

SEGURIDAD CIUDADANA CIENCIA FRENTE AL CRIMEN

Revista de
divulgación
científica

Libros &
Ciencias

01 - ago. 2026

En esta edición

- GRACIA ANGULO
- GERMAIN GARCÍA ZANABRIA
- JUANPABLO HEREDIA
- NEYDO HIDALGO
- HANS HUERTO AMADO
- NOAM LÓPEZ VILLANES
- FELIPE MORENO - VERA
- LIZBARD ORELLANO BENANCIO
- JORGE POCO
- ANÍBAL SÁNCHEZ AGUILAR

Libros & Ciencias
Revista de divulgación científica
Año 6 N.º 9 - 2026

Editada por:

© Consejo Nacional de Ciencia, Tecnología e Innovación
Av. Del Aire N° 485, San Borja. Lima, Perú

© Biblioteca Nacional del Perú
Av. De la Poesía N° 160, San Borja. Lima, Perú

© Autores/as

Sixto Enrique Sánchez Calderón
Presidente del Consejo Nacional de Ciencia, Tecnología e Innovación
(CONCYTEC)

Juan Yangali Quintanilla
Jefe Institucional de la Biblioteca Nacional del Perú (BNP)

Leandro Villalobos Terán
Director de Acceso y Promoción de la Información (BNP)

Víctor Luis Izaguirre Pasquel
Director de la Dirección de Políticas y Programas de CTel (CONCYTEC)

Leandro Villalobos Terán
Coordinador de la Unidad de Investigaciones, Ediciones y Formación (BNP)

Colaboran en este número: Gracia Angulo, Germain Garcia Zanabria,
Juanpablo Heredia, Neydo Hidalgo, Hans Huerto Amado, Noam López Villanes,
Felipe Moreno - Vera, Lizbardo Orellano Benancio, Jorge Poco, Aníbal Sánchez Aguilar

Equipo editorial
Coordinación general: Neydo Hidalgo Minaya
Edición y corrección de estilo: Gracia Angulo Flores
Diagramación, diseño, portada: Kelly Vásquez Chaparro
Ilustración: IA — Copilot, Gemini, prompt y edición Kelly Vásquez Chaparro
Infografías: Héctor G. Chumpitazi C.

Agosto 2026

Depósito Legal N° 2025-13623
e-ISSN: 3119-7280 (En línea)

Licencia Creative Commons
Atribución/Reconocimiento-NoComercial-SinDerivados 4.0 Internacional



En un marco de libertad de expresión y diálogo académico cultural, declaramos que las opiniones y expresiones aquí publicadas son de exclusiva responsabilidad de sus autores.

Índice

05

PRESENTACIÓN

07

PANORAMA DE LA CIENCIA

INTELIGENCIA URBANA PARA LA SEGURIDAD
PÚBLICA: DEL ANÁLISIS ESPACIAL A LA ACCIÓN

Germain Garcia Zanabria

Juanpablo Heredia

Felipe Moreno - Vera

Jorge Poco

29

CIENCIA Y SOCIEDAD

EL DELITO YA NO ESTÁ SOLO EN LA CALLE:
ANÁLISIS FORENSE DIGITAL FRENTE AL CRIMEN
INFORMÁTICO EN EL PERÚ

Lizbardo Orellano Benancio

47

CIENCIA Y SOCIEDAD

DATA CRIM: UNA POTENTE HERRAMIENTA
PARA LA LUCHA CONTRA EL CRIMEN

Aníbal Sánchez Aguilar

63

INVESTIGACIÓN EN EL PERÚ

ECOSISTEMAS DE CONOCIMIENTO PARA LA
SEGURIDAD :¿POR QUÉ LA EVIDENCIA AÚN NO
ESTÁ TRANSFORMANDO A LA POLICÍA?

Noam López Villanes

79

INVESTIGACIÓN EN MARCHA

CIENCIA PARA ENTENDER EL RASTRO DEL
CRIMEN: PROYECTOS E INVESTIGACIONES
FRENTE A UN MONSTRUO DE MÚLTIPLES
CABEZAS: LA INSEGURIDAD

Hans Huerto Amado

91

CIENCIA SOBRE EL PAPEL

LA OSCURIDAD BAJO ACECHO: TECNOLOGÍA
Y CONTROL DEL ORDEN PÚBLICO EN EL PERÚ
DEL SIGLO XIX

Neydo Hidalgo

107

DE LA ANTROPOLOGÍA CRIMINAL A LOS
ALGORITMOS: LA EVOLUCIÓN CIENTÍFICA DE
LA SEGURIDAD

Gracia Angulo

113

RESEÑAS DE AUTORES Y AUTORAS

Presentación

Estimados lectores,

Me es muy grato presentarles un nuevo número de *Libros & Ciencia*, la revista de divulgación científica del Consejo Nacional de Ciencia, Tecnología e Innovación (CONCYTEC), editada en un valioso esfuerzo con la Biblioteca Nacional del Perú (BNP). En esta ocasión, llamamos la atención de la comunidad académica y de la ciudadanía en general sobre el desafío más urgente e insoslayable de la sociedad peruana contemporánea: la seguridad ciudadana.

Los datos del alarmante incremento de la delincuencia en nuestro país y la consecuente percepción de inseguridad generan temor diario del ciudadano y constituyen uno de los elementos principales de freno al desarrollo humano y económico del Perú. Tradicionalmente, la respuesta estatal y social frente a este flagelo ha priorizado los enfoques punitivos y/o reactivos que, si bien son necesarios, resultan insuficientes para resolver una problemática tan profunda y multifactorial.

Este número de *Libros & Ciencia* propone un cambio de paradigma audaz y necesario: abordar la inseguridad ciudadana aprovechando las ventajas de la ciencia, la tecnología y la innovación (CTI). Desde el CONCYTEC venimos promoviendo decididamente este enfoque, organizando espacios de debate de alto nivel y abriendo convocatorias de financiamiento para proyectos de investigación que generen soluciones basadas en la evidencia científica desde

la prevención, predicción y manejo de la inseguridad ciudadana. Estamos convencidos de que la ciencia es una herramienta indispensable para la construcción de la paz social.

A lo largo de esta publicación, destacados investigadores nos demuestran el poder transformador de la CTI. Contamos con las valiosas perspectivas de analistas y científicos como Aníbal Sánchez, Noam López Villanes, Jorge Poco, Lizbardo Orellano, Hans Huerto, Gracia Angulo y Neydo Hidalgo, quienes abordan el fenómeno desde diversas disciplinas de vanguardia.

Los artículos de esta edición exploran, por ejemplo, la manera en la que el análisis de datos masivos (Big Data) permite predecir patrones delictivos y optimizar los recursos policiales, y cómo la inteligencia artificial revoluciona los sistemas de video vigilancia. Asimismo, se explora la importancia de las ciencias del comportamiento, rescatando los aportes fundamentales de la neurociencia y la psicología social para comprender las raíces de la violencia, de manera que se puedan diseñar estrategias efectivas de prevención temprana.

Adicionalmente, gracias al invaluable acervo y rigurosa perspectiva de la Biblioteca Nacional del Perú, este documento nos ofrece una mirada a la historia de la criminalidad y el pensamiento criminológico en nuestro país, como un ejercicio indispensable para entender la genealogía de esta crisis previniendo así estrategias erróneas usadas en el pasado.

Los invito a disfrutar de esta lectura que no solo busca diagnosticar el problema, sino también generar propuestas y soluciones tangibles. Frente al crimen y la violencia, la respuesta más inteligente, sostenible y humana es la que nace del conocimiento.

Dr. Sixto Sánchez Calderón
Presidente del CONCYTEC

An aerial night view of a city, likely Bogotá, Colombia, showing a complex highway interchange and surrounding urban areas. A glowing blue network of lines and nodes is superimposed over the city, representing data or connectivity. A full moon is visible in the dark sky above the city.

PANORAMA DE LA CIENCIA

INTELIGENCIA URBANA PARA LA SEGURIDAD PÚBLICA: DEL ANÁLISIS ESPACIAL A LA ACCIÓN

*Germain García Zanabria
Juanpablo Heredia
Felipe Moreno
Jorge Poco*

INTRODUCCIÓN:

EL ECOSISTEMA CIENTÍFICO CONTRA EL CRIMEN

La seguridad pública constituye uno de los desafíos más complejos de las sociedades contemporáneas. En las ciudades, la violencia y la criminalidad no responden a una única causa ni pueden explicarse únicamente por la reacción policial frente a los delitos. Son el resultado de la interacción entre factores sociales, características del espacio urbano, debilidades institucionales y oportunidades que favorecen la comisión de actos delictivos. Por ello, diversos organismos internacionales sostienen que la seguridad urbana requiere enfoques integrales, capaces de abordar simultáneamente los múltiples factores que generan violencia, delito e inseguridad, especialmente en ciudades densamente pobladas y marcadas por profundas desigualdades (UNODC, s. f.).

En el Perú, este desafío adquiere una relevancia particular. La percepción de inseguridad se ha mantenido elevada durante los últimos años. Según el Instituto Nacional de Estadística e

Informática (INEI, 2025), entre enero y junio de 2025, el 85,1 % de la población urbana de 15 años o más consideró probable ser víctima de un delito durante los siguientes doce meses; en Lima Metropolitana y el Callao, esta cifra alcanzó el 86,3 %. Estos datos reflejan no solo la magnitud del problema, sino también la necesidad de fortalecer las capacidades analíticas del Estado para comprender patrones delictivos cada vez más complejos, dinámicos y diferenciados según el territorio. Para ello no basta con incorporar nuevas herramientas tecnológicas: también es necesario mejorar la calidad de los datos, integrarlos y facilitar su intercambio entre las distintas instituciones responsables de la seguridad ciudadana.

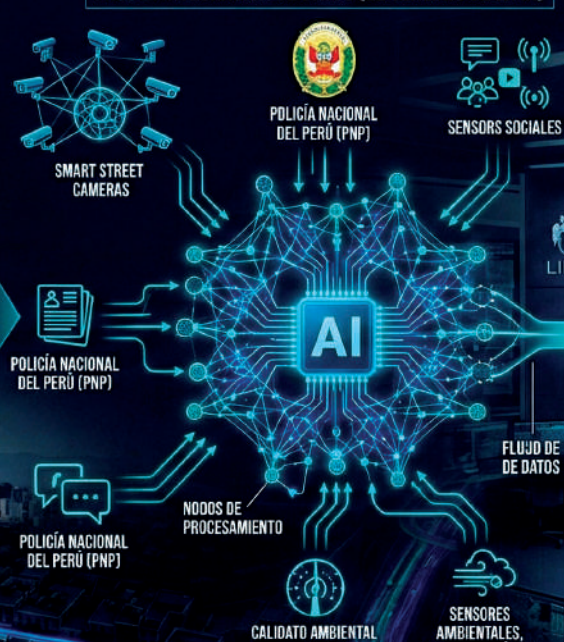
Comprender estos desafíos exige una mirada multidisciplinaria. Hoy, el estudio del crimen reúne aportes provenientes de disciplinas tan diversas como la neurociencia, la informática, la estadística, la geografía, la psicología y el urbanismo. Por ejemplo, la neurociencia investiga cómo determinados procesos cerebrales influyen en los comportamientos antisociales y en la interacción entre el individuo y su entorno (Kahhale, 2022). Al mismo tiempo, el análisis computacional permite estudiar cómo



PASO 1: ANÁLISIS ESPACIAL



PASO 2: INTEGRACIÓN DE DATOS (EL CEREBRO DE LA IA)



PASO 3: ACCIÓN - DESPLIEGUE OPERATIVO



Ilustración: IA — Copilot, prompt y edición Kelly Vásquez Chaparro

la configuración física de una ciudad influye tanto en la ocurrencia de delitos como en la percepción de seguridad de sus habitantes (Jacobs, 1961). Gracias a estas herramientas ha sido posible visualizar patrones delictivos en distintas escalas urbanas (García-Zanabria et al., 2020), identificar regularidades espaciales en grandes ciudades (García-Zanabria et al., 2021) y analizar cómo las personas perciben la seguridad de una calle a partir de sus características visuales (Moreno-Vera et al., 2021a).

En este contexto, el análisis de datos y la inteligencia artificial desempeñan un papel cada vez más importante. La posibilidad de procesar grandes volúmenes de información, identificar patrones espaciales y temporales y

optimizar la asignación de recursos está permitiendo que la gestión de la seguridad evolucione desde estrategias predominantemente reactivas hacia enfoques preventivos. Así, la ciencia del crimen deja de ser únicamente una herramienta para describir lo que ocurre y se convierte en un soporte para comprender los fenómenos delictivos, anticipar escenarios y diseñar políticas públicas sustentadas en evidencia.

Según el INEI, entre enero y junio de 2025, el 85,1 % de la población urbana de 15 años o más consideró probable ser víctima de un delito.

TENDENCIAS GLOBALES: ALGORITMOS, TECNOLOGÍA DE VIGILANCIA Y CIBERSEGURIDAD

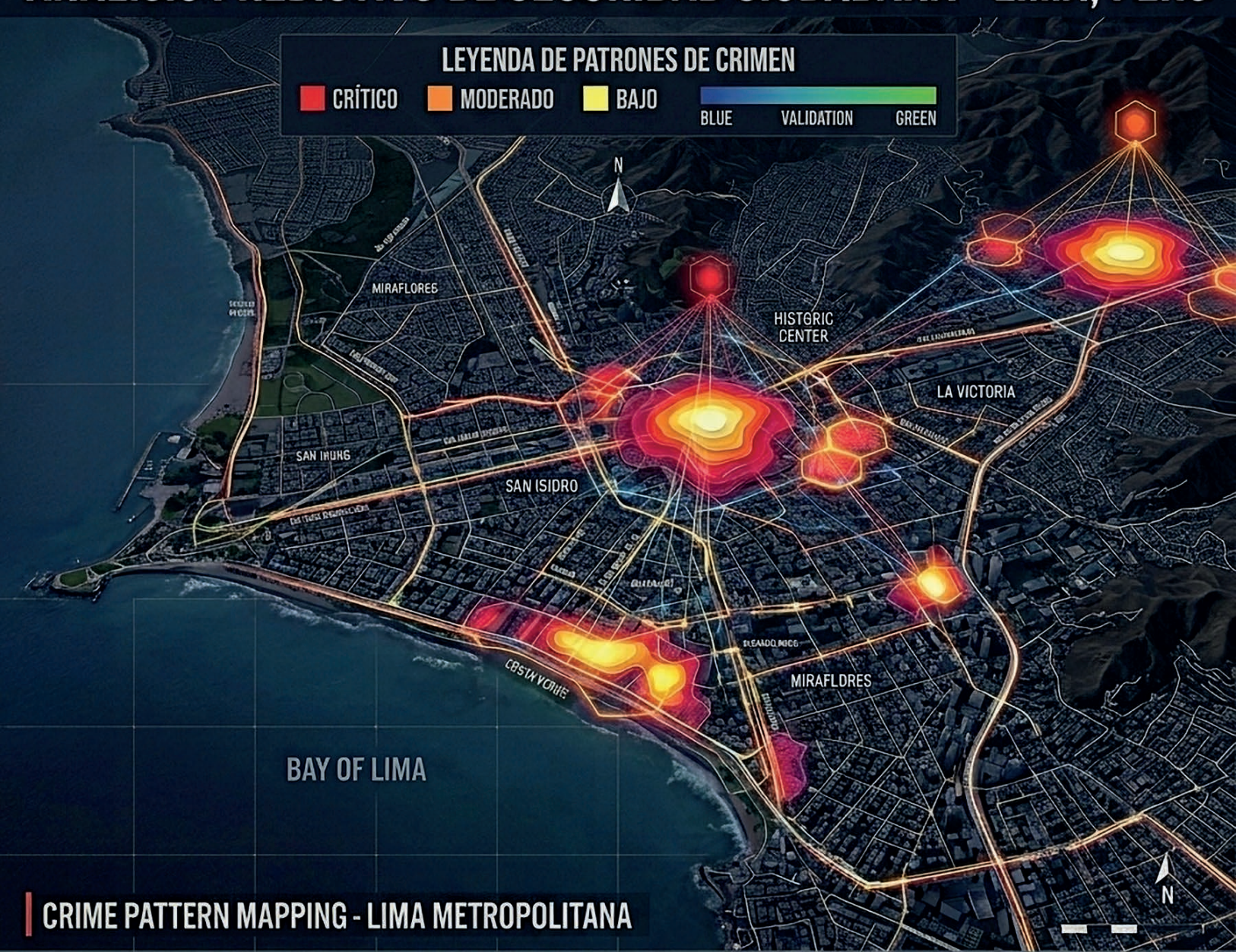
Durante las últimas décadas, la gestión de la seguridad pública ha experimentado una profunda transformación. La protección de las ciudades ya no depende exclusivamente de la presencia policial, sino también del uso de tecnologías capaces de recopilar, monitorear y procesar información de manera continua. En el contexto de las llamadas ciudades inteligentes (*smart cities*), la seguridad se apoya cada vez más en cámaras de vigilancia, sensores urbanos, plataformas de monitoreo y protocolos de ciberseguridad destinados tanto a proteger a la población como a garantizar el funcionamiento de servicios esenciales, como el transporte, la salud o las comunicaciones (Shaffer, 2024).

Este cambio tecnológico también ha transformado la manera de comprender la seguridad urbana. Los datos se han convertido en un recurso estratégico y su utilidad depende de factores como la calidad de la información, su

actualización permanente, la integración entre instituciones y la posibilidad de rastrear su origen y uso. En otras palabras, cuanto mejor sea la gestión de los datos, mayor será la capacidad del Estado para tomar decisiones fundamentadas y transparentes.

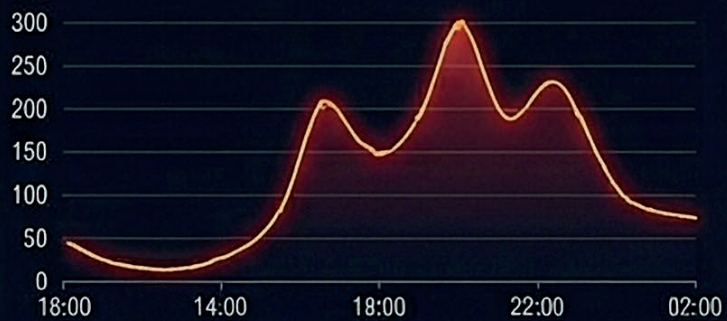
Como consecuencia de esta transformación, los métodos computacionales y matemáticos ocupan hoy un lugar central en la planificación de la seguridad pública. Entre ellos destacan las técnicas de machine learning o aprendizaje automático, es decir, algoritmos capaces de aprender a partir de grandes cantidades de datos para identificar patrones, clasificar información o realizar predicciones. Estas herramientas permiten detectar hotspots o zonas con alta concentración delictiva, reconocer patrones espaciales y temporales y estimar dónde existe una mayor probabilidad de que ocurran determinados delitos a partir del análisis de registros policiales y datos geoespaciales (García-Zanabria et al., 2021).

A ello se suma el *deep learning* o aprendizaje profundo, una rama del aprendizaje automático basada en redes neuronales artificiales que permite analizar información mucho

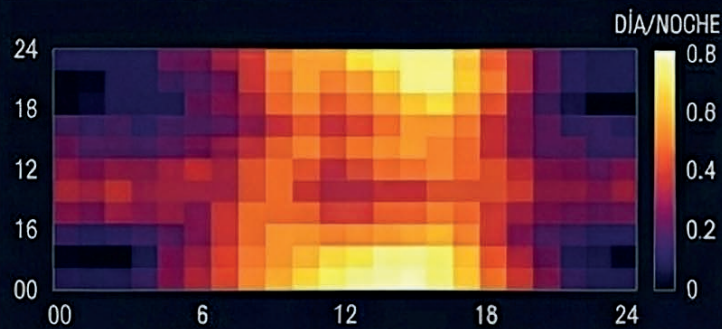


CRIME PATTERN MAPPING - LIMA METROPOLITANA

ANÁLISIS TEMPORAL: OCURRENCIA POR HORA



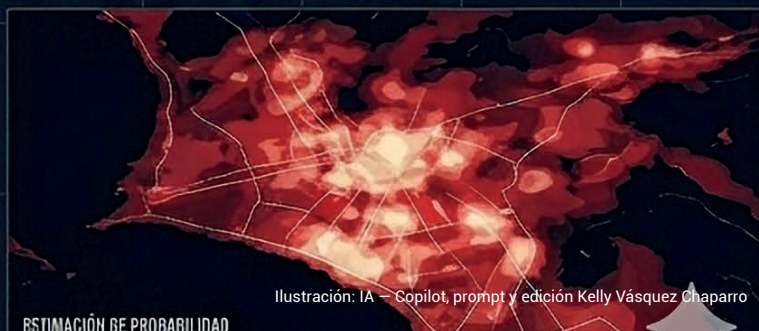
PROBABILIDAD DELICTIVA PREDICHA



REGISTROS POLICIALES INTEGRADOS



ESTIMACIÓN DE PROBABILIDAD

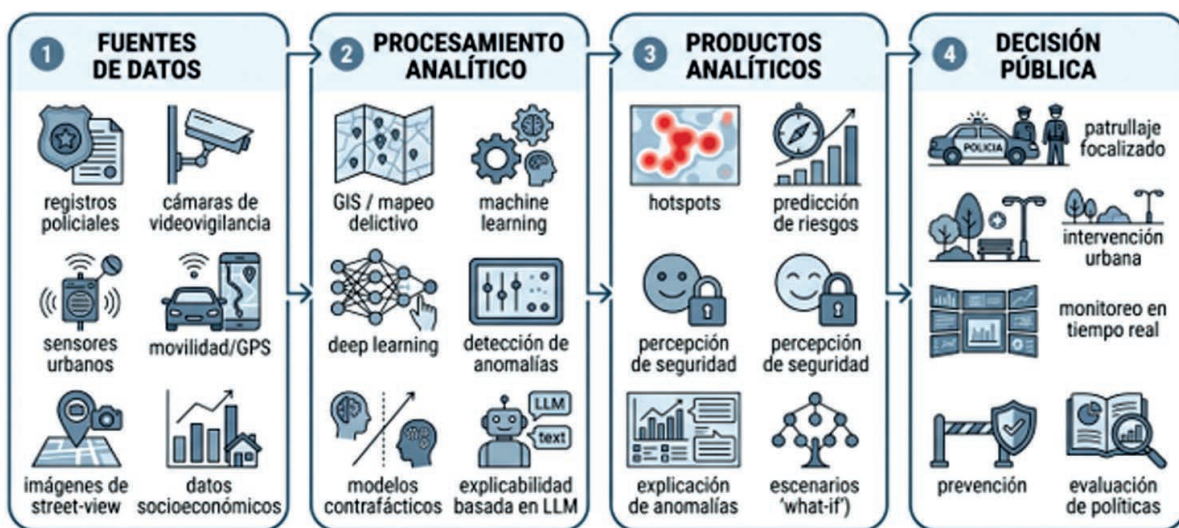


más compleja, como imágenes urbanas. Gracias a estas técnicas es posible clasificar automáticamente distintos entornos según el nivel de seguridad que perciben los ciudadanos, aportando nuevas herramientas para comprender la relación entre las características físicas del espacio, la percepción de inseguridad y el riesgo delictivo (Moreno-Vera et al., 2021a).

En conjunto, estas aproximaciones permiten superar muchas de las limitaciones de los análisis estadísticos

tradicionales y optimizar la asignación de recursos públicos. Como muestra la Figura 1, distintas fuentes de información urbana —registros policiales, cámaras de videovigilancia, sensores, datos de movilidad, imágenes de calles o información socioeconómica— pueden integrarse mediante herramientas analíticas para generar diagnósticos, predicciones y escenarios que apoyen la toma de decisiones, siempre bajo criterios de gobernanza, transparencia, privacidad y ciberseguridad.

FIGURA N.º 1



De las fuentes de datos a la inteligencia urbana para la seguridad pública. El esquema resume cómo distintos tipos de datos urbanos alimentan métodos analíticos que producen diagnósticos, predicciones y explicaciones útiles para la toma de decisiones, todo ello bajo las exigencias de gobernanza, privacidad, transparencia y ciberseguridad.

Un ejemplo ampliamente conocido es PredPol,¹ desarrollado en Estados Unidos para estimar las zonas con mayor probabilidad de ocurrencia de delitos a partir de patrones espaciales y temporales. En el Reino Unido, la Policía Metropolitana de Londres ha incorporado sistemas de reconocimiento facial en tiempo real, una tecnología que ha impulsado un intenso debate sobre privacidad, vigilancia y derechos civiles. En América Latina, aunque la incorporación de inteligencia artificial ha sido más gradual, ya existen experiencias relevantes de videovigilancia, análisis en tiempo real y visualización de patrones criminales (García-Zanabria et al., 2020). Entre ellas destaca SITIA,² en Chile, que integra la información obtenida por cámaras de vigilancia con bases de datos policiales para fortalecer las capacidades de análisis.

Más allá de la infraestructura tecnológica, uno de los principales aportes proviene de la criminología ambiental. Esta disciplina sostiene que el delito tiende a concentrarse en microespacios urbanos específicos, como determinadas esquinas o segmentos de calle, frecuentemente asociados con lugares que atraen o facilitan la actividad delictiva (García-Zanabria et al., 2021).



Asimismo, investigaciones recientes muestran que el estado físico del entorno —por ejemplo, la presencia de basura, infraestructura deteriorada o espacios abandonados— influye en la percepción de seguridad de las personas y puede incorporarse a modelos que ayudan a simular distintos escenarios de intervención urbana para evaluar cuáles podrían resultar más eficaces (Lavi et al., 2022; Moreno-Vera et al., 2025; Raimundo et al., 2025).

ANÁLISIS CRIMINALÍSTICO Y EVOLUCIÓN DE LOS MAPAS DE CALOR

A lo largo de las últimas décadas, los Sistemas de Información Geográfica (GIS, por sus siglas en inglés) han desempeñado un papel decisivo en el análisis del crimen. Mediante la elaboración de mapas delictivos (*crime mapping*), estas herramientas han permitido visualizar cómo se distribuyen los delitos en el territorio, analizar su comportamiento a lo largo del tiempo e incorporar variables urbanas, sociales y ambientales asociadas a la generación de oportunidades delictivas. Gracias a ello, el estudio del crimen ha evolucionado desde un enfoque

principalmente descriptivo hacia una perspectiva interdisciplinaria que integra la estadística, el aprendizaje automático, la visualización de datos y las ciencias sociales (García-Zanabria et al., 2021).

Uno de los métodos más utilizados en este ámbito es el análisis de hotspots o zonas de alta concentración delictiva. Su objetivo consiste en identificar aquellos lugares donde los delitos ocurren con mayor frecuencia para orientar mejor las acciones de prevención y la asignación de recursos (Chainey et al., 2008). Sin embargo, los mapas de calor tradicionales presentan una limitación importante: privilegian la cantidad de delitos registrados y tienden a invisibilizar lugares donde determinados delitos, aunque menos numerosos, ocurren de manera persistente y reiterada (García-Zanabria et al., 2020, 2021).

Esta dificultad se relaciona con la forma en que tradicionalmente se representa el espacio urbano. Con frecuencia, las ciudades se dividen en cuadrículas regulares o unidades territoriales amplias que simplifican la realidad, pero también ocultan diferencias relevantes entre calles, esquinas o pequeños sectores urbanos.

Como se observa en la Figura 2, este tipo de representación puede diluir la concentración delictiva al promediar eventos que, en realidad, se concentran en puntos muy específicos, como intersecciones o determinados tramos de una vía (Bernasco & Block, 2011; Clarke & Eck, 2007; Weisburd, 2015).

Los mapas de calor tradicionales presentan una limitación importante: privilegian la cantidad de delitos registrados y tienden a invisibilizar lugares donde determinados delitos, aunque menos numerosos, ocurren de manera persistente y reiterada.

FIGURA N.º 2

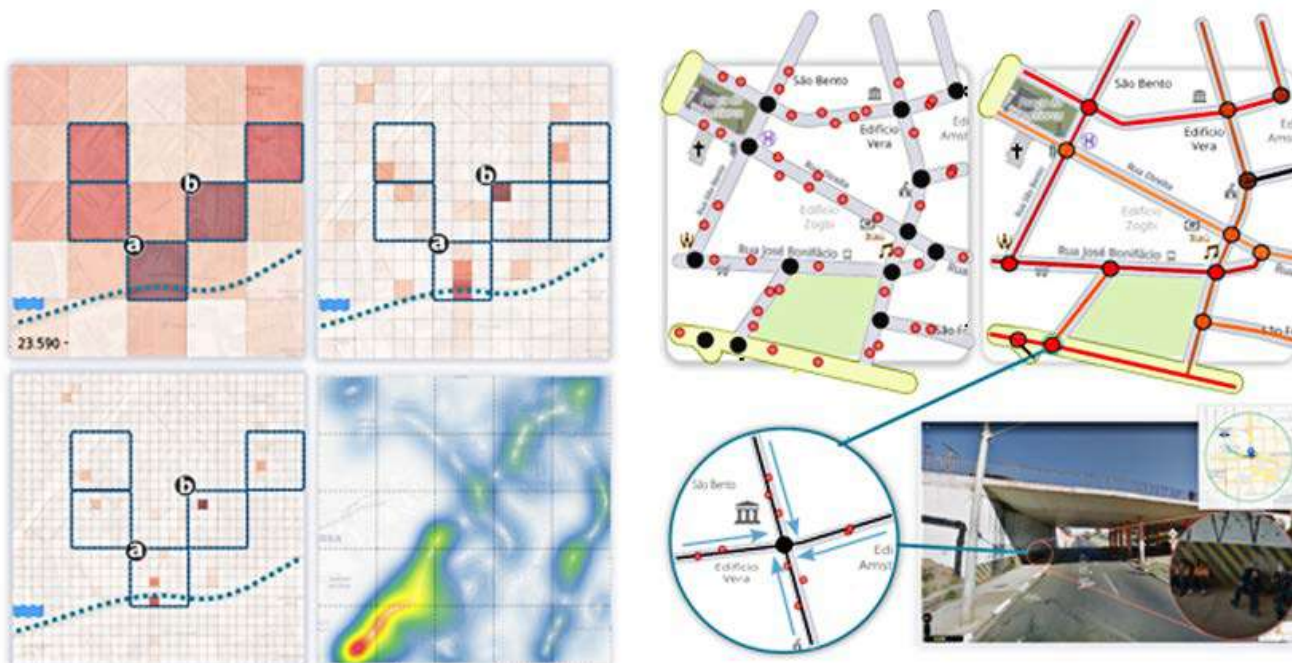


Figura 2. Comparación entre la discretización espacial mediante cuadrículas y la representación basada en una red de calles. A la izquierda, la agregación en celdas regulares puede ocultar variaciones en microlugares. A la derecha, la discretización por intersecciones y segmentos viales permite identificar con mayor precisión la concentración delictiva en esquinas y en tramos. Adaptado de García-Zanabria et al. (2020, 2021).

Frente a estas limitaciones surgieron nuevas formas de analizar el espacio urbano a una escala mucho más detallada. Entre ellas destacan herramientas como Mirante y CrimAnalyzer, que marcaron un cambio importante en la manera de estudiar la distribución del delito. Mientras Mirante propuso una representación basada en la red real de calles, CrimAnalyzer incorporó técnicas matemáticas para identificar hotspots considerando no solo la cantidad de delitos, sino también la intensidad, la frecuencia y la recurrencia de los patrones delictivos (Garcia-Zanabria et al., 2020, 2021).

Este desarrollo metodológico dio un paso adicional con CriPAV (véase la Figura 3), una plataforma que integra el análisis a nivel de calle con modelos probabilísticos para estimar la probabilidad de ocurrencia del delito. Además de identificar patrones espaciales, el sistema incorpora imágenes de Street View para relacionar la dinámica delictiva con las características físicas del entorno urbano y agrupa segmentos de calles que presentan comportamientos similares (Garcia-Zanabria et al., 2022). De este modo, el análisis deja de centrarse únicamente en la ubicación de los delitos y comienza a incorporar información sobre el contexto donde estos ocurren.

FIGURA N.º 3

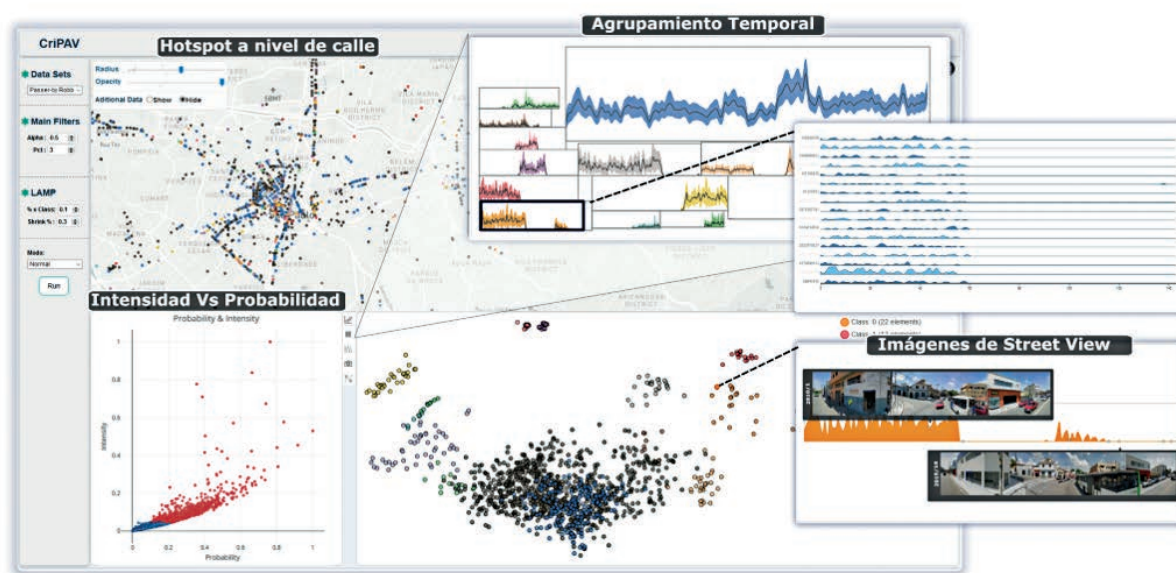


Figura 3. SS. Adaptado de Garcia-Zanabria et al. (2022).

Mientras Mirante propuso una representación basada en la red real de calles, CrimAnalyzer incorporó técnicas matemáticas para identificar hotspots considerando no solo la cantidad de delitos, sino también la intensidad, la frecuencia y la recurrencia de los patrones delictivos (García-Zanabria et al., 2020, 2021).

Esta evolución refleja un cambio más amplio en la investigación sobre seguridad urbana. Mientras los primeros mapas delictivos respondían principalmente a la pregunta "¿dónde ocurre el delito?", las herramientas actuales buscan responder también "¿por qué ocurre precisamente allí?" y "¿qué características del entorno ayudan a explicarlo?". Ese cambio de perspectiva resulta fundamental para diseñar estrategias preventivas más precisas y eficaces.

EL ENTORNO URBANO Y LA PERCEPCIÓN DE SEGURIDAD

La relación entre el entorno físico y el comportamiento humano constituye uno de los temas centrales de la psicología social, la criminología y los estudios urbanos (Keuschnigg & Wolbring, 2015). Una de las teorías más influyentes en este campo es la teoría de las ventanas rotas, que sostiene que los signos visibles de deterioro —como grafitis, acumulación de basura, infraestructura dañada o un exceso de cableado aéreo— transmiten la sensación de que un espacio carece de control y supervisión, lo que puede incrementar la percepción de inseguridad (Wilson & Kelling, 1982).

Desde esta perspectiva, la seguridad urbana no depende únicamente del número de delitos registrados. También está relacionada con la manera en que las personas perciben y experimentan los espacios públicos. Esa percepción influye en decisiones cotidianas tan diversas como caminar por una calle, permanecer en una plaza o utilizar determinados servicios urbanos, y termina afectando la calidad de vida de quienes habitan la ciudad (Moreno-Vera et al., 2021b).

Durante los últimos años, el desarrollo de técnicas de visión por computadora ha permitido estudiar este fenómeno de una manera inédita. Mediante imágenes obtenidas a nivel de calle —por ejemplo, a través de Street View— y bases de datos construidas a partir de las opiniones de los ciudadanos, diversas investigaciones han demostrado que es posible estimar la percepción de seguridad asociada a un entorno urbano analizando sus características visuales.

En una primera etapa, los modelos de inteligencia artificial utilizaron técnicas de segmentación semántica y redes neuronales convolucionales para identificar los elementos presentes en una escena urbana y relacionarlos con la percepción de seguridad expresada

por las personas (Moreno-Vera et al., 2021a, 2021b). De este modo, un juicio que tradicionalmente se consideraba subjetivo pudo transformarse en un fenómeno susceptible de ser analizado y cuantificado.

La Figura 4 resume este proceso. En primer lugar, los participantes observan pares de imágenes urbanas y responden una pregunta sencilla: ¿Cuál de estas dos calles le parece más segura? A partir de miles de respuestas de este tipo, los modelos de aprendizaje profundo identifican patrones visuales recurrentes y estiman un puntaje de seguridad percibida para nuevas imágenes. Así, el sistema aprende qué características del entorno suelen asociarse con una mayor o menor sensación de seguridad.

FIGURA N.º 4

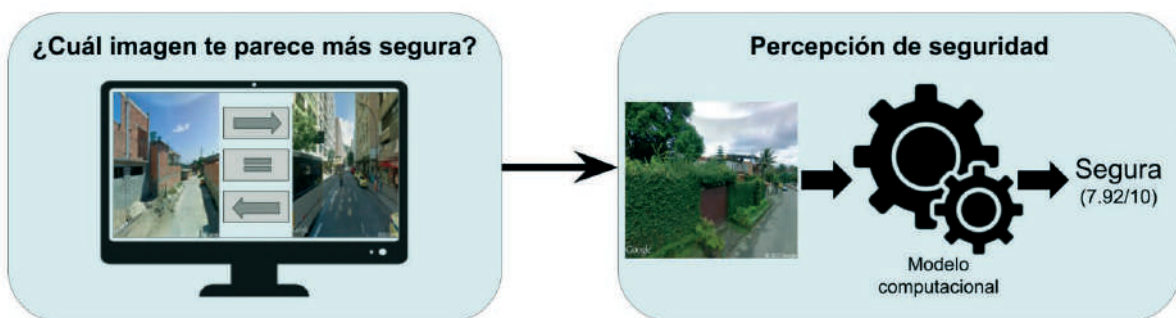


Figura 4. Proceso de cuantificación de la percepción urbana. A la izquierda, tenemos el método de recolección de preferencias mediante una encuesta en línea que compara dos imágenes urbanas. A la derecha se muestra el flujo para cuantificar la percepción urbana aplicando modelos de aprendizaje profundo; es posible extraer características y elementos visuales para estimar la percepción de seguridad urbana a partir de la composición de la escena. Adaptado de Moreno-Vera et al. (2021a).

Más recientemente, el desarrollo de modelos multimodales —capaces de combinar distintos tipos de información, como imágenes y texto— y de enfoques contrafactuales ha permitido avanzar un paso más. Ya no se trata únicamente de predecir cómo será percibido un lugar, sino también de explicar por qué genera esa percepción.

Las investigaciones más recientes, como UrbanVLM y UrbanPhysicalDisorder-4K, muestran que determinados elementos del entorno tienen un impacto especialmente importante. La presencia de infraestructura deteriorada, basura, grafitis o exceso de cableado aéreo suele asociarse con una menor percepción de

seguridad, mientras que la vegetación, el mantenimiento de los espacios públicos y un entorno ordenado contribuyen a mejorarla (Lavi et al., 2022; Moreno-Vera et al., 2025; Moreno-Vera & Poco, 2025).

La Figura 5 ilustra este enfoque mediante un ejemplo contrafactual. En lugar de limitarse a indicar que una calle parece insegura, el modelo modifica virtualmente algunos elementos de la escena —por ejemplo, elimina grafitis o incorpora árboles— y estima cómo cambiaría la percepción de seguridad. Este tipo de simulaciones permite explorar el posible impacto de distintas intervenciones urbanas antes de ejecutarlas.

FIGURA N.º 5

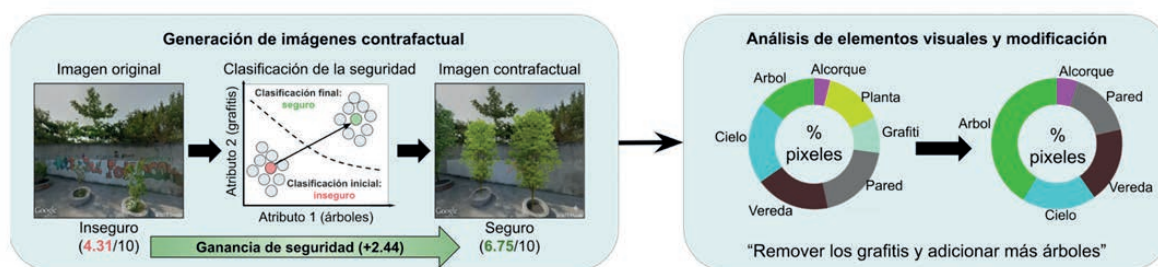


Figura 5. Análisis contrafactual del desorden físico urbano. La figura ilustra el proceso para analizar y modificar la distribución de los objetos presentes. A la izquierda mostramos una imagen inicial percibida como insegura (puntaje de 4.31), una imagen contrafactual generada (puntaje de 6.75) y la relación entre los atributos árbol y grafiti que determinan la percepción. En la derecha mostramos el análisis y los atributos a añadir y remover, mejorando la estimación de seguridad urbana. Este proceso demuestra el impacto causal de estos componentes en la percepción de seguridad. Adaptado de Moreno-Vera et al. (2025).

En conjunto, estas herramientas representan un cambio importante en la forma de comprender la seguridad urbana. Más allá de identificar dónde ocurren los delitos, permiten analizar cómo las características físicas del entorno influyen en la experiencia cotidiana de las personas y ofrecen información valiosa para orientar intervenciones urbanas que contribuyan a generar espacios más seguros.

ANÁLISIS DE DATOS APLICADOS A LA VIGILANCIA PREDICTIVA DE LA DELINCUENCIA

El análisis del crimen ha dejado de limitarse a describir patrones o identificar zonas de riesgo. En la actualidad, también busca comprender las causas de los fenómenos delictivos y explorar posibles escenarios de intervención que faciliten la toma de decisiones. En este contexto, la vigilancia predictiva ya no responde únicamente a la pregunta «¿dónde podría ocurrir un delito?», sino también a otras igualmente relevantes: «¿qué cambios podrían reducir ese riesgo?» y «¿por qué ocurrió un hecho inesperado?».

Este cambio refleja una evolución importante en el uso de la inteligencia artificial aplicada a la seguridad. Los avances recientes en métodos

de explicabilidad y en explicaciones contrafactuales permiten comprender mejor cómo llegan los modelos a determinadas conclusiones y explorar qué condiciones deberían modificarse para obtener resultados distintos (Ribeiro et al., 2016; Wachter et al., 2018). En otras palabras, la inteligencia artificial ya no solo predice: también comienza a explicar.

El desarrollo de modelos multimodales —capaces de combinar distintos tipos de información, como imágenes y texto— y de enfoques contrafactuales ha permitido avanzar un paso más.

Una de las herramientas desarrolladas con este propósito es CounterCrime, un sistema que incorpora explicaciones contrafactuales al análisis del crimen. En lugar de limitarse a señalar qué regiones presentan mayores niveles de riesgo, la plataforma analiza qué variables urbanas y socioeconómicas deberían modificarse para que una zona cambie de una condición de mayor riesgo a otra más favorable (Raimundo et al., 2025).

Como muestra la Figura 6, el sistema permite simular distintos escenarios considerando cambios en variables como la densidad de establecimientos comerciales, las paradas de transporte público, el nivel de ingresos o la población residente. Su principal aporte consiste en que estas propuestas no son arbitrarias

sino que se basan en configuraciones observadas en otras áreas de la ciudad con características similares. De este modo, el análisis deja de ser exclusivamente predictivo y adquiere una dimensión propositiva, capaz de orientar intervenciones urbanas plausibles.

FIGURA N.º 6

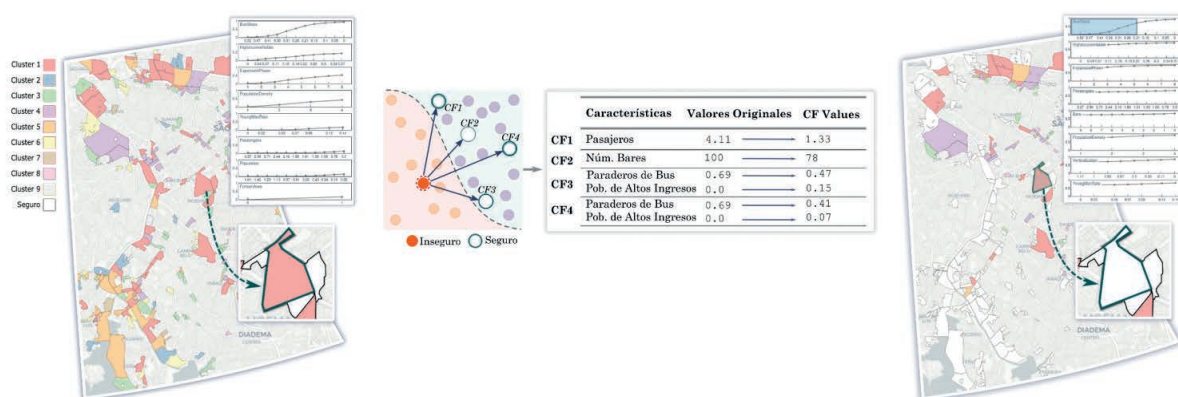


Figura 6. Exploración de escenarios con CounterCrime. A la izquierda, se muestran las regiones y sus características originales, destacando una región "insegura". En el centro, se ilustra su transformación mediante contrafactuales (CF1–CF4) hacia una región "segura", junto con los cambios en variables urbanas y socioeconómicas. A la derecha, se muestra el impacto espacial de estas modificaciones, en la reclasificación de regiones bajo distintos escenarios. Adaptado de Raimundo et al. (2025).

Una segunda aproximación corresponde a AnomalyExplain, una plataforma diseñada para explicar por qué se producen determinados cambios inesperados en los patrones delictivos. Mientras CounterCrime explora qué modificaciones podrían reducir el riesgo, AnomalyExplain intenta responder a la pregunta inversa: ¿qué factores explican una anomalía que ya ocurrió?

Para ello, el sistema integra información espacial, series temporales, modelos de lenguaje e información procedente de fuentes externas (Heredia et al., 2025). Esta combinación permite contextualizar las anomalías y transformarlas en explicaciones comprensibles para quienes toman decisiones.

La Figura 7 resume este funcionamiento. En lugar de generar únicamente una alerta estadística, la plataforma relaciona la anomalía con información espacial, temporal y contextual para construir una explicación fundamentada. En estudios realizados sobre robos de teléfonos móviles en São Paulo, por ejemplo, el sistema logró

asociar determinados incrementos delictivos con eventos masivos, como el Carnaval o festividades religiosas, evidenciando cómo las modificaciones en la movilidad y en la concentración de personas alteran también las oportunidades para la comisión de delitos (Heredia et al., 2025).

FIGURA N.º 7



Figura 7. Descripción general de AnomalyExplain. La plataforma integra datos espaciales, series temporales y contexto externo (1) en un flujo que combina análisis (2), visualización interactiva (3) y un módulo LLM (4) para generar explicaciones sobre posibles causas de anomalías criminales, apoyadas en evidencia espacial y temporal, así como en fuentes externas. Adaptado de Heredia et al. (2025).

En conjunto, ambas herramientas ilustran la dirección que está tomando la investigación en inteligencia urbana. El objetivo ya no consiste únicamente en anticipar dónde podría ocurrir un delito, sino también en comprender por qué sucede, explicar los factores que intervienen y evaluar posibles alternativas de intervención antes de implementarlas. Este cambio representa un paso importante hacia una gestión de la seguridad pública más transparente, fundamentada y orientada al aprendizaje continuo.

CONCLUSIONES: HACIA UN MODELO APLICABLE PARA EL PERÚ

La persistente percepción de inseguridad en el Perú —donde más del 85 % de la población urbana considera posible ser víctima de un delito— evidencia la necesidad de fortalecer las capacidades del Estado mediante un enfoque científico para la gestión de la seguridad pública. Este desafío exige superar una lógica centrada exclusivamente en la

reacción frente al delito y avanzar hacia estrategias preventivas sustentadas en el análisis criminal a microescala, el estudio de patrones espaciales, la explicabilidad de los modelos de inteligencia artificial y la evaluación sistemática de distintos escenarios de intervención.

La evidencia presentada a lo largo de este artículo muestra que la seguridad urbana no depende únicamente de la cantidad de delitos registrados. También está profundamente relacionada con la manera en que las personas experimentan y perciben los espacios que habitan. Por ello, comprender el papel del entorno físico, de las dinámicas sociales y de los factores que generan desorden urbano resulta indispensable para

identificar riesgos y diseñar estrategias de prevención más eficaces.

Las herramientas descritas en este trabajo demuestran que la inteligencia artificial, el análisis espacial y la ciencia de datos pueden contribuir significativamente a mejorar la gestión de la seguridad pública. Sin embargo, su verdadero potencial no reside únicamente en la capacidad de producir predicciones cada vez más precisas. Su principal aporte consiste en ofrecer explicaciones, simular escenarios y proporcionar evidencia que permita tomar decisiones mejor fundamentadas.

En conjunto, estas aproximaciones ofrecen una base científica para



Ilustración: IA — Copilot, prompt y edición Kelly Vásquez Chaparro

La evidencia presentada a lo largo de este artículo muestra que la seguridad urbana no depende únicamente de la cantidad de delitos registrados. También está profundamente relacionada con la manera en que las personas experimentan y perciben los espacios que habitan.

diseñar políticas públicas más precisas, transparentes y viables. Desde esta perspectiva, la aplicación de métodos científicos al estudio del crimen configura una oportunidad relevante para el Perú, donde la tecnología no sustituye la acción del Estado, sino que la fortalece mediante mejores capacidades de análisis, prevención y planificación.

No obstante, para que este modelo pueda implementarse de manera efectiva, no basta con disponer de herramientas tecnológicas avanzadas. También es indispensable contar con datos confiables, sistemas interoperables, instituciones capaces de analizar la información y mecanismos de gobernanza que garanticen la transparencia, la protección de los derechos ciudadanos y el uso responsable de la inteligencia artificial.

En definitiva, la inteligencia urbana representa mucho más que un conjunto de tecnologías aplicadas a la seguridad. Constituye una nueva forma de comprender el territorio, anticipar riesgos y construir políticas públicas sustentadas en evidencia. Su mayor contribución no radica únicamente en hacer más eficiente la respuesta frente al delito, sino en fortalecer la capacidad del Estado para prevenirlo y mejorar la calidad de vida de la ciudadanía.

Referencias bibliográficas

- Bernasco, W., & Block, R. (2011). Robberies in Chicago: A block-level analysis of the influence of crime generators, crime attractors, and offender anchor points. *Journal of Research in Crime and Delinquency*, 48(1), 33–57. <https://doi.org/10.1177/0022427810384135>
- Chainey, S., Tompson, L., & Uhlig, S. (2008). The utility of hotspot mapping for predicting spatial patterns of crime. *Security Journal*, 21(1–2), 4–28. <https://doi.org/10.1057/palgrave.sj.8350066>
- Clarke, R. V., & Eck, J. E. (2007). Understanding risky facilities (Problem-Oriented Guides for Police, Problem-Specific Guide Series No. 6). Office of Community Oriented Policing Services, U.S. Department of Justice. <https://portal.cops.usdoj.gov/resourcecenter/content.ashx/cops-p118-pub.pdf>
- Garcia-Zanabria, G., Gomez-Nieto, E., Silveira, J., Poco, J., Nery, M., Adorno, S., & Nonato, L. G. (2020). Mirante: A visualization tool for analyzing urban crimes. En 2020 33rd SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI) (pp. 148–155). IEEE. <https://doi.org/10.1109/SIBGRAPI51738.2020.00028>
- Garcia-Zanabria, G., Raimundo, M. M., Poco, J., Nery, M. B., Silva, C. T., Adorno, S., & Nonato, L. G. (2022). CriPAV: Street-level crime patterns analysis and visualization. *IEEE Transactions on Visualization and Computer Graphics*, 28(12), 4000–4015. <https://doi.org/10.1109/TVCG.2021.3111146>
- Garcia-Zanabria, G., Silveira, J., Poco, J., Paiva, A., Nery, M. B., Silva, C. T., Adorno, S., & Nonato, L. G. (2021). CrimAnalyzer: Understanding crime patterns in São Paulo. *IEEE Transactions on Visualization and Computer Graphics*, 27(4), 2313–2328. <https://doi.org/10.1109/TVCG.2019.2947515>
- Heredia, J., Estrada-Rayme, L., Matos-Cangalaya, J., & Poco, J. (2025). Interactive exploration and explanation of spatio-temporal anomalies with Graph-LLM integration. En 2025 38th SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI) (pp. 1–6). IEEE. <https://doi.org/10.1109/SIBGRAPI67909.2025.11223398>

Instituto Nacional de Estadística e Informática. (2025). Estadísticas de seguridad ciudadana: Informe técnico (N.º 05). <https://www1.inei.gob.pe/media/MenuRecursivo/boletines/informe-tecnico-estadisticas-de-seguridad-ciudadana.pdf>

Jacobs, J. (1961). *The death and life of great American cities*. Random House.

Kahhale, I. (2022). Neural basis of antisocial behaviour. *Nature Reviews Psychology*, 1(3), 129. <https://doi.org/10.1038/s44159-022-00027-1>

Keuschnigg, M., & Wolbring, T. (2015). Disorder, social capital, and norm violation: Three field experiments on the broken windows thesis. *Rationality and Society*, 27(1), 96–126. <https://doi.org/10.1177/1043463114561749>

Lavi, B., Tokuda, E., Moreno-Vera, F., Nonato, L., Silva, C., & Poco, J. (2022). 17K-Graffiti: Spatial and crime data assessments in São Paulo city. En *Proceedings of the 17th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications* (pp. 968–975). <https://doi.org/10.5220/0010883300003124>

Moreno-Vera, F., De-la-Puente, A., & Poco, J. (2025). UrbanPhysicalDisorder-4K: Understanding urban perception via counterfactuals and Street View signs of physical disorder. En 2025 IEEE International Conference on Big Data (BigData) (pp. 5194–5200). IEEE. <https://doi.org/10.1109/BigData66926.2025.11401786>

Moreno-Vera, F., Lavi, B., & Poco, J. (2021a). Quantifying urban safety perception on Street View images. En IEEE/WIC/ACM International Conference on Web Intelligence (pp. 611–616). <https://doi.org/10.1145/3486622.3493975>

Moreno-Vera, F., Lavi, B., & Poco, J. (2021b). Urban perception: Can we understand why a street is safe? En I. Batyrshin, A. Gelbukh, & G. Sidorov (Eds.), *Advances in Computational Intelligence* (Vol. 13067, pp. 277–288). Springer. https://doi.org/10.1007/978-3-030-89817-5_21

Moreno-Vera, F., & Poco, J. (2025). Assessing urban environments with vision-language models: A comparative analysis of AI-generated ratings and human volunteer evaluations. En 2025 *International Joint Conference on Neural Networks (IJCNN)* (pp. 1–8). IEEE. <https://doi.org/10.1109/IJCNN64981.2025.11229058>

- Raimundo, M. M., Garcia-Zanabria, G., Nonato, L. G., & Poco, J. (2025). CounterCrime: Using counterfactual explanations to explore crime reduction scenarios. *IEEE Transactions on Visualization and Computer Graphics*, 31(10), 9008–9023. <https://doi.org/10.1109/TVCG.2025.3586202>
- Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?": Explaining the predictions of any classifier. En *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 1135–1144). <https://doi.org/10.1145/2939672.2939778>
- Shaffer, B. (2024). The data-driven city: Analytics for smart urbanism. <https://www.amazon.com.br/Data-Driven-City-Analytics-Urbanism-English-ebook/dp/B0D1NZ6XYH>
- United Nations Office on Drugs and Crime. (s. f.). Crime prevention. <http://www.unodc.org/unodc/en/urban-safety/crime-prevention.html>
- Wachter, S., Mittelstadt, B., & Russell, C. (2018). Counterfactual explanations without opening the black box: Automated decisions and the GDPR. *Harvard Journal of Law & Technology*, 31(2), 841–887. <https://doi.org/10.2139/ssrn.3063289>
- Weisburd, D. (2015). The law of crime concentration and the criminology of place. *Criminology*, 53(2), 133–157. <https://doi.org/10.1111/1745-9125.12070>
- Wilson, J. Q., & Kelling, G. L. (1982). Broken windows. *The Atlantic Monthly*, 249(3), 29–38.

INTELIGENCIA URBANA PARA LA SEGURIDAD PÚBLICA: DEL ANÁLISIS ESPACIAL A LA ACCIÓN



El 85.1% de la población urbana en Perú **considera posible ser víctima de un delito.**



El desorden físico visible como grafitis y basura deteriora la percepción de seguridad urbana.



Los mapas de calor tradicionales ocultan la **concentración delictiva real ocurrida en microlugares.**



Sistemas como CounterCrime usan contrafactuales para simular escenarios de reducción del delito.

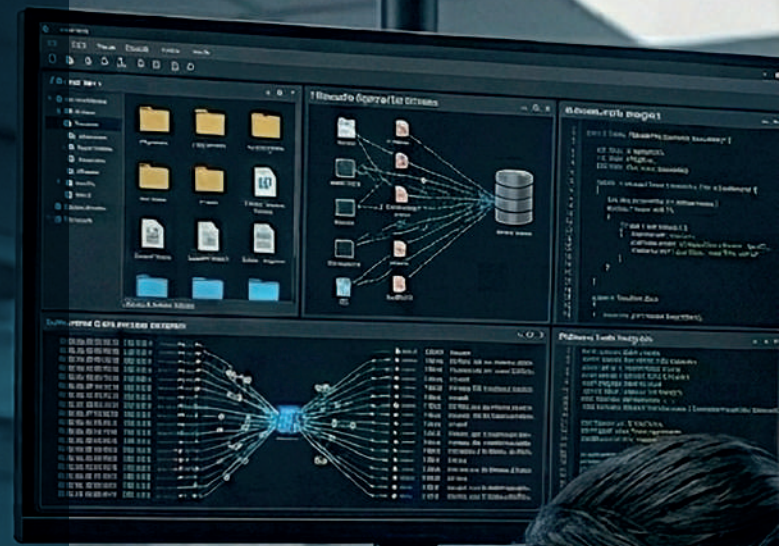


AnomalyExplain integra modelos de lenguaje para traducir anomalías delictivas en narrativas.

CIENCIA Y SOCIEDAD

EL DELITO YA NO ESTÁ SOLO EN LA CALLE: ANÁLISIS FORENSE DIGITAL FRENTE AL CRIMEN INFORMÁTICO EN EL PERÚ

Lizbardo Orellano Benancio



Como perito en análisis forense digital, he conocido diversos casos en los que la tecnología aparece como medio, escenario o fuente de evidencia de un delito. Por estrictas razones de confidencialidad, en las siguientes líneas no haré referencia a carpetas fiscales, nombres reales ni datos que permitan identificar a personas o investigaciones concretas. Las situaciones mencionadas han sido adaptadas con fines estrictamente explicativos, buscando ilustrar cómo el crimen se expresa hoy en los entornos virtuales.

Recuerdo claramente el caso de un aparente buen padre de familia y esposo, cuyas conversaciones telefónicas y mensajes cotidianos podían parecer similares a los de cualquier ciudadano

común, salvo por un perturbador detalle: su «trabajo». Este individuo tenía un horario definido, generalmente de 3:00 p. m. a 11:00 p. m., operaba solo ciertos días de la semana y sus labores se interrumpían abruptamente si aparecía alguna patrulla en la zona. Su empleo consistía, en realidad, en robar y asaltar a mano armada.

Este caso evidencia una transformación menos visible de la criminalidad: mientras los delitos tradicionales incorporan cada vez más herramientas digitales, los ciberdelitos surgen y evolucionan como nuevas formas de conducta delictiva. Dispositivos móviles, mensajes de texto, redes sociales y otras herramientas digitales sirven actualmente para coordinar, ejecutar, ocultar o ampliar el alcance de las conductas delictivas.



Durante mucho tiempo, la seguridad ciudadana se entendió principalmente desde el espacio físico: calles, viviendas, vehículos, patrullaje y zonas de riesgo. Sin embargo, la masificación de internet y el uso cotidiano de teléfonos inteligentes han configurado un nuevo escenario donde el delito se despliega sin necesidad de presencia física. En este entorno digital, la delincuencia común ha encontrado un espacio fértil para la extorsión mediante aplicativos de mensajería rápida, fraudes bancarios en línea, suplantación de identidad y el acoso virtual. La calle ya no es el único espacio donde el ciudadano se expone al peligro; la vulnerabilidad ahora viaja en el bolsillo, dentro de cada dispositivo móvil conectado a la red.

Este caso evidencia una mutación invisible: a la criminalidad tradicional se integran hoy, de forma sistemática, los ciberdelitos.

EL NUEVO ESCENARIO DEL CRIMEN DIGITAL

Para comprender cómo opera la informática forense, es necesario analizar cómo los entornos virtuales transforman la ejecución del delito. Para una mejor comprensión de estas dinámicas, presentaré algunos casos prácticos.

Caso 1

Una niña de 11 años, a quien llamaremos Elena, empezó a mostrarse más distraída de lo habitual con su teléfono celular. Una noche, mientras estaba sentada en la sala frente al televisor, sus padres la llamaron varias veces para cenar, pero ella continuó concentrada en la pantalla. Ante la preocupación, su padre se acercó, le retiró el celular y observó una conversación con una persona que decía ser menor de edad.

Al ser consultada, Elena contó que se trataba de un supuesto chico de 12 años a quien no conocía personalmente, pero con quien había desarrollado una relación de confianza. Con el tiempo, esa persona le pidió imágenes íntimas y luego la amenazó con difundirlas si no enviaba más contenido. Posteriormente, se descubrió que no era un menor de edad, sino un adulto.

Este caso muestra cómo una conversación aparentemente privada e inofensiva puede convertirse en una forma de manipulación, acoso y violencia digital. Asimismo, evidencia la importancia de la prevención, el acompañamiento familiar y la educación digital desde edades tempranas.

Caso 2

Otro caso frecuente es la suplantación de una página web bancaria. Esta modalidad suele iniciar con el smishing, una forma de fraude en la que el ciberdelincuente envía un mensaje de texto con un enlace que dirige a una página falsa, diseñada minuciosamente para parecerse a la web oficial de una entidad financiera.

La víctima ingresa sus datos creyendo que está en un entorno seguro. Luego, con la información previamente obtenida (como el número telefónico, el nombre u otros datos personales), el delincuente realiza una llamada haciéndose pasar por personal del banco. Durante la comunicación, indica que se ha detectado una transferencia sospechosa y que se necesita un código para anularla; sin embargo, ese código suele ser el token o la clave de autorización que permite ejecutar la transferencia fraudulenta real.

El escenario digital actual ofrece múltiples oportunidades, pero también ha generado nuevos riesgos debido a la conectividad global, la rapidez de la información y el anonimato que facilita internet. Por ello, el ciberdelito no solo afecta a los sistemas informáticos, sino también directamente a las personas. En consecuencia, se requiere de prevención, educación digital, investigación especializada y una estrecha coordinación entre el Estado, la sociedad y el sistema de justicia.

LA CIENCIA FRENTE AL CRIMEN: ANÁLISIS FORENSE DIGITAL

En la actualidad, la mayoría de los hechos delictivos dejan algún tipo de rastro digital, los cuales pueden constituir indicios o evidencias tangibles. Estos rastros se alojan en documentos, imágenes, videos, audios, metadatos, registros de sistemas, comunicaciones electrónicas, dispositivos físicos o servicios en la nube. En este contexto, la evidencia digital se convierte en un elemento fundamental para la investigación, siempre y cuando sea obtenida, preservada y analizada bajo parámetros rigurosos que respeten la legalidad, la objetividad, la cadena de custodia y la integridad de la información.

192.168.1.115

192.168.1.115

192.168.1.115

192.168.1.115

192.168.1.115

192.168.1.115

192.168.1.115

192.168.1.115

192.168.1.115

192.168.1.115

192.168.1.115

192.168.1.115

192.168.1.115

192.168.1.115

GET /api/users HTTP/1.1

GET /api/users HTTP/1.1

GET /api/users HTTP/1.1

GET /api/users HTTP/1.1

GET /api/session HTTP/1.1

GET /api/products HTTP/1.1

POST /api/login HTTP/1.1

POST /api/login HTTP/1.1

POST /api/data HTTP/1.1

Caso 1: Documentos digitales

Por ejemplo, en procesos de contratación pública como las licitaciones, los documentos digitales bajo análisis suelen ser estudios de mercado, cuadros comparativos, propuestas, informes, actas, resoluciones o archivos firmados. Estos elementos pueden ser objeto de alteraciones mediante cambios en el contenido, modificación de fechas, eliminación de metadatos, inserción de firmas falsas o manipulación de cláusulas.

Cuando se cuenta con el soporte original donde el documento fue creado o almacenado, la pericia permite evaluar con mayor precisión su autenticidad e integridad. En cambio, cuando no se dispone de ese origen, el análisis se orienta a identificar posibles señales de

edición, manipulación o inconsistencias técnicas a través de la revisión exhaustiva de metadatos, firmas digitales, marcas de tiempo, estructura interna, valores hash y la trazabilidad del documento.

Caso 2: Imágenes

Una imagen objeto de peritaje puede provenir de un teléfono celular, una cámara fotográfica, un dron, un sistema de videovigilancia, un escáner, un satélite u otro dispositivo de captura. El análisis forense de estos archivos es de gran utilidad para contribuir con la identificación de personas, placas vehiculares, objetos, armas, escenarios geográficos o posibles signos de manipulación digital.

En la actualidad, la mayoría de los hechos delictivos dejan algún tipo de rastro digital, los cuales pueden constituir indicios o evidencias tangibles. Estos rastros se alojan en documentos, imágenes, videos, audios, metadatos, registros de sistemas, comunicaciones ...

Cuando se dispone del dispositivo original, la pericia evalúa la autenticidad e integridad de la imagen mediante el examen de sus metadatos, la estructura del archivo, los parámetros de captura y su consistencia técnica. Si no se conoce el medio de origen, el análisis se enfoca en detectar indicios de edición, montaje, recortes, compresión anómala, alteración de metadatos o clonación de zonas, incluyendo la revisión profunda de los datos EXIF y, cuando corresponda, los datos de geolocalización.

Caso 3: Video

El análisis forense de video se asemeja al de las imágenes, pero este estudia una secuencia continua de fotogramas que puede incluir audio, metadatos, marcas temporales y datos específicos de codificación. Su utilidad y nitidez dependen de factores como el dispositivo de grabación, la resolución, la tasa de fotogramas, el códec empleado, el nivel de compresión, la iluminación y la estabilidad de la cámara.

Este análisis es clave para identificar personas, vehículos, placas, rutas de escape, dinámicas de accidentes, hechos registrados por cámaras de seguridad o posibles manipulaciones. Cuando se cuenta con el dispositivo original o el sistema grabador (DVR/NVR), es posible realizar una evaluación más sólida. Si solo se dispone de una



Ilustración: IA — Copilot, prompt y edición Kelly Vásquez Chaparro

copia exportada, enviada por mensajería o descargada de una plataforma virtual, la pericia se orienta a detectar signos de edición, cortes, pérdida de continuidad o manipulación mediante la revisión minuciosa de fotogramas, metadatos, la línea de tiempo y la sincronización entre el audio y el video.

Caso 4: Audios

El análisis forense de audios es uno de los más complejos debido a que no solo se evalúa el contenido audible, sino también la estructura técnica de la señal, su continuidad, calidad, frecuencia, ruido, posibles cortes, superposiciones,

ediciones y las características del dispositivo de grabación.

En una pericia de audio se analizan la temporalidad, el oscilograma, el espectrograma, la frecuencia, la intensidad, los silencios, los ruidos de fondo, el formato y la presencia de alteraciones.

- El oscilograma es la representación gráfica de la señal sonora en función del tiempo. Este permite observar la amplitud de la onda, los silencios, los cortes abruptos, las variaciones de intensidad, las saturaciones y las posibles discontinuidades.

- El espectrograma es la representación visual de las frecuencias que componen el sonido a lo largo del tiempo. Su análisis permite identificar patrones de voz, ruidos de fondo, cambios en el ambiente acústico, empalmes, interferencias o alteraciones que no son evidentes para el oído humano.

Cuando se conoce el medio de grabación original, se realiza una pericia de autenticidad e integridad para determinar si el audio corresponde al dispositivo indicado y si mantiene continuidad técnica. Cuando no se cuenta con el dispositivo original o solo se dispone de una copia, la pericia se orienta al análisis de edición, manipulación, cortes, empalmes o alteraciones de la señal.

Caso 5: Código fuente y software

El código fuente también constituye una evidencia digital relevante cuando está relacionado con delitos de fraude, sabotaje, malware, manipulación de sistemas, alteración de bases de datos, robo de información o afectación de servicios digitales.

Su análisis puede ser estático, cuando se revisa el código lineal sin ejecutarlo, o dinámico, cuando se evalúa el comportamiento del software en pleno funcionamiento. En sistemas

críticos, este examen se complementa con la revisión de dependencias, configuraciones, registros de actividad (logs), pruebas de seguridad autorizadas y la verificación de integridad de los archivos.

Este tipo de análisis permite identificar funciones maliciosas, credenciales expuestas o insertadas directamente en el código, validaciones débiles, fallas en el control de acceso, dependencias vulnerables, scripts, instaladores o componentes alterados. En plataformas sensibles —como las electorales, financieras, sanitarias o gubernamentales— resulta una labor clave para proteger la integridad, disponibilidad, confidencialidad y trazabilidad de la información institucional.



Ilustración: IA — Gemini IA, prompt y edición Kelly Vásquez Chaparro

Caso 6: Datos satelitales y geolocalización

Los datos satelitales y de geolocalización son fundamentales para estimar la ubicación, el desplazamiento, la permanencia o la proximidad de una persona, vehículo, dispositivo u objeto de interés criminal.

Las coordenadas geográficas (latitud y longitud) pueden adquirirse de teléfonos celulares, sistemas GPS de vehículos, relojes inteligentes, drones, antenas de telecomunicaciones, servicios en la nube o imágenes satelitales. Su análisis pericial permite determinar la ubicación aproximada del dispositivo, así como establecer si estuvo en movimiento o reconstruir su trayectoria.

Caso 7: Registros, logs y eventos del sistema

Los logs o registros de eventos son una fuente esencial de evidencia digital, ya que permiten reconstruir cronológicamente las acciones realizadas en un sistema, los accesos de usuarios,

los errores generados, los cambios de configuración, las conexiones remotas, las operaciones administrativas, las transferencias de archivos y los eventos de seguridad.

En investigaciones de ciberseguridad, fraude o manipulación de sistemas, los logs de los eventos y determinar, con base en los registros disponibles, qué ocurrió, cuándo ocurrió, desde dónde ocurrió y qué usuario o proceso automatizado estuvo involucrado. Estos registros pueden provenir del sistema



Ilustración: IA — Gemini IA, prompt y edición Kelly Vásquez Chaparro



operativo, aplicaciones, servidores web, bases de datos, mecanismos de autenticación, cortafuegos (firewalls), proxies, redes virtuales privadas (VPN), sistemas EDR, registros de auditoría o eventos de creación, modificación y eliminación de archivos.

Caso 8: Casos complejos

Los casos complejos son aquellos en los que la evidencia digital no se limita a un solo archivo o dispositivo, sino que involucra infraestructuras tecnológicas completas: código fuente, bases de datos, redes de comunicación, usuarios, procesos, controles de seguridad, registros de auditoría y procedimientos operativos interactuando entre sí.

Un ejemplo de este tipo de complejidad es la Solución Tecnológica de Apoyo al Escrutinio (STAE), utilizada por la Oficina Nacional de Procesos Electorales (ONPE) en determinados procesos y ámbitos electorales. Al tratarse de una solución tecnológica de apoyo a un proceso crítico para la democracia su evaluación forense y de seguridad no debe limitarse únicamente al funcionamiento visible del sistema, sino que debe considerar la seguridad desde el diseño, la implementación, la ejecución y la operación general. En sistemas de esta naturaleza, pueden aplicarse distintas metodologías y pruebas de seguridad, cada una con un propósito específico:

a) **Modelado de amenazas (Threat Modeling):** Debe aplicarse antes o durante el diseño del sistema. Su finalidad es identificar, desde etapas tempranas, los activos críticos, los posibles atacantes, las rutas de ataque, los puntos débiles del diseño y los controles necesarios para reducir riesgos. En un sistema como el STAE, esta técnica permite responder a preguntas críticas: ¿qué activos deben protegerse?, ¿qué pasaría si se clona un dispositivo autorizado?, ¿qué controles impiden la ejecución en equipos no permitidos?, ¿qué componentes requieren firma digital o validación criptográfica?, y ¿qué eventos deben quedar registrados para garantizar la trazabilidad? El modelado de amenazas es netamente preventivo; su objetivo no es explotar vulnerabilidades, sino anticiparlas antes de que el sistema sea construido o desplegado.

Los casos complejos son aquellos en los que la evidencia digital no se limita a un solo archivo o dispositivo, sino que involucra infraestructuras tecnológicas completas.

b) **Prueba estática de seguridad de aplicaciones (SAST):** Se utiliza cuando se cuenta con el acceso al código fuente, los binarios o los artefactos de desarrollo. No requiere ejecutar la aplicación debido a que analiza la estructura interna del software. Sirve para detectar problemas como contraseñas, claves o tokens expuestos dentro del código, validaciones incompletas, uso inseguro de archivos, falta de control de acceso, dependencias vulnerables, funciones peligrosas, errores lógicos de seguridad, controles deshabilitados o condicionados por variables internas, rutas inseguras o la posibilidad de escritura fuera de los directorios autorizados. En un sistema crítico, el SAST permite identificar debilidades antes de que el software sea instalado o usado en producción. Sin embargo, su limitación radica en que no siempre demuestra el impacto real de la vulnerabilidad, por lo que debe complementarse con pruebas dinámicas.

c) **Prueba dinámica de seguridad de aplicaciones (DAST):** Se emplea cuando la aplicación ya se encuentra en plena ejecución. A diferencia del SAST, no revisa directamente el código fuente, sino el comportamiento externo del

sistema frente a estímulos. Sirve para detectar fallas de autenticación, omisión de controles, inyección SQL o inyección de comandos, exposición de información sensible, configuraciones inseguras, errores en el manejo de sesiones, respuestas inseguras del sistema, comportamientos no previstos frente a entradas manipuladas o la aceptación de dispositivos, archivos o credenciales no autorizadas. En un caso como el STAE, una prueba dinámica permite verificar si el sistema realmente valida el entorno, si rechaza dispositivos no autorizados,

si registra eventos críticos, si impide operaciones indebidas y si mantiene la integridad de todo el flujo operativo.

d) Prueba de penetración (Pentesting):

Es una prueba de intrusión autorizada y controlada que permite comprobar si una vulnerabilidad detectada puede ser explotada en un sistema real y cuál sería su impacto efectivo. Se aplica cuando el sistema ya está en funcionamiento y busca determinar si un atacante real podría ingresar, alterar datos, evadir controles, escalar privilegios o comprometer la confiabilidad,



integridad y disponibilidad de la información, o incluso modificar, borrar o sustituir evidencia digital. Esta prueba incluye actividades de reconocimiento, análisis de la superficie de ataque, enumeración de servicios, pruebas de autenticación, explotación controlada, escalamiento de privilegios y recomendaciones de mitigación. A diferencia del SAST o el DAST, el pentesting no solo identifica las vulnerabilidades de forma teórica, sino que demuestra de manera práctica qué ocurriría si estas fueran aprovechadas por un ciberdelincuente.

- e) **Hacking ético:** Es una prueba integral y expresamente autorizada por una determinada institución que busca identificar vulnerabilidades en sistemas, redes, aplicaciones, procesos o infraestructuras bajo estrictos criterios técnicos, legales y éticos. Puede incluir la ejecución coordinada de pruebas de penetración, simulaciones de ataques y defensas mediante equipos especializados (Red Team, Blue Team, Purple Team) y la revisión exhaustiva de las políticas de seguridad de la información de la entidad, entre otros parámetros estratégicos.

EL PERITAJE FORENSE DIGITAL EN LA INVESTIGACIÓN PENAL

Ante esta migración delictiva hacia el ciberespacio, la criminalística ha tenido que evolucionar drásticamente. Es aquí donde el análisis forense digital adquiere un rol protagónico en el marco del proceso penal peruano. Esta disciplina técnico-científica no se limita a revisar un teléfono o encender una computadora; consiste en la aplicación de metodologías rigurosas para la identificación, recolección, adquisición, preservación, análisis e interpretación de la evidencia digital. El objetivo final es garantizar que la información extraída mantenga su integridad y fidelidad de tal manera que pueda ser admitida como prueba válida en un juicio oral.

El perito informático se enfrenta a un desafío contrarreloj. Los datos digitales son volátiles por naturaleza: un mensaje puede ser borrado de forma remota en segundos.

En la práctica, cuando la Policía Nacional del Perú (PNP) o el Ministerio Público intervienen en la escena de un crimen —sea un caso de corrupción, crimen organizado o extorsión—, el perito informático se enfrenta a un desafío contrarreloj. Los datos digitales son volátiles por naturaleza: un mensaje puede ser borrado de forma remota en segundos, un disco duro puede ser encriptado o la memoria RAM de un servidor puede borrarse al apagar el equipo. Por ello, el análisis forense digital se rige por estándares internacionales estrictos para asegurar la cadena de custodia.

Un concepto fundamental en nuestro trabajo es el principio de mismidad, el cual garantiza que la evidencia digital presentada ante el juez sea exactamente la misma que se recolectó en la escena del delito o el entorno virtual, sin haber sufrido alteraciones, modificaciones o contaminaciones durante su traslado o análisis en el laboratorio. Para asegurar este principio, los peritos utilizamos funciones criptográficas conocidas como algoritmos hash (como el MD5 o SHA-256), los cuales generan una «huella digital» única para cada archivo o soporte de almacenamiento. Si un solo bit de la información original cambia, el valor hash se modifica por completo, alertando sobre una manipulación de la prueba.

ESTÁNDARES INTERNACIONALES Y EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL

Para que las conclusiones de un peritaje informático resistan el cuestionamiento de las partes en un tribunal, el proceso pericial debe seguir procedimientos técnicamente verificables y reproducibles, cuando corresponda. Por ello, la informática forense se rige a nivel global por los estándares internacionales desarrollados por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. Entre ellos, destacan la norma ISO/IEC 27037:2012, que establece las directrices fundamentales para la identificación, recolección, adquisición y preservación de la evidencia digital, y la norma ISO/IEC 27042:2015, enfocada en los lineamientos metodológicos para el análisis y la interpretación de los datos extraídos.

La adopción de estos estándares y sus diversas actualizaciones es la garantía de que un perito en Lima, en el Callao o en cualquier región del país actúe bajo los mismos principios técnicos que se emplean en los laboratorios forenses más avanzados del mundo.



se suma hoy una herramienta revolucionaria: la Inteligencia Artificial. La IA está transformando el análisis forense digital al automatizar el procesamiento de volúmenes masivos de datos que antes tomaba semanas examinar. En la actualidad, los algoritmos avanzados permiten realizar búsquedas semánticas profundas, correlacionar eventos temporales entre múltiples dispositivos, detectar patrones de comunicación en redes criminales e identificar de forma automatizada imágenes o videos potencialmente vinculados a delitos graves.

El potencial de esta tecnología en el ámbito pericial es tan amplio que ya se encuentra contemplado en la Estrategia Nacional de Inteligencia Artificial 2026-2030, liderada por la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros (PCM). Este documento destaca la importancia de incorporar la IA para fortalecer las capacidades analíticas y predictivas del Estado, lo que abre nuevas posibilidades para la modernización de la investigación criminal y del sistema de justicia

DIAGNÓSTICO NACIONAL: RETOS Y MARCO LEGAL EN EL PERÚ

A pesar de la disponibilidad de herramientas tecnológicas de vanguardia y estándares internacionales claros, la realidad operativa en el Perú presenta desafíos estructurales complejos. Según el Informe Defensorial N.º 001-2023-DP/ADHPD de la Defensoría del Pueblo, titulado «La ciberdelincuencia en el Perú: Estrategias y retos del Estado», las unidades especializadas en investigación de delitos informáticos enfrentan severas limitaciones. Entre las principales brechas destacan la escasez de recursos humanos altamente especializados, la insuficiencia de laboratorios equipados con software forense licenciado de última generación y las demoras burocráticas para obtener información oportuna de entidades tanto públicas como privadas.

Frente a este panorama, el marco normativo peruano ha buscado adaptarse a las demandas del ciberespacio. La columna vertebral de esta lucha es la Ley N.º 30096 (Ley de Delitos Informáticos), cuyo objeto central es prevenir y sancionar las conductas ilícitas cometidas mediante el uso de las tecnologías de la información y comunicación. Esta ley

no solo busca proteger la integridad de los sistemas y los datos informáticos, sino también salvaguardar otros bienes jurídicos penalmente relevantes pueden verse vulnerados mediante el uso de estas tecnologías, como la indemnidad sexual, el patrimonio y la fe pública.

La lección que nos deja el avance de la criminalidad informática es clara: el delito ya no se limita a las fronteras de la calle física. La seguridad ciudadana del siglo XXI requiere de un Estado interconectado, con peritos forenses digitales fortalecidos y equipados con tecnología de IA, capaces de convertir los rastros invisibles de los bits en evidencias evidencia digital técnicamente sustentada para la justicia.

Referencias bibliográficas

Defensoría del Pueblo (2023). La ciberdelincuencia en el Perú: Estrategias y retos del Estado (Informe Defensorial N.º 001-2023-DP/ADHPD). Lima: Defensoría del Pueblo.

International Organization for Standardization & International Electrotechnical Commission (2015). ISO/IEC 27042:2015: Information technology—Security techniques—Guidelines for the analysis and interpretation of digital evidence. Ginebra: ISO.

Nessi, A. M. (2017). *Manual de evidencia digital*. American Bar Association Rule of Law Initiative; Proyecto de Apoyo al Sector Justicia.

Presidencia del Consejo de Ministros (2026). Estrategia Nacional de Inteligencia Artificial 2026-2030. Lima: Secretaría de Gobierno y Transformación Digital.

International Organization for Standardization & International Electrotechnical Commission. (2012). Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO/IEC 27037:2012). International Organization for Standardization.

Oficina Nacional de Procesos Electorales. (2026). Solución Tecnológica de Apoyo al Escrutinio (STAE).

OWASP Foundation. (2020). OWASP Web Security Testing Guide

EL DELITO YA NO ESTÁ SOLO EN LA CALLE: ANÁLISIS FORENSE DIGITAL FRENTE AL CRIMEN INFORMÁTICO EN EL PERÚ



El delito tradicional se ha adaptado a los entornos digitales mediante el uso de herramientas informáticas.



*El análisis forense digital convierte rastros tecnológicos **en evidencia legal bajo estricta cadena de custodia.***



*Las pericias especializadas analizan la autenticidad de archivos **mediante metadatos, oscilogramas y espectrogramas.***



*Para evaluar sistemas complejos **se aplican metodologías rigurosas como Threat Modeling, SAST y DAST.***



*En el Perú, las denuncias por ciberdelitos ante la Policía Nacional **se cuadruplicaron entre 2018 y 2021.***

CIENCIA Y SOCIEDAD

ANÁLISIS Y PREDICCIÓN DE DELITOS - LIM

MUNTING PATTERN: SL AGUSTINO

UNIDAD DE INTELIGENCIA
DE DATOS Y ANALISIS
CRIMINAL

DATA CRIM: UNA POTENTE HERRAMIENTA PARA LA LUCHA CONTRA EL CRIMEN

Aníbal Sánchez Aguilar

En la sociedad actual, los problemas que afectan a los ciudadanos se tornan cada vez más complejos y difíciles de abordar. Sus soluciones requieren el respaldo estratégico de la tecnología, las comunicaciones y los sistemas de información, los cuales constituyen herramientas excepcionales para la toma de decisiones informadas y basadas en evidencia. En múltiples ocasiones, estos sistemas han garantizado el éxito en la gestión de la problemática tanto en el ámbito público como en el privado.

Al permitir la recolección, procesamiento, sistematización e integración de ingentes cantidades de datos provenientes de múltiples fuentes, los sistemas de información ponen a disposición de los usuarios —incluso en tiempo real— alertas e indicadores valiosos. Esta información optimiza los procesos de administración, seguimiento y monitoreo en el cumplimiento de objetivos y metas de las políticas públicas, elevando la productividad y reduciendo significativamente la incertidumbre.



En la actualidad, estos sistemas de información estadística se nutren de tecnología de vanguardia y de la inteligencia artificial (IA), convirtiéndose en herramientas imprescindibles para solucionar las crisis estructurales de los países. El aprovechamiento de la IA brinda notables ventajas: ayuda a depurar, validar y analizar grandes volúmenes de datos, lo que reduce el margen de error humano y permite obtener estadísticas de alta calidad. Asimismo, facilita la identificación de patrones y tendencias que hacen posible predecir las zonas y los horarios de mayor incidencia delictiva, e incorpora recursos como los chatbots inteligentes para agilizar el acceso ciudadano a la información.

Al respecto, la Comisión Económica para América Latina y el Caribe (CEPAL) define a los sistemas estadísticos de seguridad pública como el «conjunto de información estadística en la materia, misma que, para el proceso de producción, manejo, análisis y difusión, requiere de la interacción de instituciones y organismos que se encuentran vinculados entre sí». Por su parte, el Banco Interamericano de Desarrollo (BID) precisa que los sistemas de información permiten tomar decisiones desde una perspectiva

técnica en esferas independientes de la administración pública, abarcando tres ámbitos esenciales: administración, planificación e investigación en políticas públicas.

De este modo, estas plataformas son de utilidad en los diferentes momentos del proceso de las políticas públicas, desde su identificación, planificación y diseño, hasta su implementación y evaluación. No obstante, para asegurar la calidad de los registros de información estadística, la Oficina de las Naciones Unidas (2014) destaca que se deben cumplir criterios rigurosos: la integración de distintas fuentes de información, la oportunidad y la credibilidad de los datos para facilitar la recolección y lograr legitimidad, y el aseguramiento de su sostenibilidad financiera.

El aprovechamiento de la IA brinda notables ventajas: ayuda a depurar, validar y analizar grandes volúmenes de datos, lo que reduce el margen de error humano y permite obtener estadísticas de alta calidad.

¿CUÁNDO SURGE EL DATA CRIM Y CUÁLES SON SUS POTENCIALIDADES?

En ese marco, a inicios de 2016, el Instituto Nacional de Estadística e Informática (INEI) —institución que preside el Comité Estadístico Interinstitucional de la Criminalidad (CEIC), órgano de apoyo al Consejo Nacional de Política Criminal (CONAPOC)— destacó a un equipo multidisciplinario compuesto por estadísticos, cartógrafos e informáticos para diseñar una plataforma digital donde confluya la información estadística del Estado en materia del delito, el delincuente y la pena. El reto consistía en cruzar bases de datos administrativas con mapas detallados de todo el territorio nacional. Para lograrlo, se integró la información de las instituciones que conforman el Sistema de Justicia Penal: el Poder Judicial, el Ministerio Público, la Policía Nacional del Perú (PNP), el Ministerio de Justicia y Derechos Humanos, el Instituto Nacional Penitenciario (INPE) y el propio INEI, que incluyó los datos recogidos a través de sus encuestas periódicas, logrando así unificar un «mismo lenguaje» estadístico.

De esta forma, en agosto de ese mismo año, se realizó la primera

presentación del Sistema Integrado de Estadísticas de la Criminalidad y Seguridad Ciudadana (DATA CRIM). Esta plataforma se convirtió, por un lado, en una herramienta estratégica para combatir el delito y, por el otro, en un hito para la estandarización estadística mediante el uso de definiciones, códigos y nomenclaturas comunes. Lo más importante fue su capacidad para impulsar la integración y coordinación de la información sobre justicia entre las distintas entidades del Estado. Su creación, a iniciativa del INEI, ha significado un paso sustantivo en línea con la innovación científico-técnica en materia estadística.

Otro atributo fundamental de DATA CRIM es la integración de la información geoespacial con la analítica estadística. Esto posibilita una visión panorámica del territorio y de los fenómenos sociales y económicos que ocurren en él, lo que permite focalizar el accionar del Estado, optimizar las intervenciones y generar un ahorro significativo de recursos. La información del sistema permite conocer al detalle las características y comportamientos de la actividad delictiva en las diversas regiones del país. Gracias a este diagnóstico actualizado por modalidad delictiva y ámbito territorial, las autoridades pueden evaluar los impactos sociales

y económicos, así como el nivel de afectación a la población, respaldando con eficacia el diseño de las políticas públicas contra el crimen.

En la práctica, la plataforma traduce la complejidad de los datos a través de un «mapa de calor» que señala visualmente las zonas con mayor y menor incidencia delictiva (indicadas generalmente en rojo y verde). El sistema permite visualizar datos actualizados sobre robos, hurtos

y otros delitos cometidos en calles y avenidas específicas. Asimismo, incluye la ubicación de las comisarías más cercanas como puntos de auxilio rápido para el ciudadano y facilita a investigadores y autoridades el acceso a estadísticas consistentes y confiables. Debido a este impacto, en el año 2017, el sistema ganó el premio especial a la mejor práctica en la categoría de Datos Abiertos en la Gestión Pública, otorgado por la organización Ciudadanos al Día.



Ceremonia de entrega del premio a las Buenas Prácticas en Gestión Pública 2017, galardón obtenido por el desarrollo de DATA CRIM.

CARACTERÍSTICAS Y MÓDULOS DEL SISTEMA

DATA CRIM¹ es un sistema pionero y perfectible que promueve la normatividad e interoperabilidad entre los distintos sistemas de información sectorial.

La plataforma integra fuentes clave como los registros policiales, fiscales, judiciales y penitenciarios, además de las encuestas de victimización del

¹ <https://datacrim.inei.gob.pe>

INEI e indicadores socioeconómicos sobre pobreza, vivienda, negocios y distribución poblacional. Si bien el sistema se encuentra activo y plenamente funcional, requiere de actualización constante, sostenibilidad financiera y un marco legal que garantice la obligatoriedad de la transferencia de datos por parte de los sectores involucrados para elevarlo hacia una plataforma tecnológica mucho más moderna y escalable.

Para facilitar la experiencia del usuario, la página principal cuenta con tres módulos de consulta especializados:

i) Módulo Ciudadanos: Permite a cualquier persona que se desplace por el entorno urbano conocer la ubicación de las comisarías, así como la densidad y el tipo de delitos que ocurren en las cuadrículas de sus calles y avenidas. Además, habilita una opción para que el ciudadano reporte incidencias de las que sea protagonista o testigo.

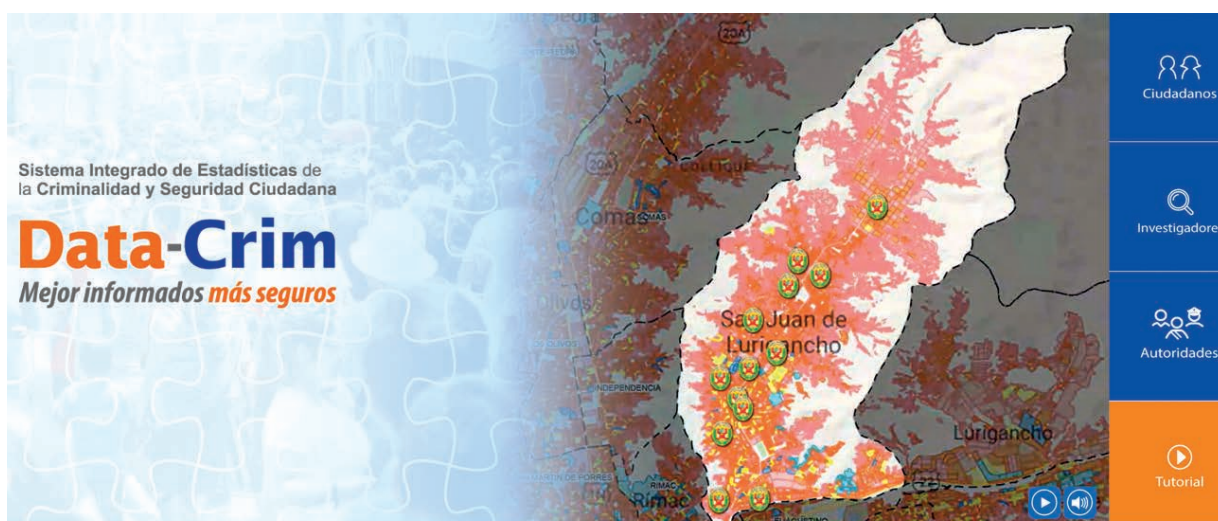
ii) Módulo Investigadores: Da acceso al núcleo analítico del sistema. Permite navegar por todo el índice temático de los sectores comprometidos, consultar la información histórica del INEI y acceder a diferentes capas de frecuencias delictivas, mapas de calor



y variables demográficas, herramientas indispensables para estudios de correlación y focalización criminal.

iii) Módulo de Autoridades: Diseñado para que los distintos sectores carguen su información estadística, compartan

datos y enriquezcan la plataforma, consolidándose como el principal medio de estandarización informativa del Estado en materia de seguridad.

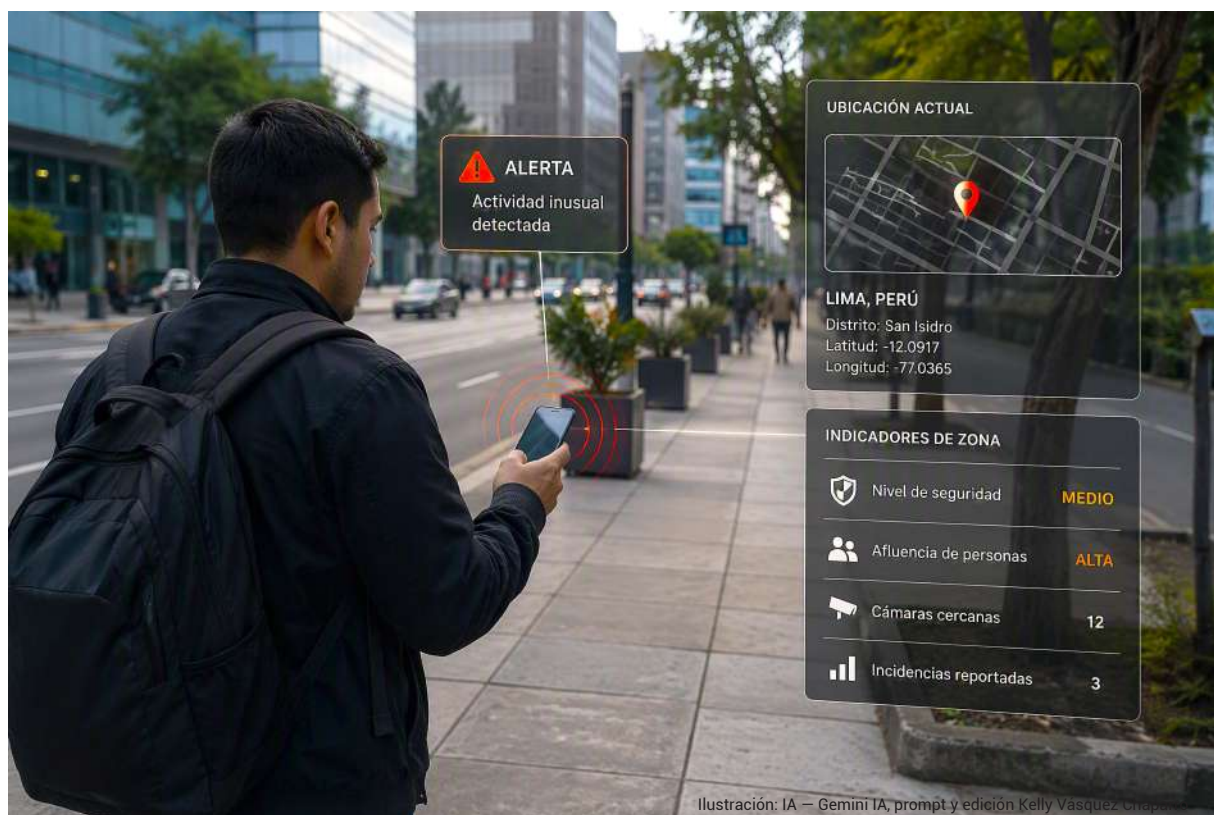


EL PROBLEMA PÚBLICO

A pesar del sostenido crecimiento económico que ha registrado el Perú en las últimas tres décadas, el país aún arrastra graves problemas estructurales que limitan la construcción de una sociedad pacífica, equitativa y con oportunidades reales en salud, educación y empleo. Hoy en día, la corrupción y la delincuencia se erigen como los dos principales desafíos nacionales según la percepción ciudadana. De acuerdo con los datos del segundo semestre del año 2025, el 60,3 % de la población identifica a la corrupción como la mayor problemática

del país, seguida de cerca por la delincuencia con un 53,7 %. En menores porcentajes, los ciudadanos señalan factores conexos como la pobreza, el desempleo, los bajos sueldos, el alza del costo de vida y la deficiente calidad de la educación pública.

Las cifras asociadas a la inseguridad ciudadana son alarmantes: durante el año 2025, el 83,9 % de los peruanos mayores de 15 años manifestó una alta percepción de inseguridad en su vida cotidiana. Asimismo, el 57,9 % declaró sentir temor de caminar a solas por su barrio durante la noche, mientras que la tasa de victimización efectiva alcanzó



al 25,2 % de la población urbana, consolidando un escenario donde uno de cada cuatro ciudadanos ha sido víctima directa de un delito.

La delincuencia común y el crimen organizado no solo quiebran la tranquilidad pública a nivel nacional, sino que golpean severamente la economía de los hogares y los negocios. Los ataques extorsivos han proliferado con especial crueldad contra los pequeños emprendedores y los comercios locales de los sectores más vulnerables,

sembrando muerte y desazón. Según registros de la Policía Nacional del Perú, las denuncias por extorsión —una de las modalidades delictivas de mayor crecimiento— ascendieron a 25 585 durante el año 2025, lo que representa un incremento exponencial del 62,6 % en los últimos cuatro años. Detrás de esta ola de extorsiones se articulan otros delitos graves como la intimidación, el sicariato y las muertes violentas, que exhiben un alto grado de ferocidad principalmente en Lima Metropolitana y en las grandes ciudades de la costa peruana.

Radiografía de la Inseguridad en el Perú (2024-2025)

- 83,9 % de percepción de inseguridad
- 25,2 % de tasa de victimización urbana
- 75 % de aumento en la tasa de homicidios (2020-2024)
- 25 585 denuncias por extorsión en 2025

Debido a esta dinámica violenta, la tasa de homicidios en el Perú ha experimentado un crecimiento crítico en el último lustro. El índice pasó de 6 muertes por cada cien mil habitantes en el año 2020 a 10 muertes por cada cien mil habitantes en el 2024; un incremento del 75,0 % que, en otros contextos de

la región, habría encendido alarmas internacionales de emergencia. Sin embargo, la persistencia y la rutina diaria del crimen han provocado que este aumento de la violencia criminal pase casi desapercibido en la agenda pública.

La gravedad del escenario se explica por la presencia activa de organizaciones criminales transnacionales cuyas operaciones trascienden nuestras fronteras y afectan a múltiples naciones de América Latina, desde México, Brasil y Colombia, hasta Ecuador, Chile y el Perú. Al respecto, la experta Lucía Dammert señala en uno de sus estudios sobre la materia:

«El crimen organizado se ha convertido en el problema de seguridad más grave de la región, no solo por los altos niveles de violencia que trae aparejados, posicionando a América Latina como la región sin conflictos

Las cifras asociadas a la inseguridad ciudadana son alarmantes: durante el año 2025, el 83,9 % de los peruanos mayores de 15 años manifestó una alta percepción de inseguridad en su vida cotidiana. Asimismo, el 57,9 % declaró sentir temor de caminar a solas por su barrio durante la noche.

bélicos más violenta del mundo, sino también por la aparición de espacios de gobernanza criminal que no hacen más que poner de manifiesto la debilidad de los Estados latinoamericanos» (Dammert y Sampó, 2025)

Esta proliferación delictiva se ha consolidado frente a la ineficacia de las políticas públicas tradicionales. Por ejemplo, la extracción ilegal de oro no solo alimenta las redes criminales, sino que destruye la biodiversidad y contamina los ríos de la Amazonía, comprometiendo la sostenibilidad ambiental y el futuro de las próximas generaciones. Ante esta realidad, resulta imperativo diseñar y ejecutar estrategias de seguridad basadas en evidencia científica, donde plataformas como el Sistema Integrado DATA CRIM sirvan de soporte para devolverle la eficiencia al Estado en su lucha por disminuir la victimización de la ciudadanía.

EL FRACASO DE LAS POLÍTICAS PÚBLICAS Y LA INESTABILIDAD INSTITUCIONAL

Si algo ha caracterizado al Perú en la última década es la profunda inestabilidad política que ha fracturado



Esta proliferación delictiva se ha consolidado frente a la ineficacia de las políticas públicas tradicionales.

la continuidad de sus instituciones. La sucesión de ocho presidentes de la República en diez años es la expresión más aguda de una crisis democrática que, si bien coexiste con un relativo crecimiento económico, impide consolidar políticas públicas eficientes para abordar problemas estructurales. Esta preocupante realidad se refleja con nitidez en el sector seguridad: el hecho de que veinte ministros del Interior hayan jurado en los últimos cinco años evidencia la imposibilidad de darle sostenibilidad a los planes contra el crimen, mantener activa la logística necesaria para el accionar del Estado y evitar la alta rotación de funcionarios que paraliza los programas sectoriales.

En el combate al delito interviene un engranaje complejo de instituciones que conforman el Sistema de Justicia Penal: el Poder Judicial, el Ministerio Público, el Ministerio del Interior, la Policía Nacional del Perú, el Ministerio de Justicia y Derechos Humanos, y el Instituto Nacional Penitenciario (INPE). No obstante, todas estas entidades operan con severas carencias presupuestales y sin una visión conjunta e integral del problema; actúan, en muchas circunstancias, como islas ajenas a una estrategia común y a

una visión compartida. Para diseñar políticas efectivas, es indispensable analizar el fenómeno criminal de forma integral y lineal, lo que exige información rigurosa sobre las características del delito, sus dimensiones territoriales, las motivaciones de los infractores, el entorno social, el perfil de las víctimas que claman justicia y los impactos socioeconómicos que el crimen genera.

Un reflejo crítico de esta falta de articulación se observa en la política penitenciaria, cuya misión constitucional orientada a la rehabilitación e integración social se encuentra severamente mermada. A inicios de 2026, el hacinamiento penitenciario en las cárceles del país ascendió al 128 %, registrando una sobrepoblación del 148 % según las últimas cifras del INPE. Esta alarmante saturación demuestra que la capacidad de albergue en los penales no ha crecido en la misma proporción que la criminalidad. Asimismo, los recursos humanos, la logística y el cuerpo de agentes penitenciarios necesarios se encuentran desbordados al no haberse duplicado para equiparar la demanda, una crisis estructural que se ve agudizada por focos de corrupción interna que urgen una reforma integral del sistema de justicia.

EL CONOCIMIENTO ESTADÍSTICO COMO PILAR ESTRATÉGICO CONTRA EL CRIMEN

Ante este complejo panorama, las políticas de seguridad ciudadana no pueden seguir guiándose por la improvisación; requieren de manera mandatoria evidencia empírica e información estadística oportuna, de calidad y georreferenciada. Un sistema de información efectivo e integral resulta vital para suministrar los insumos necesarios en el desarrollo de planes estratégicos, un rol fundamental que

hoy cumple la plataforma DATA CRIM. Este enfoque se alinea con los principios de buena gobernanza en las políticas de seguridad y justicia promovidos por el BID: coordinación, integralidad, transversalidad, corresponsabilidad y focalización.

Hace más de cuatro siglos, el filósofo Francis Bacon acuñó la célebre máxima «la información es poder». En la actual era de la inteligencia artificial, esta frase cobra una vigencia renovada, prefigurando la trascendencia de los datos estadísticos para generar conocimiento y estructurar herramientas sutiles y potentes capaces de abordar



Ilustración: IA — Gemini IA, prompt y edición Kelly Vásquez Chaparro

las problemáticas sociales. Disponer de información oportuna democratiza el conocimiento, mitiga los riesgos, eleva las capacidades del recurso humano y optimiza la toma de decisiones estratégicas ante el control de las crisis.

Finalmente, el desarrollo del Sistema Integrado DATA CRIM ha establecido un valioso canal de cooperación interinstitucional dentro de la administración pública peruana. Sin importar el nivel de desarrollo tecnológico de cada sector, la plataforma propicia el uso de estándares abiertos y aplicaciones tecnológicas de vanguardia para construir estadísticas de criminalidad en tiempo real. Al adoptar un marco conceptual común, normalizar los registros y visibilizar la trazabilidad del hecho delictivo — desde la víctima y el delincuente hasta la ejecución de la pena—, el Perú no solo mejora su capacidad de respuesta interna, sino que facilita su comparación internacional. Esto se logra adaptando a nuestra realidad la Clasificación Internacional de Delitos con Fines Estadísticos (ICCS) de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) a través de una tabla de equivalencias con el Código Penal Peruano.

La finalidad suprema de este esfuerzo científico y tecnológico es respaldar políticas públicas eficientes que disminuyan los índices delictivos. Paralelamente, busca apuntalar programas de atención social, educación, salud y empleo enfocados en los segmentos juveniles con mayor vulnerabilidad frente al crimen. Solo a través de datos confiables y transparentes será posible devolverle al ciudadano la confianza en sus instituciones y en los actores esenciales de su seguridad: sus policías, fiscales, jueces y agentes penitenciarios.

Referencias bibliográficas

Banco Interamericano de Desarrollo – BID (2020, marzo). “Líderes para la gestión en Seguridad Ciudadana y Justicia”. Washington D.C.

Comisión Económica para América Latina y el Caribe - CEPAL (2014). Documento conceptual de los sistemas estadísticos de seguridad pública y justicia en los países de América Latina y el Caribe. Conferencia Estadística de las Américas. México, Naciones Unidas, CEPAL y el Centro de Excelencia para Información Estadística de Gobierno, Seguridad Pública, Victimización y Justicia.

Dammert, L. y Sampó, C. (2025, enero). “La evolución del crimen organizado en América Latina”. Friedrich Ebert Stiftung.

Instituto Nacional de Estadística e Informática – INEI (2026, febrero). Informe Técnico: “Percepción Ciudadana sobre la Gobernabilidad, Democracia y Confianza en las Instituciones, julio-diciembre 2025.

Instituto Nacional de Estadística e Informática – INEI (2026, enero). Informe Técnico: “Evolución de la Tasa de Homicidios e Indicadores de Seguridad, 2022-2025.

Ministerio de Justicia del Perú (2013, 22 de octubre). Decreto Supremo N° 013-2013-JUS, que crea el Comité Estadístico Interinstitucional de la Criminalidad (CEIC).

DATA CRIM: UNA POTENTE HERRAMIENTA PARA LA LUCHA CONTRA EL CRIMEN



DATA CRIM integra datos del **Sistema de Justicia Penal** y **mapas para combatir el delito.**



El sistema **une variables geospaciales con estadísticas** para focalizar la acción del Estado.



En el año 2025, **el 53.7% de los peruanos indicó que la delincuencia es el principal problema.**



La tasa de homicidios en el Perú subió drásticamente de **6 a 10 por cada 100 mil habitantes.**



A enero de 2026, **el hacinamiento en los centros penitenciarios del país alcanzó el 128%.**

INVESTIGACIÓN EN EL PERÚ

ECOSISTEMAS DE CONOCIMIENTO PARA LA SEGURIDAD

¿POR QUÉ LA
EVIDENCIA AÚN NO ESTÁ
TRANSFORMANDO
A LA POLICÍA?

Noam López Villanes

Instituto de Analítica Social e Inteligencia Estratégica - Pulso
PUCP

El Perú nunca había contado con tanta información sobre seguridad ciudadana como en la actualidad. Sin embargo, sus instituciones policiales continúan actuando, muchas veces, como si avanzaran a oscuras. Hoy existen encuestas de victimización, observatorios, mapas de calor, centros de comando, plataformas digitales y diagnósticos cada vez más sofisticados. Pese a ello, esta creciente disponibilidad de información no ha logrado consolidar, de manera sostenida, una policía capaz de aprender con la misma rapidez con la que evolucionan los mercados criminales.

Esa es la paradoja que atraviesa este artículo. La evidencia está cada vez más disponible y circula en informes técnicos, discursos públicos y planes de gobierno. Sin embargo, rara vez transforma el núcleo de la organización policial: sus incentivos, sus rutinas, los criterios de mando, los sistemas de información, la coordinación con fiscales y municipios, la forma de evaluar resultados o su relación con la ciudadanía. En muchos países, la evidencia ayuda a comprender mejor el problema, pero no modifica de manera duradera la forma de enfrentarlo.

La tesis que aquí se plantea es que la policía basada en evidencia mantiene plena vigencia científica, pero no puede transformar las instituciones únicamente mediante la acumulación de estudios, datos o herramientas tecnológicas. Para generar cambios sostenibles necesita desarrollarse dentro de verdaderos ecosistemas institucionales de conocimiento, donde confluyan información confiable, capacidades analíticas, mecanismos de evaluación, legitimidad pública y una colaboración permanente con la comunidad académica. Las cámaras de vigilancia, los algoritmos o las bases de datos pueden ser herramientas muy valiosas, pero solo cuando la institución cuenta con la capacidad de interpretarlos, cuestionarlos y aprender de ellos. De lo contrario, la tecnología se convierte en una vitrina, la evidencia en un elemento decorativo y la seguridad en una sucesión de respuestas improvisadas.

CIENCIA APLICADA AL TRABAJO POLICIAL

La idea de aplicar el conocimiento científico al trabajo policial es muy anterior a la inteligencia artificial o a los modernos centros de comando. Se



trata de una tradición intelectual con varias décadas de desarrollo. Uno de sus principales impulsores fue Herman Goldstein (1979, 1990), quien propuso que la policía dejara de organizar su trabajo únicamente en función de los incidentes o de las llamadas de emergencia. Su modelo de policiamiento orientado a problemas cambió el foco de la pregunta: ya no se trataba solo de responder con mayor rapidez, sino de comprender por qué un problema se repetía. El cambio era profundo, pues suponía pasar de una lógica centrada en la reacción inmediata a otra basada en el aprendizaje institucional, capaz de identificar patrones, analizar causas y diseñar respuestas específicas.

Años después, Lawrence Sherman (1998) trasladó esa intuición a un enfoque explícitamente científico mediante el concepto de policía basada en evidencia. Su propuesta era sencilla, aunque exigente: las estrategias policiales debían apoyarse en pruebas que permitieran identificar qué funciona, qué no funciona y qué intervenciones muestran resultados prometedores. La experiencia profesional, el conocimiento del territorio y el criterio operativo seguían siendo indispensables, pero ya no bastaban por sí solos. También era necesario demostrar, mediante evidencia, que las decisiones producían los resultados esperados. De esta manera, la evaluación dejó de ser una

Las cámaras de vigilancia, los algoritmos o las bases de datos pueden ser herramientas muy valiosas, pero solo cuando la institución cuenta con la capacidad de interpretarlos, cuestionarlos y aprender de ellos.

tarea exclusivamente académica para convertirse en un componente esencial de la reforma policial.

Posteriormente, David Weisburd (2015) demostró que el delito no se distribuye de manera uniforme en las ciudades, sino que tiende a concentrarse en determinados lugares. Sus investigaciones sobre la criminología del lugar revelaron que una proporción muy pequeña de calles o microterritorios puede concentrar una cantidad desproporcionada de hechos delictivos. Sobre esa base, Anthony Braga, Andrew Papachristos y David Hureau (2014) mostraron que dirigir recursos policiales hacia estos denominados puntos calientes puede reducir el crimen, siempre que las

intervenciones estén cuidadosamente diseñadas y sean objeto de evaluación. Más adelante, Cynthia Lum y Christopher Koper (2011) contribuyeron a traducir ese conocimiento científico en herramientas útiles para la gestión policial, como la Evidence-Based Policing Matrix, que organiza la evidencia disponible para facilitar la toma de decisiones.

El National Research Council (2004) añadió un elemento fundamental a este enfoque: la eficacia policial no puede analizarse de manera aislada de la legitimidad institucional. Una intervención puede reducir ciertos delitos en el corto plazo y, al mismo tiempo, deteriorar la confianza ciudadana, favorecer abusos o concentrar controles sobre poblaciones vulnerables. En sociedades donde la denuncia depende, en gran medida, de la confianza en las instituciones, la legitimidad adquiere un valor práctico: cuanto mayor es la confianza de la ciudadanía, mayor es también la disposición a colaborar, denunciar y aportar información útil para la prevención y la investigación del delito.

Esta evolución permite comprender una idea central: la evidencia no consiste únicamente en acumular estudios sobre tácticas exitosas. Constituye, sobre todo, una forma de organizar el aprendizaje

institucional. Cuando el ciclo que va desde la identificación del problema hasta el diagnóstico, la intervención, la evaluación y la posterior mejora de las políticas no llega a completarse, la evidencia termina reducida a un lenguaje moderno que sigue sustentando prácticas tradicionales.

LA EVIDENCIA EN LOS ESTUDIOS POLICIALES

La segunda lección es que la focalización puede dar buenos resultados, aunque exige mucho más que incrementar la presencia policial en una zona crítica. Diversos estudios sobre los llamados puntos calientes muestran que intervenir en lugares donde el delito se concentra puede reducir su incidencia, siempre que exista un diagnóstico adecuado, supervisión constante y mecanismos de evaluación. La guía elaborada por Chainey, Alvarado y Serrano (2024) para el Banco Interamericano de Desarrollo actualiza esta evidencia para América Latina y el Caribe, y subraya la importancia de trabajar con método, realizar un seguimiento permanente y evaluar posibles efectos, como el desplazamiento del delito hacia otras zonas. Una presencia policial ocasional o improvisada difícilmente puede

considerarse una estrategia basada en evidencia. Lo determinante es el diseño de la intervención: definir con claridad qué problema se busca resolver, qué recursos se utilizarán, durante cuánto tiempo se aplicarán y cómo se medirán sus resultados.

La tercera lección es que la evidencia necesita ser traducida al lenguaje de la gestión pública. Un alcalde, un comisario o un jefe de región policial no toman decisiones consultando decenas de artículos científicos. Necesitan información sintetizada, criterios claros y equipos capaces de convertir los datos en herramientas útiles para la acción. En ese sentido, el aporte de Lum y Koper (2011) resulta especialmente relevante, pues demuestra que la investigación



Ilustración: IA — Gemini IA, prompt y edición: Keliyvasan — ChatGPT

solo influye en las decisiones cuando logra incorporarse a los procesos cotidianos de gestión policial.

Sin embargo, la propia literatura también advierte los límites de este enfoque. Goldstein parte del supuesto de que las instituciones cuentan con capacidades analíticas suficientes para comprender los problemas que enfrentan, algo que muchas policías todavía no poseen. Sherman asume que las organizaciones estarán dispuestas a privilegiar la evidencia por encima de las presiones políticas de corto plazo, una condición que no siempre se cumple. Por su parte, Weisburd y Braga

muestran el potencial de la focalización territorial, aunque también advierten que un uso inadecuado puede derivar en fenómenos de sobrepoliciamiento, por lo que resulta indispensable establecer mecanismos de control y supervisión.

A ello se suma una advertencia formulada por el National Research Council: la evidencia nunca debe evaluarse únicamente en términos de eficacia. También es necesario considerar su impacto sobre la justicia, la legalidad y la confianza ciudadana. En otras palabras, hoy conocemos bastante sobre las prácticas policiales que ofrecen resultados prometedores;



Ilustración: IA — Gemini IA, prompt y edición Kelly Vásquez Chaparro

sin embargo, sabemos mucho menos acerca de las condiciones institucionales que permiten sostener esos resultados en el tiempo.

LA PARADOJA: ¿POR QUÉ LA EVIDENCIA NO SE APLICA?

La evidencia, por sí sola, no transforma a las instituciones policiales porque no ingresa automáticamente a sus procesos de toma de decisiones. Una institución puede contar con diagnósticos sólidos y, aun así, seguir respondiendo a la coyuntura mediática, a las presiones políticas de corto plazo o a indicadores internos que premian la actividad antes que los resultados. En ese contexto, la evidencia termina utilizándose para justificar decisiones ya adoptadas, en lugar de orientar mejores decisiones.

La literatura reciente sobre implementación refuerza esta idea. Jaitman (2023) sostiene que el avance de la policía basada en evidencia enfrenta barreras institucionales, culturales, políticas y de capacidades técnicas. Esta perspectiva desplaza la atención desde la producción de conocimiento

utilizarlo. Incluso los mejores estudios o los sistemas de información más sofisticados tendrán un impacto limitado si la organización no cuenta con incentivos adecuados, personal capacitado, liderazgo y continuidad para convertir ese conocimiento en decisiones concretas.

Uno de los principales obstáculos es la cultura organizacional. Muchas instituciones policiales se han desarrollado alrededor de valores como la disciplina jerárquica, la capacidad de reacción inmediata y el control visible del territorio. Estas competencias siguen siendo importantes, pero pueden entrar en tensión con una cultura de aprendizaje, que exige formular hipótesis, evaluar resultados, reconocer errores y modificar las prácticas cuando la evidencia así lo aconseja. Evaluar una intervención implica aceptar la posibilidad de que no haya funcionado como se esperaba. En organizaciones donde el error se castiga o se oculta, ese proceso resulta especialmente difícil.

Otro obstáculo importante es el sistema de incentivos. Si el desempeño de una comisaría se mide por el número de operativos realizados, personas detenidas o patrullajes efectuados, la

organización tenderá a concentrar sus esfuerzos en incrementar esas cifras. Sin embargo, una alta actividad no necesariamente se traduce en mejores resultados. Reducir la extorsión, esclarecer homicidios, fortalecer la confianza ciudadana o desarticular organizaciones criminales requiere indicadores mucho más complejos que simplemente contabilizar acciones. Cuando predominan las métricas de actividad sobre las métricas de impacto, la evidencia pierde capacidad para orientar la gestión.

A ello se suma la fragmentación de la información. La policía registra las denuncias; el Ministerio Público conduce las investigaciones; la

medicina legal produce evidencia forense; el Poder Judicial resuelve los casos; los gobiernos locales monitorean las dinámicas territoriales, y las encuestas de victimización permiten conocer aquellos delitos que nunca fueron denunciados. Cuando estas fuentes permanecen desconectadas, ninguna institución logra reconstruir la trayectoria completa de un caso. El resultado es un conocimiento fragmentado que limita la capacidad del Estado para comprender y prevenir el delito.

La relación entre la policía y la academia constituye otro desafío. La investigación universitaria puede aportar métodos rigurosos,



Ilustración: IA — Gemini IA, prompt y edición, Kelly Vázquez Chaparro

independencia analítica y experiencias comparadas, pero con frecuencia se desarrolla lejos de las necesidades operativas de las instituciones policiales. En ocasiones, los investigadores no acceden a la información necesaria; en otras, los estudios llegan demasiado tarde o responden a preguntas distintas de las que enfrenta la gestión cotidiana. Superar esta brecha exige construir agendas compartidas, establecer mecanismos seguros de acceso a los datos, desarrollar proyectos piloto susceptibles de evaluación y crear espacios donde policías e investigadores puedan discutir los resultados sin que estos sean percibidos como una amenaza para la institución.

EL CASO PERUANO

El Perú refleja con claridad la brecha que puede existir entre disponer de información y convertirla en conocimiento útil para la toma de decisiones. El país cuenta con diversas fuentes de información sobre seguridad ciudadana. La Encuesta Nacional de Programas Presupuestales (ENAPRES), elaborada por el Instituto Nacional de Estadística e Informática (INEI), mide la victimización urbana y la percepción

*Reducir la extorsión,
esclarecer homicidios,
fortalecer la confianza
ciudadana o desarticular
organizaciones criminales
requiere indicadores
mucho más complejos que
simplemente contabilizar
acciones.*

de inseguridad. A ello se suman los registros administrativos de la Policía Nacional del Perú (PNP), la información producida por el Ministerio Público y el Poder Judicial sobre investigación y procesamiento de delitos, así como los análisis elaborados por el Observatorio Nacional de Seguridad Ciudadana.

Este último desempeña un papel importante en el seguimiento de la política pública, aunque no funciona como una unidad de análisis orientada al trabajo operativo cotidiano de policías o fiscales. En otras palabras, el país dispone de datos, pero estos permanecen fragmentados y todavía se integran de manera limitada en los procesos de toma de decisiones.

Algunas cifras permiten dimensionar la magnitud del desafío. Durante el primer semestre de 2024, el 27,7 % de la población urbana de 15 años o más fue víctima de algún delito, mientras que el 86,1 % manifestó considerar probable convertirse en víctima durante los siguientes doce meses, según el INEI. Al mismo tiempo, la tasa estimada de homicidios alcanzó los 10,7 casos por cada 100 000 habitantes en 2025 y las denuncias por extorsión aumentaron de 22 361 en 2024 a 26 585 en 2025. Estos indicadores muestran que el escenario de la seguridad ciudadana se ha vuelto más complejo, pues hoy conviven delitos patrimoniales, violencia letal y economías criminales, como la extorsión, que requieren respuestas diferenciadas.

Sin embargo, uno de los datos más reveladores es el relacionado con la denuncia. Apenas el 16,7 % de las víctimas urbanas presentó una denuncia formal durante el primer semestre de 2024. Esto significa que una parte importante de los delitos nunca ingresa al sistema de información policial. No se trata simplemente de un problema estadístico, sino de una limitación estructural para la gestión de la seguridad. Cuando las personas dejan de denunciar por desconfianza, temor o la percepción de que hacerlo no tendrá

resultados, el Estado pierde información valiosa sobre víctimas, modalidades delictivas, lugares, horarios y posibles responsables.

Esta situación se agrava por los bajos niveles de confianza ciudadana en la Policía Nacional del Perú, que alcanzaron apenas el 14,2 % durante el primer semestre de 2025. Como señalan León Borja, Wyngart Ferruzo y Díaz Vargas (2025), la confianza en la institución policial depende de una combinación de factores, entre ellos la eficacia operativa, la proximidad con la ciudadanía, la profesionalización, la transparencia y la rendición de cuentas.

El país cuenta con diversas fuentes de información sobre seguridad ciudadana. La Encuesta Nacional de Programas Presupuestales (ENAPRES), elaborada por el Instituto Nacional de Estadística e Informática (INEI)

En los últimos años se han impulsado iniciativas importantes para fortalecer las capacidades institucionales. Una de ellas es el Comité Estadístico Interinstitucional de la Criminalidad (CEIC), concebido como un espacio para contrastar y articular la información producida por distintas entidades. Sin embargo, su desarrollo ha sido todavía limitado y su trabajo se ha concentrado principalmente en la elaboración de registros sobre homicidios. Como consecuencia, el país permaneció cerca de cuatro años sin contar con una tasa nacional actualizada de homicidios, hasta la publicación de la cifra de 10,7 casos por cada 100 000 habitantes correspondiente a 2025.

También se han producido avances en el ámbito de la investigación criminal. La digitalización forense impulsada por el Decreto Supremo 011-2025-IN busca integrar información balística, reconocimiento facial, huellas dactilares y perfiles genéticos. A ello se suman los anuncios oficiales sobre la modernización de los laboratorios de criminalística y la incorporación de equipos de análisis rápido de ADN. Asimismo, la creación de unidades especializadas para enfrentar la extorsión y el sicariato refleja el reconocimiento de que las organizaciones criminales se han vuelto más sofisticadas.

No obstante, todos estos avances conducen a la misma pregunta de fondo: ¿están contribuyendo realmente a construir un sistema capaz de aprender? Una base de datos forense, por sí sola, no mejora las investigaciones si no existen protocolos comunes, coordinación entre policías y fiscales, y mecanismos permanentes de seguimiento de los casos. Del mismo modo, una unidad especializada difícilmente transformará la respuesta institucional si no evalúa sus resultados ni comparte el conocimiento que genera.

El caso peruano confirma, así, la tesis central de este artículo. Existe una cantidad creciente de información, pero todavía no un verdadero ecosistema de conocimiento. La presión operativa favorece respuestas inmediatas; la fragmentación limita la comprensión integral de los fenómenos criminales; la baja tasa de denuncias reduce la calidad del diagnóstico; y la evaluación



Ilustración: IA — Gemini IA, prompt y edición Kelly Vásquez Chaparro

de las políticas públicas continúa siendo una práctica excepcional. El desafío consiste en construir una arquitectura institucional donde los datos, el análisis, la investigación criminal, la legitimidad y la toma de decisiones se fortalezcan mutuamente.

HACIA UN ECOSISTEMA DE CONOCIMIENTO EN SEGURIDAD

La agenda peruana debería partir de una premisa sencilla: disponer de datos no es suficiente para generar conocimiento útil. Para que la información contribuya realmente a mejorar la seguridad, debe integrarse, depurarse, compararse y convertirse en un insumo para la toma de decisiones. En ese sentido, fortalecer el Comité Estadístico Interinstitucional de la Criminalidad (CEIC), mejorar la calidad de los registros policiales e impulsar la interoperabilidad entre la policía, el Ministerio Público, el Poder Judicial, el sistema de salud, los gobiernos locales y las encuestas de victimización permitiría reconstruir el recorrido completo de un caso: desde la ocurrencia del delito y la denuncia hasta la investigación, la obtención de pruebas y la sanción. Sin esa visión integral, el Estado solo accede a fragmentos de la realidad.

El segundo eje consiste en medir aquello que hoy permanece oculto. La baja tasa de denuncias obliga a complementar los registros administrativos con encuestas de victimización y percepción que permitan conocer mejor la realidad de distintos territorios y grupos de población. Los riesgos que enfrentan los transportistas víctimas de extorsión, los comerciantes, los jóvenes, las mujeres o quienes viven en zonas rurales y corredores de economías ilegales no siempre aparecen reflejados en las estadísticas generales. Identificar esas diferencias no constituye únicamente un ejercicio académico; es una condición indispensable para diseñar políticas públicas proporcionales a los problemas que buscan resolver.

El tercer eje propone convertir el análisis territorial en una práctica permanente de gestión. Diversos estudios realizados en el país han identificado concentraciones espaciales de robos, hurtos y extorsiones en determinados distritos. Esta información debería orientar el diseño del patrullaje focalizado, las estrategias de prevención situacional, la investigación de redes criminales y la coordinación con los gobiernos locales. Sin embargo, ninguna de estas intervenciones debería evaluarse por el número de operativos

realizados o de cámaras instaladas. Lo verdaderamente importante es medir su impacto sobre la reducción del delito, el posible desplazamiento de la actividad criminal, la confianza ciudadana y el esclarecimiento de los casos.

El cuarto eje corresponde al fortalecimiento de la ciencia forense. En la investigación de los delitos más complejos, herramientas como el análisis de ADN, la balística, las huellas dactilares, la informática forense o el análisis de comunicaciones resultan fundamentales para esclarecer los hechos y vincular a los responsables. No obstante, la modernización tecnológica solo produce resultados cuando forma parte de un sistema articulado con fiscales, jueces y unidades de investigación. Un laboratorio aislado puede acelerar una pericia; un sistema forense integrado puede contribuir de manera decisiva a reducir la impunidad.



El quinto eje plantea consolidar una colaboración permanente entre la academia, la policía y el Estado. En este ámbito, el Concytec podría desempeñar un papel estratégico mediante el financiamiento de investigaciones aplicadas sobre prevención del delito, inteligencia policial, evaluación de políticas públicas, ciencias sociales y tecnologías emergentes. Para que estas investigaciones generen un impacto real, deberían partir de problemas concretos, acceder a información mediante reglas claras y retornar a las instituciones en forma de proyectos piloto, protocolos, programas de formación o mejoras en la gestión.

Este ecosistema también debe incorporar a quienes diseñan las políticas públicas y a quienes las implementan diariamente: autoridades del Poder Ejecutivo, parlamentarios, gobiernos regionales y locales, directivos públicos, investigadores y funcionarios de primera línea. Michael Lipsky (1980) demostró que profesionales como policías, docentes o trabajadores sociales terminan dando forma concreta a las políticas públicas a través de las decisiones que adoptan en su contacto cotidiano con la ciudadanía. En materia de seguridad, los policías que patrullan las calles también forman parte del sistema de conocimiento, pues interpretan información, ejercen

discrecionalidad y transforman normas generales en respuestas concretas. Por ello, la agenda científica no debería entenderse como un conjunto de proyectos aislados, sino como un circuito permanente de aprendizaje en el que los datos, la evaluación, el análisis territorial, la ciencia forense y la interoperabilidad se fortalezcan mutuamente.

CONCLUSIÓN

La evidencia, por sí sola, no ha logrado transformar el trabajo policial porque se le ha exigido producir cambios sin contar con las condiciones institucionales necesarias. Un estudio puede demostrar que una intervención funciona, pero no puede modificar los incentivos de una organización, integrar bases de datos, formar analistas, coordinar instituciones, fortalecer la legitimidad o proteger una política pública frente a los cambios del ciclo político. Para que la evidencia tenga un impacto real, necesita instituciones capaces de utilizarla, cuestionarla y convertirla en parte de su funcionamiento cotidiano.

Ese es el sentido de comprender la seguridad como un ecosistema de conocimiento: conectar el trabajo en las calles con la investigación científica; el

patrullaje con el análisis; la tecnología con la comunidad. Cuando esas dimensiones se articulan, la acción policial deja de ser una sucesión de respuestas aisladas y comienza a convertirse en un proceso continuo de aprendizaje. La seguridad pública mejora cuando el Estado comprende mejor los problemas que enfrenta, y no únicamente cuando incrementa el número de intervenciones.

En el caso peruano, esta discusión resulta especialmente urgente. Los altos niveles de victimización, la persistente percepción de inseguridad, el subregistro de delitos y la baja confianza en las instituciones de seguridad y justicia muestran que las respuestas tradicionales ya no son suficientes. El país necesita organizaciones capaces de comprender la realidad a partir de la evidencia, actuar de manera preventiva y corregir sus estrategias antes de que la siguiente crisis las obligue a hacerlo.

La idea final puede resumirse en una afirmación sencilla: una policía que no aprende está condenada a repetir sus rutinas; un Estado que aprende está en mejores condiciones de comprender las causas de la inseguridad y de responder a ellas con mayor eficacia.

Referencias bibliográficas

Braga, A. A., Papachristos, A. V., & Hureau, D. M. (2014). *The effects of hot spots policing on crime*. Campbell Systematic Reviews.

Chainey, S., Alvarado, N., & Serrano, R. (2024). *Hot spot policing: An evidence-based practice guide for police in Latin America and the Caribbean*. Banco Interamericano de Desarrollo.

Comité Estadístico Interinstitucional de la Criminalidad. (2024–2026). Boletines e informes técnicos sobre criminalidad y homicidios en el Perú. Gobierno del Perú.

Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica. (2024). Financiamiento de proyectos de investigación aplicada orientados a la prevención y el control de la criminalidad violenta en el Perú.

Goldstein, H. (1979). Improving policing: A problem-oriented approach. *Crime & Delinquency*.

Goldstein, H. (1990). Problem-oriented policing. McGraw-Hill.

Instituto Nacional de Estadística e Informática. (2024). Estadísticas de seguridad ciudadana. Encuesta Nacional de Programas Presupuestales (ENAPRES), enero-junio 2024.

Jaitman, L. (2023). Towards implementing evidence-based policing. En *The future of evidence-based policing*. Cambridge University Press.

León, J., Wyngart, W., & Díaz, C. (2025). De la percepción a la realidad: Factores críticos en la construcción de confianza ciudadana hacia la Policía Nacional del Perú. *Revista Académica de la Escuela de Posgrado de la Policía Nacional del Perú*.

Lipsky, M. (1980). *Street-level bureaucracy: Dilemmas of the individual in public services*. Russell Sage Foundation.

Lum, C., Koper, C. S., & Telep, C. W. (2011). The evidence-based policing matrix. *Journal of Experimental Criminology*.

Ministerio del Interior del Perú. (2025). Comunicaciones oficiales sobre modernización criminalística y fortalecimiento de laboratorios forenses.

National Research Council. (2004). *Fairness and effectiveness in policing: The evidence*. The National Academies Press.

Sherman, L. W. (1998). *Evidence-based policing*. Police Foundation.

Weisburd, D. (2015). *The law of crime concentration and the criminology of place*. Cambridge University Press.



INVESTIGACIÓN EN MARCHA

CIENCIA PARA ENTENDER EL RASTRO DEL CRIMEN

PROYECTOS E
INVESTIGACIONES
FRENTE A UN
MONSTRUO
DE MÚLTIPLES
CABEZAS: LA
INSEGURIDAD

Hans Huerto Amado

Entra una llamada. Número desconocido. Pero la voz al otro lado sabe tu nombre, sabe dónde trabajas, incluso a qué hora suele cerrar tu negocio.

Ese tipo de llamada dejó de ser un hecho aislado en el Perú desde hace tiempo. De enero a julio de 2025, la Policía Nacional ya había recibido más de 20 mil denuncias por extorsión, una cifra que se ha incrementado de manera sostenida en los últimos años. Detrás de cada una hay algo más que una amenaza, hay una organización, patrones e información que se filtra a más actores delictivos.

El crimen ya no es sólo violencia, es hoy sistema, y como toda estructura que aprende se adapta, se mueve, cambia de forma. Como una hidra: cortas una cabeza y te salen otras.

¿Cómo anticipar al próximo movimiento del monstruo?

LEER LA AMENAZA ANTES DE QUE TOME FORMA

Las extorsiones no comienzan con el dinero. Empiezan con datos. En un país

donde más del 90% de los hogares tiene acceso a telefonía móvil, según el INEI, el teléfono se ha convertido en uno de los principales canales para operar delitos a distancia, pues prescinde del contacto físico y la exposición, haciendo un uso perverso de la información a mano.

Ahí ha decidido intervenir un grupo de investigadores. El proyecto "Detección en tiempo real de llamadas extorsivas mediante inteligencia artificial y georreferenciación", que desarrollan Renzo Espinoza Bonifaz y su equipo de la Universidad de San Martín de Porres, plantea un sistema que examina grandes cantidades de datos de telecomunicaciones para encontrar patrones que correspondan a la extorsión. El objetivo es desarrollar una plataforma digital interoperable con operadores de telecomunicaciones y entidades de seguridad. A partir del cruce entre frecuencia de llamadas, comportamiento de números sospechosos, ubicación geográfica y reportes ciudadanos, el modelo permite reconocer zonas de riesgo y posibles focos de operación criminal. Esta integración permite identificar dinámicas que no resultan evidentes mediante análisis convencionales. El objetivo en la mira es intervenir antes de que el delito se concrete,

utilizando aprendizaje automático para transformar datos dispersos en señales operativas para la prevención.

El proyecto propone algo que, hasta hace poco, parecía difícil de aterrizar: detectar en tiempo real llamadas extorsivas mediante inteligencia artificial y geolocalización. No se trata solamente de identificar una llamada sospechosa, sino de reconocer patrones: frecuencia, rutas, zonas de origen, comportamiento de las redes. Y con eso, la posibilidad de construir alertas y mapas en movimiento, útiles para quienes tienen que tomar decisiones.

La extorsión no ocurre al azar, se repite, se concentra y se organiza. Y cuando se cruzan esos datos —con reportes ciudadanos, con registros de operadores, con ubicación— lo que emerge con la alerta es un mapa delictivo dinámico. Un mapa que permite anticipar y no tan solo reaccionar.

*Las extorsiones no
comienzan con el dinero.
Empiezan con datos.*



GEOLOCALIZACIÓN E INTELIGENCIA ARTIFICIAL PARA DETECTAR LLAMADAS EXTORSIVAS EN TIEMPO REAL



Derecho



CECRIM

Gino Ríos Patio
Renzo Espinoza Bonifaz
Alexis Ruiz Páucar

INTRODUCCIÓN

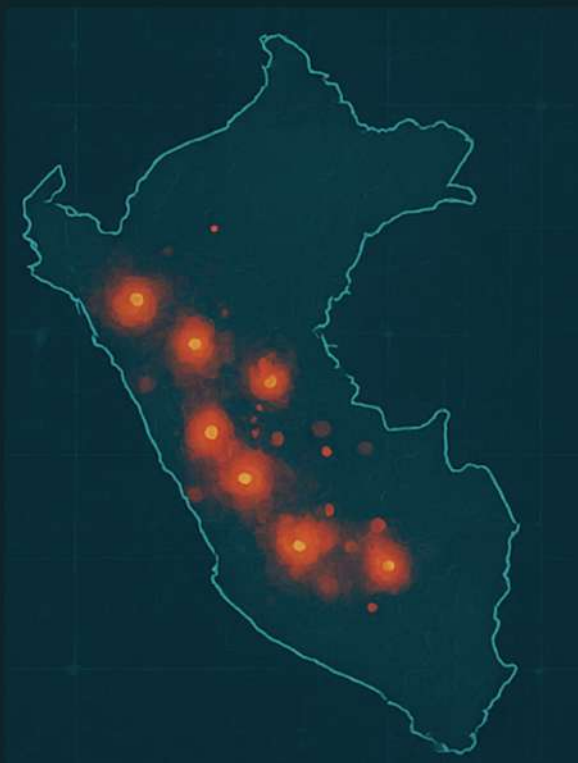
El incremento alarmante de extorsiones telefónicas en el Perú demanda soluciones tecnológicas innovadoras. Este proyecto propone un sistema de localización de llamadas extorsivas basado en Inteligencia Artificial (IA) y geolocalización (GPS), aprovechando metadatos de telecomunicaciones y reportes ciudadanos para proteger a la ciudadanía y reducir el margen de acción del crimen organizado.

OBJETIVOS

- Detectar y localizar llamadas extorsivas mediante IA y GPS.
- Trazar zonas de operación de redes delictivas.
- Desarrollar un modelo predictivo de riesgo geográfico.
- Integrar el sistema con plataformas de seguridad ciudadana respetando la privacidad.

METODOLOGÍA

- Estudio exploratorio-descriptivo.
- Datos anonimizados de operadoras móviles y reportes ciudadanos.
- Población objetivo: víctimas de extorsión.
- Análisis geoespacial, aprendizaje automático y visualización interactiva.
- Colaboración con la Policía Nacional, gobiernos locales y operadores de telefonía.



RESULTADOS ESPERADOS

- Rutas y patrones identificados de actividad extorsiva.
- Zonas de riesgo geográfico delimitadas.
- Interfaz de visualización interactiva para uso policial.
- Sistema interoperable con plataformas de emergencia.
- (Gráficos sugeridos: mapa de calor, flujo de llamadas, predicción por zonas)

CONCLUSIONES

- La IA y geolocalización son herramientas clave para combatir la extorsión.
- El modelo permite una respuesta rápida y eficaz de la policía.
- Se respeta la privacidad y se mejora la prevención del delito.

REFERENCIAS

- García Torres, M. L. (2024). La inteligencia artificial predictiva al servicio de la prevención e investigación del delito y del proceso penal. *Ciencia Policial*, 183, 91-132. <https://doi.org/10.14201/cp.32177>
- Espinoza-Ramírez, Abraham, Nakano, Mariko, Sánchez-Pérez, Gabriel, & Arista-Jalife, Antonio. (2018). Sistemas de Información Geográfica y su Análisis Aplicado en Zonas de Delincuencia en la Ciudad de México. *Información tecnológica*, 29(5), 235-244. <https://dx.doi.org/10.4067/S0718-07642018000500235>

AGRADECIMIENTOS Y CONTACTO

- Agradecimientos: Universidad de San Martín de Porres.
- Contacto: aespinozab@usmp.pe.

EL CRIMEN TAMBIÉN TIENE GEOGRAFÍA

Pero una llamada, no lo explica todo. Otra capa que aparece cuando se contempla el fenómeno en conjunto es la del territorio.

En el Callao, por ejemplo, la incidencia de delitos como la extorsión ha tenido un crecimiento sostenido desde el 2021, según reportes del Ministerio del Interior. Y sin embargo gran parte de la respuesta institucional sigue siendo reactiva. Ante este escenario, un equipo de investigación decidió cambiar ese punto de partida.

El proyecto “Sistema de Geolocalización y Análisis Digital Forense con Componentes Predictivos para la Prevención del Crimen Urbano en el Callao”, desarrollado por Jesús Eusebio Talla De La Cruz, Edward Luis Flores Romero y César Felipe Chávez Navarro de la Pontificia Universidad Católica del Perú, propone la creación de un sistema que integre datos históricos de denuncias, registros georreferenciados y reportes ciudadanos para identificar patrones espacio-temporales del crimen. Para ello, trabaja con grandes volúmenes de información que se procesan y analizan para identificar

relaciones que no son evidentes a simple vista: por ejemplo, coincidencias entre horarios, zonas y tipos de delito que se repiten en el tiempo. A partir de ese análisis, el sistema genera mapas de calor y representaciones visuales que permiten focalizar el patrullaje y mejorar la capacidad de respuesta policial. La propuesta incluye también la creación de un Departamento especializado en geolocalización y análisis digital forense dentro de la estructura policial, para fortalecer la toma de decisiones basada en evidencia.

La geolocalización, el análisis forense digital y un componente predictivo para comprender cómo se distribuye el crimen en el tiempo y en el espacio, hacen posible identificar dónde es más probable que ocurra el siguiente delito, pues estos no se analizan como eventos aislados, sino como un sistema que deja huellas.

En pruebas piloto, más del 70% de los participantes consideró viable la implementación de este tipo de herramientas para mejorar la planificación del patrullaje y la respuesta policial. No es menor. Implica pasar de patrullar por intuición... a patrullar con evidencia.

Sistema de Geolocalización y Análisis Digital Forense con Componentes Predictivos para la Prevención del Crimen Urbano en el Callao



GOBIERNO Y
POLÍTICAS PÚBLICAS
PUCP

65%



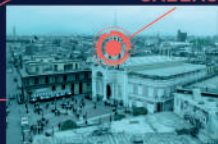
Elaborado por:

Jesús Eusebio Talla De La Cruz, Edward Luis Flores Romero y César Felipe Chávez Navarro, graduados de la Maestría en Gobierno y Políticas Públicas.

Introducción

- La Provincia Constitucional del Callao presenta una problemática creciente de criminalidad asociada principalmente a delitos de extorsión, los cuales han mostrado un alarmante incremento desde el año 2021. Pese a esta situación, la estrategia estatal en la zona continúa siendo predominantemente reactiva y enfrenta limitaciones significativas por la falta de herramientas tecnológicas que permitan una investigación oportuna y eficaz. Esta carencia afecta la capacidad operativa de las fuerzas del orden y contribuye a la expansión de la criminalidad organizada.

CALLAO



Frente a este contexto, el presente proyecto se justifica por su potencial para transformar la gestión de la seguridad mediante la implementación de tecnologías de geolocalización, análisis digital forense y un componente predictivo básico que permita fortalecer la planificación del patrullaje y mejorar la capacidad de respuesta policial.

Objetivo

Diseñar e implementar un sistema tecnológico con capacidades de geolocalización, análisis digital forense y un componente predictivo básico que mejore la capacidad de investigación y prevención policial en el Callao.

Antecedentes

Experiencias internacionales, como las implementadas en Guatemala y Brasil, demuestran que la aplicación de tecnologías de geolocalización y análisis de información digital puede contribuir significativamente a mejorar la capacidad de respuesta policial y reducir la incidencia de delitos.

En el contexto peruano, el proyecto se alinea con la Política Nacional de Transformación Digital y la Política Nacional Multisectorial de Seguridad Ciudadana al 2030, que promueven el uso de tecnologías emergentes para el bienestar ciudadano.

2030
PERÚ

Metodología

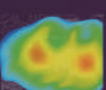
La metodología combina el enfoque cuantitativo de análisis de datos con herramientas de ciencia de datos aplicada a la gestión pública. Se trabajó con datos históricos de denuncias policiales, reportes ciudadanos y registros de geolocalización para identificar patrones espacio-temporales de incidencia delictiva. Se aplicaron técnicas de minería de datos para procesar y analizar la información recopilada. La visualización de los resultados se realizó mediante la generación de mapas de calor y representaciones geoespaciales que facilitan la interpretación operativa por parte de la policía y las autoridades locales. La validación del sistema se efectuó a través de pruebas piloto y simulaciones con datos reales del Callao, evaluando su viabilidad operativa y su potencial para integrarse en las plataformas institucionales existentes.

RESULTADOS



DEPARTAMENTO DE
GEOLocalización
Y ANÁLISIS DIGITAL

70%+
MUY PROBABLE



Se identificó la eficacia de la creación del Departamento especializado en geolocalización y análisis digital forense en la DIVINCRI-Callao, con personal capacitado y recursos tecnológicos adecuados para la gestión eficiente de la información criminal. Este departamento será responsable no solo de la organización de la información digital, sino también de la operación de un sistema tecnológico robusto y confiable. El sistema estará diseñado para capturar, procesar y analizar información geoespacial y digital de manera continua, lo que permitirá mejorar sustancialmente los tiempos de procesamiento, la trazabilidad de los casos y la calidad de las investigaciones policiales.

Según la evaluación realizada, el 70% de los participantes en la validación del prototipo señalaron que es 'Muy probable' que el sistema propuesto pueda desarrollarse y escalar para lograr un mayor impacto en la población, lo que evidencia una alta percepción de viabilidad y aplicabilidad del proyecto.

Generación sistemática de mapas de calor a partir del análisis de datos históricos de denuncias, reportes ciudadanos y registros geolocalizados, que permitirán visualizar las zonas y horarios de mayor incidencia delictiva. Estos mapas servirán como herramienta de apoyo para la toma de decisiones estratégicas y operativas por parte de la policía y las autoridades locales, facilitando la priorización de áreas críticas para el patrullaje preventivo y las intervenciones focalizadas.

La hipótesis central del trabajo sostiene que la aplicación del prototipo mejorará la capacidad de las investigaciones policiales por delitos de extorsión, permitirá esclarecer las denuncias con mayor rapidez y facilitará la identificación y captura de los extorsionadores de manera más efectiva.

MEJORA EN PLANIFICACIÓN + FORTALECIMIENTO DE CAPACIDADES

El impacto esperado del sistema es mejorar la planificación del patrullaje preventivo y focalizar recursos en zonas críticas, fortaleciendo la capacidad de respuesta policial ante los delitos de extorsión. Para su adecuada implementación, se requiere fortalecer las capacidades técnicas del personal policial y garantizar el acceso a información actualizada y de calidad.

Conclusiones

El proyecto plantea una solución tecnológica integral que combina geolocalización, análisis digital forense y un componente predictivo básico para fortalecer la capacidad de respuesta policial ante delitos de extorsión en el Callao. La creación del Departamento especializado permitirá mejorar la gestión de la información criminal y focalizar las intervenciones en las zonas de mayor riesgo de manera más eficiente. Además, el 70% de los participantes en la validación del prototipo consideró muy probable que el sistema pueda desarrollarse y escalar, lo que refuerza la viabilidad del proyecto y su relevancia para la seguridad ciudadana. Este respaldo evidencia la pertinencia de continuar con la implementación y evolución del sistema propuesto.

Referencias bibliográficas

- Ministerio del Interior del Perú. (2022). Política Nacional Multisectorial de Seguridad Ciudadana al 2030.
- Cerdá, M. et al. (2020). Data-Driven Policing and Urban Crime. *Journal of Urban Affairs*.
- Alcaldía de Bogotá. (2021). Sistema de Análisis Predictivo de Criminalidad.
- OECD. (2019). *Artificial Intelligence in Society*.

CUANDO LA AMENAZA SE VUELVE VISIBLE

Pero no todo sucede o se traduce en datos. A veces el crimen entra por la puerta o deja un explosivo junto a ella.

En América Latina, el asalto a mano armada continúa siendo una de las principales formas de victimización, especialmente en pequeños comercios y entornos urbanos. En el Perú, el INEI ha señalado que más del 25% de la población ha sufrido algún delito en el último año, el más frecuente de los cuales es el robo.

En ese escenario la pregunta es otra: ¿qué se hace cuando ya se está frente a la amenaza?

A ello responde un prototipo desarrollado en el ámbito de la ingeniería mecatrónica: un sistema capaz de detectar y seguir armas en tiempo real mediante visión computacional.

El proyecto "Prototipo de un sistema inteligente de detección y seguimiento de armas en tiempo real para seguridad de negocios urbanos" liderado por Joseph Ricaldi junto un equipo del Centro de Desarrollo e Investigación en Mecatrónica de la

Universidad Nacional de Ingeniería, desarrolla un sistema basado en visión computacional que puede identificar armas de fuego en tiempo real a partir de imágenes capturadas por cámaras de videovigilancia. El modelo, que se ha entrenado con distintas bases de datos y configurado para trabajar en entornos urbanos, procesa imágenes en unos 0,08 segundos por cuadro y alcanza niveles de detección cercanos al 95 %, activando mecanismos de seguimiento automatizado ante posibles amenazas. El sistema está diseñado como una solución de bajo costo orientada a MYPES y busca reducir los tiempos de reacción frente a robos a mano armada, una de las modalidades más frecuentes de victimización en los contextos urbanos.

Una cámara. Un algoritmo que ha sido entrenado con miles de imágenes. Y un sistema que no se desconcentra, aunque aún es perfectible. La luz, los reflejos o los objetos similares pueden afectar su rendimiento. Pero deja una puerta abierta: la posibilidad de detectar una amenaza antes de que nadie reaccione tarde.

En espacios en los que cada segundo cuenta, esto cambia la ecuación y el resultado final.

PROTOTIPO DE UN SISTEMA INTELIGENTE DE DETECCIÓN Y SEGUIMIENTO DE ARMAS EN TIEMPO REAL PARA SEGURIDAD DE NEGOCIOS URBANOS

Joseph Ricaldi¹, Francisco Rodriguez², Heinz Gutierrez³, Yosip Quispe⁴, Rodrigo Ramirez⁵

Escuela Profesional de Ingeniería Mecatrónica
PhD Roberto Furukawa, Msc Jose Becerra

RESUMEN:

Este prototipo diseñado económicamente es un sistema de seguridad inteligente diseñado para mitigar el riesgo de robo en pequeñas empresas y hogares de Latinoamérica. Esta innovación integra de forma única todas las funcionalidades clave en un único producto cohesivo. El sistema combina una ESP32-CAM para captura de imágenes en tiempo real, conectividad WiFi y control directo de dos servos SG90 para movimiento de doble eje, con un microcontrolador PIC16F887A que activa un módulo láser KY-008 al recibir una señal digital alta. La ESP32CAM establece un servidor local para transmitir video en vivo a una computadora portátil, donde un algoritmo de detección en cascada identifica posibles amenazas.

PROBLEMÁTICA:

Uno de los problemas más importantes en las últimas décadas para la población latinoamericana es la inseguridad ciudadana. Los robos a mano armada son muy comunes entre peatones y en pequeños o medianos negocios [1]. Debido a esta problemática, nos hemos interesado en la detección y seguimiento de armas y elaborar una solución inteligente. Este sistema se justifica como respuesta a esta problemática. Mediante la implementación de algoritmos avanzados de procesamiento de imágenes, análisis de patrones y seguimiento de amenazas, el sistema podrá detectar proactivamente comportamientos sospechosos y activar respuestas automatizadas [2].



ANTECEDENTES:

El reconocimiento de imágenes ha evolucionado significativamente en los últimos años, desde la detección de objetos simples hasta la de objetos complejos en tiempo real, mediante aplicaciones en automatización, seguridad e interacción persona-computadora [2]. Algunas herramientas como MATLAB y Python han demostrado su viabilidad en la detección de objetos de color para sistemas, aunque presenta limitaciones debido a factores variables como las condiciones de iluminación y los reflejos de los objetos en el entorno. Por otro lado, los métodos de aprendizaje profundo han demostrado mayor precisión y robustez [3][4]. Estos modelos, al ser entrenados con diversas bases de datos, pueden personalizarse para diversas aplicaciones, como la monitorización de la seguridad, la automatización industrial y la optimización del tráfico [2]. No obstante, el costo computacional y el procesamiento en tiempo real siguen siendo un reto. A partir de estos avances, es esencial desarrollar soluciones que integren tanto la precisión de un modelo entrenado como un sistema con respuestas en tiempo real.

OBJETIVOS:

- Desarrollar un sistema de seguridad inteligente que combata en buena medida la problemática propuesta, diseñando una solución con componentes de bajo costo (nivel prototipo).
- Para el estado del arte: Entrenar un modelo de detección de armas eficiente bajo aprendizaje profundo además de diseñar un control de respuesta real.
- Integrarlos eficientemente bajo dichos conocimientos de software y hardware; y evaluar la eficacia del sistema mediante pruebas en escenarios reales con los permisos necesarios.

METODOLOGÍA:

Se planteó la necesidad de un sistema automatizado que permite responder en tiempo real las amenazas planteadas, para ello se diseñó de distintos base de datos un modelo de aprendizaje profundo entrenado de distintas armas de fuego en diferentes ángulos e iluminaciones, finalmente este diseño está orientado a MYPES en el contexto peruano ya que es la región donde más ocurren este tipo de crímenes.



RESULTADOS:

En pasos de n de 256×256 píxeles, el clasificador se aplica automáticamente a ventanas de 160×120 píxeles de cada imagen de entrada para determinar si contiene un arma. El proceso de detección completa tarda 0,08 segundos en una ventana de 640×480 píxeles y tiene una eficiencia del 95 % según la tasa de detección utilizada. Además, el sistema implementa seguimiento láser, dirigiendo el haz hacia el área de interés, lo que mejora la visibilidad y la precisión del seguimiento. La precisión estimada para el seguimiento es del 94 % debido al umbral de 5 en el código, que equivale a un error del 6 %.

CONCLUSIONES:

Las principales contribuciones de este trabajo incluyen el diseño de un mecanismo de movimiento preciso y la implementación de un algoritmo de detección eficiente. Sin embargo, el sistema presenta limitaciones en entornos con iluminación variable, así como en la detección de objetos negros similares, lo que sugiere la necesidad de futuras investigaciones para la integración de sensores adicionales y técnicas avanzadas de procesamiento de imágenes. En trabajos futuros se podría explorar el uso de otros algoritmos de aprendizaje profundo para mejorar el sistema en condiciones adversas.

BIBLIOGRAFÍA:

- [1] F. Carrión, "La inseguridad ciudadana en América Latina: Un análisis desde la perspectiva urbana". In: Revista Latinoamericana de Seguridad Ciudadana (2018). [En línea]. Disponible: <https://scielo.conicyt.cl>.
- [2] GridTICs Research Group, "Deep learning for object detection in security applications". In: AI & Security Journal 15.3 (2020), pp. 220-235.
- [3] E. Torres and P. Silva. Diseño de un sistema de seguridad basado en IoT para la detección de amenazas. Tech. rep. [En línea]. Disponible: <http://repositorio.ulima.edu.pe>. Universidad de Lima (Perú), 2022.
- [4] Y. Zhang and X. Li, "Weapon Detection in Surveillance Videos Using Deep Learning". In: IEEE Transactions on Image Processing 29.1 (2020). [En línea]. Disponible: <https://scholar.google.com>, pp. 1234-1245.

LO QUE QUEDA CUANDO TODO HA PASADO

No todos los delitos son interceptados a tiempo. Algunos dejan algo más difícil de procesar: la ausencia. En Perú, más de 17.000 personas fueron reportadas como desaparecidas en el 2024, según los registros policiales. Muchas están localizadas. Otras, todavía no. Y en los casos más complejos —trata de personas, homicidios, desplazamientos forzados— la misma identidad puede volverse incierta.

Es aquí donde se recurre a la ciencia, específicamente a la Genética forense, para hacer frente a la situación. Un equipo de investigación ha trabajado en mejorar la capacidad de identificar vínculos biológicos en contextos complejos, como los que plantea la comisión de un delito. El proyecto "Plataformas de STR extendida: una solución a la baja resolución en la identificación de vínculos de parentescos genéticos complejos", desarrollado por el equipo del laboratorio BIO LINKS integrado por A. Badillo, S. Reyes, A. Torres y M. Gavilán, propone ampliar el número de marcadores genéticos analizados en pruebas de ADN —de los 15 a 28 loci convencionales hasta 60— para mejorar la precisión en la identificación de personas y relaciones

biológicas. Un locus (plural: loci) es, en términos simples, un punto específico del ADN donde los científicos "leen" información para identificar a una persona o comparar parentescos. A partir del análisis de 135 casos reales de parentesco, el estudio demuestra que esta ampliación incrementa la tasa de resolución por encima del 95% y permite alcanzar niveles de certeza superiores al 99,99%, incluso en contextos complejos donde hay escasez de familiares directos o fragmentación de vínculos. La propuesta apunta a optimizar los procesos de identificación en investigaciones criminales y casos de personas desaparecidas, reduciendo tiempos y aumentando la confiabilidad de la evidencia genética



Ilustración: IA — Gemini IA, prompt y edición Kelly Vásquez Chaparro

Plataformas de STR Extendida: Una Solución a la Baja Resolución en la Identificación de Vínculos de Parentescos Genéticos Complejos

A. Badillo¹; S. Reyes¹; A. Torres¹; M. Gavilan¹

1. Unidad de Paternidad, Parentesco e Identidad Humana – Laboratorios BIO LINKS S.A.

INTRODUCCIÓN

La criminalidad y violencia han alcanzado escalas sin precedentes en América Latina en los últimos años. En el Perú, las principales economías ilegales asociadas a redes criminales son: minería ilegal, trata de personas, narcotráfico, extorsión, entre otras (1). Las desapariciones de personas y los homicidios son manifestaciones directas de estas actividades delictivas. Al cierre del 2024, se reportaron un total de 17737 personas desaparecidas, habiendo sido ubicadas 9286, entre vivos y fallecidos (2). Además, se reportaron 2011 asesinatos, 34% más que el año anterior, y 1125 fueron resultado del sicariato (3). Para las autoridades resulta complejo establecer la identidad de las personas cuando fueron sustraídas del entorno familiar, movilizadas a través de frontera, victimadas en crímenes violentos, entre otros.

Las regiones STR (Short Tandem Repeats), son secuencias cortas de ADN de carácter polimórfico que se distribuyen a lo largo del genoma humano, que siguen patrones de herencia mendeliana. Su aplicación en la ciencia forense, hace posible generar perfiles genéticos únicos para cada individuo, estableciendo la identidad de una persona y filiación a grupos familiares. No obstante, la baja resolución que ofrecen las plataformas de análisis STR convencionales, limitadas a paneles de 15 a 28 loci reduce la solidez de los valores de probabilidad, y obliga a incorporar familiares para alcanzar niveles de certeza aceptables, dificultando la resolución de casos de parentesco indirecto o familias fragmentadas. De ese modo, el uso de plataformas STR extendidas maximiza la resolución de casos, permitiendo reducir el número de familiares, con índices de verosimilitud (LR) con mayor grado de certeza (4).

En este sentido, la genética forense aparece como una herramienta científica para la resolución de casos de identificación de personas vivas o fallecidas, cuando no se puede alegar con certeza un vínculo, que brinda evidencia sólida en procesos civiles y penales. Especialmente cuando el análisis se ve afectado por la ausencia de los progenitores o el número de familiares disponibles es limitado.

OBJETIVO

Evaluar la eficacia de una plataforma ampliada de análisis de hasta 60 loci STR para incrementar la precisión en la determinación de vínculos biológicos en casos de parentesco, reduciendo la necesidad de ampliar el grupo familiar sobre la búsqueda de personas.

MATERIALES Y METODOS

Se analizaron un total de 135 casos de parentesco, correspondientes a casos de vínculos de parentesco, recibidos durante el período 2023 al 2024. Las extracciones de ADN se realizaron a partir de muestras de sangre (COPAN-NUCLEI CARD) e hisopados bucales. El proceso de extracción de ADN de muestras de hisopado bucal fue realizado por medio de lisis directa con el Buffer Swab Solution (PROMEGA). Las muestras de sangre fueron amplificadas por método de PCR-Directo. Cada muestra fue amplificada mediante el uso del termociclador SimpliAmp de la marca ThermoScientific.

El análisis de los loci autosómicos STR (Short Tandem Repeats) se realizaron mediante el uso de los kits: VeriFiler™ Express, GlobalFiler™ y Microreader™ 23sp, complementadas con un panel STR in-house desarrollado por BIO-LINKS, diseñado para ampliar la resolución de loci hasta un total de 60 marcadores STR. La PCR se llevó según las recomendaciones de cada fabricante mediante electroforesis capilar: ABI 3500 Genetic Analyzer.

El análisis genético se realizó con el software GeneMapper versión 1.4. Los cálculos de índice de verosimilitud (Likelihood Ratio ó LR) se efectuaron con el programa Familias versión 3.3, aplicando frecuencias alélicas correspondientes a la población de referencia de estudio (peruana y latinoamericana). Todos los análisis se efectuaron con una corrección de subestructura poblacional de $\Theta = 0.01$.

RESULTADOS

Se analizaron un total de 135 casos de parentesco, cuya distribución por categoría se presenta en la Figura 01. Los tipos de parentesco más frecuentes fueron los casos de media hermandad (47%), hermandad completa (21%) y tío-sobrino (15%), lo que refleja la diversidad de relaciones familiares estudiadas.

La Figura 02 muestra la eficacia de las pruebas de parentesco según el número de parientes incluidos en el análisis. Se observó una mayor tasa de resolución en los casos donde participaron múltiples parientes en comparación con aquellos basados únicamente en un solo familiar.

En particular, las pruebas con dos o más parientes mostraron una mayor capacidad discriminativa, lo cual resultó fundamental para resolver casos complejos. Además, se observó una mayor tasa de resolución en los casos donde participaban pocos parientes, especialmente cuando se combinaba un mayor número de marcadores genéticos analizados. Este factor incrementó significativamente la capacidad discriminativa de las pruebas.

Figura 01: Distribución de casos de parentesco analizados

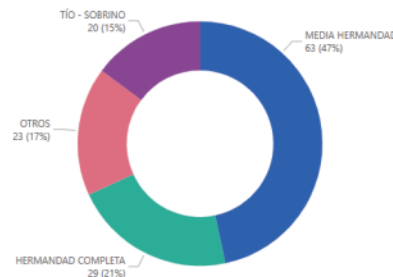
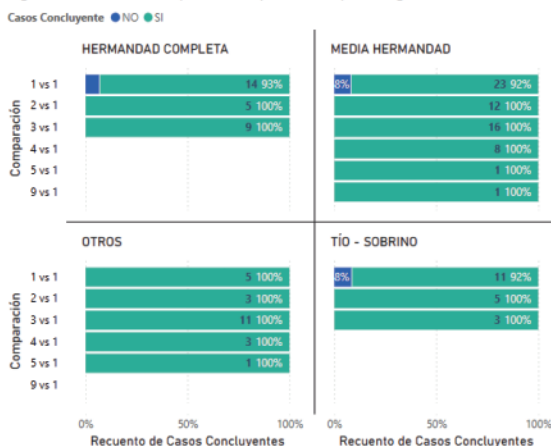


Figura 02: Eficacia de las pruebas de parentesco por categoría



CONCLUSIONES

La implementación de una plataforma extendida de hasta 60 marcadores STR incrementa la tasa de resolución de casos de parentesco biológico por encima del 95%. Incrementar el número de marcadores analizados permite obtener índices de verosimilitud (LR) más robustos, y establecer relaciones de parentesco con mayor grado de certeza, superiores al 99.99%. Esta mejora técnica, permite reducir la necesidad de incluir un grupo familiar extenso en los procesos de identificación, optimizando los recursos disponibles y acelerando la localización e identificación de personas, brindando así un respuesta forense estratégica y eficiente ante los desafíos de la realidad peruana.

BIBLIOGRAFIA

- División de Estadística de la DIRTIC PNP (2024) SIDPOL PNP
- Valdés, R., Basombrio, C. y Vera, D. (2022) Las economías criminales y su impacto en el Perú. ¿Cuáles? ¿Cuánto? ¿Dónde? ¿Cómo? (2ª ed.)
- El comercio (2025) Sangriento 2024 cerró con más de 2 mil homicidios en el Perú: en promedio cada cinco horas fue asesinada una persona
- Zhang Q, Wang X, Cheng P, Yang S, Li W, Zhou Z, Wang S. (2022) Complex kinship analysis with a combination of STRs, SNPs, and indels. Forensic Sci Int Genet:61:102749. doi: 10.1016/j.fsigen.2022.102749.

Lo hacen ampliando el número de marcadores genéticos analizados —los llamados STR— pasando de paneles convencionales a plataformas extendidas. Con más marcadores, aumenta la precisión. Y se traduce en poder resolver casos donde antes no era posible.

Casos donde no hay padres presentes. Donde las familias están fragmentadas. Donde la evidencia es mínima. La ciencia, en ese punto, no previene el crimen. Pero permite reconstruir lo que quedó y así dar con los responsables.

ENTENDER ANTES QUE REACCIONAR

Lo que une estos proyectos no es la tecnología, sino la forma de mirar el problema a través de esta. Durante mucho tiempo, la seguridad ciudadana se ha pensado como respuesta: más patrullaje, más presencia, más reacción. Pero el crimen —ese que muta, que aprende, que se reorganiza— no se enfrenta solo con presencia, sino también con información y conocimiento. Todo ello traducido en la capacidad de leer señales donde antes solo había ruido, de encontrar patrones en lo que parecía disperso, de conectar una llamada con un territorio, una

imagen con una amenaza, una muestra con una identidad. Desde una extorsión que empieza en un celular hasta un mapa que revela concentraciones invisibles, desde una cámara que detecta un arma en segundos hasta un análisis genético que reconstruye vínculos, lo que aparece es una forma distinta de aproximarse al problema. No hay una única respuesta ni un punto donde todo se resuelva de una vez, pero sí un cambio en la manera de entender el crimen: menos intuición, más evidencia; menos reacción tardía, más capacidad de anticipar.

No todos los delitos son interceptados a tiempo. Algunos dejan algo más difícil de procesar: la ausencia. En Perú, más de 17.000 personas fueron reportadas como desaparecidas en el 2024, según los registros policiales.

Referencias bibliográficas

División de Estadística de la DIRTIC PNP. (2024). Sistema de Denuncias Policiales (Sidpol).

Instituto Nacional de Estadística e Informática (INEI). (2025). Encuesta Nacional de Programas Presupuestales – Seguridad Ciudadana.

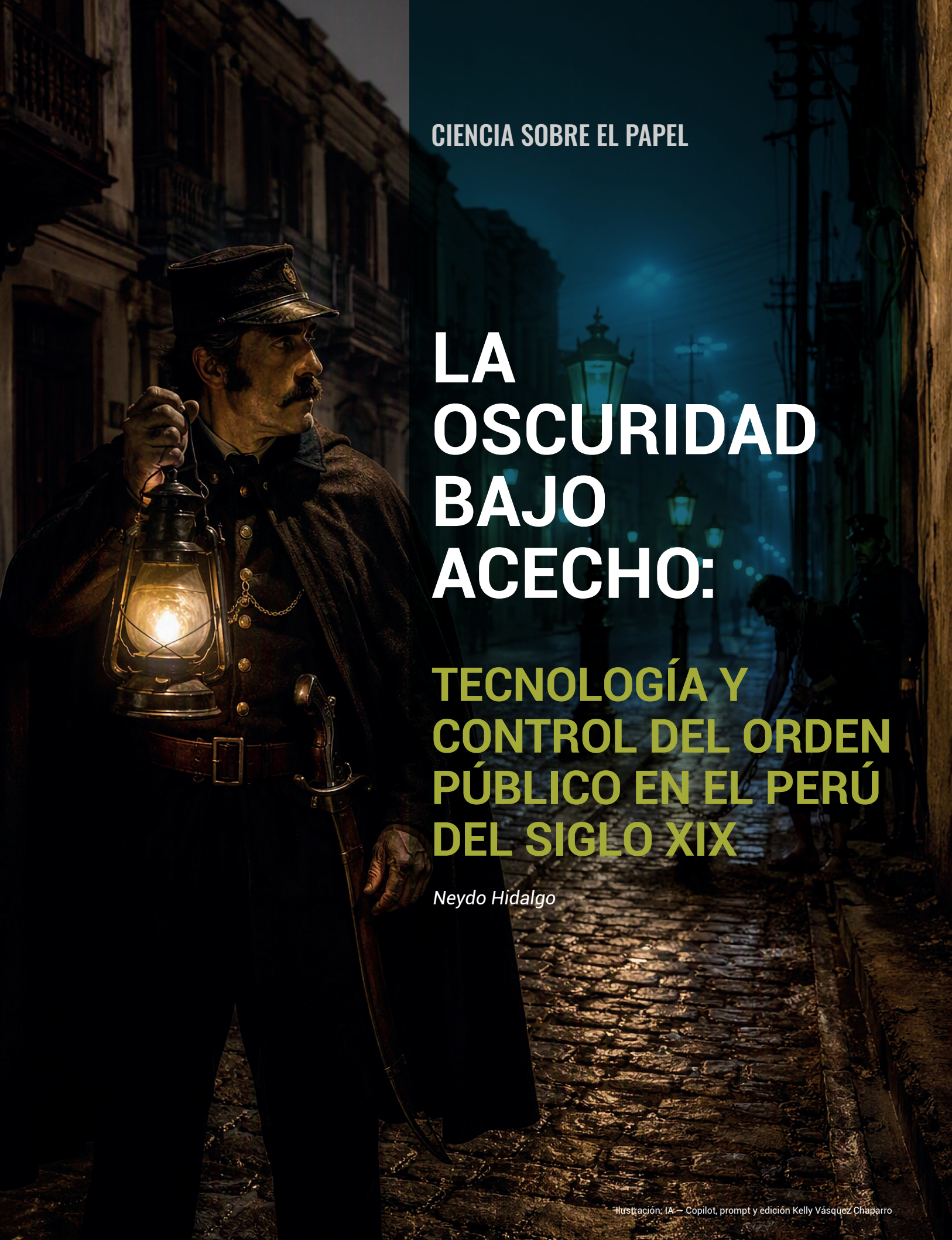
Ministerio del Interior del Perú. (2022). Política Nacional Multisectorial de Seguridad Ciudadana al 2030. Lima: Mininter.

Policía Nacional del Perú (PNP). Registros de denuncias por extorsión.

Valdés, R., Basombrío, C. y Vera, D. (2022). *Las economías criminales y su impacto en el Perú*. Vox Populi.

Organization for Economic Co-operation and Development (OECD). (2019). *Artificial Intelligence in Society*. OECD Publishing.

Zhang, Q. et al. (2022). Complex kinship analysis with a combination of STRs, SNPs, and indels. *Forensic Science International: Genetics*, 58.



CIENCIA SOBRE EL PAPEL

LA OSCURIDAD BAJO ACECHO:

TECNOLOGÍA Y
CONTROL DEL ORDEN
PÚBLICO EN EL PERÚ
DEL SIGLO XIX

Neydo Hidalgo

INTRODUCCIÓN:

EL MIEDO A LA NOCHE Y EL PREÁMBULO COLONIAL

Durante el virreinato del Perú, la noche era mucho más que el momento en que desaparecía la luz del día. Representaba un espacio de incertidumbre, vulnerabilidad y temor. A diferencia de las ciudades prehispánicas, las urbes coloniales introdujeron nuevas dinámicas de exclusión social, diferenciación de castas y desigualdad económica, factores que favorecieron el surgimiento de formas particulares de criminalidad urbana. La ausencia de un sistema permanente de alumbrado público, especialmente en Lima, conocida entonces como la Ciudad de los Reyes, convertía las calles en lugares especialmente peligrosos al caer la noche. La expresión popular «boca de lobo» reflejaba bien esa realidad: el riesgo de sufrir un asalto llevaba a muchas personas a permanecer en sus hogares una vez anochecía. Quienes debían salir por alguna necesidad procuraban hacerlo acompañados y portando una antorcha que les proporcionara tanto iluminación como una sensación de protección.

El primer intento sistemático por enfrentar este problema mediante una medida tecnológica y normativa se produjo en 1551, cuando el virrey Antonio de Mendoza dispuso la organización de una partida de rondines nocturnos. Estos vigilantes recorrían las calles portando faroles de mano o antorchas, una solución rudimentaria que el historiador José G. Clavero (1885) describió acertadamente como un «alumbrado ambulante». La tecnología disponible en esta etapa preindustrial se limitaba al uso de velas de cera o sebo animal, un sistema poco eficiente para iluminar la ciudad, pero suficiente para establecer un precedente fundamental: por primera vez, el Estado vinculaba de manera explícita la iluminación de los espacios públicos con la prevención del delito y el mantenimiento del orden.

Poco después, nuevas disposiciones ampliaron estas medidas. Entre ellas destacó la obligación impuesta a los pulperos de mantener una luz encendida en la puerta de sus establecimientos hasta determinada hora de la noche, bajo pena de multa (Hidalgo, 2007). Más allá de su aparente sencillez, esta disposición revela cómo el alumbrado comenzaba a concebirse como una responsabilidad compartida entre las autoridades y los propios vecinos.

Con la consolidación del virreinato, los esfuerzos por controlar la ciudad continuaron ampliándose. A mediados del siglo XVIII, la preocupación por la seguridad ya no se limitaba a la vigilancia nocturna, sino que también incorporaba aspectos relacionados con la organización del territorio y la protección de las comunicaciones. En 1747, tras el devastador terremoto

y tsunami ocurrido el año anterior, el virrey conde de Superunda ordenó el traslado del puerto del Callao hacia Bellavista como una medida orientada a reducir los riesgos derivados de futuros desastres naturales. Poco después, mediante una Real Cédula emitida a fines de 1768, la Corona asumió directamente la administración del servicio de correos, que desde el 1 de julio de 1769 pasó a denominarse Real

Renta de Correos. Con ello, el Estado recuperó el control de un servicio estratégico para garantizar la seguridad de la correspondencia oficial y fortalecer la administración del virreinato.

A pesar de estos avances administrativos, la oscuridad seguía siendo uno de los principales desafíos para la seguridad urbana al comenzar el siglo XIX. La limitada capacidad para iluminar las calles continuaba favoreciendo la delincuencia y condicionando la vida cotidiana de los habitantes de Lima.



Guardias con faroles de mano en tiempos coloniales

LA TEMPRANA REPÚBLICA: FAROLES, PESCANTES Y EL CONTROL PUNITIVO DE LOS CUERPOS

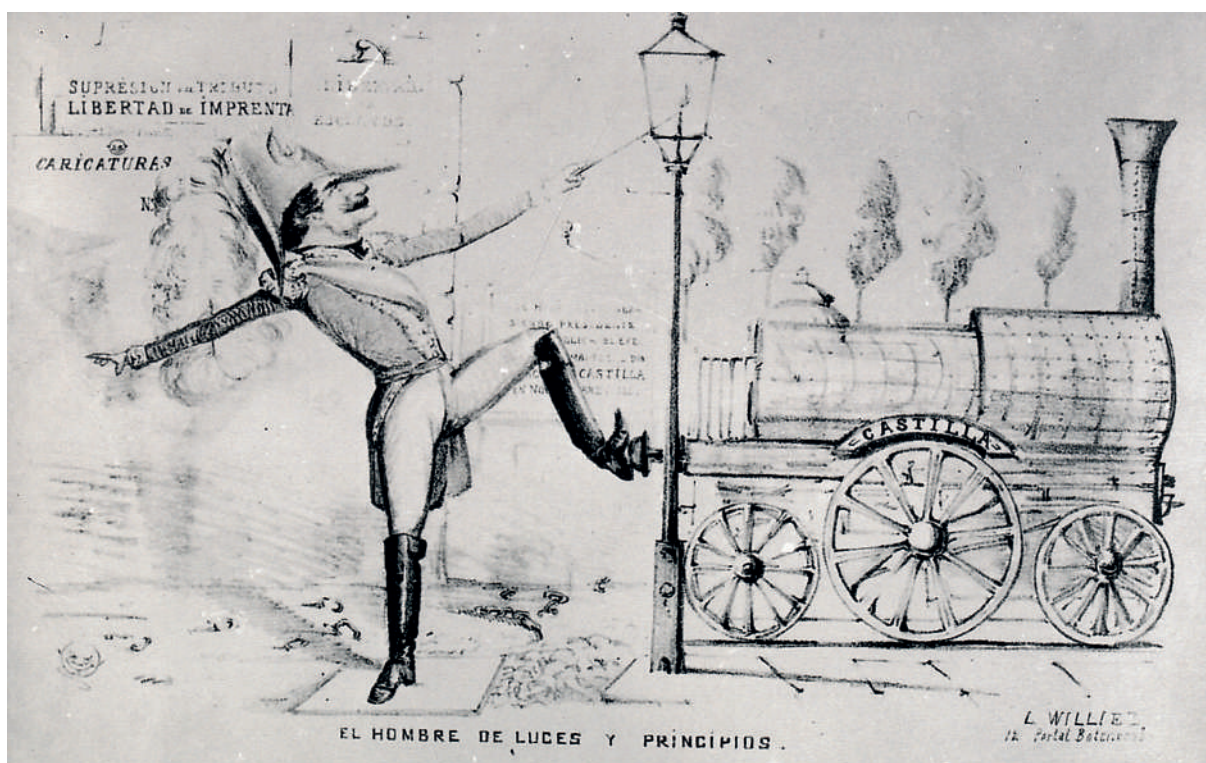
Con la proclamación de la independencia, el Perú heredó ciudades marcadas por la inestabilidad política y por una infraestructura urbana todavía insuficiente para garantizar la seguridad durante la noche. La incorporación de nuevas tecnologías de iluminación constituyó uno de los primeros esfuerzos del Estado republicano por reducir la delincuencia y facilitar la vigilancia de los espacios públicos.

En 1822 se instaló en Lima el primer farol fijo alimentado con vela de sebo, ubicado en la calle de los Santiagos (actual sexta cuadra del jirón Huancavelica) (Capelo, 1895). Años más tarde, durante los gobiernos del general Agustín Gamarra (1833 y 1838), se introdujo una mejora significativa mediante la instalación obligatoria de pescantes de hierro fijados a las fachadas, desde los cuales se suspendían los faroles (Clavero, 1885). Al elevar las fuentes de luz, se ampliaba el campo visual de las calles, disminuían los espacios donde podían ocultarse los

delincuentes y se facilitaba el trabajo de los serenos encargados de la vigilancia nocturna (Ministerio de Gobierno, 1839).

El sistema continuó perfeccionándose. En 1847 comenzó a utilizarse aceite de ballena como combustible para el alumbrado público, una innovación que producía una luz más intensa y de mayor duración que las velas de sebo. No obstante, también presentaba inconvenientes, pues el mantenimiento deficiente de los faroles generaba olores desagradables y problemas de salubridad (Capelo, 1895). Desde sus primeras etapas, la incorporación de nuevas tecnologías mostró así una característica que se repetirá a lo largo del siglo XIX: cada avance resolvía ciertos problemas, pero también planteaba nuevos desafíos.

La tecnología disponible en esta etapa preindustrial se limitaba al uso de velas de cera o sebo animal, un sistema poco eficiente para iluminar la ciudad, pero suficiente para establecer un precedente.



Caricatura "el hombre de las luces y principios" (L. Williez)

Paralelamente a estas innovaciones técnicas, el Estado buscó fortalecer el control del orden público mediante una regulación policial más estricta. El principal hito fue el Reglamento de Policía para la Capital de la República y su Provincia, promulgado por el presidente Agustín Gamarra el 11 de noviembre de 1839 (Ministerio de Gobierno, 1839). Este documento refleja una concepción de la seguridad basada en la vigilancia permanente, el control de la movilidad y el uso de medidas coercitivas para preservar el orden.

El reglamento organizó formalmente el servicio policial en dos cuerpos

diferenciados. Los serenos tenían a su cargo la vigilancia nocturna y la custodia del alumbrado público, mientras que los vigilantes, organizados como caballería armada, realizaban el patrullaje durante el día. El armamento asignado —sables, espadas, pistolas y tercerolas— evidencia la estrecha relación que aún existía entre las funciones policiales y la organización militar del Estado (Ministerio de Gobierno, 1839).

Las sanciones previstas para combatir la delincuencia menor también reflejan la lógica punitiva de la época. El artículo 264 establecía que quienes cometieran hurtos o

robos inferiores a 25 pesos serían juzgados verbalmente por el intendente de Policía y condenados a barrer las calles encadenados, alimentados por el Estado pero sin recibir remuneración, hasta compensar con su trabajo el valor de lo sustraído (Ministerio de Gobierno, 1839). Asimismo, se imponían multas a quienes adquirieran objetos robados o protegieran a los responsables de estos delitos.

El reglamento también convirtió la vagancia en un problema de orden público. Se consideraba “vagos” a quienes carecían de un oficio conocido,

así como a los jugadores habituales y a los ebrios consuetudinarios, quienes podían ser destinados forzosamente al servicio del ejército o la marina (Calle, 1906). Esta disposición adquiere un significado particular cuando se observa el contexto histórico. Tras las guerras de independencia, miles de excombatientes quedaron sin empleo ni medios de subsistencia. Como señala Charles Walker (1999), muchos de ellos pasaron a integrar los sectores populares urbanos y terminaron siendo perseguidos por las mismas autoridades que anteriormente habían requerido sus servicios militares.



Ilustración: IA – Gemini IA, prompt y edición Kelly Vásquez Chaparro

Otro aspecto revelador del reglamento fue el control ejercido sobre la población esclavizada. Los esclavos que huían de las haciendas podían recibir entre seis y doce azotes y, si permanecían prófugos durante largos periodos o se vinculaban con bandas de salteadores, las autoridades ordenaban su venta obligatoria a más de cincuenta leguas de Lima (Ministerio de Gobierno, 1839). Estas disposiciones muestran cómo la seguridad pública también se utilizaba como un mecanismo para preservar el orden social vigente.

Las restricciones alcanzaban igualmente la vida cotidiana de la población. Las pulperías y chinganas debían cerrar a las diez de la noche, y se prohibía realizar mudanzas desde el toque de oraciones hasta el amanecer. Cualquier persona sorprendida transportando muebles durante ese horario podía ser detenida mientras las autoridades verificaban la procedencia de los bienes, pues se presumía que podían provenir de un robo (Ministerio de Gobierno, 1839).

En conjunto, estas medidas muestran que la incorporación de nuevas tecnologías de iluminación fue acompañada por una creciente institucionalización del control policial.

La mejora del alumbrado no solo facilitó la vigilancia de las calles, sino que se integró a un sistema más amplio de regulación social, donde la tecnología y la legislación avanzaban de manera paralela para fortalecer la capacidad del Estado de mantener el orden público.

LA REVOLUCIÓN TECNOLÓGICA DEL GAS Y LA REORGANIZACIÓN DE LA POSTGUERRA

La segunda mitad del siglo XIX marcó un cambio decisivo en la historia de la seguridad urbana en el Perú. La incorporación de nuevas tecnologías industriales transformó no solo la iluminación de las ciudades, sino también la forma en que el Estado ejercía el control del territorio y protegía a la población.

Uno de los hitos más importantes ocurrió el 25 de mayo de 1851, cuando el Gobierno firmó el contrato para implantar el alumbrado público mediante gas de hulla. Esta innovación exigió una compleja infraestructura de aproximadamente 37 kilómetros de tuberías de hierro fundido instaladas bajo las calles del centro de Lima.

Gracias a este sistema, la ciudad pudo contar con una iluminación mucho más estable que la proporcionada por los antiguos faroles de aceite o de sebo, reduciendo progresivamente los espacios dominados por la oscuridad y facilitando la vigilancia nocturna.



Luz eléctrica

Sin embargo, como ocurrió con muchas innovaciones tecnológicas del siglo XIX, este avance también generó nuevos problemas. El sociólogo Joaquín Capelo (1895) observó que las

excavaciones necesarias para reparar las tuberías removían materiales en descomposición y contribuían a la propagación de enfermedades, un aspecto que abrió nuevas preocupaciones sobre la relación entre infraestructura urbana, salud pública y seguridad.

Mientras la iluminación transformaba la ciudad, las telecomunicaciones comenzaban a modificar la capacidad del Estado para administrar el territorio. El 6 de marzo de 1857 se inauguró la primera línea telegráfica entre Lima y el Callao (Clavero, 1885). Mucho antes de la expansión del alumbrado eléctrico, la telegrafía constituyó una de las primeras aplicaciones masivas de la electricidad y revolucionó la velocidad con la que circulaba la información oficial.

La segunda mitad del siglo XIX marcó un cambio decisivo en la historia de la seguridad urbana en el Perú. La incorporación de nuevas tecnologías industriales transformó no solo la iluminación de las ciudades.



Ilustración: IA – Gemini IA, prompt y edición Kelly Vázquez Chaparro

El control de las comunicaciones pronto adquirió una dimensión política. En 1874, ante el riesgo de disturbios en el sur del país, el presidente Manuel Pardo intervino el servicio telegráfico y designó un funcionario encargado de supervisar los mensajes privados, al considerar que la circulación de la información era un elemento estratégico para preservar el orden público (Clavero, 1885). Cuatro años más tarde, el Congreso declaró el servicio telegráfico propiedad exclusiva del Estado, consolidando así el control gubernamental sobre una infraestructura considerada esencial para la seguridad nacional.

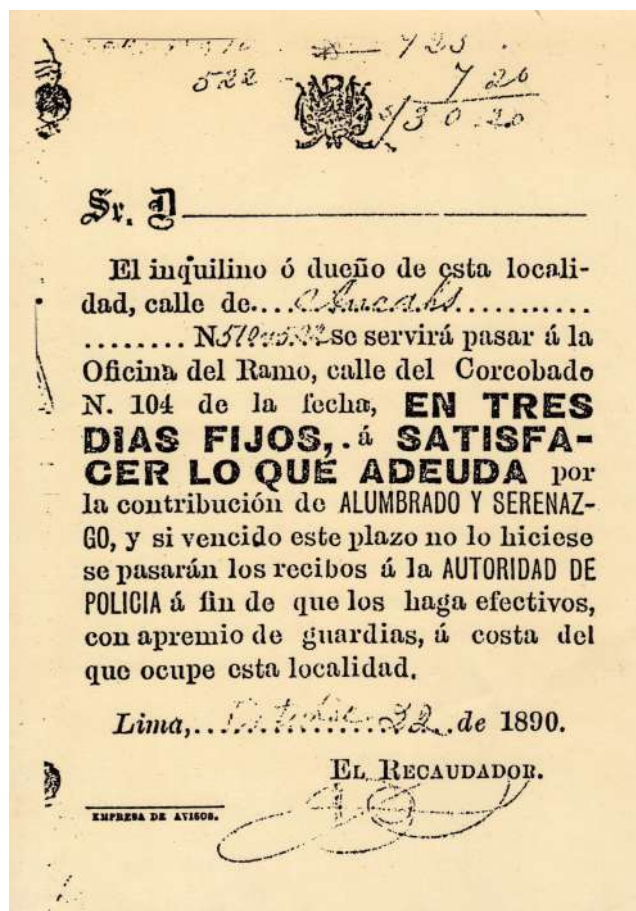
La Guerra del Pacífico (1879-1883) interrumpió este proceso de modernización y dejó una profunda huella sobre la infraestructura urbana y las instituciones del país. Tras la ocupación chilena, Lima debió reconstruir buena parte de sus servicios públicos en un contexto de graves limitaciones económicas.

En ese escenario se produjeron dos transformaciones estrechamente vinculadas con la seguridad ciudadana. La primera fue la introducción del alumbrado público eléctrico, inaugurado en mayo de 1886 gracias al marco legal

que facilitó la importación de dínamos eléctricos. Durante varios años, las nuevas luminarias convivieron con los tradicionales faroles de gas, ampliando progresivamente la cobertura del alumbrado urbano y mejorando las condiciones de vigilancia nocturna.

La segunda transformación correspondió a la reorganización del financiamiento de la seguridad pública. En junio de 1887, durante la alcaldía del general César Canevaro, la Municipalidad de Lima unificó la recaudación de los arbitrios de Serenazgo y Alumbrado Público, destinando una partida fija para el sostenimiento de la Guardia Civil (Canevaro, 1889). Esta decisión fortaleció la estabilidad financiera del servicio policial y redujo su dependencia de las dificultades fiscales que enfrentaba el Estado después de la guerra.

Ese mismo año se produjo otro avance significativo con la creación de la Oficina Rectificadora del Consumo de Gas, instalada en la Casa de Moneda. Equipada con instrumentos científicos importados de Europa, esta dependencia permitía medir la calidad, intensidad y pureza del gas utilizado para el alumbrado público, verificando el cumplimiento de los estándares



establecidos por la administración municipal (Canevaro, 1889). La innovación resulta especialmente interesante porque muestra un cambio en la forma de supervisar los servicios públicos: ya no bastaba con instalar infraestructura; también era necesario evaluar científicamente su funcionamiento.

La modernización tecnológica continuó en 1888 con la incorporación del teléfono. Los sistemas Bell y Ericsson permitieron conectar mediante líneas

directas los principales cuarteles y la Penitenciaría de Lima, reduciendo los tiempos de comunicación y facilitando la coordinación de las fuerzas encargadas del orden público (Clavero, 1885).

En conjunto, estos avances evidencian una transformación profunda. A mediados del siglo XIX, la seguridad dependía principalmente de la presencia física de vigilantes y patrullas. Hacia finales del mismo siglo, comenzaba a sustentarse también en redes de infraestructura, sistemas de comunicación y mecanismos técnicos de supervisión que ampliaban la capacidad del Estado para prevenir riesgos y responder con mayor rapidez a las situaciones de emergencia.

EL SIGLO XX Y LA TRANSICIÓN HACIA LA POLICÍA SANITARIA Y TECNOLÓGICA

El tránsito hacia el siglo XX estuvo acompañado por una transformación profunda en la manera de entender la seguridad pública. El crecimiento del Estado, la expansión hacia la Amazonía y los avances científicos modificaron progresivamente las funciones tradicionales de las instituciones

encargadas del orden. La seguridad dejó de centrarse exclusivamente en la vigilancia de las calles para incorporar nuevos ámbitos de intervención, como la salud pública, el control sanitario, la infraestructura y las comunicaciones.

Uno de los primeros ejemplos de este cambio fue el Reglamento de Explotaciones Agrícolas en la Montaña, promulgado por el presidente Nicolás de Piérola el 12 de junio de 1897 (Calle, 1906). La expansión de la actividad cauchera y la incorporación de maquinaria de vapor en la Amazonía obligaron al Estado a establecer nuevas normas para garantizar el funcionamiento de los campamentos y mantener el orden en regiones alejadas de los principales centros urbanos.

La policía en estas zonas quedó bajo la responsabilidad de los comisarios, quienes contaban con pequeñas unidades armadas de caballería. Ante posibles motines o conflictos, el reglamento autorizaba la organización de milicias civiles y permitía que haciendas y fundos dispusieran de un número limitado de armas para su defensa. Al mismo tiempo, el Estado fortaleció los mecanismos administrativos de control mediante el uso de libretas de tareas, documentos que registraban la actividad laboral

de los trabajadores y facilitaban su identificación. Asimismo, se prohibió el funcionamiento de cantinas dentro de los campamentos para reducir los conflictos asociados al consumo de alcohol (Calle, 1906).

La preocupación por el orden público también alcanzó los espacios de entretenimiento. El Reglamento de Teatros de Lima, promulgado en 1898, estableció normas destinadas a preservar el orden y la moral durante las funciones públicas. Entre otras disposiciones, prohibía que los artistas se dirigieran directamente al público o realizaran representaciones consideradas contrarias al decoro, otorgando a la autoridad municipal facultades para intervenir cuando estimara que estas afectaban el orden social (Calle, 1906).

Sin embargo, el cambio más significativo se produjo en el ámbito de la salud pública. Durante siglos, buena parte del abastecimiento de agua de Lima y el Callao había dependido de acequias y conducciones vulnerables a la contaminación. A comienzos del siglo XX, las investigaciones desarrolladas por Ramón Ribeyro, Ricardo Flores, Alberto García y Miguel Tamayo en el Instituto de Higiene transformaron

la comprensión de este problema mediante métodos bacteriológicos y análisis microscópicos (Calle, 1906).

Los estudios demostraron que el agua distribuida a la población contenía elevados niveles de bacterias y evidencias de contaminación fecal, además de microorganismos asociados con enfermedades como la fiebre tifoidea (Puente Arnao, 1907). Estos hallazgos proporcionaron una base científica para replantear las políticas sanitarias y mostraron que la protección de la población dependía también del conocimiento microbiológico.

Las investigaciones tuvieron consecuencias inmediatas. En marzo de 1905, el Gobierno ordenó cancelar las licencias de los aguadores ambulantes de Piura, quienes distribuían agua obtenida directamente del río, y dispuso que el abastecimiento se realizara exclusivamente mediante sistemas considerados seguros por las autoridades sanitarias (Puente Arnao, 1907). Esta decisión refleja un cambio importante en la forma de ejercer el control estatal: las medidas de seguridad comenzaron a sustentarse en evidencia científica producida por laboratorios especializados.

Paralelamente, el desarrollo de las comunicaciones continuó fortaleciendo la capacidad del Estado para administrar el territorio. Hacia 1907 se ampliaron la red ferroviaria y la telegrafía inalámbrica hacia la Amazonía, permitiendo una comunicación mucho más rápida entre Lima e Iquitos. Ese mismo año, los reglamentos expedidos por el gobierno de José Pardo declararon la telegrafía inalámbrica un recurso estratégico para la seguridad nacional, restringiendo el uso de claves cifradas por particulares y facultando a las autoridades para controlar determinados mensajes cuando consideraran que podían alterar el orden público.

El avance tecnológico también produjo efectos no previstos. La expansión del sistema de tranvías eléctricos en Lima, especialmente desde 1910, facilitó el desplazamiento de miles de personas por la ciudad, pero también creó nuevas oportunidades para la delincuencia. Los vagones abarrotados favorecieron el surgimiento del carterismo, una modalidad de hurto que aprovechaba la proximidad física entre los pasajeros para sustraer objetos personales sin recurrir a la violencia. Como señalan Jiménez Espinosa e Hidalgo Minaya (2009), el transporte masivo modificó no solo la movilidad urbana, sino también algunas formas de criminalidad cotidiana.



Este ejemplo ilustra una constante presente a lo largo de todo el artículo: cada innovación tecnológica amplía las capacidades del Estado para prevenir y controlar determinados riesgos, pero también genera nuevos desafíos que exigen respuestas institucionales y normativas. La historia de la seguridad ciudadana es, en buena medida, la historia de esa adaptación permanente.

CONCLUSIONES: EL COMÚN DENOMINADOR TECNOLÓGICO DE LA SEGURIDAD

El recorrido histórico presentado en este artículo muestra que la evolución de la seguridad pública en el Perú estuvo estrechamente vinculada a la incorporación de nuevas tecnologías. Desde los rondines nocturnos con antorchas organizados en el siglo XVI hasta la telegrafía inalámbrica, los laboratorios bacteriológicos y las primeras redes telefónicas de comienzos

del siglo XX, cada innovación amplió las capacidades del Estado para prevenir riesgos, vigilar el territorio y responder a situaciones de emergencia.

La siguiente tabla comparativa resume esta evolución del control del orden frente al delito a lo largo de este proceso histórico:

Dimensión de Control	Fase Republicana Temprana (1839)	Fase de Inicios del Siglo XX (1907)
Mecanismo de Vigilancia	Física, territorial y armada (Serenos con pistolas y sables)	Redes e infraestructuras técnicas (Ondas de radio, hilos telefónicos)
Enfoque contra el Crimen	Represión directa sobre los cuerpos (Cadenas, azotes, arresto nocturno)	Prevención y censura estratégica (Censura de claves, resguardo de archivos)
Prevención Social	Criminalización de la vagancia mediante el reclutamiento forzoso	Control documental del operario industrial (Libretas de tareas, agencias de enganche)
Policía de Salud Pública	Confinamiento por pestes y quema exterior de ropas de fallecidos	Microbiología aplicada (Clausura de aguadores, filtración bacteriológica)

La comparación permite apreciar una transformación profunda. Durante las primeras décadas republicanas, la seguridad descansaba principalmente en la vigilancia presencial y en mecanismos coercitivos dirigidos a controlar a las personas. Hacia comienzos del siglo XX, sin abandonar por completo esas prácticas, el Estado comenzó a incorporar herramientas científicas, sistemas de comunicación e infraestructura tecnológica que ampliaron significativamente sus capacidades de prevención y gestión.

Este proceso demuestra que la construcción de la seguridad ciudadana no dependió únicamente del fortalecimiento de las fuerzas del orden. También fue el resultado de la adopción progresiva de innovaciones científicas y tecnológicas que modificaron la forma de iluminar las ciudades, transmitir

información, supervisar los servicios públicos, controlar epidemias y administrar el territorio.

En perspectiva, la historia analizada permite comprender que muchos de los debates actuales sobre inteligencia artificial, vigilancia digital o análisis de datos tienen antecedentes de larga duración. Cada generación ha incorporado nuevas tecnologías para enfrentar los desafíos de su tiempo y, con ellas, ha debido responder también a preguntas sobre sus límites, riesgos e implicancias para la sociedad.

Comprender esa trayectoria histórica permite valorar la tecnología no solo como un conjunto de herramientas, sino como un factor que ha transformado, de manera continua, la relación entre el Estado, la ciencia y la seguridad ciudadana.



Referencias bibliográficas

Calle, J. J. (1906). *Diccionario de la legislación municipal del Perú* (Vol. 1). Imprenta Torres Aguirre.

Capelo, J. (1895). *Sociología de Lima*. Imprenta Masías.

Canevaro, C. (1889). *Memoria de la administración municipal de Lima (julio de 1887 a diciembre de 1888)*. Imprenta de Juan Francisco Solís.

Clavero, J. G. (1885). *Demografía de Lima en 1884*. Imprenta de Juan Francisco Solís.

Hidalgo, N. (2007). *Tejedores de luz: Homenaje a los forjadores de la transmisión eléctrica en el Perú*. REP.

Jiménez Espinosa, C., & Hidalgo Minaya, N. (2009). *Los tranvías de Lima (1878-1965)*. Museo de la Electricidad.

Ministerio de Gobierno del Perú. (1839). *Reglamento de Policía para la capital de la República y su provincia*. Imprenta de José Masías.

Puente Arnao, J. A. (1907). *Compilación de leyes, reglamentos y resoluciones de carácter general vigentes del Ministerio de Fomento y sus dependencias* (Vol. 4). Imprenta Prisma.

Walker, C. (1999). *De Túpac Amaru a Gamarra: Cusco y la formación del Perú republicano, 1780-1840*. Centro de Estudios Regionales Andinos Bartolomé de Las Casas.



DE LA ANTROPOLOGÍA CRIMINAL A LOS ALGORITMOS:

LA EVOLUCIÓN CIENTÍFICA DE LA SEGURIDAD

Gracia Angulo

A fines del siglo XIX, la ciudad de Lima experimentaba una gran transformación. Las viejas murallas coloniales habían sido derribadas apenas unas décadas atrás, dando paso a una expansión urbana que intentaba emular la modernidad parisina. Con la paulatina instalación del alumbrado público y el nacimiento de los primeros barrios obreros, la capital peruana no solo crecía en infraestructura, sino también en complejidad social. El crecimiento demográfico trajo dio origen a un fenómeno inevitable y preocupante para las élites de la época: el aumento de la percepción de inseguridad y la diversificación del delito.

En ese escenario de transición, las autoridades y los intelectuales de la República Aristocrática se dieron cuenta de que los viejos métodos de vigilancia —basados en la intuición de los serenos, el castigo ejemplar y el patrullaje intuitivo— eran insuficientes para contener las dinámicas de una urbe en vías de modernización. Fue en este momento histórico cuando la preocupación por el orden y la seguridad ciudadana abandonó los terrenos de la mera represión policial para buscar refugio en el rigor de la ciencia. La criminología, una disciplina naciente

en Europa, echó raíces en el Perú bajo una premisa ambiciosa: el delito no era simplemente un acto de maldad o de libre albedrío, sino un fenómeno físico, biológico y social que la ciencia podía —y debía— explicar, medir y, sobre todo, predecir.

EL CASO MAQUIAVELLO: LA CIENCIA ENTRA AL TRIBUNAL

Uno de los episodios más fascinantes de este despertar científico en el Perú se encuentra resguardado en la memoria impresa de la Biblioteca Nacional; específicamente, en su hemeroteca.

Se trata del célebre caso de Lorenzo Maquiavello (registrado en las fuentes de la época también como Machiavello), un joven impresor que en mayo de 1888 protagonizó un horrendo crimen múltiple en el puerto del Callao que conmocionó a la sociedad peruana. Más allá del impacto mediático y policial, el proceso judicial posterior —registrado exhaustivamente en folletos impresos por el Estado y debatido en las páginas de la emblemática Gaceta Médica de Lima— se convirtió en el primer gran laboratorio de debate científico sobre la criminalidad en nuestro país.



Portada del primer número de la Gaceta médica de Lima, fundada en 1827, y considerada la primera revista médica publicada por médicos peruanos

¿Por qué este caso marcó un hito? Porque por primera vez en los tribunales peruanos, los jueces no se limitaron a preguntar qué había hecho el acusado, sino por qué lo había hecho, convocando a la comunidad científica para hallar una respuesta. Influenciados directamente por la escuela del positivismo italiano, liderada por Cesare

Lombroso, los médicos, alienistas (los primeros psiquiatras) y juristas peruanos de la época intentaron aplicar las herramientas de la "antropología criminal".

Bajo esta corriente, se creía firmemente que el criminal era un ser atávico, un eslabón perdido en la

evolución humana cuyos instintos violentos estaban codificados en su propia anatomía. Así, los científicos de la Lima de inicios del siglo XX se dedicaron a medir cráneos, examinar los rasgos faciales, estudiar la asimetría de los rostros y escudriñar la herencia biológica de los procesados. El debate en torno a Maquiavello giró sobre si sus facultades mentales estaban alteradas por una "enfermedad cerebral" hereditaria o si su fisonomía revelaba la naturaleza de un "criminal nato". La ciencia de la época estaba convencida de que el secreto de la seguridad pública residía en descifrar la anatomía humana; si se lograba identificar físicamente los rasgos del delincuente, el Estado podría intervenir antes de que el delito se cometiera.

EL CAMBIO DE PARADIGMA: DEL INDIVIDUO AL ENTORNO URBANO

Visto con los ojos del siglo XXI, aquel enfoque biologicista nos resulta obsoleto, éticamente cuestionable y profundamente cargado de sesgos sociales. Hoy sabemos que la forma del cráneo o los rasgos faciales no determinan la conducta de una persona.

Sin embargo, si despojamos a la criminología positivista de sus teorías erradas, descubrimos que el impulso metodológico de fondo sigue siendo exactamente el mismo que nos mueve hoy: la necesidad imperiosa de utilizar el conocimiento empírico, la recolección de datos y la evidencia científica para prevenir el delito y garantizar la tranquilidad pública.

Casi un siglo y medio después del caso Maquiavello, la ciencia aplicada a la seguridad ciudadana ha dado un salto cuántico gracias a la revolución digital. La innovación contemporánea ha desplazado por completo la mirada desde la biología del individuo hacia las dinámicas del entorno urbano. Las herramientas de medición ya no son los calibradores craneales ni las autopsias psicológicas rudimentarias, sino los sistemas de información geográfica (SIG), el análisis de datos masivos (big data) y el desarrollo de la inteligencia artificial (IA).

La gran ventaja de la ciencia de datos moderna es que permite estudiar el delito como un fenómeno geográfico y temporal. Hoy en día, los algoritmos de analítica predictiva no intentan adivinar qué persona va a delinquir basándose en quién es, sino que analizan miles

de variables externas para determinar dónde y cuándo es más probable que ocurra un hecho delictivo. Estos sistemas procesan en tiempo real denuncias históricas, llamadas de emergencia, iluminación pública, flujos peatonales, cercanía a comercios, festividades e incluso variables climáticas. El resultado son los denominados “mapas de calor” dinámicos o hotspots, que permiten a las municipalidades y a la Policía Nacional del Perú (PNP) planificar un patrullaje integrado inteligente, optimizando los recursos humanos allí donde la matemática demuestra que se necesitan más.

VIGILANCIA INTELIGENTE Y EL RETO DE LOS SESGOS

La tecnología no solo predice, sino que vigila activamente de formas que los antiguos policías de Lima jamás habrían imaginado. Las cámaras de videovigilancia que pueblan nuestros distritos han dejado de ser simples grabadoras pasivas de video que requieren que un operario humano pase horas frente a una pantalla. Gracias al aprendizaje profundo (deep learning), estos dispositivos de última generación cuentan con sistemas de

analítica de video capaces de detectar comportamientos anómalos de manera automatizada: un vehículo circulando en sentido contrario, la aglomeración inusual de personas en una esquina oscura, o el abandono de un objeto sospechoso en la vía pública. Al emitir alertas instantáneas a los centros de monitoreo, la tecnología reduce los tiempos de respuesta de los serenazgos de minutos a escasos segundos.

No obstante, esta transición de la antropología criminal a los algoritmos también nos impone una profunda lección ética que conecta el pasado con el presente. Así como los científicos del siglo XIX introdujeron sus propios prejuicios de clase y raza en sus “estudios científicos” sobre el crimen, los algoritmos actuales corren el riesgo de perpetuar sesgos si las bases de datos con las que entrenamos a la IA están contaminadas por la discriminación. La verdadera innovación científica en seguridad ciudadana no solo implica desarrollar el software más avanzado, sino garantizar que estas herramientas digitales se utilicen bajo un marco de respeto estricto a los derechos humanos y la equidad social.

A MODO DE CIERRE

La evolución que va desde aquellos densos debates médicos en la Lima decimonónica hasta los modernos centros de control digital nos demuestra que la tecnología actual es la maduración de un viejo anhelo social. La ciencia y la innovación siempre han sido aliadas de la justicia, adaptando las herramientas de cada época a las necesidades de la comunidad.

Al hojear los folletos de juicios antiguos, las tesis universitarias olvidadas y las páginas amarillentas de los diarios que custodia la Biblioteca Nacional del Perú, descubrimos una valiosa continuidad histórica. Los algoritmos predictivos, las cámaras inteligentes y los softwares de georreferenciación que hoy resguardan nuestras calles no nacieron de la nada en un laboratorio extranjero: son los herederos modernos y perfeccionados de una larga, persistente y muy peruana búsqueda por poner la luz de la ciencia al servicio de la paz y la tranquilidad ciudadana.

La verdadera innovación científica en seguridad ciudadana no solo implica desarrollar el software más avanzado, sino garantizar que estas herramientas digitales se utilicen bajo un marco de respeto estricto a los derechos humanos y la equidad social.



Ilustración: IA — Gemini IA, prompt y edición Kelly Vásquez Chaparro

RESEÑAS DE AUTORES Y AUTORAS

Gracia Angulo Flores



Licenciada en Literatura por la Pontificia Universidad Católica del Perú, con más de quince años de experiencia en edición de publicaciones y gestión de proyectos de promoción y difusión del libro. Se ha desempeñado como investigadora literaria en la Casa de la Literatura (CASLIT). Asimismo, ha ocupado la coordinación del Área de Producción y Circulación del Libro de la Dirección del Libro y la Lectura del Ministerio de Cultura del Perú. Desde septiembre de 2018, se desempeña como editora de publicaciones de la Biblioteca Nacional del Perú.

Germain Garcis Zanabria



Docente auxiliar del Departamento de Ciencia de Computación y Datos de la Universidad de Ingeniería y Tecnología (UTEC). Obtuvo su grado de doctor [2017-2021] en Ciencia de la Computación de la Universidad de São Paulo (USP), Brasil. Obtuvo su maestría [2014-2016] en ciencia de la computación en la Universidad Católica San Pablo (UCSP), Perú. Realizó un posdoctorado en el Centro de Investigación e Innovación en Ciencia de la Computación (RICS) de la Universidad Católica San Pablo, donde investigó patrones de deserción en las universidades peruanas. Fue investigador invitado [2019] del Visualization Imaging and Data Analysis Center (VIDA) de la Universidad de Nueva York (NYU), EE. UU. Sus áreas de interés son: visualización de datos, visual analytics, machine learning, data science, análisis de crímenes, predicción de crímenes, análisis de dropout, datos georreferenciados, análisis espaciotemporales y computación aplicada a problemas sociales (AI for social good).

Juanpablo Heredia



Doctorando en ciencia de datos afiliado al laboratorio de Visual Data Science de la Fundação Getulio Vargas (FGV), en Río de Janeiro, Brasil, bajo la supervisión del Prof. Jorge Poco, beneficiario de una beca doctoral completa de la Fundação de Amparo à Pesquisa do Estado de São Paulo en la modalidad de Doctorado Directo. Su investigación se enfoca en el análisis de datos espaciotemporales y la analítica visual, con especial interés en el aprendizaje profundo geométrico y la inteligencia artificial explicable. Previamente, fue investigador en el proyecto RUTAS de la Universidad Católica San Pablo (Arequipa, Perú), donde trabajó en visión por computador y en aprendizaje profundo multimodal. Es bachiller en ciencia de la computación (2021) por la misma institución.

Neydo Hidalgo



Historiador y museólogo, especializado en historia de la tecnología y la energía en el Perú. Ha desempeñado roles clave en la preservación y difusión del patrimonio científico y tecnológico del país. Fue secretario ejecutivo del Comité Peruano de Patrimonio Industrial y estuvo a cargo del Museo de la Electricidad hasta 2016. Actualmente se desempeña como Coordinador de la Unidad de Popularización de la CTI, CONCYTEC. Es miembro de la Asociación Peruana de Historia y Estudios Sociales de la Ciencia, la Tecnología y la Salud (APHESCTS).

Noam López Villanes



Es politólogo y asesor internacional especializado en reforma policial, gobernanza forense y modernización del sector seguridad. Ha ocupado cargos de alta dirección en instituciones del Estado peruano, donde dirigió el análisis criminal estratégico, sistemas de gestión del conocimiento en seguridad e iniciativas de modernización institucional.

Noam se desempeñó como asesor para el Perú del Proyecto Justicia Forense de GTH-DNA, apoyando esfuerzos legislativos e institucionales para fortalecer los sistemas forenses y los marcos nacionales de bases de datos de ADN. Asimismo, coordinó la iniciativa "Assisting Security" del John Jay College of Criminal Justice, promoviendo estrategias de policiamiento basadas en datos y el fortalecimiento de capacidades institucionales.

Con más de una década de experiencia en políticas públicas y gobernanza de la seguridad, ha asesorado a entidades gubernamentales en sistemas de información para la toma de decisiones, modernización policial y estrategias de seguridad basadas en evidencia. Su trabajo integra diseño institucional, desarrollo normativo y analítica avanzada de datos.

Actualmente es candidato a doctor en Ciencia Política y Gobierno por la Pontificia Universidad Católica del Perú (PUCP). Cuenta con una Maestría en Ciencias con mención en Proyectos de Inversión por la Universidad Nacional de Ingeniería y es Licenciado en Ciencia Política y Gobierno por la PUCP.

Felipe Moreno-Vera



Doctorando en ciencia de datos afiliado al laboratorio de Visual Data Science de la Fundação Getulio Vargas (FGV), en Río de Janeiro, Brasil, bajo la supervisión del Prof. Jorge Poco. Su investigación se centra en el análisis de datos sobre la percepción urbana, la IA generativa y la interpretabilidad de los modelos. Previamente, obtuvo su título de maestría en la Universidad Católica San Pablo (Arequipa, Perú), donde trabajó en visión por computador y en aprendizaje profundo aplicado a la percepción urbana. Es bachiller en Ciencia de la Computación (2017) por la Universidad Nacional de Ingeniería (UNI), Lima, Perú.

Lizbardo Orellano



Ingeniero en Sistemas e Informática, magíster en Ciencia Criminalística y en Ciberseguridad, investigador RENACYT-CONCYTEC y perito en análisis digital forense del Ministerio Público. Cuenta con experiencia especializada en informática forense, ciberdelincuencia, ciberseguridad, análisis de evidencias digitales, inteligencia artificial aplicada a investigaciones criminalísticas y respuesta ante incidentes relacionados con hacking, phishing, ransomware, malware, suplantación de identidad y ataques a sistemas informáticos.

Se desempeña como docente de posgrado en la Universidad Norbert Wiener y la Universidad Continental, en programas vinculados a ciberseguridad, criminalística, informática forense, metodología de la investigación y tesis. Posee certificaciones en ISO/IEC 27001, ciberseguridad, Scrum e inteligencia artificial generativa, además de formación nacional e internacional en análisis forense

digital, ciberdefensa, ciberdelincuencia, fotografía forense, audio, imagen y video forense.

Su perfil integra artículos científicos, publicaciones académicas y experiencia técnica, académica e investigativa, orientada al fortalecimiento de la seguridad digital, la investigación criminalística, la formación especializada y el uso responsable de tecnologías emergentes como la inteligencia artificial.

Jorge Poco



Es profesor asociado en la Escuela de Matemática Aplicada de la Fundação Getulio Vargas (FGV), en Brasil, donde lidera el Visual Data Science Lab. Obtuvo el doctorado en Computer Science en New York University, la maestría en Computer Science en la Universidade de São Paulo (USP) y el título de ingeniero de sistemas en la Universidad Nacional de San Agustín (UNSA), en Perú. Anteriormente fue profesor asistente en la Universidad Católica San Pablo (UCSP), en Perú, y research associate en el Interactive Data Lab (IDL) de la University of Washington. En el ámbito profesional, también trabajó como ingeniero de software en zAgile Inc. y realizó prácticas en Google, Kitware, Oak Ridge National Laboratory y Xerox Research. Su investigación se centra en la visualización de datos, el análisis visual, el aprendizaje automático y la ciencia de datos, con colaboraciones interdisciplinarias orientadas al análisis de datos urbanos, climáticos y sociales, así como al estudio de la percepción urbana, la seguridad pública y la interpretación automática de gráficos mediante inteligencia artificial. Además, ha participado activamente en comités de programas de conferencias como IEEE SciVis, IEEE InfoVis, IEEE VAST, EuroVis y CHI.



Economista, con grado académico de Doctor en Economía, otorgado por la Universidad Nacional Mayor de San Marcos, además con grados académicos de Magíster en Economía con mención en Política Económica, y en Gestión Pública de la Universidad del Pacífico. Es también, egresado de la Maestría en Estadística e Informática de la Facultad de Matemáticas de la UNMSM.

Ha cursado estudios de especialización del BID, FM y otras instituciones. Se desempeñó como Sub jefe de Estadística del Instituto Nacional de Estadística e Informática - INEI, por 16 años (2006-2022). Ha sido jefe del INEI (2015-2017). Con una fructífera carrera en la gestión pública de más de cuarenta años, ejerciendo diversos cargos de responsabilidad en materia estadística, y con experiencia en el planeamiento, organización, ejecución, supervisión y control de Censos y Encuestas Especializadas.

Ha ejercido la docencia en la Unidad de Postgrado de Ciencias Económicas y de Ciencias Sociales de la Universidad Nacional Mayor de San Marcos, también en el Post Grado de la Universidad Católica Santa María, y otras universidades. Es autor de varias publicaciones: "Acumulación de Capital y Reproducción en la Agricultura Peruana, 1970-2008" (2012), "Cambios demográficos y movilidad laboral en Asia Pacífico" (2010), "La Fuerza económica de las migraciones internas" (2014), "Criminalidad y Seguridad Ciudadana en el Perú del siglo XXI" (2018). Es autor del ensayo "Delincuencia y Seguridad Ciudadana, Mirando al Bicentenario" (2014) que ganó el Primer lugar del Concurso: "Peruanos del Bicentenario" organizado por el diario El Comercio en la Categoría de Seguridad Ciudadana.

