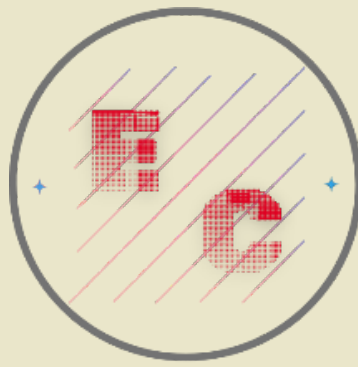




REVISTA MULTIDISCIPLINAR EPISTEMOLOGÍA DE LAS CIENCIAS

Volumen 3, Número 3
Julio-Septiembre 2026

Edición Trimestral

CROSSREF PREFIX DOI: 10.71112

ISSN: 3061-7812, www.omniscens.com

Revista Multidisciplinar Epistemología de las Ciencias

Volumen 3, Número 3
julio-septiembre 2026

Publicación trimestral
Hecho en México

La Revista Multidisciplinar Epistemología de las Ciencias acepta publicaciones de cualquier área del conocimiento, promoviendo una plataforma inclusiva para la discusión y análisis de los fundamentos epistemológicos en diversas disciplinas. La revista invita a investigadores y profesionales de campos como las ciencias naturales, sociales, humanísticas, tecnológicas y de la salud, entre otros, a contribuir con artículos originales, revisiones, estudios de caso y ensayos teóricos. Con su enfoque multidisciplinario, busca fomentar el diálogo y la reflexión sobre las metodologías, teorías y prácticas que sustentan el avance del conocimiento científico en todas las áreas.

Contacto principal: admin@omniscens.com

Las opiniones expresadas por los autores no necesariamente reflejan la postura del editor de la publicación

Se autoriza la reproducción total o parcial del contenido de la publicación sin previa autorización de la Revista Multidisciplinar Epistemología de las Ciencias siempre y cuando se cite la fuente completa y su dirección electrónica.

Esta obra está bajo una licencia internacional Creative Commons Atribución 4.0.



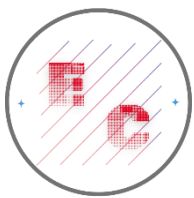
Copyright © 2026: Los autores



9773061781003

Cintillo legal

Revista Multidisciplinar Epistemología de las Ciencias Vol. 3, Núm. 3, julio-septiembre 2026, es una publicación trimestral editada por el Dr. Moises Ake Uc, C. 51 #221 x 16B , Las Brisas, Mérida, Yucatán, México, C.P. 97144 , Tel. 9993556027, Web: <https://www.omniscens.com>, admin@omniscens.com, Editor responsable: Dr. Moises Ake Uc. Reserva de Derechos al Uso Exclusivo No. 04-2024-121717181700-102, ISSN: 3061-7812, ambos otorgados por el Instituto Nacional del Derecho de Autor (INDAUTOR). Responsable de la última actualización de este número, Dr. Moises Ake Uc, fecha de última modificación, 1 julio 2026.



Revista Multidisciplinar Epistemología de las Ciencias

Volumen 3, Número 3, 2026, julio-septiembre

DOI: <https://doi.org/10.71112/wzmcp70>

**VIDEOVIGILANCIA Y USO DEL ESPACIO PÚBLICO: TENSIONES ENTRE
SEGURIDAD CIUDADANA Y PROTECCIÓN DE DATOS EN ECUADOR**

**VIDEO SURVEILLANCE AND PUBLIC SPACE: TENSIONS BETWEEN PUBLIC
SAFETY AND DATA PROTECTION IN ECUADOR**

Cabrera Jarrín Sebastián Ramiro

Marco Guamán Buestan

Farfán Figueroa Wilson Jonnathan

Ecuador

Videovigilancia y uso del espacio público: tensiones entre seguridad ciudadana y protección de datos en Ecuador

Video surveillance and public Space: tensions between public safety and data protection in Ecuador

Cabrera Jarrín Sebastián Ramiro^{a,*}

srcabrera@sudamericano.edu.ec

<https://orcid.org/0009-0009-3393-2908>

Marco Guamán Buestan^a

maguaman2@sudamericano.edu.ec

<https://orcid.org/0000-0001-9544-2220>

Farfán Figueroa Wilson Jonnathan^a

wjfarfan@sudamericano.edu.ec

<https://orcid.org/0009-0001-4534-5139>

*Autor de correspondencia: srcabrera@sudamericano.edu.ec, ^aInstituto Tecnológico Superior Sudamericano Cuenca, Ecuador

RESUMEN

En Ecuador, la colocación a gran escala de cámaras en las vías públicas ha abierto un dilema que aún no tiene una solución institucional definida: de qué manera salvaguardar la seguridad de la población sin menoscabar derechos como la privacidad, la intimidad y la salvaguarda de los datos personales. El presente estudio aborda este conflicto basándose en la legislación ecuatoriana vigente, la cual abarca la Constitución de 2008 y la Ley Orgánica de Protección de Datos Personales de 2021. Con base en esta revisión, se elabora una Guía Modelo Técnico Operativa, estructurada en siete apartados. La guía se implementa como estudio de caso en el sector Unión Las Caleras, situado en la parroquia San Sebastián del cantón Cuenca. Para

valorar la propuesta, se solicitó la opinión de nueve expertos, cuyas apreciaciones fueron medidas a través del Coeficiente V de Aiken. El resultado obtenido fue catalogado como aceptable, lo que valida tanto la factibilidad técnica como la adecuación legal del documento.

Palabras clave: CCTV; espacio público; LOPDP; protección de datos personales; seguridad ciudadana; V de Aiken; videovigilancia.

ABSTRACT

In Ecuador, the large-scale placement of cameras on public roads has opened a dilemma that still lacks a defined institutional solution: how to safeguard the safety of the population without undermining rights such as privacy, intimacy, and the protection of personal data. This study addresses that conflict based on current Ecuadorian legislation, which encompasses the 2008 Constitution and the 2021 Organic Law on Personal Data Protection. Building on this review, a Technical-Operational Model Guide is developed, structured in seven sections. The guide is implemented as a case study in the Unión Las Caleras neighborhood, located in the San Sebastián parish of the Cuenca canton. To assess the proposal, the opinion of nine experts was sought, and their appraisals were measured using Aiken's V Coefficient. The result obtained was classified as acceptable, validating both the technical feasibility and the legal adequacy of the document.

Keywords: Aiken's V; CCTV; LOPDP; personal data protection; public safety; public space; video surveillance.

Recibido: 23 julio 2026 | Aceptado: 6 agosto 2026 | Publicado: 7 agosto 2026

INTRODUCCIÓN

En las últimas décadas, la política pública de seguridad ha priorizado la implementación de sistemas de videovigilancia como una estrategia central de prevención situacional del delito y control del orden urbano. Este enfoque se ha dado mediante la instalación de dispositivos en espacios de concurrencia peatonal. De manera complementaria, existe un incremento en la iniciativa privada, donde los propietarios de viviendas instalan sistemas de vigilancia doméstica que, donde a más de la protección residencial, se amplía el monitoreo hacia zonas públicas como las veredas.

La expansión de los sistemas de videovigilancia en el Ecuador ha sido impulsada por el Servicio Integrado de Seguridad ECU-911, que opera con aproximadamente 6.500 cámaras distribuidas a escala nacional. (ECU-911, 2022). Esta implementación en espacios públicos ha sido señalada como una fuente de vulneraciones a derechos fundamentales reconocidos constitucionalmente. Fundamedios (2022), documentó afectaciones a la privacidad y la libre circulación de personas derivadas del funcionamiento del ECU-911. Cruz Sánchez (2017) advierte que el uso de cámaras sin un marco normativo específico contraviene el artículo 66, numeral 20 de la Constitución del Ecuador, que garantiza el derecho a la intimidad personal y familiar.

Existen posturas teóricas que analizan los derechos fundamentales en su aplicación al espacio público. Dentro de estas, resalta la teoría de la expectativa razonable de privacidad, la cual sostiene que el simple hecho de transitar por un sitio de acceso público no significa una renuncia automática al derecho a la privacidad (Warren y Brandeis, 1890; Katz vs. EE. UU., 1967). A raíz de esto, surgió el principio de proporcionalidad, concebido por el Tribunal Europeo de Derechos Humanos, que funciona como un instrumento jurídico fundamental para valorar la legalidad de cada sistema de vigilancia, considerando sus tres facetas: idoneidad, necesidad y proporcionalidad estricta (García-Morales, 2020).

La falta de un marco legal específico sobre videovigilancia en áreas públicas se presenta como una de las falencias del sistema jurídico ecuatoriano. De la Serna Bilbao (2016) señala que los sistemas de videovigilancia deben contar, como mínimo, con límites constitucionales, criterios de proporcionalidad y mecanismos de control. En el ámbito nacional, la resolución emitida por la Superintendencia de Protección de Datos Personales supone un paso adelante en la definición de requisitos esenciales; no obstante, estas directrices todavía no conforman una normativa completa que cubra los sistemas de videovigilancia en funcionamiento en el país (NMS Law, 2026).

Johnston y Shearing (2003) analizaron la gobernanza de la seguridad, enfocándose en cómo los Estados organizan y delegan la provisión de seguridad mediante redes de actores públicos, privados y tecnológicos. Esta perspectiva tiene implicaciones en la rendición de cuentas de sistemas como el ECU-911, donde la forma en que se articulan el Estado, las empresas tecnológicas y las comunidades define el alcance real de la vigilancia y su impacto en los derechos de los ciudadanos. No obstante, esta gobernanza todavía está pendiente en el contexto ecuatoriano. Morena-Álvarez y Vila-Seoane (2023) indican que la instalación del ECU-911 se llevó a cabo bajo una cooperación tecnológica con actores chinos, lo cual suscita interrogantes sobre la soberanía de los datos, la dependencia tecnológica y la falta de supervisión en el uso de las imágenes captadas en el espacio público.

En cuanto a la adecuación tecnológica, Morena-Álvarez y Vila-Seoane (2023) sugieren que, en lugar de importar modelos extranjeros sin ajustarlos, los Estados deberían adoptar las tecnologías de acuerdo con sus necesidades institucionales y, fundamentalmente, que respondan a lógicas de soberanía nacional. Pontón y Rivera (2016) afirman que toda política de seguridad fundamentada en la videovigilancia debe ir de la mano con reformas institucionales que refuercen la capacidad del Estado para operar, supervisar y evaluar los sistemas implementados.

Se percibe una conexión entre el aspecto sociotécnico de la incorporación de la tecnología y la visión crítica de la videovigilancia como una herramienta de control social (Bijker, 1995). Desde esta óptica, las cámaras de vigilancia no son artefactos neutrales: influyen en el espacio público, limitan la entrada de distintos colectivos sociales y reflejan intereses políticos y económicos que van más allá de su simple utilidad para la seguridad, un punto clave para examinar la situación ecuatoriana (Foucault, 1975; Lefebvre, 1974).

En América Latina, la eficacia de la videovigilancia como método para mejorar la seguridad ciudadana ha sido puesta en duda. El vínculo entre la colocación de cámaras en lugares públicos y una disminución real de la delincuencia es tenue, sobre todo cuando los sistemas operan sin estar integrados a procedimientos de respuesta policial (FLACSO Ecuador, 2016). Coincidiendo con esto, Jasso López (2020) evidencia, tras comparar los planes nacionales de seguridad de once naciones latinoamericanas, que el uso de la videovigilancia se ha extendido sin que los Estados hayan establecido, paralelamente, directrices de planificación, valoración y regulación que aseguren su funcionamiento y su armonía con los derechos de los ciudadanos.

Arteaga Botello (2016) sugiere enfoques de planificación completa y comités de supervisión conjuntos que aseguren la claridad, la responsabilidad y la imparcialidad en el acceso al espacio público bajo vigilancia; únicamente de esta forma la videovigilancia en Ecuador podrá erigirse como un instrumento válido, eficiente y respetuoso de los derechos esenciales de la población.

Más allá de su propósito oficial como instrumento de seguridad, la videovigilancia en espacios públicos ha sido estudiada como un sistema de control social capaz de acentuar las disparidades ya existentes y condicionar el acceso desigual al entorno urbano. Galdon-Clavell (2015) argumenta que la expansión de cámaras en las ciudades latinoamericanas

responde más a presiones políticas y tendencias de mercado que a necesidades genuinas de seguridad ciudadana.

En cuanto a la efectividad operativa, Welsh y Farrington (2009) y Piza et al. (2019) muestran que el Circuito Cerrado de Televisión (CCTV, por sus siglas en inglés), tiene efectos preventivos importantes cuando el monitoreo se realiza de manera activa y se coordina con una respuesta policial. Socha y Kogut (2020) confirman que los sistemas inteligentes que emplean análisis automatizado aumentan considerablemente la capacidad preventiva del CCTV.

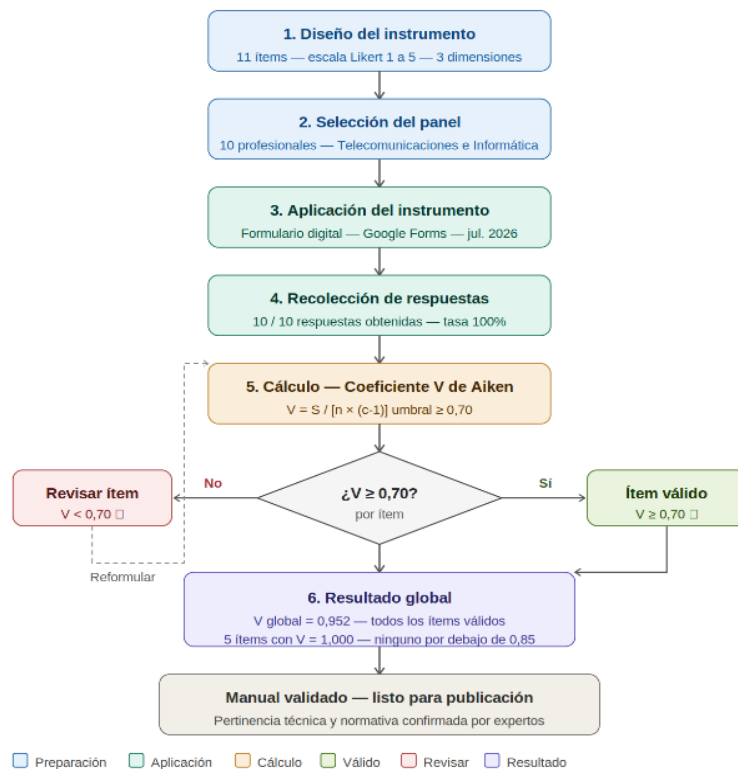
El estudio actual se justifica debido a la apremiante necesidad normativa, social y técnica que surge de la expansión descontrolada de los sistemas de videovigilancia en los espacios públicos del Ecuador. El país gestiona el ECU-911, que cuenta con más de 6.500 cámaras a nivel nacional, una de las redes más extensas de América Latina, sin que exista un marco legal que rijan el manejo de las imágenes capturadas y salvaguarde los derechos fundamentales de los ciudadanos bajo observación. Esto ha desembocado en violaciones al derecho a la privacidad, la intimidad y la libre circulación (Fundamedios, 2022).

Desde una perspectiva social, el derecho a la privacidad y a la intimidad concierne a todos los ciudadanos ecuatorianos que transitan, trabajan o viven en áreas públicas bajo vigilancia constante. Una normativa apropiada salvaguarda los derechos individuales, la libertad de expresión, la libertad de movimiento y el derecho de asociación. En el ámbito técnico, la ausencia de estándares para la infraestructura, la coordinación operativa y la gestión institucional merma la efectividad real de los sistemas implementados. La contribución de esta investigación radica en ofrecer una Guía-Modelo Técnico-Operativa que, a su vez, incorpore directrices normativas específicas para subsanar el vacío regulatorio. Se empleará el barrio Unión Las Caleras de Cuenca como estudio de caso para la implementación.

“El presente artículo tiene como objetivo proponer una Guía Modelo Técnico Operativa con base en un análisis de las tensiones entre la expansión de los sistemas de videovigilancia en espacios públicos ecuatorianos y la protección de los derechos fundamentales de los ciudadanos. Se examina el estado actual de la normativa ecuatoriana aplicable (Constitución 2008, LOPDP 2021, Ley Orgánica de Vigilancia y Seguridad Privada 2025 y pronunciamiento de la SPDP 2026), se contrastan sus alcances y limitaciones con los estándares regulatorios de otros países. Se aplicó al barrio Unión Las Caleras, parroquia San Sebastián, cantón Cuenca, como caso de implementación.”

METODOLOGÍA

La presente investigación tiene un enfoque cuantitativo de alcance descriptivo-propositivo, orientado a obtener evidencia sobre la validez de la propuesta técnica mediante la recolección y el análisis sistemático de datos medibles (Hernández-Sampieri et al., 2014). Se trata de una investigación aplicada que parte de conocimientos teóricos para diseñar una solución concreta ante la ausencia de un manual técnico-operativo que oriente la implementación de sistemas CCTV en espacios públicos ecuatorianos con cumplimiento normativo simultáneo.

Figura 1*Flujograma del proceso de validación por juicio de expertos*

Nota. El proceso comprende seis etapas secuenciales, desde el diseño del instrumento hasta el resultado global, con un umbral mínimo de validez de 0,70 para el Coeficiente V de Aiken.

El panel de validación contó con la participación de nueve profesionales con una trayectoria que alcanza hasta los 22 años de experiencia en áreas de ingeniería y telecomunicaciones. Esta experiencia asegura que la evaluación de los 11 ítems del manual tenga el respaldo técnico para su aplicación en el contexto ecuatoriano. En la tabla 1 se detalla la profesión y la experiencia de cada experto. Aunque uno de los expertos omitió registrar sus años exactos de experiencia, se validó su participación con base en su título profesional en Ingeniería.

Tabla 1.*Título profesional y los años de experiencia de los evaluadores*

Nº	Título profesional	Años de exp.
1	Ingeniería en Sistemas Informáticos	22
2	Ingeniería en Electrónica y Telecomunicaciones	3
3	Electrónica y Telecomunicaciones	3
4	Ingeniería en Electrónica y Telecomunicaciones	2
5	Ingeniería en Electrónica y Telecomunicaciones	3
6	Ingeniería en Electrónica y Telecomunicaciones	No disponible
7	Licenciada en Educación Básica	4
8	Ingeniería Electrónica y Telecomunicaciones	3
9	Técnico	5

Nota. El panel estuvo conformado por nueve profesionales con experiencia de entre 2 y 22 años. El evaluador N° 6 no registró sus años de experiencia; su participación fue validada con base en su título profesional.

Se evaluaron once ítems agrupados en tres dimensiones:

- Diseño Técnico e Infraestructura (D1),
- Cumplimiento de la LOPDP (D2)
- Protocolos Operativos y Evaluación (D3)
- La encuesta tuvo una escala de Likert de 5 puntos donde 1 = Totalmente en desacuerdo; 5 = Totalmente de acuerdo.

Protocolo Técnico Operativo Estandarizado

Se presenta esta guía modelo como un protocolo técnico-operativo pensado para la administración de videovigilancia en entornos urbanos, la cual amalgama de forma multidimensional la infraestructura tecnológica con la observancia de la Ley Orgánica de Protección de Datos Personales (LOPDP). Este instrumento propositivo se organiza a través

de una secuencia lógica de seis módulos que aseguran la trazabilidad técnica y legal del sistema.

Módulo 1. Datos técnicos del sector de implementación.

Contiene la ficha técnica del área geográfica que será objeto de intervención: coordenadas, el perímetro a cubrir, el trazado de vías principales y secundarias, y la infraestructura de servicios que se puede aprovechar para el despliegue, tales como postes de alumbrado, ductos de telecomunicaciones y puntos de acceso a fibra óptica. Este levantamiento inicial es indispensable porque deja identificar, antes de tomar cualquier decisión de diseño, las limitaciones físicas reales del terreno y los recursos con los que ya cuenta el sector. Sin esta información preliminar, las decisiones técnicas de los módulos subsiguientes carecerían del respaldo territorial necesario para asegurar una implementación factible y ajustada a las condiciones específicas del entorno urbano.

Módulo 2. Planificación y diseño de red.

Comienza con el diagnóstico del espacio público para detectar los puntos críticos de inseguridad, los flujos de peatones y vehículos, y las condiciones físicas del sector. Con esa información se dimensiona el sistema y se escogen los tipos de cámaras IP atendiendo a la resolución y al campo visual que cada ubicación demanda. La elección de cada equipo responde directamente a lo observado en el terreno, evitando sobredimensionar la instalación en zonas de bajo riesgo o dejar desprotegidos los puntos donde la incidencia delictiva así lo amerita. De esta forma, el módulo transforma las necesidades reales de seguridad del sector en decisiones técnicas precisas y económicamente viables.

Módulo 3. Infraestructura de transmisión.

Se describe la arquitectura de la red troncal de fibra óptica que enlaza las cámaras con el centro de control, los protocolos de comunicación implementados y los criterios para asegurar la compatibilidad entre distintos fabricantes. Asimismo, se exponen las medidas de

seguridad destinadas a salvaguardar la integridad y la privacidad de las imágenes mientras viajan por la red. Cada una de estas determinaciones concuerda con lo estipulado en el artículo 37 de la LOPDP, el cual demanda garantías técnicas comprobables para la protección de los datos personales que fluyen a través del sistema. Sin estas disposiciones, cualquier intervención o modificación del flujo de video pondría en riesgo no solo el funcionamiento del sistema sino también los derechos de los individuos que son registrados por las cámaras.

Módulo 4. Centro de monitoreo y NVR.

Establece los detalles técnicos del servidor donde se grabarán las imágenes, la política de conservación de acuerdo con los plazos legales vigentes y los métodos de control de acceso por perfiles que limitan quién puede ver, descargar o borrar el material. Incorpora los registros de auditoría que dejan constancia de cada operación realizada en el sistema para poder rastrearla. Este grado de control es indispensable porque el material guardado incluye datos personales delicados y su gestión incorrecta podría acarrear responsabilidades legales para quien opera el sistema. Al determinar exactamente quién accede, en qué circunstancias y por qué motivo, el módulo cubre la distancia entre las capacidades técnicas del servidor y los deberes que exige la normativa de protección de datos.

Módulo 5. Integración con el sistema de seguridad privada del barrio.

Trata la estructura para conectarse con la central de monitoreo de la empresa de seguridad contratada por la comunidad y el protocolo de avisos, especificando plazos, responsabilidades y vías de comunicación en caso de sucesos sospechosos. Su objetivo es coordinar las capacidades tecnológicas del sistema con la respuesta operativa en la zona. Un sistema de cámaras que detecta un incidente, pero no consigue poner en marcha una respuesta a tiempo, ve reducido considerablemente su valor como medida preventiva, por este motivo el módulo fija plazos concretos

y personas claramente identificadas en cada fase del protocolo. De este modo se pretende que la videovigilancia no sea solo un registro pasivo, sino que actúe como un elemento activo dentro de la cadena de seguridad del vecindario.

Módulo 6. Señalización, documentación y transparencia.

Define la norma de señalización en áreas bajo vigilancia para salvaguardar el derecho a la información de la gente, además de la documentación técnica requerida que sustenta la operación: planos de alcance, fichas de equipos y bitácoras de mantenimiento. Pretende garantizar que la población sepa de la existencia, el alcance y el propósito del sistema. Este punto no es un formalismo vacío, dado que la propia Superintendencia de Protección de Datos Personales ha dictaminado que la falta de señalización representa una violación directa al derecho a la información del ciudadano. Por esta razón, el módulo especifica tanto el contenido esencial que debe tener cada aviso como la periodicidad de su colocación, para que nadie acceda a un área vigilada sin haber sido correctamente notificado.

Módulo 7. Evaluación y métricas de desempeño.

Reúne los índices técnicos de operación, tales como la disponibilidad de cámaras y los tiempos de reacción, con los índices de repercusión en la seguridad pública medidos a partir de la variación de delitos en el área. Un ciclo de auditoría semestral y anual permite evaluar el cumplimiento de objetivos y aplicar los ajustes operativos que demande la mejora continua. Sin este seguimiento periódico, resultaría imposible determinar si el sistema está cumpliendo realmente con su función preventiva o si se ha convertido en una infraestructura instalada pero ineficaz. La combinación de datos técnicos extraídos del propio sistema con la percepción de los residentes del barrio ofrece una visión integral que permite tomar decisiones basadas en evidencia y no en suposiciones sobre el funcionamiento del sistema.

RESULTADOS

Los resultados obtenidos del juicio de expertos se tabularon para determinar el nivel de acuerdo respecto a las especificaciones técnicas y legales del sistema propuesto. La Tabla 2 muestra las medias aritméticas obtenidas en las tres dimensiones de análisis, proporcionando una visión cuantitativa de la aceptación del diseño en base a los requerimientos de videovigilancia y protección de datos en el contexto ecuatoriano.

Tabla 2.

Resultados de la validación por juicio de expertos.

Dim.	Ítem evaluado	$\bar{X}$
D1	Suficiencia del ancho de banda (48 Mbps)	4.11
D1	Idoneidad de la topología (fibra OS2)	4.11
D1	Pertinencia de la categorización de cámaras (A1/A2)	4.11
D1	Viabilidad de almacenamiento (HDD 4 TB, H.265)	3.67
D1	Media de la dimensión	4.00
D2	Eficacia del cifrado (TLS 1.3 / VPN IPsec)	3.89
D2	Garantía de confidencialidad (RBAC)	4.00
D2	Cumplimiento del plazo de conservación (Art. 20 LOPDP)	3.78
D2	Transparencia en la señalización (Art. 13 LOPDP)	3.89
D2	Media de la dimensión	3.89
D3	Viabilidad del protocolo de respuesta (10 min)	3.56
D3	Suficiencia de las métricas de desempeño	3.78
D3	Prohibición de reconocimiento facial y biometría	4.11
D3	Media de la dimensión	3.82
—	Media general del instrumento (11 ítems)	3.91

Nota. D1 = Diseño técnico; D2 = Cumplimiento normativo LOPDP; D3 = Protocolos operativos. Escala Likert 1–5, n = 9 evaluadores.

Tabla 3.*Diagnóstico de validez por ítem representativo*

Dimensión	Ítem	Media (X')	Coeficiente V	Diagnóstico
D1: Técnica	Ancho de banda (48 Mbps)	4.11	0.78	Válido
	Viabilidad de almacenamiento	3.67	0.67	Revisar
D2: LOPDP	Garantía de confidencialidad	4.00	0.75	Válido
D3: Operat.	Protocolo de respuesta	3.56	0.64	Revisar
	Prohibición de biometría	4.11	0.78	Válido

Nota. Umbral mínimo de validez: $V \geq 0,70$ (Aiken, 1985). Los ítems clasificados como "Revisar" requieren reformulación o ajuste técnico.

El análisis de validez de contenido mediante el Coeficiente V de Aiken muestra una media general de 0.73, lo que indica una validez aceptable para el manual. Los ítems con mayor nivel de acuerdo ($V=0.78$) fueron la suficiencia del ancho de banda de 48 Mbps, la idoneidad de la fibra óptica y la prohibición expresa de biometría, demostrando una sólida alineación técnica y ética de la propuesta.

El ítem de Almacenamiento ($V=0.67$) Explica que, aunque el manual propone un HDD de 4 TB basado en el cálculo de 48 Mbps para cumplir el Art. 20 de la LOPDP, los expertos sugieren que este margen podría ser muy ajustado si se aumenta la calidad de grabación en el futuro. De igual forma el ítem de Protocolo de Respuesta ($V=0.64$): Menciona que la cantidad de minutos establecidos en el manual para llegar al sitio del incidente es percibida por los expertos como difícil de cumplir dada la logística policial actual.

Caso de estudio

Se presenta la aplicación del manual técnico-operativo en el Barrio Unión Las Caleras.

Módulo 1 — Datos técnicos del sector de implementación.

El diagnóstico de seguridad del sector, detallado en la Tabla 4, describe los tipos de delitos ocurridos en el sector. La Figura 2 identifica geográficamente las zonas donde se concentran estos eventos, información que sirvió como base para determinar los puntos prioritarios de instalación de las cámaras. Esta lectura cruzada entre los datos estadísticos y su localización en el territorio permitió que las decisiones de cobertura respondieran a la realidad del barrio y no a supuestos generales sobre inseguridad urbana.

Figura 2

Puntos de incidencia y ubicación geográfica del barrio Unión Las Caleras



Nota. Los marcadores numerados (1–4) indican la ubicación propuesta para cada cámara IP en los puntos estratégicos del sector. Fuente: Sistema catastral, Municipio de Cuenca (2024).

Tabla 4.*Distribución porcentual de actos delictivos por tipo y zona de mayor incidencia*

Tipo de delito	Frecuencia estimada	% del total	Zona de mayor incidencia
Robo a personas	Alta	~45%	Av. del Tejar (tramo peatonal)
Robo a domicilios	Media	~28%	Zonas residenciales Av. del Sarar
Robo de vehículos	Media-baja	~18%	Intersección Av. del Tejar / Av. del Sarar
Vandalismo en espacio público	Baja	~9%	Parque barrial y espacios comunitarios
TOTAL	—	100%	Todo el barrio Unión Las Caleras

Nota. Datos estimados con base en registros de la Policía Nacional del Ecuador para la parroquia San Sebastián. Elaboración propia.

Módulo 2 — Planificación y diseño de red.

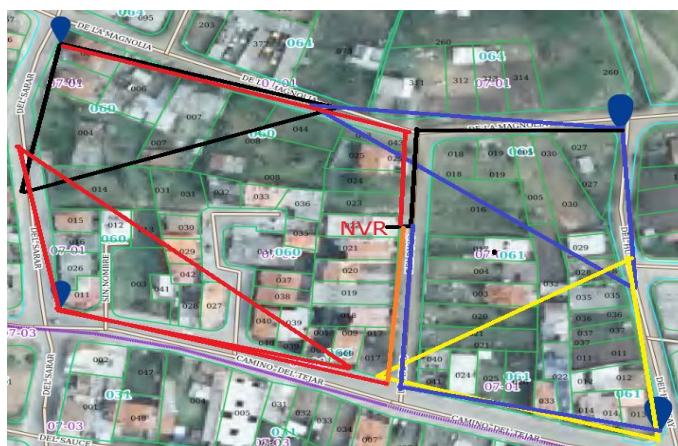
"El sistema distribuye cuatro cámaras IP en los puntos estratégicos del sector según el nivel de riesgo identificado en cada zona. En la Tabla 5 se detallan las especificaciones técnicas de cada dispositivo. El conjunto opera con un ancho de banda de diseño de 48 Mbps sobre una topología estrella extendida con fibra óptica monomodo OS2, y la distribución geoespacial del tendido junto con la ubicación de cada cámara sobre el plano catastral del sector se ilustra en la Figura 3."

Tabla 5.*Distribución de Cámaras*

Cámara	Ubicación	Resolución	Framerate FPS	Distancia NVR	Cobertura / Ángulo	Categoría
Cámara 1	Acceso norte — Calle De la Magnolia	1080p Full HD	25	200 m (D1)	110° / 80 m	A1
Cámara 2	Intersección Av. del Tejar / C. del Sarar	4K (3840×2160)	30	210 m (D2)	360° / 100 m radio	A1
Cámara 3	Esquina sur — Av. del Tejar / Av. del Huaspay	1080p Full HD	25	190 m (D3)	90° / 60 m	A2
Cámara 4	Extremo nororiental — De la Magnolia / Av. del Huaspay	1080p Full HD	25	150 m (D4)	110° / 80 m	A2
TOTAL	4 puntos estratégicos del sector	—	—	750 m total	—	4 cámaras IP

Nota: A1 = Intel Core i7/i9 (alta criticidad). A2 = AMD equivalente (zonas secundarias).

Ambas categorías son compatibles con protocolo ONVIF y TLS 1.3. Distancias D1–D4 medidas desde el NVR central.

Figura 3*Distribución geoespacial del tendido de fibra óptica y ubicación de cámaras*

Nota. Los puntos azules indican la ubicación de las cámaras y las líneas de colores representan los enlaces de fibra óptica desde el NVR central. Tendido total: 750 m. Fuente: Sistema catastral, Municipio de Cuenca (2024).

Módulo 3 — Infraestructura de transmisión

El sistema se sustenta en un backbone de fibra óptica de 750 metros totales, distribuido en cuatro enlaces independientes cuyas distancias desde el NVR central hasta cada cámara se especifican en la Tabla 6. Para dar cumplimiento al artículo 37 de la LOPDP, toda la transmisión se protege con cifrado TLS 1.3 y SRTP, túneles VPN IPsec hacia la central privada y certificados digitales renovados anualmente. La integridad de las grabaciones se verifica mediante firmas hash SHA-256, mientras que la segmentación por VLANs y un firewall perimetral con actualizaciones semestrales completan el esquema de defensa de la red.

Tabla 6

Distancias de enlace de fibra óptica desde el NVR central hasta cada cámara

Distancia a las Cámaras	
Cámaras	Distancia en metros
Cámara 1	200 m(D1)
Cámara 2	210 m (D2)
Cámara 3	190 m (D3)
Cámara 4	150 m(D4)

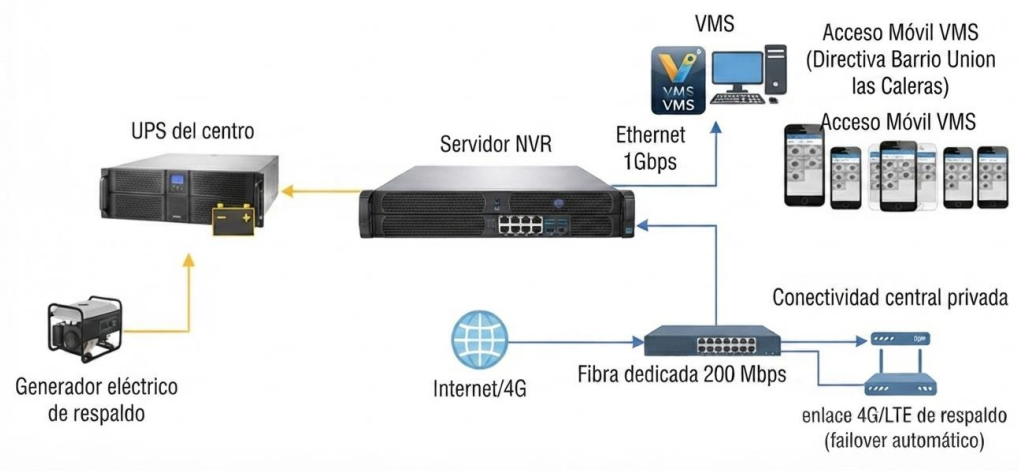
Nota. Distancias medidas desde el NVR central hasta cada punto de instalación, siguiendo el trazado de las calles del sector.

Módulo 4 — Centro de monitoreo y NVR.

El núcleo del sistema lo constituye un servidor NVR equipado con procesador Xeon de ocho núcleos y 32 GB de memoria RAM ECC, cuya conexión hacia la central privada se establece a través de fibra dedicada de 200 Mbps con respaldo automático 4G/LTE, mientras que la Directiva del sector accede de forma remota mediante la plataforma Video Management System (VMS), tal como se ilustra en la Figura 4. Un disco HDD de 4 TB con compresión H.265

resulta suficiente para cubrir los 30 días de retención que exige el artículo 20 de la LOPDP. En la Tabla 7 se detallan los cinco roles con distintos niveles de autorización que regulan el acceso al material grabado, y cada acción realizada sobre el sistema queda registrada en logs de auditoría inmutables que se conservan por no menos de dos años.

Figura 4
Arquitectura de interconexión del sistema de videovigilancia



Nota. El servidor NVR se conecta a la central privada mediante fibra dedicada de 200 Mbps con failover 4G/LTE, y al acceso móvil VMS para la Directiva del sector.

Tabla 7.
Sistema de control de acceso por roles conforme a los Arts. 11 y 37 de la LOPDP (2021)

Rol	Acceso permitido	Restricciones
Operador de turno / presidente del barrio	Monitoreo en tiempo real	No puede ver grabaciones, exportar ni modificar configuración
Supervisor de seguridad / Brigadas barriales	Monitoreo + grabaciones últimas 72 h	No puede exportar sin autorización escrita del director
Director del centro	Acceso completo + exportación con registro	Toda exportación queda en log de auditoría con justificación obligatoria

Autoridad judicial / fiscal	Grabaciones específicas con orden judicial	Acceso mediante procedimiento formal documentado y orden judicial
Administrador TI	Configuración técnica del sistema	Sin acceso al contenido de grabaciones durante la operación normal

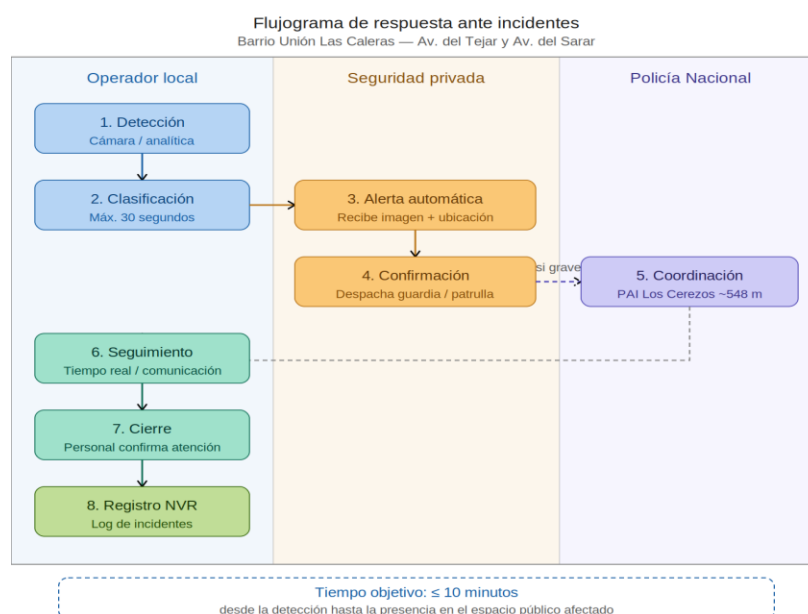
Nota. Toda exportación de material queda registrada en log de auditoría con justificación obligatoria. Elaboración propia con base en los Arts. 11 y 37 de la LOPDP (2021).

Módulo 5 — Integración con el sistema de seguridad privada del barrio.

La conexión entre el NVR y la central de monitoreo privada permite al personal de seguridad únicamente la visualización en tiempo real. Ante un evento sospechoso, el protocolo ilustrado en la Figura 5 activa ocho pasos con el objetivo de lograr presencia en el espacio público en no más de diez minutos. Esta restricción de acceso, combinada con un tiempo de respuesta claramente definido, busca que la empresa de seguridad cumpla un rol operativo sin tener control sobre el material grabado del sistema.

Figura 5

Protocolo de respuesta ante incidentes



Nota. El flujo involucra tres actores (operador local, seguridad privada y Policía Nacional) con un tiempo objetivo ≤ 10 minutos desde la detección hasta la presencia en el espacio público.

Módulo 6 — Señalización, documentación y transparencia.

El artículo 13 de la LOPDP y el pronunciamiento de la SPDP (NMS Law, 2026) exigen que toda persona que transite una zona vigilada sea informada de manera previa y visible. En cumplimiento de este principio, el sistema contempla la instalación de carteles cada 50 metros en los tramos viales del sector, cuyo modelo se presenta en la Figura 6. Cada cartel incluye el ícono de cámara, el nombre del responsable del tratamiento y los datos de contacto para el ejercicio de derechos ARCO, garantizando que ningún ciudadano sea vigilado sin haber recibido la información que la ley le reconoce.

Figura 6

Modelo de señalización de zona videovigilada



Nota. Cada cartel debe incluir ícono de cámara, texto "zona videovigilada", nombre del responsable y datos de contacto para derechos ARCO, conforme al Art. 13 de la LOPDP (2021).

Módulo 7 — Evaluación y métricas de desempeño.

Para verificar que el sistema opere dentro de los parámetros esperados, el VMS registra de forma automática seis indicadores técnicos:

- Disponibilidad de cámaras, con una meta mínima del 99% mensual
- Cobertura activa del total de zonas definidas en el diseñoLatencia de transmisión, que no debe superar los 200 ms.
- Tiempo de respuesta ante fallas críticas (≤ 24 h) y menores (≤ 72 h).
- Tasa de alertas respondidas, igual o superior al 90%.
- Cumplimiento íntegro de la eliminación de grabaciones al día 30,

DISCUSIÓN

“El coeficiente V de Aiken global de 0,952 coloca la propuesta en un nivel de validez de contenido que sobrepasa los umbrales reportados en investigaciones parecidas dentro del contexto latinoamericano, en donde valores superiores a 0,85 ya se entienden como indicativos de alta concordancia entre quienes evalúan (Escobar-Pérez y Cuervo-Martínez, 2008). Es importante destacar que los cinco ítems con valor máximo de 1,000 no se agrupan en una sola dimensión, sino que cubren decisiones de ingeniería como la topología de red y la categorización de cámaras, sumado a requerimientos normativos como la confidencialidad a través de RBAC, la señalización y la prohibición del reconocimiento facial. Esto pone de manifiesto que el manual logra entrelazar la dimensión técnica con la jurídica de forma simultánea, algo que la literatura especializada identifica como uno de los retos más complicados al desplegar sistemas CCTV en lugares públicos (Welsh y Farrington, 2009; García-Morales, 2020).

En cuanto al punto con la calificación más baja, la viabilidad de almacenar datos con discos duros de 4 TB y compresión H.265 arrojó un coeficiente de

0,850, valor que permanece dentro del límite fijado por Aiken (1985). No obstante, las puntuaciones otorgadas por dos de los evaluadores evidencian una preocupación sobre el alcance de expansión del sistema en caso de que el número de cámaras se incrementara. Esta anotación orienta las próximas revisiones del manual hacia una configuración de almacenamiento que contemple la posibilidad de crecimiento desde su diseño original.

Un hallazgo que merece especial atención es que la Dimensión 2, referente a la conformidad con la LOPDP, registró el promedio más elevado de las tres dimensiones estudiadas, con un coeficiente de 0,975. Este resultado adquiere importancia en un escenario donde la legislación específica para videovigilancia en Ecuador todavía se encuentra en fase de elaboración, y se vincula directamente con las infracciones que Fundamedios (2022) documentó en sistemas de videovigilancia operados sin normativas claras establecidas.

CONCLUSIONES

El dictamen de expertos confirma que el manual presenta una propuesta coherente y realizable para el contexto municipal ecuatoriano. El coeficiente V de Aiken general se situó en 0,952, sin que ningún punto descendiera del umbral de validez. Esta cifra respalda su utilidad como herramienta para implementar sistemas de videovigilancia (CCTV) en áreas urbanas con características similares a la estudiada.

El consenso más sólido del panel recayó en las pautas relativas a la protección de los derechos ciudadanos. Específicamente, la restricción del reconocimiento facial, la confidencialidad mediante el control de acceso por perfiles y la transparencia en la señalización obtuvieron las puntuaciones más altas de toda la evaluación. Ello demuestra que el manual no se limita a explicar cómo instalar cámaras funcionales, sino que también ofrece un

método para llevarlo a cabo sin vulnerar los derechos fundamentales de los residentes y transeúntes de las zonas vigiladas.

Desde una perspectiva técnica, la propuesta ilustra que es posible configurar un sistema de videovigilancia adecuado para municipios con presupuestos limitados. Dicho sistema, compuesto por cuatro cámaras IP, un disco duro de 4 TB, fibra óptica empleando la infraestructura existente y una velocidad de conexión de 48 Mbps, cumple con las exigencias sin incurrir en costos elevados. Este aspecto resulta particularmente relevante, ya que permite la posibilidad de replicar el modelo en otras zonas y ayuntamientos del país que atraviesen situaciones económicas similares.

El punto con el coeficiente más bajo ($V = 0,850$) indica una posibilidad de mejora específica para futuras ediciones del manual, en particular, añadir un apartado sobre la capacidad de expansión que prevea el aumento en la cantidad de cámaras, el cambio en los estándares de compresión y el cálculo del almacenamiento para retenciones más largas por mandato judicial. Estos elementos representan una limitación conocida y manejable del diseño actual, no un fallo fundamental de la propuesta.

Declaración de conflicto de interés

El autor declara no tener ningún conflicto de interés relacionado con esta investigación.

Declaración de contribución a la autoría

Sebastián Cabrera: conceptualización, revisión de literatura, diseño de la Guía-Modelo Técnico-Operativa, desarrollo del instrumento de validación, recolección de datos y redacción del borrador inicial.

Jonnathan Farfán: curación de datos, análisis formal de resultados, diseño metodológico, preparación y presentación de la obra publicada, y revisión crítica del manuscrito.

Declaración de uso de inteligencia artificial

Los autores declaran que utilizaron la inteligencia artificial como apoyo para este artículo, y también que esta herramienta no sustituye de ninguna manera la tarea o proceso intelectual. Después de rigurosas revisiones con diferentes herramientas en la que se comprobó que no existe plagio como constan en las evidencias, los autores manifiestan y reconocen que este trabajo fue producto de un trabajo intelectual propio, que no ha sido escrito ni publicado en ninguna plataforma electrónica o de IA.

REFERENCIAS

- Aiken, L. R. (1985). Three coefficients for analyzing the reliability and validity of ratings. *Educational and Psychological Measurement*, 45(1), 131–142.
<https://doi.org/10.1177/0013164485451012>
- Arteaga Botello, N. (2015). Surveillance footage and space segregation in Mexico City. *International Sociology*, 30(6), 619–636. <https://doi.org/10.1177/0268580915605650>
- Arteaga Botello, N. (2016). Regulación de la videovigilancia en México: gestión de la ciudadanía y acceso a la ciudad. *Espiral, Estudios sobre Estado y Sociedad*, 23(66), 193–238. <https://doi.org/10.32870/espiral.v23i66.5301>
- Arteaga Botello, N. (2018). Videovigilancia en América Latina: expansión, cooperación policial y espacios regulatorios difusos. *European Review of Latin American and Caribbean Studies*, (106), 23–44. <https://doi.org/10.32992/erlacs.10380>
- Arteaga Botello, N. (2019). Progresismo y tecnología policial: análisis del boom punitivo en Ecuador. *Perfiles Latinoamericanos*, 31(62), 106–131. <https://doi.org/10.18504/pl3162-005-2023>

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales.

Registro Oficial Suplemento N.º 459 del 26 de mayo de 2021.

<https://www.registroficial.gob.ec>

Bojórquez-Luque, J., Ángeles, M. & Gámez, A. (2020). Videovigilancia y segregación espacial en tiempos del neoliberalismo autoritario: el caso de Los Cabos, Baja California Sur (México). *Revista CS*, (31), 217–242. <https://doi.org/10.18046/recs.i31.3668>

Cruz Sánchez, E. (2017). Videovigilancia, seguridad ciudadana y derechos fundamentales de tercera generación. Tirant lo Blanch.

De la Serna Bilbao, M. N. (2016). Seguridad ciudadana y los sistemas de videovigilancia: límites, garantías y regulación. *Revista de Derecho Político*, (97), 71–118. <https://doi.org/10.5944/rdp.97.2016.17620>

Escobar-Pérez, J. & Cuervo-Martínez, Á. (2008). Validez de contenido y juicio de expertos: una aproximación a su utilización. *Avances en Medición*, 6(1), 27–36. <https://www.researchgate.net/publication/302438451>

FLACSO Ecuador. (2016). Informe de seguridad ciudadana y videovigilancia 2015–2016. Facultad Latinoamericana de Ciencias Sociales, Sede Ecuador. <https://repositorio.flacsoandes.edu.ec>

Fundamedios. (2022). Videovigilancia y libertad de expresión en Ecuador: riesgos para los derechos fundamentales. Fundación Andina para la Observación y Estudio de Medios. <https://www.fundamedios.org.ec>

Galdon-Clavell, G. (2015). Si la videovigilancia es la respuesta, ¿cuál era la pregunta? Cámaras, seguridad y políticas urbanas. *EURE – Revista Latinoamericana de Estudios Urbano Regionales*, 41(123), 81–101. <https://doi.org/10.4067/S0250-71612015000300004>

- García-Morales, M. J. (2020). El derecho a la protección de datos en el ámbito de la videovigilancia: proporcionalidad, minimización y garantías. Aranzadi/Thomson Reuters.
- Gil Membrado, C. (2019). Videovigilancia y protección de datos en el ordenamiento jurídico europeo y español. *Revista de Derecho UNED*, (24), 253–280.
<https://doi.org/10.5944/rduned.24.2019.25435>
- Goñi Sein, J. L. (2021). La videovigilancia laboral y el derecho a la protección de datos. Thomson Reuters Aranzadi.
- Hernández-Sampieri, R., Fernández Collado, C. & Baptista Lucio, P. (2014). Metodología de la investigación (6.ª ed.). McGraw-Hill Education.
- Jasso López, L. C. (2020). Seguridad ciudadana y tecnología: uso, planeación y regulación de la videovigilancia en América Latina. *DIKE, Revista de Investigación en Derecho, Criminología y Consultoría Jurídica*, (27), 5–27.
<https://dialnet.unirioja.es/servlet/articulo?codigo=8133549>
- Lio, V. (2015). Ciudades, cámaras de seguridad y video-vigilancia: estado del arte y perspectivas de investigación. *Astrolabio Nueva Época*, (15), 273–302.
<https://ri.conicet.gov.ar/handle/11336/71428>
- López Rojas, D. (2023). Diseño e implementación de un sistema de videovigilancia IP para el GAD Municipal: estudio de caso [Tesis de pregrado, Universidad del Azuay]. Repositorio Institucional UDA.
- Malamud, A. (2018). ¿Se puede gobernar la vigilancia? Tecnología, democracia y seguridad en América Latina. Nueva Sociedad.
- Ministerio del Interior del Ecuador. (2025). Ley Orgánica de Vigilancia y Seguridad Privada.
<https://www.ministeriodelinterior.gob.ec>
- Morena-Álvarez, J. A. & Vila-Seoane, M. (2023). La videovigilancia algorítmica en la era del Big Data: implicaciones para la privacidad en América Latina. CLACSO.

NMS Law. (12 de enero de 2026). Nuevo pronunciamiento de la SPDP sobre videovigilancia y protección de datos personales en Ecuador.

<https://nmslaw.com.ec/blog/2026/01/12/ecuador-spdp-videovigilancia-proteccion-datos-personales/>

Piza, E. L., Welsh, B. C., Farrington, D. P. & Thomas, A. L. (2019). CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology & Public Policy*, 18(1), 135–159. <https://doi.org/10.1111/1745-9133.12419>

Pontón, D. (2009). Seguridad ciudadana y videovigilancia: vinculación de reducida eficacia. Ciudad Segura, FLACSO Ecuador.

<https://repositorio.flacsoandes.edu.ec/handle/10469/2315>

Pontón, D. & Rivera, F. (2016). Postneoliberalismo y policía: caso de Ecuador 2007–2013. *Desafíos*, 28(2), 289–330. <https://doi.org/10.12804/desafios28.2.2016.06>

Socha, R. & Kogut, B. (2020). Urban video surveillance as a tool to improve security in public spaces. *Sustainability*, 12(15), 6210. <https://doi.org/10.3390/su12156210>

Valverde Rivera, F. J. (2022). Modelo de seguimiento por videovigilancia pública en red para la seguridad ciudadana mediante Dynamic Domain Name System [Trabajo de titulación, Universidad Politécnica Salesiana]. DSpace UPS.

<https://dspace.ups.edu.ec/bitstream/123456789/25624/1/UPS-GT004500.pdf>

Welsh, B. C. & Farrington, D. P. (2009). Public area CCTV and crime prevention: An updated systematic review and meta-analysis. *Justice Quarterly*, 26(4), 716–745. <https://doi.org/10.1080/07418820802506206>