Universidad Andrés Bello

Caso de estudio — Seguridad en Smart Cities

Tecnologías Disruptivas (**NRC:** 8090)

Profesor a cargo: Álvaro Sánchez Colmenares

Integrantes

Gabriel Cuevas
g.cuevasortzar@uandresbello.edu

Alfredo Fuentes
a.fuentesnavarrete@uandresbello.edu

Felipe Ochoa
f.ochoajohn@uandresbello.edu

Alonso Rodrigo Urra Villagra
a.urravillagra@uandresbello.edu

Antonia Valdebenito
a.valdebenitofuentes@uandresbello.edu

4 de septiembre de 2025

Contexto del caso — Seguridad

La ciudad ficticia *Nueva Aurora* enfrenta un rápido crecimiento poblacional y se encuentra en un proceso de transformación hacia una *Smart City*. En el eje de seguridad ciudadana, el desafío principal se manifiesta en el aumento de robos y en la baja integración de cámaras y sensores a nivel urbano, situación que limita la prevención, la reacción oportuna y la trazabilidad de incidentes.

Ante este contexto, la ciudad evalúa la adopción de tecnologías propias de las ciudades inteligentes —entre ellas, Internet de las Cosas (IoT), Inteligencia Artificial (IA), Big Data, *blockchain*, 5G y soluciones energéticas asociadas— como base para articular un ecosistema de seguridad más proactivo, interoperable y basado en datos. Estas capacidades tecnológicas se consideran habilitadoras para la detección temprana de eventos, la coordinación táctica y la rendición de cuentas, con énfasis en el uso de IA en cámaras urbanas y el despliegue de sensores distribuidos.

1. Definición del problema y alcance

Problemas prioritarios

P1. Robos en espacio público y comercio de alta afluencia. La ciudad evidencia un aumento sostenido de delitos contra la propiedad en zonas céntricas y nodos de transporte, afectando a peatones y locales comerciales.

P2. Baja integración operativa de cámaras y sensores urbanos. La infraestructura de videovigilancia y sensorización existe de forma fragmentada, sin interoperabilidad suficiente para detección temprana, trazabilidad ni coordinación de respuesta.

Causas principales

- *Fragmentación tecnológica*: parques de cámaras heterogéneos, protocolos manuales y ausencia de estándares de intercambio de datos.
- *Ceguera situacional*: escasa analítica de video en tiempo real y cobertura desigual de sensores (iluminación, aforos, botonería de alerta).
- *Procesos reactivos*: tiempos de verificación largos por falta de correlación automática de eventos y evidencias.
- *Limitaciones de infraestructura urbana*: iluminación deficiente y mobiliario que dificulta líneas de visión en puntos críticos.

Consecuencias

- *Impacto ciudadano*: aumento de victimización y disminución de la percepción de seguridad.

- *Ineficiencias operativas*: respuesta tardía y uso subóptimo de recursos de patrullaje y atención de emergencias.
- *Baja trazabilidad*: dificultades para esclarecer hechos por falta de evidencia unificada y cadena de custodia digital.

Alcance del proyecto (fase piloto)

Área geográfica: distrito céntrico de alta concurrencia (aprox. 3–4 km^2), que incluye eje comercial, dos estaciones de transporte masivo y tres intersecciones críticas.
Horizonte temporal: 12 meses (3 meses diseño/instalación, 6 meses operación y ajuste, 3 meses evaluación).
Cobertura funcional: integración de videovigilancia y sensores urbanos existentes, analítica de video en tiempo real para detección de eventos de riesgo, y tablero operativo para coordinación interinstitucional.
Procesos incluidos: monitoreo preventivo, verificación de incidentes, despacho coordinado, preservación de evidencia digital y reportabilidad.

Fuera de alcance

- Reformas normativas o penales; reestructuración orgánica de fuerzas de orden.
- Vigilancia intrusiva en recintos privados o sin habilitación legal.
- Sustitución total de infraestructura existente fuera del polígono piloto.

Objetivos medibles (12 meses)

- Reducir en $\geq 15\,\%$ los delitos contra la propiedad en el polígono piloto, respecto de la línea base.
- Disminuir en $\geq 30\,\%$ el tiempo promedio de verificación y despacho ante eventos detectados.
- Alcanzar $\geq 95\,\%$ de disponibilidad de la plataforma integrada (cámaras, sensores, analítica y tablero).
- Lograr que $\geq 60\,\%$ de los incidentes relevantes sean *detectados automáticamente* por analítica de video/sensores.

Restricciones y supuestos

- *Legales y de privacidad*: tratamiento de datos personales sujeto a principios de finalidad, minimización y seguridad; difusión acotada de imágenes.

- *Técnicas*: heterogeneidad de dispositivos; conectividad variable; necesidad de estándares abiertos (ONVIF, APIs seguras).
- *Operativas*: coordinación interinstitucional y continuidad operativa 24/7 con personal capacitado.

Actores involucrados

- Municipio (gestión urbana y seguridad), centros de monitoreo y emergencia.
- Fuerzas de orden y equipos de respuesta (coordinación táctica y despacho).
- Comunidad y comercio local (canales de reporte y prevención situacional).
- Proveedores tecnológicos e integradores (infraestructura, software y soporte).

Riesgos y salvaguardas éticas

- *Riesgos*: sesgos algorítmicos, vigilancia excesiva, ataques a la infraestructura, uso indebido de datos.
- *Salvaguardas*: evaluación de impacto en privacidad, anonimización cuando corresponda, controles de acceso y auditoría, cifrado extremo a extremo, políticas de retención y uso proporcional de la información.

2. Mapa de problemas (Causa - Consecuencias)

Problema 1: Robos en vía pública

Robos en vía pública en zonas de alta influencia y nodos de transporte, con afectación directa a peatones y comercios. Vease la figura 1

Figura 1: Diagrama de Ishikawa del problema *Robos en vía pública*.

Causas inmediatas

- *Fragmentación tecnológica*: Cámaras y sensores heterogéneos, con baja interoperabilidad y flujos manuales.
- *Ceguera situacional*: Analítica de video limitada para detección temprana de eventos y cobertura desigual de sensorización.
- *Procesos reactivos*: Verificación lenta por falta de correlación automática de alertas y evidencias.
- *Infraestructura urbana subóptima*: Iluminación deficiente, mobiliario y arbolado que generan puntos ciegos.

Causa subyacentes

- *Estándares y gobierno de datos insuficientes*: ausencia de APIs y protocolos abiertos para intercambio seguro.

- *Capacidades operativas dispares*: roles, turnos y procedimientos no unificados entre vigilancia, monitoreo y despacho.
- *Conectividad irregular*: tramos sin fibra/5G y respaldo eléctrico limitado que afectan la disponibilidad de equipos.
- *Mantenimiento correctivo predominante*: fallas recurrentes y tiempos de reparación prolongados.

Consecuencias

- *Impacto ciudadano*: Mayor victimización y disminución de la percepción de seguridad.
- *Ineficiencias operativas*: Respuesta tardía y uso subóptimo de recursos de patrullaje y emergencia.
- *Baja trazabilidad*: Dificultad para esclarecer hechos por carencia de evidencia integrada y cadena de custodia digital.
- *Costos socioeconómicos*: Pérdidas para el comercio local y reducción de actividad en zonas críticas.

Relación causa–efecto (síntesis)

Cuadro 1: Vinculación de causas con efectos del problema "Robos en vía pública".

Categoría de causa	**Evidencia/manifestación típica**	**Efecto principal**
Tecnología	Heterogeneidad de cámaras/sensores; sin correlación automática	Verificación lenta; baja detección temprana
Métodos	Patrullaje no dirigido por datos; rutas subóptimas	Cobertura reactiva; menor disuasión
Mano de obra	Roles/protocolos no unificados; capacitación desigual	Coordinación limitada en incidentes
Materiales	Iluminación insuficiente; señalética disuasiva escasa	Puntos ciegos y mayor oportunidad delictiva
Medio ambiente	Arbolado/mobiliario obstruyen; flujos peatonales desbalanceados	Zonas de riesgo persistentes
Mediciones	Falta de KPIs operativos; alto nivel de falsas alarmas	Mejora continua limitada

Indicadores asociados (línea base y metas)

- **Tasa de delitos contra la propiedad** (por 10 000 hab.) en el polígono piloto: reducción relativa de $\geq 15\,\%$ a 12 meses respecto de la línea base.

- **Tiempo medio de verificación y despacho (TTR)** desde la alerta hasta el envío de recurso: disminución de $\geq 30\,\%$.
- **Disponibilidad de la plataforma integrada** (cámaras, sensores, analítica y tablero): $\geq 95\,\%$.
- **Detección automática de incidentes relevantes** (analítica de video/sensores): $\geq 60\,\%$ del total de incidentes registrados.
- **Tasa de falsas alarmas** (proporción sobre alertas totales): reducción a $\leq 10\,\%$ mediante calibración y verificación.

Supuestos críticos

- Disponibilidad de conectividad (fibra/5G) y respaldo energético en puntos críticos.
- Acceso legal y seguro a datos para fines de prevención, reacción y trazabilidad, con políticas de minimización y retención.
- Coordinación interinstitucional efectiva para operación 24/7 y mantenimiento preventivo.

Problema 2: Baja integración operativa de cámaras y sensores

La infraestructura de videovigilancia y sensorización urbana opera de forma fragmentada, con dispositivos heterogéneos y flujos de datos dispares. La ausencia de interoperabilidad y estandarización limita la detección temprana, la trazabilidad de incidentes y la coordinación de la respuesta.

Causas inmediatas

- *Fragmentación tecnológica*: dispositivos de distintos fabricantes sin adopción consistente de estándares abiertos (p. ej., ONVIF, APIs REST).
- *Falta de integración*: inexistencia de un bus/middleware que unifique ingestión, normalización y distribución de eventos.
- *Conectividad y energía irregulares*: enlaces sin redundancia y sin telemetría de salud en tiempo real.
- *Procesos manuales*: verificación y correlación dependientes del operador, con alta variabilidad.

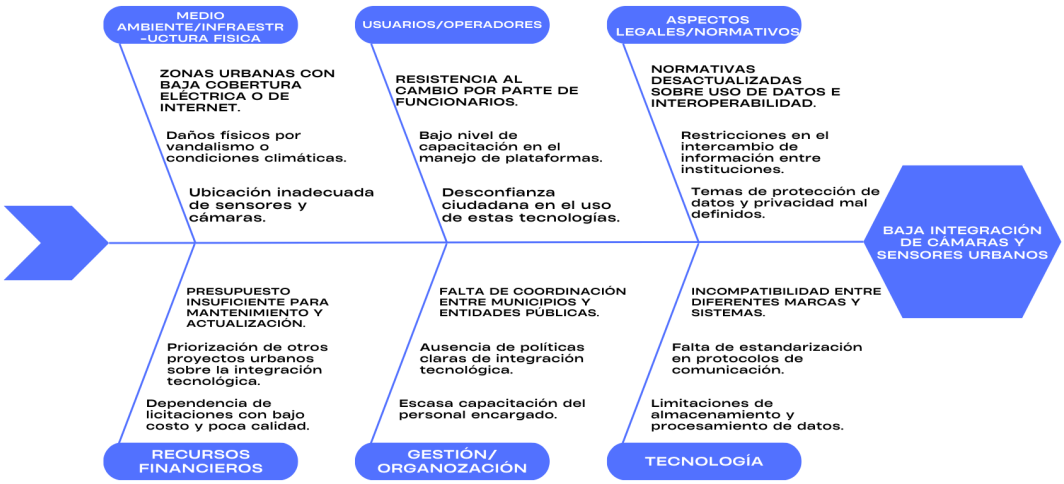

Figura 2: Diagrama de Ishikawa — Problema 2: Baja integración operativa de cámaras y sensores.

Causas subyacentes

- *Gobierno de datos insuficiente*: políticas débiles de calidad, seguridad, retención y auditoría.
- *Contratación por silos*: adquisiciones sin requisitos de interoperabilidad ni pruebas cruzadas.
- *Observabilidad limitada*: carencia de métricas, logs y trazas end-to-end.
- *Mantenimiento correctivo predominante*: inventario y versionamiento desactualizados.

Consecuencias

- *Latencia operacional*: tiempos altos de detección y verificación con pérdida de ventanas de intervención.
- *Baja trazabilidad*: dificultades probatorias por registros inconexos y cadena de custodia débil.
- *Uso subóptimo de recursos*: despacho tardío y fatiga de operadores por falsas alarmas.

Cuadro 2: Vinculación de causas con efectos del problema “Baja integración operativa”.

Categoría de causa	**Evidencia/manifestación típica**	**Efecto principal**
Tecnología	Sistemas heterogéneos, sin perfiles ONVIF ni APIs alineadas	Imposibilidad de correlación; mayor latencia
Métodos	Verificación manual y scripts ad-hoc	Variabilidad operativa; tiempos de respuesta altos
Mano de obra	Capacitación dispar; dependencia del operador	Mayor tasa de error y falsas alarmas
Materiales	Falta de respaldo eléctrico y racks adecuados	Caídas de servicio; pérdida de datos
Medio ambiente	Interferencias/saturación en tramos inalámbricos	Pérdida de paquetes; jitter en video/eventos
Mediciones	Sin KPIs ni telemetría de salud	Mejora continua limitada; fallas no detectadas

Relación causa–efecto (síntesis)

Indicadores asociados (línea base y metas)

- **Cobertura integrada** (% de cámaras/sensores gestionados desde la plataforma): meta $\geq 85\,\%$.
- **Latencia de ingestión y correlación**: tiempo desde evento a alerta unificada; meta ≤ 5 s en críticos.
- **Incidentes con correlación automática**: proporción con video, georreferencia y recurso vinculado; meta $\geq 70\,\%$.
- **Disponibilidad del servicio de integración**: meta $\geq 99.5\,\%$ mensual.
- **Tasa de falsas alarmas**: meta $\leq 10\,\%$.

Supuestos críticos

- Disponibilidad de enlaces confiables (fibra/5G) y respaldo energético en sitios críticos.
- Acceso legal a flujos de datos para prevención, reacción y trazabilidad, con principios de minimización y seguridad.
- Inventario técnico actualizado (modelos, firmware, topología) y adopción de estándares de interoperabilidad.
- Coordinación operativa 24/7 y mantenimiento preventivo programado.

3. Ciudad referente

1. Ciudad estudiada

Barcelona, España. Ciudad europea pionera en infraestructura digital urbana, gobierno de datos y despliegues de sensorización y videovigilancia con analítica.

2. Tecnología concreta aplicada

Plataforma urbana basada en estándares abiertos (p. ej., *Sentilo* para IoT) que integra:

- Red de *CCTV* con cámaras IP y perfiles ONVIF, enlazada a centros de control operativos.
- Sensores urbanos (iluminación telegestionada, aforo, acústica, calidad de aire, botonería de alerta).
- Analítica de video en tiempo real (detección de intrusión/merodeo, objetos abandonados, lectura de placas).
- Tableros operativos y geoespaciales para correlación evento–ubicación–recurso y despacho coordinado.
- Conectividad sobre fibra y redes móviles, con telemetría de salud para garantizar disponibilidad.

3. Resultados medibles reportados

- *Operación*: incremento sostenido de disponibilidad de cámaras y reducción de tiempos de reparación al consolidar inventario y mantenimiento preventivo.
- *Respuesta*: disminución de tiempos de verificación y despacho en zonas priorizadas gracias a la correlación automática (video + posición + recurso).
- *Eficiencia energética*: ahorros significativos en alumbrado público por LED y telegestión (del orden de decenas de puntos porcentuales en áreas intervenidas).
- *Investigación*: mayor proporción de incidentes con evidencia audiovisual útil y cadena de custodia digital.

4. Desafíos o riesgos observados

- Interoperabilidad y dependencia de proveedores: necesidad de exigir APIs abiertas y pruebas cruzadas.
- Continuidad operativa: vandalismo, energía y tramos con conectividad no redundada.

- Privacidad y ética: tratamiento proporcional de datos personales y mitigación de sesgos algorítmicos.
- Sostenibilidad: costos de mantenimiento/actualización y formación continua de operadores.

Adaptación al caso *Nueva Aurora* (contexto latinoamericano)

- **Polígono piloto y línea base**: seleccionar zonas críticas y medir tasas de delitos, TTR y falsas alarmas previas a la intervención.
- **Interoperabilidad desde la compra**: requerir perfiles ONVIF, *Sentilo*/APIs abiertas y pruebas de integración en licitaciones.
- **Middleware y tablero**: priorizar un bus de eventos y un tablero único con correlación video–evento–recurso.
- **Conectividad y energía**: fibra/5G con QoS y respaldo eléctrico en puntos críticos; telemetría de salud 24/7.
- **Gobierno de datos**: políticas de minimización, retención, auditoría y evaluación de impacto en privacidad.
- **Participación ciudadana**: botones de alerta, campañas de uso responsable y mecanismos de transparencia.

4. Plan de implementación (pasos priorizados)

Cuadro 3: Fases y entregables para materializar la propuesta.

Fase	Periodo	Pasos priorizados	Entregables clave
0	Mes 1	Línea base (delitos, TTR, falsas alarmas); inventario técnico; polígono piloto; requisitos y pruebas de interoperabilidad en compras.	Informe de línea base; pliego técnico; cronograma detallado.
1	Meses 2–4	Gateway y bus de eventos; integración de $\geq$2 fabricantes por categoría; tablero mínimo viable; telemetría de salud; capacitación inicial.	Plataforma MVP operativa; manuales iniciales; tablero v1.
2	Meses 5–8	Analítica de video en tiempo real; motor de correlación; calibración para reducir falsas alarmas; procedimientos 24/7 y cadena de custodia.	Modelos calibrados; SOPs 24/7; auditoría de evidencias.
3	Meses 9–12	Escalamiento y hardening; redundancia de conectividad/energía; formación avanzada; evaluación contra KPIs; plan de expansión.	Informe de resultados; plan de mejora y escalamiento.

5. Cuadro de gestión de recursos

Cuadro 4: Recursos requeridos para el piloto y su gestión.

Categoría	Descripción	Cantidad/Alcance	Responsable/Métrica
Materiales	Postes, gabinetes, UPS/energía, racks, cableado y protecciones.	Según polígono (puntos críticos)	Uptime energético; tiempo medio de reparación.
Equipos	Cámaras IP 4K-IR, sensores (botón, conteo, acústicos), switches PoE, gateways, servidores/almacenamiento.	$\sim$X cámaras, Y sensores, Z gateways	Disponibilidad por dispositivo; tasa de fallas/mes.
Tecnología	Bus de eventos, APIs, tablero unificado, analítica de video, observabilidad, IAM y seguridad.	Licencias/servicios + despliegue	Latencia $\leq$ 5 s; metadatos completos $\geq 95\,\%$.
Personas	Jefatura de proyecto, arquitecto/integrador, ciberseguridad, analista/IA, operadores 24/7, mantenimiento, jurídico/datos.	Roles y turnos definidos	SLA de atención; cumplimiento SOP; auditorías OK.

6. Impacto del proyecto en la ciudadanía

Beneficios esperados

- **Seguridad y confianza**: detección y despacho más rápidos; mayor trazabilidad probatoria.
- **Calidad de vida**: reducción de falsas alarmas y patrullajes innecesarios; percepción de seguridad al alza.
- **Eficiencia pública**: mejor uso de recursos operativos; continuidad del comercio en zonas críticas.
- **Sostenibilidad**: menor huella por optimizar desplazamientos y telegestión de iluminación.

Indicadores de impacto (12 meses)

- **TTR verificación/ despacho**: reducción $\geq 30\,\%$ en el polígono piloto.
- **Delitos contra la propiedad**: reducción relativa $\geq 15\,\%$ vs. línea base.
- **Tasa de falsas alarmas**: $\leq 10\,\%$ del total de alertas.
- **Percepción ciudadana**: mejora ≥ 10 p.p. en encuestas locales.
- **Disponibilidad de plataforma**: $\geq 95\,\%$ (operativa integral).