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

7 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. Véase 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.

## Causas 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**: 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 e impactos (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 $\leq 5$ 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 $\leq 10\,\%$.


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

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 |

### 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.** Pionera en arquitectura digital urbana, plataforma IoT *Sentilo* y despliegues de sensorización, alumbrado y videovigilancia.

## 2. Tecnología concreta aplicada

Plataforma urbana basada en estándares abiertos (*Sentilo*) 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, riego).
- Analítica en tiempo real y tableros geoespaciales para correlación evento–ubicación–recurso.
- Conectividad sobre fibra y redes móviles; telemetría de salud para garantizar disponibilidad.

(*Base tecnológica:* [5, 4])

## 3. Resultados medibles reportados (benchmark)

- **Ahorro energético en alumbrado público:** $\sim 30\,\%$ de reducción del consumo gracias a LED + telegestión en el sistema urbano de iluminación [1].
- **Gestión del agua:** reportes de ahorro del orden de ∼US$58 millones por iniciativas IoT (p. ej., riego inteligente, medición y control) [1].
- **Ingresos de estacionamiento:** incremento aproximado de ∼US$50 millones/año atribuible a soluciones de *smart parking* y gestión IoT [1].

- **Magnitud del sistema de alumbrado y consumo:** >146 000 puntos de luz; $\sim$ 82,000 MWh/año ($\approx$ 20 % del consumo energético municipal), lo que contextualiza el potencial de ahorro por telegestión [2].
- **Evolución reciente:** plan de renovación para aumentar LED del 35 % al 50 % y avanzar hacia **gestión remota 100 %** del alumbrado [3].

## 4. Desafíos o riesgos observados

- Interoperabilidad y dependencia de proveedores: exigir APIs abiertas y pruebas cruzadas ([5]).
- 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*

- **Línea base y KPIs:** medición inicial de delitos, TTR, falsas alarmas y disponibilidad, para contrastar reducciones/ahorros esperados siguiendo el enfoque de Barcelona.
- **Interoperabilidad desde la compra:** perfiles ONVIF, *Sentilo*/APIs abiertas y pruebas de integración en licitaciones [5].
- **Telegestión de iluminación:** adopción de LED + control punto a punto para perseguir ahorros cercanos a los observados ($\sim$ 30 %) [1, 2].
- **Riego inteligente y agua:** sensorización y control remoto de riego para replicar ahorros operacionales en agua [4].

# 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 $\geq 10$ p.p. en encuestas locales.
- **Disponibilidad de plataforma**: $\geq 95\,\%$ (operativa integral).

# 7. Implementación del eje Seguridad

## 7.1. Alcance y criterios de ubicación

El despliegue se concentra en el polígono céntrico de Nueva Aurora, priorizando el **eje comercial**, las **estaciones Norte/Sur** y los **accesos viales**. La ubicación de cada dispositivo responde a: (i) afluencia peatonal/vehicular y reportes de incidentes, (ii) visibilidad y cobertura sin puntos ciegos, (iii) disponibilidad eléctrica y de postes/soportes, (iv) factibilidad de *backhaul* (fibra/5G). La explicación siguiente referencia el mapa limpio (ver Fig. 3).

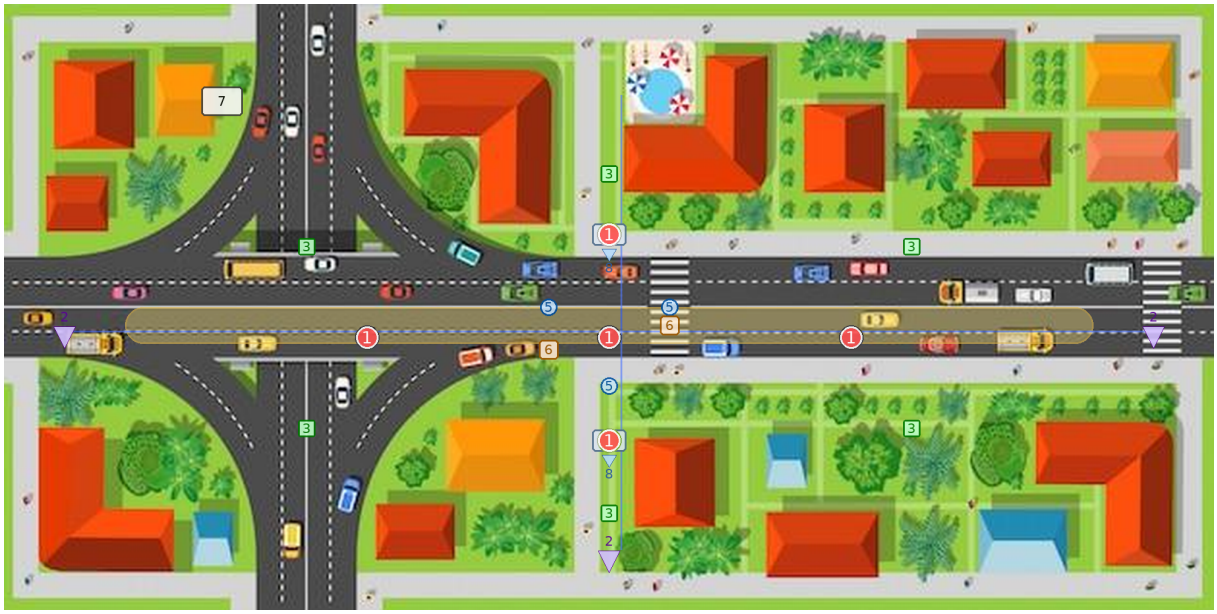

Figura 3: Mapa con puntos de control aplicados a las soluciones propuestas.

## 7.2. Despliegue por componente (según marcadores del mapa)

1. **CCTV + IA (cruces y estaciones).** En los cruces A, B y C y en ambas estaciones se instalan cámaras fijas (cobertura de calzada y banquetas) y, donde aplique, una PTZ para seguimiento. Alimentación *PoE* desde gabinetes cercanos; el **gateway/edge (6)** aplica analítica (merodeo, objetos abandonados, cruce en contrasentido) y envía eventos al COC (7). Se calibra zona/máscaras y se define repositorio/retención.

2. **LPR/ANPR (accesos).** Cámaras de lectura de patentes en accesos oriente/poniente y salida sur, con iluminación IR y ángulo controlado. Generan metadatos (placa, fecha/hora, sentido) que se cruzan con alertas y listas de interés en el COC.

3. **Botones de alerta SOS (paraderos/plazas).** Tótems con botón, cámara integrada, altavoz y baliza. Conexión *PoE* o 5G; al activarse abren incidente en la consola del COC con **geolocalización** y previsualización de video.

4. **Iluminación LED telegestionada (eje comercial).** Reemplazo/adecuación de luminarias por LED con control punto a punto (nodo NEMA/Zhaga y CMS). Escenas nocturnas con *dimming* adaptativo (mayor nivel en cruces/paraderos), telemetría de fallas y base para sensores futuros.

5. **Sensores acústicos (anomalías).** Malla de 2–3 nodos que triangulan eventos de **disparos/roturas** en el corredor. Disparan ticket automático con **verificación cruzada** en cámaras cercanas para reducir falsas alarmas.

6. **Gateways/Edge (IoT/Video).** Gabinetes con *switch* PoE, equipo industrial (CPU/GPU ligera) y **UPS**. Funciones: agregación de cámaras/sensores, *buffering* local, analítica en borde y publicación de eventos (MQTT/REST) hacia la plataforma central.

7. **COC – Centro de Operaciones.** Sala con *video wall*, VMS/analítica, CAD para despacho, gestión de evidencias (cadena de custodia), y panel de KPIs. Roles: operador 24/7, supervisor y analista. Protocolos de atención, escalamiento y privacidad.

8. **Backhaul Fibra + 5G.** Tramo principal sobre el eje y vertical de refuerzo; arquitectura en **anillo** con *switches* L2/L3 y VLAN de seguridad. 5G en estaciones como redundancia de subida; microondas donde la fibra no esté disponible.

## 7.3. Arquitectura y flujo de datos

Dispositivo (1–5) → **Edge (6)** (normalización/analítica/*buffer*) → **Backhaul (8)** → **Plataforma** (VMS/EMS/CMS) → **COC (7)** → Despacho (policía/seguridad municipal). Se registran *logs* y evidencias con control de acceso y auditoría.

## 7.4. Operación, privacidad y mantenimiento

- **Operación:** monitoreo 24/7, verificación en $\leq 2$ min, despacho coordinado, auditoría semanal de alarmas.
- **Privacidad:** señalética visible, enmascaramiento de zonas privadas, retención definida (p. ej., 15–30 días), control de accesos y registro de consultas.
- **Mantenimiento:** preventivo trimestral (limpieza ópticas, *firmware*, recalibración analítica), correctivo con SLA, stock crítico de repuestos.

## 7.5. Indicadores de éxito (KPI)

*Uptime* de plataforma y dispositivos; tiempo de detección, verificación y despacho; reducción de incidentes en zona priorizada; % de falsas alarmas; incidentes resueltos con evidencia útil; ahorro energético por telegestión.

# Glosario de Términos y Siglas

**APIs REST** Interfaces HTTP siguiendo principios REST.

**CCTV + IA** Videovigilancia con analítica inteligente.

**COC** Centro de Operaciones de Control.

**Gateways / Edge** Agregan y procesan datos localmente.

**IAM** Gestión de identidades y accesos.

**KPIs** Indicadores clave de rendimiento.

**LPR / ANPR** Reconocimiento automático de matrículas.

**ONVIF** Estándar de interoperabilidad en videovigilancia IP.

**QoS** Calidad de servicio de red.

**SLA** Acuerdo de nivel de servicio.

**TTR** Tiempo de resolución (o de verificación/ despacho, según se use).

**UPS** Sistema de alimentación ininterrumpida.

# Referencias

# Referencias

[1] Adler, L. (2016, 18 de febrero). *How Smart City Barcelona Brought the Internet of Things to Life*. Data-Smart City Solutions, Harvard Kennedy School. Disponible en: https://datasmart.hks.harvard.edu/news/article/how-smart-city-barcelona-brought-the-internet-of-things-to-life-789

[2] Ajuntament de Barcelona (s. f.). *Street lighting management*. Área de Urbanismo, Transición Ecológica, Servicios Urbanos y Vivienda. Disponible en: https://ajuntament.barcelona.cat/ecologiaurbana/en/services/the-city-works/maintenance-of-public-areas/energy-management/street-lighting-management

[3] Ajuntament de Barcelona (2024, 14 de julio). *More work to renew and improve lighting in the city*. Disponible en: https://www.barcelona.cat/infobarcelona/en/tema/urban-planning-and-infrastructures/more-work-to-renew-and-improve-lighting-in-the-city_1419476.html

[4] Cisco (2015). *IoE-Driven Smart City Barcelona Initiative Cuts Water Bills, Increases Parking Revenues, and Creates Jobs*. Perfil de jurisdicción. Disponible en: https://www.cisco.com/c/dam/m/en_us/ioe/public_sector/pdfs/jurisdictions/Barcelona_Jurisdiction_Profile_final.pdf

[5] Bain, M. (2014). *Sentilo Case Study*. Interoperable Europe. Disponible en: https://interoperable-europe.ec.europa.eu/sites/default/files/document/2014-06/SENTILO%20case_joinup_v_1%202.pdf