y su aprovechamiento estratégico (4.3.1, 4.8).

2. **Gestión operativa y toma de decisiones**

Los registros operativos y encuestas al personal técnico y operativo (Tablas 5–7) evidencian que la información disponible se utiliza mayoritariamente de manera reactiva. La falta de integración de cámaras corporales, móviles y alarmas con sistemas de análisis en tiempo real restringe la toma de decisiones estratégicas.

Se concluye que el modelo operativo actual responde principalmente a un enfoque reactivo de atención de incidentes, con limitada utilización de análisis predictivo o priorización dinámica de recursos. La incorporación de alertas tempranas basadas en IA podría fortalecer la gestión bajo los principios de Intelligence-Led Policing y Evidence-Based Policing (Ratcliffe, 2008; Lum et al., 2012), siempre que se establezcan indicadores claros de desempeño y mecanismos de evaluación continua.

3. **Percepción del personal y consideraciones éticas**

El personal reconoce la necesidad de modernizar los sistemas y resalta la importancia de capacitación, lineamientos estratégicos claros y protocolos éticos (Tablas 5–8). La adopción de IA requiere garantizar transparencia, protección de datos y supervisión humana (“human-in-the-loop”), evitando sesgos algorítmicos y asegurando confianza institucional y ciudadana, conforme a estándares internacionales (UNODC, BID; Hernández Valle, 2015).

Se determina que la aceptación institucional de la inteligencia artificial está condicionada a la existencia de procesos formales de capacitación, supervisión humana permanente y lineamientos normativos claros. La implementación

tecnológica, por tanto, no puede desvincularse de un marco robusto de gobernanza de datos, transparencia y protección de derechos fundamentales, evitando riesgos asociados a sesgos algorítmicos o uso indebido de información.

4. **Impacto potencial en la seguridad ciudadana**

Los resultados de la encuesta ciudadana (Tablas 9–12) indican que la implementación de IA y alertas tempranas puede mejorar la percepción de seguridad y reducir tiempos de respuesta.

No obstante, el impacto real en la reducción del delito dependerá de factores organizativos, normativos y presupuestarios, así como de la correcta integración entre tecnología, procesos y capital humano. En este sentido, la evidencia sugiere que la tecnología constituye un facilitador estratégico, pero no un sustituto de la gestión institucional eficiente.

5. **Valor estratégico y gerencial**

La adopción de un modelo inteligente de monitoreo trasciende la operación y se constituye en una estrategia de gestión que optimiza recursos, mejora eficiencia organizacional y fortalece la toma de decisiones basada en evidencia.

Desde una perspectiva administrativa, la propuesta representa una herramienta de modernización institucional orientada a resultados, alineada con tendencias de ciudades inteligentes y gestión pública basada en datos, siempre que se garantice sostenibilidad financiera y control institucional adecuado.

6. Transferibilidad y replicabilidad

El modelo propuesto podría ser adaptable a otros municipios con características similares de infraestructura tecnológica y marco normativo, aunque su implementación requerirá ajustes contextuales.

Dado el diseño metodológico de estudio de caso, los resultados no son generalizables en términos estadísticos; sin embargo, el modelo podría servir como referencia técnica para otros gobiernos locales con condiciones institucionales comparables, previa adaptación a sus contextos específicos.

7. Síntesis de hallazgos

En conjunto, los hallazgos evidencian una brecha entre la capacidad tecnológica y su aprovechamiento estratégico para prevención del delito, la necesidad de integración de IA, protocolos claros, capacitación del personal y gobernanza de datos.

En síntesis, la investigación confirma que la implementación de un modelo de monitoreo inteligente con alertas tempranas requiere no solo innovación tecnológica, sino transformación organizacional, fortalecimiento normativo y gestión estratégica del cambio.

5.2 Recomendaciones

Para optimizar la capacidad del Centro de Monitoreo y cerrar las brechas identificadas, se proponen recomendaciones priorizadas por fases y áreas de acción.

Las siguientes recomendaciones se fundamentan directamente en los hallazgos empíricos obtenidos y buscan garantizar viabilidad técnica, sostenibilidad institucional y coherencia normativa.

Dado que el análisis evidenció una subutilización de capacidades analíticas existentes, se recomienda priorizar acciones de integración tecnológica que permitan transformar el enfoque reactivo actual en uno preventivo.

A. Integración tecnológica y uso de IA (prioritario – corto plazo)

- Implementar un sistema de alertas tempranas basado en IA, integrado con cámaras, alarmas y registros de patrullaje, con visualización en tiempo real.
- Establecer protocolos operativos claros para gestión de alertas, criterios de activación, responsables de verificación y flujos de acción.
- Evaluar periódicamente la precisión de las alertas generadas por IA y ajustar algoritmos según resultados operativos.
- Establecer una fase inicial de validación técnica para medir tasas de falsos positivos y confiabilidad del sistema antes de su expansión operativa.

B. Gestión y gobernanza de datos (prioritario – corto/mediano plazo)

- Fortalecer coordinación interinstitucional para intercambio de información entre Policía Municipal, Fuerza Pública y otras entidades.
- Definir KPIs: tasa de detección temprana, cobertura de cámaras, tiempos de respuesta y cumplimiento de protocolos.
- Establecer un plan de gobernanza de datos que asegure integridad, trazabilidad y cumplimiento de la Ley 8968 y estándares internacionales (Privacy by Design, ISO 27001).
- Aprobar un reglamento interno específico sobre uso de inteligencia artificial y tratamiento de datos derivados de sistemas automatizados.

C. Capacitación y gestión del cambio (prioritario – mediano plazo)

- Capacitar al personal operativo, técnico y de supervisión en uso de IA, análisis de datos y protocolos de actuación.
- Implementar estrategias de gestión del cambio que promuevan aceptación de nuevas tecnologías y optimización de procesos internos.
- Incorporar evaluación periódica de competencias digitales para garantizar apropiación tecnológica sostenida.

D. Ética y derechos humanos (prioritario – corto/mediano plazo)

- Garantizar supervisión humana en todas las alertas generadas por IA.
- Realizar auditorías periódicas para detectar sesgos algorítmicos y evaluar impactos en privacidad y derechos humanos.

- Comunicar a la ciudadanía beneficios y protocolos del sistema, fortaleciendo confianza y legitimidad.
- Realizar evaluaciones de impacto en protección de datos antes de la implementación total del sistema.

E. Fases de implementación (mediano/largo plazo)

- Iniciar con un proyecto piloto en áreas de alta incidencia delictiva, monitorear resultados, ajustar parámetros tecnológicos, organizativos y normativos antes de la implementación total.
- Integrar retroalimentación del personal y ciudadanía para optimizar el modelo.
- Establecer indicadores comparativos pre y post implementación para evaluar resultados con base empírica.

F. Análisis económico y sostenibilidad (largo plazo)

- Realizar análisis costo-beneficio y retorno de inversión (ROI) considerando reutilización de infraestructura existente, reducción de costos operativos y optimización de recursos humanos.
- Explorar financiamiento mixto, cooperación internacional o alianzas público-privadas, siguiendo experiencias internacionales en ciudades inteligentes.
- Elaborar un plan anual de inversión tecnológica que garantice mantenimiento, actualización y escalabilidad del sistema.

G. Escalabilidad y transferencia internacional (largo plazo)

- Documentar procesos, protocolos y lecciones aprendidas para replicabilidad en otros municipios y gobiernos locales.
- Mantener alineación con estándares internacionales de ética, gobernanza de datos y gestión por resultados, asegurando sostenibilidad y aceptación ciudadana.

5.3 Impacto esperado de la propuesta

La implementación de un modelo inteligente de monitoreo con alertas tempranas basado en IA podría:

1. Contribuir a la reducción de incidentes en zonas críticas, siempre que se garantice correcta implementación y monitoreo continuo
2. Optimizar el despliegue de recursos humanos y tecnológicos, aumentando eficiencia operativa.
3. Mejorar percepción de seguridad y confianza ciudadana, fortaleciendo legitimidad institucional.
4. Consolidar la toma de decisiones basada en evidencia y datos en tiempo real.
5. Generar un modelo replicable y sostenible, alineado con estándares globales de ciudades inteligentes y seguridad urbana.

Estos impactos deberán ser evaluados mediante mediciones longitudinales posteriores a la implementación, a fin de determinar su efectividad real en términos de reducción delictiva y eficiencia operativa.

5.4 Vinculación con el marco teórico

Las conclusiones y recomendaciones se alinean directamente con los enfoques teóricos y conceptuales desarrollados en la investigación:

- **Hot Spots Policing:** priorización de recursos y dispositivos en zonas críticas de incidencia delictiva.
- **Intelligence-Led Policing:** uso de datos y análisis predictivo para decisiones estratégicas.
- **Evidence-Based Policing:** aplicación de información empírica y registro operativo para diseñar políticas preventivas.
- **Prevención situacional:** utilización de tecnología para anticipar y reducir oportunidades delictivas.

La propuesta combina estos enfoques con un marco ético y de gobernanza de datos, asegurando que la tecnología sea un instrumento estratégico, preventivo y responsable, contribuyendo a la modernización integral del Centro de Monitoreo de San José.

En consecuencia, la propuesta desarrollada constituye una alternativa estratégica viable para fortalecer la gestión preventiva del delito en el ámbito municipal, bajo criterios de eficiencia, responsabilidad y sostenibilidad institucional.

Capítulo VI

Propuesta de Modelo de Gestión para el Centro de Monitoreo de San José con Alertas Tempranas Basadas en Inteligencia Artificial

6.1 Enfoque general

La propuesta plantea una estrategia administrativa integral para que el Centro de Monitoreo de San José (CMSJ) incorpore sistemas de alertas tempranas basadas en inteligencia artificial (IA). El objetivo es fortalecer la prevención del delito, optimizar la toma de decisiones, mejorar la eficiencia operativa y aumentar la confianza ciudadana.

La estrategia se estructura en fases secuenciales: diagnóstico, diseño del modelo, adquisición e integración tecnológica, capacitación, piloto, ajustes, implementación total y mejora continua. Esta estructura transforma el modelo reactivo actual en un modelo preventivo y predictivo, apoyado en analítica avanzada, interoperabilidad tecnológica y gobernanza institucional.

6.2 Objetivos específicos de la propuesta

1. Integrar herramientas de IA que permitan identificar patrones delictivos, anomalías y riesgos emergentes en tiempo real.
2. Fortalecer la capacidad institucional mediante procesos administrativos claros, roles definidos y protocolos de actuación basados en evidencia.
3. Garantizar la sostenibilidad técnica, financiera y operativa del sistema de alertas tempranas.
4. Alinear la estrategia con los marcos legales, éticos y de protección de datos vigentes en Costa Rica.

6.3 Componentes de la propuesta

El modelo propuesto se fundamenta en los hallazgos empíricos obtenidos en los capítulos anteriores, los cuales evidenciaron una brecha entre capacidad tecnológica instalada y uso estratégico para prevención.

1. Componente Tecnológico

- Integración de cámaras fijas, domo, corporales y vehiculares con plataformas de IA capaces de detectar patrones delictivos y generar alertas tempranas.
- Analítica de video en tiempo real, priorización automática de eventos y georreferenciación de incidentes.
- Visualización en tiempo real de audio, video y ubicación satelital de dispositivos móviles y patrullas.
- Escalabilidad de infraestructura tecnológica para futuras incorporaciones de sensores, drones y sistemas de análisis predictivo.
- Establecer mecanismos de mantenimiento preventivo y actualización periódica para asegurar confiabilidad y continuidad operativa.

2. Componente Operativo

- Protocolos claros para recepción, análisis y respuesta a alertas tempranas.
- Flujos internos de comunicación entre operadores, supervisores y unidades de respuesta.
- Capacitación continua en IA, interpretación de alertas y toma de decisiones basada en evidencia.

- Definición de KPIs operativos: TTR, tasa de detección temprana, cobertura efectiva de cámaras, reducción de incidentes recurrentes, cumplimiento de protocolos y eficiencia de recursos humanos
- Incorporación de simulaciones y ejercicios de prueba periódicos para evaluar la capacidad de respuesta del personal y la confiabilidad del sistema.

3. Componente de Gobernanza y Ética

- Protocolos de uso ético de IA, auditorías periódicas y control humano (“human-in-the-loop”).
- Cumplimiento de Ley N.° 8968 y lineamientos internacionales sobre protección de datos y derechos humanos (ISO 27001, Privacy by Design).
- Gobernanza de datos: integridad, trazabilidad, acceso controlado y protección de información sensible.
- Transparencia con la ciudadanía mediante comunicación de protocolos, beneficios y resultados del sistema.
- Comités de ética o supervisión externa para reformar legitimidad y confianza ciudadana.

4. Componente Estratégico y Evaluación

- Integración con planificación estratégica municipal y coordinación interinstitucional.
- Evaluación continua de impacto mediante indicadores cuantitativos (alertas precisas, TTR, cobertura) y cualitativos (percepción de seguridad, confianza ciudadana).

- Retroalimentación periódica para ajustes de protocolos, algoritmos y capacitación.
- Documentación y estandarización de procesos para replicabilidad en otros municipios con características institucionales comparables.

6.4 Fases de implementación

Tabla 20. *Fases de implementación*

Fase	**Actividades Principales**	**Resultado Esperado**
1. Diagnóstico y planificación	Evaluación de infraestructura, capacidades operativas, identificación de áreas críticas y definición de KPIs.	Base sólida para la implementación y priorización estratégica.
2. Proyecto piloto	Implementación de IA en zonas “hot spots”, pruebas controladas, capacitación inicial del personal.	Validación de algoritmos y protocolos antes de escalamiento.
3. Ajuste y optimización	Análisis de resultados del piloto, optimización de algoritmos, flujos y protocolos.	Mejora de precisión de alertas y eficiencia operativa.
4. Implementación gradual	Escalamiento progresivo a todos los distritos, monitoreo continuo de KPIs operativos y percepción ciudadana.	Cobertura completa, prevención proactiva y mayor efectividad.
5. Evaluación y sostenibilidad	Auditorías de desempeño, revisión ética, actualización continua del sistema, retroalimentación ciudadana.	Consolidación del modelo como herramienta estratégica y replicable.

Fuente: Elaboración propia a partir del análisis de resultados de la investigación.

6.5 Recursos e inversión

Tabla 21. *Detalle de recursos, inversión y tiempos*

Recurso	Descripción	Objetivo	Cantidad Alcance	Inversión estimada	Tiempo
Infraestructura tecnológica	Servidores de alto rendimiento	OE1	2 unidades	₡60–80 millones	2 meses
	Plataforma de integración de datos	OE1	1 sistema	₡40–60 millones	3 meses
	Paq. Licencias de software de IA y analítica	OE1 / OE2	100–20 licencias	₡50–70 millones	3 meses
	Cámaras inteligentes con analítica en borde	OE1 / OE3	50–100 cámaras	₡150–200 millones	4 meses
Talento humano	Analista de Inteligencia Preventiva	OE2	3 plazas	₡15–20 millones	Permanente
	Especialista en IA y mantenimiento de modelos	OE1 / OE2	1 plaza	₡20–25 millones	Permanente
	Capacitación del personal operativo	OE3	30 funcionarios	₡20–30 millones	2 meses
Procesos y gobernanza	Comité de Innovación y Analítica	General	1 comité	-	Permanente
	Manual atualizado de protocolos preventivos	OE3	1 documento	₡5 millones	1 mes

	Auditoría ética y de privacidad de datos	OE2	1 proceso anual	₡3–5 millones	Anual
Coordinación interinstitucional	Convenios de intercambio de datos	OE1 / OE3	3–5 convenios	-	Permanente
	Sistema de despacho policial integrado	OE3	1 sistema	₡50–70 millones	4 meses
Financiamiento	Presupuesto para adquisición tecnológica	General	Monto anual	Según proyecto	Permanente
	Fondos para capacitación y certificación	OE2	Monto anual	Según proyecto	Permanente

Fuente: Elaboración propia a partir del análisis de resultados de la investigación.

6.6 Indicadores de desempeño

- **Cuantitativos:**
    - Tiempo de respuesta promedio ante alertas.
    - Número y porcentaje de incidentes detectados por IA.
    - Cobertura efectiva de cámaras y alarmas.
    - Cumplimiento de protocolos de actuación.

- **Cualitativos:**
    - Percepción de seguridad ciudadana.
    - Confianza del personal en el sistema.
    - Evaluación ética y respeto a derechos humanos.

6.7 Resultados esperados

- Reducción progresiva del TTR sujeta a adecuada implementación y monitoreo continuo.
- Incremento en precisión y utilidad de alertas mediante analítica avanzada.
- Mejor alineación operativa con la estrategia municipal de seguridad.
- Mayor transparencia y confianza institucional y ciudadana.
- Establecimiento de un modelo escalable y replicable en otros municipios de Costa Rica o en contextos internacionales similares.
- Fortalecimiento de la gestión basada en evidencia, promoviendo la modernización tecnológica y la sostenibilidad institucional.

6.8 Vinculación con el marco teórico

- **Hot Spots Policing:** focalización de recursos en zonas de mayor incidencia delictiva.
- **Intelligence-Led Policing:** decisiones estratégicas basadas en análisis predictivo y alertas de IA.
- **Evidence-Based Policing:** uso de datos operativos para ajustar protocolos y medir resultados.
- **Prevención situacional:** anticipación de incidentes mediante tecnología, procesos y participación ciudadana.

La propuesta consolida un enfoque **socio-técnico, ético y estratégico**, asegurando que la tecnología sea un instrumento preventivo y responsable, contribuyendo a la modernización integral del Centro de Monitoreo de San José.

Bibliografía

Angrosino, M. (2007). *Doing ethnographic and observational research*. SAGE Publications.

Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory, 18*(4), 543–571.

Babbie, E. (2016). *The practice of social research* (14th ed.). Cengage Learning.

Bazeley, P., & Jackson, K. (2013). *Qualitative data analysis with NVivo* (2nd ed.). SAGE Publications.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.

Clarke, R. V. (1995). Situational crime prevention. *Crime and Justice, 19*, 91–150.

Clarke, R. V. (1997). *Situational crime prevention: Successful case studies* (2nd ed.). Harrow and Heston.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

Gill, M., Spriggs, A., Allen, J., Jessiman, P., Kara, D., Kilworth, J., Little, R., & Swain, D. (2005). *Assessing the impact of CCTV*. Home Office.

Goldstein, H. (1979). Improving policing: A problem-oriented approach. *Crime & Delinquency, 25*(2), 236–258.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. del P. (2018). *Metodología de la investigación* (6.ª ed.). McGraw-Hill Education.

Hernández Valle, R. (2015). *Derechos fundamentales y nuevas tecnologías*. Editorial Jurídica Continental.

Instituto Nacional de Estadística y Censos (INEC) (2021). *Censo poblacional de Costa Rica*.

Jiménez Corrales, R. (2018). *Protección de datos personales y videovigilancia en Costa Rica*. Editorial Investigaciones Jurídicas.

Kelling, G. L., & Wilson, J. Q. (1982). Broken windows: The police and neighborhood safety. *The Atlantic Monthly, 249*(3), 29–38.

Kotter, J. P. (1996). *Leading change*. Harvard Business School Press.

Koper, C. S. (1995). Just enough police presence: Reducing crime and disorderly behavior by optimizing patrol time in crime hot spots. *Justice Quarterly, 12*(4), 649–672.

Kvale, S., & Brinkmann, S. (2009). *InterViews: Learning the craft of qualitative research interviewing* (2nd ed.). SAGE Publications.

Lewin, K. (1947). Frontiers in group dynamics. *Human Relations, 1*(1), 5–41.

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology, 22*(140), 1–55.

Lum, C., Koper, C. S., & Telep, C. W. (2012). The evidence-based policing matrix. *Journal of Experimental Criminology, 7*(1), 3–26.

Observatorio de la Violencia, Ministerio de Justicia y Paz (2022). *Informe anual de criminalidad*.

Organismo de Investigación Judicial (OIJ) (2023). *Estadísticas nacionales de homicidios*.

Patton, M. Q. (2015). *Qualitative research & evaluation methods* (4th ed.). SAGE Publications.

Ratcliffe, J. H. (2008). *Intelligence-led policing*. Willan Publishing.

Ratcliffe, J. H. (2016). *Intelligence-led policing* (2nd ed.). Routledge.

Sherman, L. W., & Weisburd, D. (1995). General deterrent effects of police patrol in crime hot spots: A randomized, controlled trial. *Justice Quarterly, 12*(4), 625–648.

United Nations Office on Drugs and Crime. (2019). *Handbook on crime prevention guidelines: Making them work*. United Nations.

Banco Interamericano de Desarrollo. (2018). *Seguridad ciudadana y justicia: Guía para la formulación de políticas públicas*.

Costa Rica. (2011). *Ley N.º 8968: Protección de la persona frente al tratamiento de sus datos personales*. Diario Oficial La Gaceta.

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.

Apéndice A. *Encuesta Centro de Monitoreo de San José*

Encuesta Centro de Monitoreo de San José

Objetivo: Recopilar información técnica, operativa y estratégica para diagnosticar el estado actual del Centro de Monitoreo y sustentar una propuesta de modelo de gestión con alertas tempranas basadas en inteligencia artificial, orientada a la prevención del delito y la toma de decisiones institucionales.

Instrucciones:

- Lea cuidadosamente cada pregunta antes de responder.
- Para preguntas cerradas, marque con una “X” la opción que mejor refleje su respuesta.
- Para preguntas abiertas, escriba su respuesta de forma clara y concisa.
- Sus respuestas serán **confidenciales y anónimas**.

I. Datos sociodemográficos y profesionales

1. Cargo que desempeña.

   ( ) Jefatura ( ) Supervisor ( ) Operador ( ) Técnico ( ) Policía

2. Años de experiencia en el Centro de Monitoreo:
   ( ) Menos de 3 años ( ) 3–5 años ( ) 6–10 años ( ) Más de 10 años

3. Área bajo su responsabilidad directa:
   ( ) Operaciones ( ) Tecnología ( ) Análisis de información

II. Evaluación de infraestructura, procesos y gestión

4. ¿Cómo califica el nivel de infraestructura tecnológica del Centro de Monitoreo?
   ( ) Muy deficiente ( ) Deficiente ( ) Regular ( ) Buena ( ) Robusta

5. El sistema actual permite análisis automatizados de eventos (patrones sospechosos, alertas)?
   ( ) Nada ( ) Poco ( ) Parcialmente ( ) Bastante ( ) Totalmente

6. Desde su criterio, el Centro de Monitoreo opera principalmente bajo un enfoque:
   ( ) Totalmente reactivo ( ) Reactivo ( )Mixto ( ) preventivo ( )Totalmente preventivo

7. ¿Qué tan utilizada considera la información generada por las cámaras en la toma de decisiones?
   ( )Nada ( ) Poco ( ) Moderadamente ( ) Mucho ( ) Totalmente

8. Indique las principales limitaciones actuales para un análisis más avanzado de la información (marque todas las que apliquen):
   ( ) Falta de herramientas tecnológicas
   ( ) Falta de personal especializado
   ( ) Falta de integración de datos
   ( ) Limitaciones presupuestarias
   ( ) Falta de lineamientos estratégicos
   ( ) Otras: _____

III. Viabilidad y aportes de la inteligencia artificial

9. ¿Considera viable la incorporación de herramientas de inteligencia artificial en el Centro de Monitoreo?
   ( ) Nada viable ( ) Poco viable ( )Parcialmente viable ( ) Viable ( ) Totalmente viable

10. **En cuáles áreas considera que la IA aportaría mayor valor? (marque todas las que correspondan)**
    ( ) Detección temprana de incidentes
    ( ) Identificación de patrones delictivos
    ( ) Priorización de recursos policiales
    ( ) Reducción de carga operativa humana
    ( ) Apoyo a la toma de decisiones estratégicas

11. Desde su rol, ¿qué tipo de alertas tempranas serían más estratégicas para la prevención del delito?

    _____

    _____

    _____

12. El uso de IA y alertas tempranas estaría alineado con los objetivos estratégicos de la Municipalidad?
    ( ) Nada alineado ( ) Poco alineado ( ) Parcialmente alineado ( ) Mayormente alineado ( ) Totalmente alineado

13. Considera que la estructura del Centro de Monitoreo permite implementar un modelo de gestión basado en IA?
( ) Nada ( ) Parcialmente con ajustes normativos ( ) Parcialmente con ajustes de personal y horarios ( ) Sí, con mínimos ajustes ( ) Sí, totalmente

14. ¿Qué cambios considera indispensables para una implementación exitosa?

_____
_____
_____

15. Qué modalidad de implementación considera más viable?
( ) Proyecto piloto ( ) Implementación gradual ( ) Implementación total inmediata

16. Qué indicadores considera clave para evaluar el impacto del uso de IA en el Centro de Monitoreo?

_____
_____
_____

Apéndice B. *Encuesta dirigida a ciudadanos del Cantón*

Encuesta dirigida a ciudadanos del Cantón Central de San José.

Objetivo del instrumento: Recopilar información sobre la percepción ciudadana en relación con la seguridad, la cobertura tecnológica municipal y la aceptación de sistemas de inteligencia artificial para la prevención del delito.

Instrucciones:
Lea cuidadosamente cada afirmación y marque la opción que mejor refleje su opinión. La información es anónima y será utilizada únicamente con fines académicos.

Datos generales

1. Edad:

   ( ) Menos de 18 años

   ( ) 18–30 años

   ( ) 31–45 años

   ( ) 46–60 años

   ( ) Más de 60 años

2. Sexo:

   ( ) Femenino ( ) Masculino ( ) Prefiero no decirlo

3. Distrito de residencia: _____

4. Ocupación:

( ) Estudiante ( ) Empleado/a ( ) Comerciante ( ) Otro

5. ¿Se siente seguro en su barrio?

( ) Totalmente en desacuerdo ( ) En desacuerdo ( ) Neutral ( ) De acuerdo ( ) Totalmente de acuerdo

6. ¿Cree que la presencia de cámaras de vigilancia ha mejorado la seguridad en su comunidad?

( ) Totalmente en desacuerdo ( ) En desacuerdo ( ) Neutral ( ) De acuerdo ( ) Totalmente de acuerdo

7. ¿Confía en la capacidad del Centro de Monitoreo de San José para responder a incidentes?

( ) Totalmente en desacuerdo ( ) En desacuerdo ( ) Neutral ( ) De acuerdo ( ) Totalmente de acuerdo

8. ¿Cree que la tecnología de vigilancia contribuye a prevenir delitos

( ) Totalmente en desacuerdo ( ) En desacuerdo ( ) Neutral ( ) De acuerdo ( ) Totalmente de acuerdo

9. ¿Considera que la cobertura actual de cámaras y sistemas tecnológicos en el cantón es adecuada?.

( ) Totalmente en desacuerdo ( ) En desacuerdo ( ) Neutral ( ) De acuerdo ( ) Totalmente de acuerdo

10. ¿Considera que es importante implementar sistemas de inteligencia artificial para generar alertas tempranas en el cantón?

( ) Totalmente en desacuerdo ( ) En desacuerdo ( ) Neutral ( ) De acuerdo ( ) Totalmente de acuerdo

11. ¿Cree que la implementación de inteligencia artificial podría mejorar la prevención del delito?

( ) Totalmente en desacuerdo ( ) En desacuerdo ( ) Neutral ( ) De acuerdo ( ) Totalmente de acuerdo

12. En su opinión, ¿Cree que el uso de inteligencia artificial en seguridad debe aplicarse con controles éticos y supervisión humana?

( ) Totalmente en desacuerdo ( ) En desacuerdo ( ) Neutral ( ) De acuerdo ( ) Totalmente de acuerdo

13. ¿Conoce la existencia de cámaras de vigilancia u otras herramientas tecnológicas municipales en su distrito?

( ) Sí ( ) No

14. ¿Ha utilizado alguna herramienta tecnológica municipal para reportar incidentes?

( ) Sí ( ) No

15. En el último año. ¿Ha sido víctima de algún delito en el cantón?

16. ( ) Sí ( ) No

Si respondió “Sí”, indique el tipo de delito (opcional):_____

_____

17. ¿Qué aspectos cree se podrían mejorar para fortalecer la seguridad en el cantón?

_____

_____

_____

18. ¿Qué sugerencias propone para mejorar la cobertura tecnológica y el funcionamiento del Centro de Monitoreo?

_____

_____

_____