PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ESCUELA DE POSGRADO

Aseguramiento de la Disponibilidad de Metadatos de Localización de Dispositivos Móviles para Potenciar la Investigación Criminal

Trabajo de Investigación para obtener el grado académico de Maestro en Gobierno y Políticas Públicas que presenta:

Walter Lozano Pajuelo

Juan Carlos Samaniego Miranda

Asesor:

Luis Felipe Soltau Salcedo

Lima, 2025

INFORME DE SIMILITUD

Yo, Luis Felipe Soltau Salcedo, docente de la Escuela de Posgrado de la Pontificia Universidad Católica del Perú, asesor del trabajo de investigación titulado "Aseguramiento de la disponibilidad de metadatos de localización de dispositivos móviles para potenciar la investigación criminal", de los autores Walter Lozano Pajuelo y Juan Carlos Samaniego Miranda, dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 15%. Así lo consigna el reporte de similitud emitido por el software *Turnitin* el 06/08/2025.
- He revisado con detalle dicho reporte y el trabajo de investigación, y no se advierte indicios de plagio.
- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lugar y fecha:
Lima, 17 de septiembre del 2025.

<table>
<tr><td colspan="2">Apellidos y nombres del asesor / de la asesora:

Soltau Salcedo, Luis Felipe</td></tr>
<tr><td>DNI: 10273813</td><td rowspan="2">Firma:
  </td></tr>
<tr><td>ORCID: 0000-0003-4304-5893</td></tr>
</table>

RESUMEN

El proyecto de innovación aborda el incremento de delitos violentos cometidos por bandas y organizaciones criminales en Lima Metropolitana durante 2021-2023, periodo en el que se registró un aumento del 107.5% en estos ilícitos. Frente a esta problemática, se propone desarrollar el "Sistema Integrado de Gestión de Metadatos de Localización (SIGMEL)", una solución innovadora que potencia las capacidades de investigación criminal mediante el acceso controlado a los metadatos de localización de dispositivos móviles. El sistema aprovecharía la infraestructura del "Programa Constelación" - Sistema de Intervención Legal de las Comunicaciones e incorpora tres componentes fundamentales: un marco legal específico que regula la retención y acceso a metadatos, una plataforma tecnológica integrada y un programa de capacitación especializada. La evaluación de deseabilidad, factibilidad y viabilidad confirma que SIGMEL representa una solución técnicamente viable, económicamente sostenible y jurídicamente válida para fortalecer la persecución penal del crimen organizado, garantizando simultáneamente el respeto a los derechos fundamentales de los ciudadanos.

ABSTRACT

The innovation project addresses the increase in violent crimes committed by gangs and criminal organizations in Metropolitan Lima during 2021-2023, a period in which a 107.5% increase in these crimes was recorded. Faced with this problem, it is proposed to develop the "Sistema Integrado de Gestión de Metadatos de Localización (SIGMEL)", an innovative solution that enhances criminal investigation capabilities through controlled access to the location metadata of mobile devices. The system would take advantage of the infrastructure of the "Programa Constelación" - Sistema de Intervención Legal de las Comunicaciones and incorporates three fundamental components: a specific legal framework that regulates the retention and access to metadata, an integrated technological platform, and a specialized training program. The desirability, feasibility, and viability assessment confirm that SIGMEL represents a technically viable, economically sustainable, and legally valid solution to strengthen the criminal prosecution of organized crime, while simultaneously guaranteeing respect for the fundamental rights of citizens.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

INTRODUCCIÓN

La seguridad pública representa uno de los desafíos más críticos que enfrenta el Perú contemporáneo. En un país que alberga más de 33 millones de habitantes, según las proyecciones del Instituto Nacional de Estadística e Informática (INEI, 2023b), el incremento sostenido de los índices de criminalidad genera profunda preocupación. Las estadísticas del 2022 son reveladoras: más de 300,000 denuncias por delitos de robo y hurto violentos, además de más de 2,000 homicidios registrados (SIDPOL, 2023), cifras que muestran la gravedad del problema y sus consecuencias en el bienestar de nuestra nación.

El panorama criminal en el Perú ha experimentado una transformación alarmante en los últimos años. Las bandas criminales han evolucionado desde estructuras simples hacia organizaciones complejas que aprovechan las tecnologías de comunicación para coordinar sus actividades delictivas. La UNODC confirmó en el 2019 que estas redes se han vuelto sofisticadas, adoptando métodos de operación que desafían los enfoques tradicionales de investigación criminal. Esta evolución tecnológica del crimen organizado contrasta dramáticamente con las limitaciones que enfrentan nuestras instituciones de justicia para acceder a la evidencia digital necesaria en las investigaciones.

Los métodos tradicionales de investigación criminal - declaraciones testimoniales, interrogatorios y análisis de evidencia física - siguen siendo fundamentales, pero resultan insuficientes para desmantelar las redes criminales contemporáneas que operan en el entorno digital. El sistema de justicia penal requiere necesariamente una actualización cualitativa de sus capacidades investigativas para enfrentar eficazmente la criminalidad organizada moderna.

En este contexto, emerge como alternativa innovadora el aprovechamiento de los metadatos de localización generados por los dispositivos móviles en las plataformas tecnológicas de los operadores de telecomunicaciones. Los metadatos de localización constituyen elementos informativos que documentan las coordenadas geográficas (latitud, longitud, altitud), la precisión espacial, la marca temporal y la fuente de posicionamiento utilizada para determinar la ubicación geográfica de dispositivos computacionales móviles en tiempo real (World Wide Web Consortium, 2022). Para los investigadores criminales, esta información resulta de especial relevancia porque permite establecer la presencia de sospechosos en coordenadas espacio-temporales asociadas a la comisión de hechos punibles, fortaleciendo así la construcción de elementos de convicción (García Marcos, 2021).

La implementación de esta capacidad investigativa plantea, sin embargo, complejos desafíos que trascienden los aspectos meramente técnicos y legales. El equilibrio entre la eficacia investigativa y la protección de la privacidad ciudadana constituye el núcleo del debate contemporáneo sobre el uso de tecnologías digitales en la persecución penal. La experiencia internacional demuestra que es posible aprovechar los metadatos de localización para la investigación criminal sin comprometer los derechos fundamentales de las personas, siempre que se implementen marcos normativos adecuados y mecanismos de control institucional efectivos.

Este proyecto de investigación evalúa integralmente el potencial impacto del uso controlado de metadatos de localización en las investigaciones de delitos violentos en Lima Metropolitana, específicamente aquellos perpetrados por bandas y organizaciones criminales durante el periodo 2021-2023. La investigación trasciende el análisis teórico para examinar empíricamente cómo esta herramienta tecnológica podría fortalecer las capacidades del sistema de justicia penal peruano sin vulnerar los derechos constitucionales de los ciudadanos.

La metodología empleada combina el análisis de la legislación nacional con el estudio comparado de experiencias internacionales exitosas en materia de retención y acceso a metadatos de localización. Asimismo, se evalúan las capacidades técnicas e institucionales actuales de la Policía Nacional del Perú, el Ministerio Público y el Poder Judicial para implementar responsablemente un sistema de gestión de metadatos de localización.

Los resultados de esta investigación buscan proporcionar respuestas fundamentadas a interrogantes cruciales: ¿Constituye el uso de metadatos de localización una herramienta viable y efectiva para fortalecer la investigación de delitos violentos en el Perú? ¿Qué marco legal e institucional se requiere para garantizar su implementación responsable? ¿Cómo puede contribuir esta innovación a reducir los alarmantes índices de impunidad que caracterizan la persecución del crimen en nuestro país?

Más allá del diagnóstico académico, este proyecto pretende ofrecer una propuesta concreta y viable que oriente al Estado peruano hacia el fortalecimiento de sus capacidades de investigación criminal. La propuesta del Sistema Integrado de Gestión de Metadatos de Localización (SIGMEL) representa una respuesta innovadora que busca equilibrar la necesidad de herramientas investigativas efectivas con el respeto irrestricto a los derechos fundamentales y las garantías constitucionales.

En última instancia, esta investigación contribuye al desarrollo de políticas públicas basadas en evidencia para el sector justicia, explorando cómo la integración responsable de tecnologías digitales puede transformar la capacidad del Estado para proteger a sus ciudadanos del crimen. El conocimiento, como nos enseñara Francis Bacon, constituye poder; pero en la era digital, ese poder debe ejercerse con sabiduría, responsabilidad y un compromiso inquebrantable con la construcción de un Perú donde la seguridad y la justicia caminen de la mano con la protección de los derechos fundamentales.

CAPÍTULO 1: DEFINICIÓN Y DESCRIPCIÓN DEL PROBLEMA PÚBLICO

Este capítulo desarrolla integralmente el problema público identificado, trascendiendo el análisis superficial para examinar sus dimensiones fundamentales. La investigación se apoya en evidencia estadística rigurosa y análisis cualitativos que revelan la verdadera magnitud del fenómeno estudiado. Particular atención se dedica a comprender las repercusiones directas sobre la ciudadanía y el papel que desempeña cada institución involucrada en el problema. El capítulo también examina críticamente las respuestas institucionales implementadas hasta la fecha, evaluando tanto el marco normativo vigente como los programas y políticas públicas que el Estado ha desplegado para enfrentar esta problemática.

1.1. Redacción formal del problema público

La identificación precisa del problema público constituye el fundamento metodológico de todo proyecto de innovación en el sector público. Esta sección desarrolla sistemáticamente el proceso de selección, delimitación y formalización del desafío central que orienta la presente investigación.

El problema público analizado en el presente trabajo fue seleccionado mediante la evaluación sistemática de múltiples alternativas identificadas preliminarmente, aplicando criterios específicos de relevancia, disponibilidad de datos y ausencia de soluciones previas. Una vez establecido el problema central, se procedió a su redacción formal conforme a la metodología establecida.

Para conocer el proceso completo de identificación y los criterios de selección utilizados, así como la descripción de los problemas públicos alternativos considerados, consulte el Anexo 1: Descripción de los tres problemas públicos identificados en la etapa 1 y cuál de ellos ha sido seleccionado.

Construcción y redacción formal del problema

Siguiendo la metodología establecida en la Guía para Proyectos Finales de Innovación, el problema público seleccionado corresponde a la tipología de “afectación directa a la sociedad”, dado que impacta directamente en el bienestar y seguridad de la población de Lima Metropolitana.

El problema público identificado se redacta formalmente de la siguiente manera:

"Incremento significativo **[condición]** de delitos violentos cometidos por bandas y organizaciones criminales **[fenómeno social negativo]** que afectan a la población **[ciudadanos afectados]** de Lima Metropolitana **[lugar donde habitan los ciudadanos afectados]** durante el periodo 2021-2023 **[lapso de tiempo de análisis]**".

Esta estructura del problema satisfizo los cinco elementos constitutivos de un problema de una amenaza directa y directa a la sociedad.

Primero, la condición. La condición en cuestión es descrita en la palabra clave utilizada "incremento significativo"; esta condición se basa en los datos generados por el SIDPOL PNP (SIDPOL PNP, 2023) y el INEI (INEI, 2023a), que documentan un aumento del 107.5% en el número de hechos de delitos violentos cometidos por estructuras criminales organizadas.

Segundo, el fenómeno social negativo. Se expone este fenómeno en la formulación "el delito violento cometido por bandas y organizaciones criminales". Es un sistema de peligro que sistematiza la seguridad ciudadana; la investigación de IMA GO (IMA GO, 2023) corrobora que se ha registrado un miedo perenne debido a este problema, lo que empeora significativamente la calidad del hábitat urbano.

Tercero, los ciudadanos afectados. Se refieren a "la población de Lima Metropolitana" observan un impacto transversal en todos los habitantes de la capital, sin importar grupos demográficos específicos.

Cuarto, existe una delimitación geográfica: Lima Metropolitana es el territorio donde este fenómeno se manifiesta con mayor fuerza. La capital del Perú concentró el 54.5% de las bandas desarticuladas en el 2022 (Ministerio del Interior, 2022).

Finalmente, quinto, la delimitación real temporal ha definido el análisis del "periodo 2021-2023". La razón es que este es el ciclo postcovid en el que las estructuras criminales se adaptaron activamente a las nuevas condiciones sociales y tecnológicas.

1.2. Marco conceptual del problema público

Considerando que en todo trabajo de investigación se debe tener claro qué se entiende por cada uno de los términos clave que conforman el problema a investigar, procedemos a conceptualizar cada uno de ellos.

Delito violento: Un delito violento, de acuerdo con la definición del Buró Federal de Investigaciones (FBI, 2019), se entiende como el empleo o la amenaza de empleo de fuerza física contra una o varias personas. Se destacan: casos de homicidio y feminicidio, violación, robo a mano armada, asaltos agravados, secuestros, entre otros. La investigación de Jaitman y Machin (Jaitman y Machin, 2015) revela que estas acciones delictivas tienen distintos efectos nocivos muy por encima de las víctimas y generan una reacción en cadena: disolución social, la disfunción económica y el decrecimiento en la acción y capacidad comunitaria.

Bandas criminales: Según el informe del Programa de las Naciones Unidas para el Desarrollo (PNUD, 2013) una banda criminal es un grupo de personas, casi siempre jóvenes, organizados para la comisión de actividades ilícitas violentas y que operan ilícita y violentamente para el control de un territorio o mercado zonal o local. A pesar de tener los mismos intereses, tienen menos atributos complejos y son menos estacionales que las organizaciones criminales, estas últimas representan un típico riesgo a priori.

Organizaciones criminales: Son definidas por la Ley N° 30077 – Ley Contra el Crimen Organizado en su artículo 2 como "… todo grupo con compleja estructura desarrollada y mayor capacidad operativa compuesto por tres o más personas con carácter permanente o por tiempo indefinido que, de manera concertada y coordinada, se reparten roles correlacionados entre sí, para la comisión de delitos de extorsión, secuestro, sicariato …".

Percepción de inseguridad: Muratori y Zubieta (2013) conceptualizan este fenómeno como la sensación subjetiva de temor y vulnerabilidad que experimentan las personas ante la posibilidad de ser víctimas de delitos. Esta percepción resulta de la interacción compleja entre experiencias de victimización directa o indirecta, exposición mediática a información sobre criminalidad, características del entorno urbano y niveles de confianza institucional. La investigación de Vozmediano, San Juan y Vergara (2008) demuestra que la percepción de inseguridad puede operar independientemente de los índices objetivos de criminalidad.

Datos vs. Metadatos de Localización: Es crucial para apoyar la comprensión del proyecto de investigación conocer sus alcances. El primero se refiere a la información primaria generada por los dispositivos y sus productos, abarcando incluso hasta su contenido, y la segunda están referidos a la información sobre esos datos de localización, que describen sus características, sin referirse al contenido de los mismos (International Organization for Standardization, 2014).

Específicamente, los metadatos de localización constituyen elementos informativos que documentan las coordenadas geográficas, la precisión espacial, la marca temporal y la fuente de posicionamiento utilizada para determinar la ubicación geográfica de dispositivos en tiempo real, conforme a las especificaciones del estándar W3C Geolocation API (World Wide Web Consortium, 2022). Estos metadatos incluyen coordenadas geográficas, identificadores de estaciones base, marcas temporales y datos de conexión que permiten reconstruir patrones de movilidad sin comprometer la privacidad del contenido comunicacional.

Geolocalización: García Marcos (2021) la define como la tecnología que permite determinar la ubicación geográfica precisa de un dispositivo mediante coordenadas espaciales obtenidas a través de sistemas GPS, triangulación de señales celulares o identificación de redes Wi-Fi. La precisión de la geolocalización varía desde metros hasta kilómetros, dependiendo de la tecnología empleada y las condiciones ambientales (Ramírez, 2023).

Prueba: En el contexto procesal penal, Rosas Yataco (2013) define la prueba como todo medio u objeto que contribuye a acreditar un hecho delictivo y la responsabilidad penal del imputado, actuada durante el juicio oral bajo los principios de contradicción, oralidad, inmediación y publicidad.

Elemento de convicción: Villegas Paiva (2013) distingue estos elementos como medios probatorios recolectados unilateralmente durante la investigación preparatoria que permiten establecer indicios suficientes sobre la comisión del delito y la responsabilidad del imputado. A diferencia de las pruebas judiciales, los elementos de convicción son obtenidos por el fiscal con apoyo policial durante las fases preliminares de la investigación (Salinas, 2022).

1.3. Arquitectura del problema público

La comprensión integral de este problema público demanda el análisis sistemático de cuatro dimensiones fundamentales que configuran su arquitectura:

- Magnitud cuantitativa del incremento de delitos violentos en Lima Metropolitana.
- Modus operandi de las bandas y organizaciones criminales.
- Impacto social en la seguridad ciudadana y percepción de inseguridad.
- Respuesta institucional del sistema de justicia penal frente al problema.

Para estructurar el análisis de estas dimensiones, se ha desarrollado una matriz de consistencia que establece las preguntas de investigación, objetivos, hipótesis, fuentes de datos y herramientas metodológicas para cada una de ellas. Esta matriz guía el proceso de investigación, asegurando un enfoque sistemático y coherente en el estudio del incremento de delitos violentos en Lima Metropolitana.

La aplicación práctica de esta matriz metodológica requiere el desarrollo detallado de cada componente investigativo. Para una descripción exhaustiva de la matriz de consistencia, incluyendo las preguntas específicas, objetivos, hipótesis y metodologías correspondientes a cada dimensión analítica, consulte el Anexo 02: Matriz de Consistencia del Diseño de Investigación sobre la arquitectura del problema público.

1.3.1. Magnitud del incremento de crímenes violentos en Lima Metropolitana en el periodo 2021-2023

La evidencia estadística revela una tendencia alarmante en Lima Metropolitana. Según el INEI (2023a), durante el segundo semestre de 2023, el 32.3% de los habitantes mayores de 15 años experimentaron algún hecho delictivo. Esta cifra representa una escalada progresiva desde el 22.5% registrado en 2021, transitando por 26.1% en 2022, hasta alcanzar el nivel actual. El incremento acumulado de 9.8 puntos porcentuales en tres años confirma el deterioro sistemático de la seguridad en la capital.

Los datos del Sistema de Denuncias Policiales (SIDPOL, 2023) documentan incrementos específicos en delitos violentos asociados al crimen organizado:

Extorsión: Experimentó el aumento más dramático, escalando desde 928 casos en 2021 hasta 7,978 en 2023, representando un incremento acumulado del 759.5%. Esta modalidad delictiva evidencia la sofisticación creciente de las organizaciones criminales.

Homicidios: Aumentaron sostenidamente de 521 casos en 2021 a 845 en 2023, marcando un incremento del 62.2% que refleja la intensificación de la violencia criminal en la capital.

Robos: Evolucionaron desde 56,526 incidentes en 2021 hasta 111,486 en 2023, prácticamente duplicándose con un incremento del 97.2%.

Secuestros: Aunque mostraron variaciones menores, mantuvieron niveles preocupantes con 73 casos en 2021, 85 en 2022 y 58 en 2023.

En conjunto, los delitos violentos en Lima Metropolitana experimentaron un incremento del 107.5% entre 2021 y 2023, confirmando la hipótesis de investigación sobre el deterioro acelerado de la seguridad ciudadana en la capital.

Las herramientas metodológicas específicas utilizadas para esta investigación se detallan en el Anexo 03: Herramientas de recojo de información para la arquitectura del problema público.

1.3.2. Modus operandi de bandas y organizaciones criminales en Lima Metropolitana

El análisis del comportamiento delictivo revela patrones operativos característicos que permiten comprender la evolución del crimen organizado en la capital.

Concentración territorial: La labor de desarticulación policial durante 2022 documentó la eliminación de 2,706 bandas criminales en Lima Metropolitana, representando el 54.5% del total nacional (Ministerio del Interior, 2022). Esta concentración evidencia tanto la densidad del problema como la intensidad de los esfuerzos institucionales de respuesta.

Focalización geográfica: Los distritos con mayor incidencia de victimización por delitos patrimoniales fueron San Juan de Lurigancho (7,686 denuncias), Ate (5,193), San Martín de Porres (2,402), Santiago de Surco (2,003) y Los Olivos (1,718). Estos cinco distritos concentraron el 28% del total de denuncias patrimoniales en 2022, evidenciando la preferencia criminal por zonas periféricas de alta densidad poblacional con limitado acceso a servicios básicos.

Especialización delictiva: Los delitos contra el patrimonio representaron el 61% de las denuncias policiales en 2022. Dentro de esta categoría, el robo (31%) y el hurto (47%) concentraron el 78% de los casos, indicando la priorización criminal de actividades de despojo patrimonial por su rentabilidad económica y facilidad ejecutiva.

Escalamiento en el uso de armas: Entre enero y noviembre de 2023, el 11.1% de la población limeña mayor de 15 años fue víctima de delitos cometidos con arma de fuego (Ministerio del Interior, 2024), evidenciando una tendencia creciente en la disponibilidad y uso de armamento ilegal.

Vinculación con narcomenudeo: La UNODC (2022) identificó en Lima Metropolitana una relación simbiótica entre bandas criminales y redes de micro comercialización de drogas. En distritos como San Juan de Lurigancho, Ate y Comas, las bandas ejercen control territorial sobre "puntos de acopio" de drogas, proporcionando seguridad, abastecimiento y distribución. Esta simbiosis genera disputas territoriales y enfrentamientos que intensifican la violencia barrial.

Las herramientas metodológicas específicas utilizadas para esta investigación se detallan en el Anexo 3: Herramientas de recojo de información para la arquitectura del problema público.

1.3.3. Impacto en la seguridad ciudadana y percepción de inseguridad en Lima Metropolitana

La Encuesta Nacional de Programas Presupuestales (ENAPRES) documenta un deterioro objetivo de la seguridad: el porcentaje de personas mayores de 15 años victimizadas se elevó del 33.1% en 2021 al 37.8% en 2022, registrando un incremento de 4.7 puntos porcentuales (INEI, 2023b).

Percepción ciudadana: La Encuesta Lima Cómo Vamos 2022 revela que el 75% de limeños percibe incremento en la delincuencia respecto al año anterior. El 82.2% se siente inseguro en espacios públicos y el 86.7% teme ser víctima de asaltos. Estos hallazgos coinciden con la encuesta nacional de IMA GO (2023), donde el 89% de peruanos afirma sentirse inseguro al salir de casa.

Prioridades de seguridad: Los ciudadanos identifican como principales problemas los robos (65%), micro comercialización de drogas (58%) y homicidios (42%) (Lima Cómo Vamos, 2022). A nivel nacional, los asaltos a mano armada (58%) y robos motorizados (52%) concentran la preocupación ciudadana (IMA GO, 2023).

Victimización directa e indirecta: El 62% de limeños ha sido víctima directa o tiene familiares afectados por delitos en el último año (Lima Cómo Vamos, 2022). Nacionalmente, el 78% de peruanos ha experimentado asaltos o tiene allegados victimizados (IMA GO, 2023).

Adaptaciones comportamentales: La inseguridad ha obligado al 59% de limeños a modificar rutinas cotidianas, evitando zonas peligrosas (48%), reduciendo uso de efectivo

(34%), adquiriendo seguros (24%) y privilegiando transporte por aplicativos (22%). Adicionalmente, el 55% ha asumido gastos adicionales en seguridad privada para sus viviendas.

Las herramientas metodológicas específicas utilizadas para esta investigación se detallan en el Anexo 03: Herramientas de recojo de información para la arquitectura del problema público.

1.3.4. Respuesta de las instituciones del sistema de justicia penal frente al problema en Lima Metropolitana en el periodo 2021-2023

El análisis de la respuesta institucional revela limitaciones sistémicas que comprometen la eficacia de la persecución penal del crimen organizado violento.

Limitaciones policiales: El Informe Estadístico de Seguridad Ciudadana de la Municipalidad Metropolitana de Lima (2022) documenta un incremento en operativos policiales y capturas, pero apenas el 32% de cabecillas capturados recibió prisión preventiva en 2022. El informe identifica deficiencias críticas en el sustento probatorio de las investigaciones policiales, particularmente en la obtención de evidencia tecnológica.

La Policía Nacional del Perú enfrenta limitaciones tecnológicas críticas derivadas de la ausencia de un marco legal que obligue a las empresas operadoras de telecomunicaciones a retener metadatos de localización de dispositivos móviles. Los contratos de concesión vigentes y la legislación actual no establecen esta obligación, lo que impide gravemente la eficacia investigativa en casos de delitos violentos. Esta carencia resulta especialmente problemática en investigaciones de homicidios, donde resulta fundamental identificar qué dispositivos móviles estuvieron presentes en el lugar del crimen y reconstruir los patrones de seguimiento previo de las víctimas. Sin acceso a estos metadatos históricos, los investigadores pierden la capacidad de establecer la presencia espacio-temporal de sospechosos en ubicaciones críticas para la investigación, debilitando significativamente la construcción de elementos de convicción en casos de crimen organizado.

La ausencia de capacidades de geolocalización ha impactado negativamente en investigaciones criminales, donde la imposibilidad de demostrar la presencia de sospechosos en escenarios delictivos específicos constituye una limitación probatoria significativa. Esta carencia tecnológica resulta particularmente crítica en investigaciones de crimen organizado,

donde la demostración de la coordinación espacio-temporal entre miembros de organizaciones criminales constituye un elemento probatorio fundamental para establecer la estructura y operación de estas agrupaciones delictivas.

Debilidades fiscales: Según el Ministerio Público (Ministerio Público, 2023), las denuncias por criminalidad organizada se elevaron en 18% en el 2022, pero la tasa de acusación fiscal alcanzó sólo el 26% y el 61% de casos fue archivado por falta de elementos de convicción. Solamente el 12% de denuncias terminó con una sentencia firme condenatoria. El factor que se destaca como principal obstáculo para la acción fiscal es la “sobrecarga procesal y la dificultad en obtención de pruebas científicas y tecnológicas de calidad”.

Deficiencias judiciales: Según el propio Poder Judicial (Poder Judicial, 2023), el 48% de los expedientes por crimen organizado terminó en absolución en el 2022; de ellos, los procesos duraban en promedio 26 meses, cuando legalmente excedían los plazos legales. El factor principal identificado es la “deficiente valoración de las pruebas disponibles”.

Ambas evaluaciones reafirmaron la naturaleza predominantemente reactiva y desarticulada de la respuesta institucional del sistema de justicia penal. Sin perjuicio de los intentos emprendidos, esta respuesta no logró modificar el rumbo ascendente de los crímenes violentos. Persistieron deficientes condiciones en la investigación criminal, direccionamiento fiscal y valoración de pruebas que influenciaron los resultados del proceso penal, de modo que la impunidad terminó siendo a la regla mayoritaria en los casos de criminalidad organizada.

Las herramientas metodológicas específicas empleadas en la presente evaluación serán detalladas en el Anexo 03 “Herramientas de recojo de información para la arquitectura del problema público”.

1.4. Marco institucional y normativo relacionado con el problema público

El combate a la criminalidad violenta parte de una arquitectura legal que se diseña desde los principios constitucionales hasta las normativas especializadas que regulan la función coordinada de las instituciones del sistema de justicia penal. Determina competencias, responsabilidades y procedimientos para la prevención, investigación y sanción de delitos de naturaleza violenta.

En la Constitución Política del Perú, destaca el artículo 44 al establecer que “la primordial obligación del Estado es garantizar la seguridad”. Los artículos 159, 166 y 138 confirman, en distinto grado, al Ministerio Público como parte responsable de la investigación del delito; a la Policía Nacional como ejecutora de la prevención e investigación criminal y al Poder Judicial como administrador de la justicia penal.

Las políticas públicas generales, desde el Acuerdo Nacional hasta los planes sectoriales específicos, establecen estrategias multisectoriales para enfrentar integralmente la criminalidad violenta, enfatizando la modernización de sistemas y el fortalecimiento de capacidades institucionales. Las políticas específicas incluyen la Estrategia Multisectorial Barrio Seguro, el Plan Estratégico de Capacidades Policiales MS30 y el Programa Presupuestal PP030, que financian intervenciones especializadas contra el crimen organizado.

El detalle exhaustivo del marco normativo, institucional, de políticas públicas y de políticas públicas especificas se desarrollan a continuación, proporcionando el sustento legal e institucional completo para el análisis del problema y la propuesta de solución.

1.4.1. Marco normativo

Tabla 1: Marco Normativo

Norma	Componentes de la norma	Relación con el problema público
Constitución Política del Perú	Art. 44: Deberes primordiales del Estado: …; garantizar la plena vigencia de los derechos humanos, proteger a la población de las amenazas ...	Obligación del Estado de brindar seguridad ciudadana frente a amenazas.
	Art. 166: La Policía Nacional del Perú … previene, investiga y combate la delincuencia ...	La PNP previene y persigue delitos como delitos violentos.
	Art. 159: Ministerio Público … Conducir desde su inicio la investigación del delito.	El Ministerio Público conduce la investigación penal. El Poder Judicial administra justicia penal.

Norma	Componentes de la norma	Relación con el problema público
	Art. 138: La potestad de administrar justicia emana del pueblo y se ejerce por el Poder Judicial ...	
Decreto Legislativo N°1267 - Ley de la Policía Nacional del Perú	Art. III – Función Policial: … Previene, investiga los delitos y faltas, combate la delincuencia y el crimen organizado ... Art. 2 - Funciones: … De investigación policial. Art. 18 – Dirección Nacional de Investigación Criminal. Art. 22 – Regiones Policiales.	Establece las competencias de la PNP para prevenir y perseguir la criminalidad violenta en todo el territorio. Asigna la responsabilidad de liderar la investigación criminal.
Decreto Legislativo N°052 - Ley Orgánica del Ministerio Público	Artículo 9.- Intervención del Ministerio Público en etapa policial El Ministerio Público vigila e interviene en la investigación del delito desde la etapa policial …	Conducción jurídica de las investigaciones para delitos, entre los que se encuentran los delitos cometidos por bandas y organizaciones criminales violentas.
Texto Único Ordenado de la Ley DS 017-93-JUS – Ley del Poder Judicial.	Artículo 1.- Potestad de administrar justicia.	Administración de justicia según la Constitución y las leyes, garantizando procesos justos contra delitos violentos de bandas y organizaciones criminales.
Ley N°30077 - Ley contra el Crimen Organizado.	Artículo 3 - Define los delitos comprendidos en crimen organizado. Capítulo I - Investigación y proceso penal	Tratamiento penal y procesal diferenciado para investigar y juzgar delitos cometidos por organizaciones criminales violentas.
DS Nº 026-2017-IN - Reglamento	Artículo 99.- Dirección Nacional de Investigación	Precisa las funciones y atribuciones de la DIRINCRI PNP y la Región Policial Lima

Norma	Componentes de la norma	Relación con el problema público
de la Ley de la Policía.	Criminal Artículo 211.- Regiones Policiales	para prevenir e investigar delitos.

1.4.2. Marco institucional

Tabla 2: Marco Institucional

Entidad	Funciones generales	Funciones especificas	Base normativa
Ministerio del Interior	Diseñar, ejecutar y supervisar las políticas públicas en materia de orden interno y seguridad ciudadana.	Rectoría del Sistema Nacional de Seguridad Ciudadana. Formular, conducir y evaluar las políticas y planes.	Decreto Legislativo N°1266 - Ley de Organización y Funciones del MININTER.
Policía Nacional del Perú	Prevenir, investigar y combatir la delincuencia y el crimen organizado.	Garantizar, mantener y restablecer el orden interno, orden público y la seguridad ciudadana. Prevenir, combatir, investigar y denunciar la comisión de los delitos. Funciones de investigación …	Decreto Legislativo N°1267 - Ley de la PNP. Decreto Supremo N°026-2017-IN - Reglamento de la Ley PNP
Ministerio Público	Ejercer la persecución penal de los hechos punibles.	Dirigir la investigación criminal.	Decreto Legislativo N°052 - Ley Orgánica del Ministerio Público.

Entidad	Funciones generales	Funciones especificas	Base normativa
	Promover la acción de la justicia y garantizar el cumplimiento de la ley ….	Ejercer la acción penal. Proteger víctimas y garantizar un proceso legal justo.	Resolución de la Fiscalía de la Nación N°760-2020-MP-FN - ROF MP. Ley N°30077 - Ley contra el Crimen Organizado.
Poder Judicial	Juzgar y sancionar hechos delictivos. Procesar casos de crimen organizado aplicando las disposiciones de la Ley N°30077 y el Código Procesal Penal.	Impartir justicia. Llevar a cabo la etapa intermedia y el juzgamiento conforme al Código Procesal Penal. Imponer las penas y medidas legales.	Texto Único Ordenado de la Ley Orgánica del Poder Judicial. Código Procesal Penal. Ley N°30077 - Ley contra el Crimen Organizado. Acuerdos Plenarios de la Corte Suprema.

1.4.3. Políticas públicas generales

Tabla 3: Políticas Públicas Generales

Política pública	Objetivos	Componentes	Planteamientos
Acuerdo Nacional - Política de Estado N°7 Erradicación de la violencia y fortalecimiento del civismo y de la seguridad ciudadana.	Consolidar políticas orientadas a prevenir, disuadir, sancionar y eliminar conductas y prácticas de violencia. Fomentar una cultura de paz y respeto a la ley.	Plantea estrategias multisectoriales para enfrentar integralmente las múltiples manifestaciones de violencia.	Hacer más eficaces los sistemas de seguridad preventiva y sanción penal. Priorizar la adopción de políticas, normas y acciones para reducir los delitos violentos y el crimen organizado que afectan a la población.

Política pública	Objetivos	Componentes	Planteamientos
	Poner especial énfasis en extender los mecanismos legales para combatir prácticas violentas arraigadas.		Poner énfasis en mejorar las capacidades del sistema de justicia penal.
Política Nacional Multisectorial de Seguridad Ciudadana al 2030.	Reducir la victimización por robos, homicidios, extorsión y otros delitos violentos asociados al crimen organizado al 2030. Fortalecer el acceso a una justicia de calidad, oportuna y eficaz al 2030. Garantizar los recursos humanos suficientes, competentes y motivados para los servicios de seguridad ciudadana al 2030.	Propone un abordaje multisectorial y multinivel para prevenir y reducir los delitos que más afectan a la población.	Impulsa reformas normativas para facilitar la investigación y sanción de delitos violentos complejos. Plantea el desarrollo de programas especializados de lucha contra el crimen organizado. Establece como prioridad la reducción de delitos violentos patrimoniales y contra la vida, cometidos por bandas y organizaciones criminales. Enfatiza la articulación de capacidades de la PNP, MP, PJ e INPE para una persecución penal eficaz.

Política pública	Objetivos	Componentes	Planteamientos
Plan Estratégico Sectorial Multianual PESEM 2020-2024 del MININTER.	Disminuir los hechos delictivos asociados a la inseguridad ciudadana. Fortalecer la investigación del delito organizado y complejo a cargo de la PNP. Reducir los delitos perpetrados por bandas criminales y organizaciones delictivas.	Incluye indicadores para mejorar la eficacia de la PNP en la lucha contra el crimen organizado violento.	Conecta el desempeño policial con la reducción de victimización.
Plan Estratégico Institucional PEI 2021-2025 del MININTER.	Implementar nuevos sistemas de prevención e investigación del delito. Promover el cierre de brechas de infraestructura y equipamiento.	Contempla condiciones para modernizar las capacidades de investigación, inteligencia y ciberseguridad de la PNP.	Modernizar las capacidades de investigación, inteligencia y ciberseguridad de la PNP para enfrentar eficazmente el delito.

1.4.4. Políticas públicas específicas

Tabla 4: Políticas Públicas Específicas

Política pública	Objetivos	Componentes	Planteamientos
Estrategia Multisectorial	Reducir factores de riesgo asociados al	Plantea un enfoque preventivo	Se centra en el abordaje de las causas

Política pública	Objetivos	Componentes	Planteamientos
Barrio Seguro: Estrategia de Prevención Social del Crimen y la Violencia 2021-2025.	crimen organizado en territorios focalizados. Promover factores de protección comunitarios frente al crimen en poblaciones vulnerables. …	focalizado en zonas de alta incidencia criminal.	sociales subyacentes a la captación de jóvenes por bandas criminales.
Plan Estratégico de Capacidades de la Policía Nacional del Perú al 2030 "Mariano Santos Mateos" - "Plan MS30".	Desarrollar soluciones tecnológicas para potenciar el trabajo de inteligencia e investigación criminal de la Policía Nacional del Perú.	Plantea la implementación de un sistema informático integrado para la gestión criminalística y la especialización del personal policial en tecnologías modernas. Además, un Centro de Control y Coordinación (C5i) para mejorar las capacidades de respuesta e investigación criminal.	Prioriza la implementación de un Sistema Informático de Gestión Criminalística y capacitación al personal policial en tecnologías avanzadas, además de establecer un Centro de Control (C5i) para mejorar la investigación y respuesta operativa contra el crimen.
Programa Presupuestal PP030 - Reducción de los	Realizar operaciones policiales para	Financia intervenciones para prevenir y controlar delitos comunes y	Incluye acciones de desarticulación de bandas, investigación

Política pública	Objetivos	Componentes	Planteamientos
delitos y faltas que afectan la seguridad ciudadana.	reducir delitos y faltas. Mejorar las comisarías y unidades especializadas. Fomentar una comunidad organizada a favor de la seguridad ciudadana. ...	complejos que afectan la seguridad de los ciudadanos.	criminal y participación ciudadana.

Esta arquitectura normativo-institucional establece el marco integral para el combate del crimen organizado violento, definiendo competencias, recursos y estrategias que sustentan la propuesta de innovación desarrollada en el presente trabajo.

CAPÍTULO 2: CAUSAS DEL PROBLEMA PÚBLICO

En este Capítulo se explora las causas del incremento de delitos violentos cometidos por bandas y organizaciones criminales en Lima Metropolitana durante 2021-2023. Se presenta un marco teórico sobre las causas del problema, seguido de un análisis detallado de cuatro causas principales identificadas. El capítulo examina cómo estas causas interrelacionadas contribuyen al problema y destaca la importancia de los metadatos de localización en la investigación criminal.

2.1. Marco teórico sobre las causas del problema

A partir de una exhaustiva revisión de la literatura científica, se han identificado diversas causas teóricas que podrían explicar el incremento de delitos violentos cometidos por bandas y organizaciones criminales en Lima Metropolitana durante 2021-2023. Estas causas se encuentran sintetizadas en la siguiente tabla:

Tabla 5: Síntesis de causas teóricas que podrían explicar el incremento de delitos violentos cometidos por bandas y organizaciones criminales

Denominación de la causa	Descripción	Autores que plantean esta causa
Teoría de la elección racional	Plantea que los delincuentes toman decisiones racionales de cometer crímenes violentos basándose en un análisis costo-beneficio. Si perciben que los beneficios (como el dinero o el poder) superan los costos (como el riesgo de ser atrapados y sancionados), optarán por delinquir. Las bandas y organizaciones criminales realizarían esta evaluación de manera colectiva.	Tibbetts, S. G., & Hemmens, C. (2021) - Schram, P. J., & Tibbetts, S. G. (2023).
Teoría de las actividades rutinarias	Explica que la convergencia en tiempo y espacio de tres elementos incrementa las probabilidades de crímenes violentos: un delincuente motivado, un objetivo atractivo y la ausencia de un guardián capaz. Las bandas y organizaciones criminales buscan activamente esta confluencia de factores para perpetrar sus delitos.	Felson, M., & Eckert, M. (2021) - Andresen, M. A., & Farrell, G. (2022).

Denominación de la causa	Descripción	Autores que plantean esta causa
Teoría de la desorganización social	Sostiene que altos niveles de crimen en ciertas zonas se deben al debilitamiento de los lazos comunitarios y controles sociales informales que inhiben conductas delictivas. Esto generaría un entorno propicio para el surgimiento y expansión de bandas y organizaciones criminales violentas.	Sampson, R. J., & Groves, W. B. (1989) - Sampson, R. J., & Raudenbush, S. W. (2021).
Teoría del aprendizaje social	Argumenta que los comportamientos criminales se aprenden mediante la observación e imitación de modelos delictivos, especialmente dentro del entorno social cercano. Los integrantes de bandas criminales adquirirían y reforzarían mutuamente hábitos violentos.	Akers, R. L., & Jennings, W. G. (2021) - Akers, R. L., & Sellers, C. S. (2012).
Teoría de las subculturas	Enfatiza que ciertos grupos desarrollan normas, valores y códigos de conducta que legitiman y alientan el uso de la violencia para obtener estatus, respeto o resolver conflictos. Las pandillas juveniles serían un claro ejemplo de subculturas que promueven crímenes violentos.	Lilly, J. R., Cullen, F. T., & Ball, R. A. (2010) - Williams, F. P., & McShane, M. D. (2009).
Teoría del control social	Sostiene que los individuos tienen una tendencia natural a infringir las normas, pero que existen mecanismos de control social (vínculos afectivos, compromisos, participación, creencias) que inhiben tales impulsos. Cuando estos controles se debilitan, habría mayor propensión a integrar grupos criminales violentos.	Walters, G. D. (2022) - Meško, G., & Tankebe, J. (2023).
Teoría de la asociación diferencial	Señala que las conductas delictivas se aprenden mediante un proceso de comunicación e interacción con personas que tienen definiciones favorables hacia el crimen. Sugiere que los miembros de organizaciones criminales adquieren y refuerzan mutuamente valores y técnicas delictivas.	Walters, G. D. (2022) - Dearden, T., & Mazerolle, P. (2021).

Denominación de la causa	Descripción	Autores que plantean esta causa
Teoría de las oportunidades delictivas	Relaciona el incremento del crimen con la disponibilidad de oportunidades para delinquir, como víctimas vulnerables, bienes atractivos o ausencia de vigilancia. Las bandas criminales buscarían y aprovecharían activamente estas oportunidades para cometer delitos predatorios.	March Cerdà, J. C. (2023) - Felson, M., & Boba, R. (2009).
Teoría del etiquetamiento	Indica que las etiquetas negativas asignadas por el sistema de justicia penal a ciertas personas (como "delincuente" o "criminal") generan estigma, exclusión y una profecía autocumplida que refuerza carreras delictivas. Esto dificultaría que miembros de bandas criminales violentas abandonen ese estilo de vida.	Becker, H. S. (1963) - Lemert, E. M. (1951).
Teoría de los mercados ilegales	Argumenta que la violencia emerge como un mecanismo de resolución de disputas y protección de "derechos de propiedad" en mercados ilegales donde no rige la ley formal ni existen árbitros reconocidos. Muchos crímenes violentos de bandas estarían ligados al tráfico ilícito de bienes y servicios.	International Crisis Group. (2023) - Monroy Ojeda, C., Rangel Romero, X. G., & Hernández Mier, C. (2024).
Teoría de la legitimidad procesal	Sostiene que cuando las personas perciben que las autoridades actúan de manera justa, transparente y respetuosa, estarán más dispuestas a cumplir las normas y a otorgar legitimidad a la justicia. Si los procesos son considerados injustos, aumentaría el riesgo de incurrir en delincuencia violenta.	Ruiz Sánchez, M. A. (2018) - Espinoza Ramos, B. (2018).
Teoría de las limitaciones tecnológicas y de acceso a datos en la	Plantea que las restricciones legales, éticas y técnicas en el acceso y análisis de datos de localización, fuentes abiertas de información y el uso de tecnologías avanzadas dificultan la capacidad de las autoridades para investigar delitos cometidos por organizaciones criminales. La falta de recursos tecnológicos	Trottier, D. (2019) - Koops, B. J. (2021) - Bartolomé y Pérez (2020) - Ferguson

Denominación de la causa	Descripción	Autores que plantean esta causa
investigación criminal	especializados y las barreras para su uso efectivo resultan en investigaciones menos eficaces, debilidades probatorias y mayor impunidad.	(2017) - Maguire (2012).

De estas teorías se puede definir cinco perspectivas teóricas más relevantes para este contexto específico:

- **Teoría de la elección racional y oportunidades delictivas:** Esta perspectiva sugiere que los delincuentes realizan un análisis costo-beneficio antes de cometer delitos violentos. En Lima Metropolitana, la percepción de altos beneficios económicos (por ejemplo, de extorsiones o robos) frente a bajos costos (baja probabilidad de captura y sanción) podría estar incentivando la expansión de actividades criminales violentas. Ejemplo: Una banda criminal en San Juan de Lurigancho percibe que las ganancias por extorsión a comerciantes superan ampliamente el riesgo de ser capturados, debido a la sobrecarga del sistema policial y judicial.

- **Teoría de la desorganización social y subculturas:** Esta teoría enfatiza cómo entornos con débiles mecanismos de control social informal y presencia de subculturas que legitiman la violencia pueden favorecer el surgimiento de bandas criminales. En ciertas zonas de Lima con alta desorganización social, las organizaciones delictivas encontrarían condiciones propicias para establecerse y reclutar miembros. Ejemplo: En un asentamiento humano de Villa El Salvador con alta deserción escolar y presencia de pandillas, los jóvenes son más susceptibles de ser reclutados por organizaciones criminales que ofrecen sentido de pertenencia y oportunidades económicas ilícitas.

- **Teoría del aprendizaje social y asociación diferencial:** Este enfoque explica cómo las conductas delictivas violentas se aprenden y refuerzan mediante la interacción con pares criminales. En Lima, los centros penitenciarios y ciertas zonas urbanas podrían estar funcionando como "escuelas del crimen", donde se transmiten técnicas y valores delictivos. Ejemplo: En el penal de Lurigancho, internos jóvenes son reclutados por organizaciones criminales, aprendiendo tácticas de extorsión y códigos de la subcultura delictiva que luego replican al salir en libertad.

- **Teoría sobre mercados ilícitos:** La teoría postula que la violencia es un fenómeno emergente regulador cuando el lucro de los mercados ilícitos es excepcionalmente alto. En Lima Metropolitana, esto se confirma por la cantidad de información sobre los ajustes de cuentas entre las bandas u organizaciones criminales por la tenencia de territorios seleccionados utilizados para la micro comercialización de drogas. Ejemplo: Dos bandas criminales tienen una lucha sangrienta para ganar el control de la distribución de drogas en el Callao. Matar selectivamente en este contexto es la forma de mantener las cosas bajo control.

- **Teoría de las limitaciones tecnológicas y de acceso a datos en la investigación criminal:** Las teorías son más contemporáneas. Su énfasis recae en el papel de la brecha tecnológica en la investigación criminal. Se sostiene la insuficiencia de las tecnologías y, además, en las dificultades en el acceso a los datos que obstaculizan la lucha exitosa contra las organizaciones criminales. Ejemplo: la policía en Lima Metropolitana no puede desarticular una organización de chantajistas que operan impunemente desde el penal de Ancón, esto principalmente por falta de equipos y personal especializado, que impiden mapear la estructura de esta mal llamada empresa criminal.

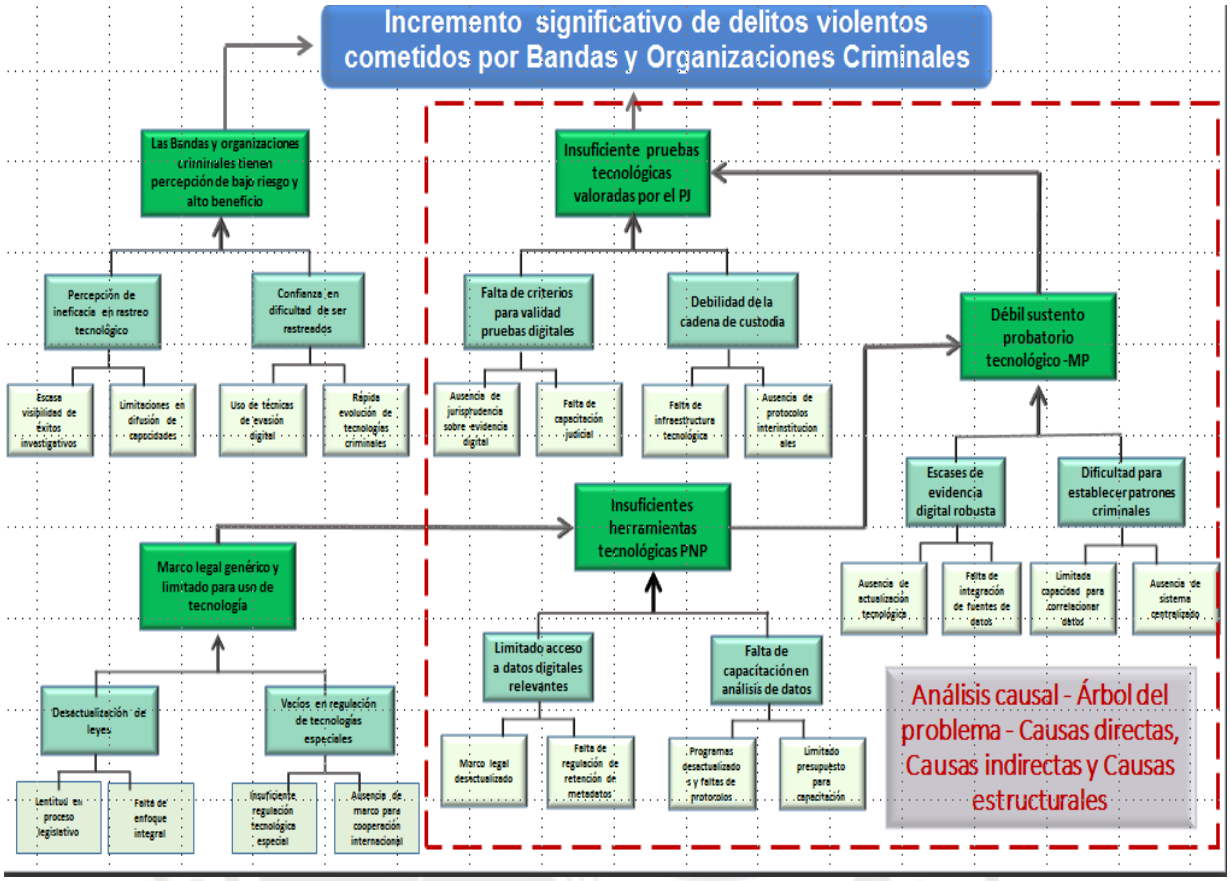
Estos enfoques teóricos demuestran varias posibles razones para el aumento de hechos delictivos fatales durante el 2021-2023. Sin embargo, es pertinente mencionar que, independientemente de los supuestos teóricos, el problema de referencia pasa por características propios del país. Como resultado, el estudio empírico, junto con la teoría recopilada, son necesarios para definir la aplicación real.

2.2. Causas del problema

En la medida en que el proyecto de innovación actúa como una comprensión integral de la lógica de desarrollo de un problema público seleccionado y su solución, resulta necesario identificar los factores que determinan el aumento de delitos violentos en Lima Metropolitana (2021-2023). Para ello, se recoge y procesa datos sobre la base de estrategias específicas para la recopilación y análisis de información, de esta manera tener la comprensión del problema.

La descripción del diseño metodológico se detallada en el Anexo 04 “Matriz de Consistencia del diseño de investigación sobre las causas del problema público”, complementado por el siguiente árbol del problema:

Ilustración 1: Diagrama del análisis causal del problema (árbol del problema)



Fuente: Elaboración de los autores

Teniendo en cuenta lo anteriormente, así como lo que se describe en el capítulo 2.1 "Marco teórico sobre las causas del problema", identificamos que las causas básicas o principales, indirectas y estructurales del problema son las siguientes:

2.2.1. Percepción de bajo riesgo y alto beneficio de bandas y organizaciones criminales violentas

Esta causa directa explica por qué los criminales operan bajo un frío cálculo costo-beneficio que actualmente favorece la actividad delictiva. La débil capacidad del Estado para investigar, perseguir y sancionar efectivamente a bandas y organizaciones criminales ha creado un contexto y circunstancias donde el crimen organizado percibe que las ganancias de sus actividades ilegales superan de lejos los riesgos de ser atrapados y encarcelados. Este desequilibrio, abonado por las deficiencias sistémicas de la administración de justicia, fomenta la expansión de la actividad criminal.

Según el "Informe Regional de Desarrollo Humano 2023-2024" del Programa de las Naciones Unidas para el Desarrollo (PNUD, 2023), en Perú la tasa de homicidios aumentó de 5.0 a 8.3 por 100,000 habitantes entre 2000 y 2020, mientras que la confianza en la Policía Nacional y el sistema judicial en 2020 fue de solo 22% y 16% respectivamente. Además, el 67% de los peruanos cree que la corrupción aumentó. Estos indicadores sugieren una percepción de bajo riesgo y alto beneficio para las actividades criminales, lo que podría estar fortaleciendo la impunidad percibida y fomentando la continuidad de estas actividades ilícitas. Se desglosa en dos causas indirectas y estas a su vez en dos causas estructurales:

Tabla 6: Causas indirectas y estructurales de la causa directa "Percepción de bajo riesgo y alto beneficio de bandas y organizaciones criminales violentas"

Nivel	Descripción	Explicación
Causa Indirecta 1	Percepción de ineficacia en el rastreo tecnológico.	Los delincuentes subestiman las capacidades de las autoridades para rastrearlos mediante tecnología. Esto se ve reforzado por la aparente falta de éxitos investigativos basados en evidencia digital y la limitada difusión de las capacidades reales en materia de investigación tecnológica.
Causa Estructural 1.1	Escasa visibilidad de éxitos investigativos.	La falta de difusión de casos emblemáticos donde se haya utilizado evidencia digital de manera efectiva para desarticular organizaciones criminales contribuye a la percepción de que las autoridades carecen de capacidades tecnológicas avanzadas.
Causa Estructural 1.2	Limitaciones en difusión de capacidades.	Las autoridades mantienen un velo estratégico sobre sus verdaderas capacidades tecnológicas. Si bien este hermetismo táctico resulta crucial para preservar la ventaja operativa, podría estar alimentando una peligrosa sobre confianza en el mundo criminal.

Nivel	Descripción	Explicación
Causa Indirecta 2	Confianza en la dificultad de ser rastreados.	Los delincuentes han desarrollado una confianza desmedida en sus capacidades de evasión digital, sustentada en la presunción de que sus herramientas tecnológicas superan los mecanismos de detección policiales.
Causa Estructural 2.1	Uso de técnicas de evasión digital.	Las organizaciones criminales han elevado significativamente la complejidad de su huella digital. El "Reporte de Ciberseguridad 2020" del BID y la OEA documenta una sofisticación creciente en las técnicas de evasión empleadas por el crimen organizado en América Latina y el Caribe. Las limitaciones técnicas y legales que enfrentan los países de la región para combatir estos ciberdelitos refuerzan la sensación de invulnerabilidad en el entorno digital.
Causa Estructural 2.1	Rápida evolución de tecnologías criminales.	La agilidad tecnológica del mundo criminal supera frecuentemente la respuesta estatal. El Instituto de Defensa Legal, en su "Informe sobre la Seguridad Ciudadana en el Perú 2022", destaca cómo la rápida adopción de tecnologías avanzadas por parte de organizaciones criminales presenta desafíos sin precedentes para las fuerzas del orden. El informe es contundente al señalar que "la capacidad de adaptación tecnológica de las organizaciones criminales supera en muchos casos la de las instituciones encargadas de combatirlas" (IDL, 2022).

Lo anterior evidencia una problemática dual: por un lado, la limitada visibilidad de los éxitos investigativos en materia digital genera una subestimación de las capacidades

policiales, mientras que el rápido avance tecnológico del crimen organizado, documentado en informes regionales recientes, refuerza la confianza de los delincuentes en sus métodos de evasión. Esta dicotomía plantea desafíos significativos para las instituciones de seguridad, especialmente en el contexto peruano.

2.2.2. Insuficientes pruebas tecnológicas valoradas por el Poder Judicial para imponer condenas a integrantes de bandas y organizaciones criminales violentas (PJ)

El Poder Judicial enfrenta deficiencias significativas para el procesamiento de evidencia digital vinculada al crimen organizado. Esta brecha técnica resulta en una preocupante escasez de condenas efectivas, alimentando el ciclo de impunidad que empodera a los grupos delictivos.

Según el "Boletín Estadístico Institucional N°04-2023" del Poder Judicial (Poder Judicial del Perú, 2023b), al inicio del 2023 había 1,017,663 procesos principales pendientes en trámite. La tasa de resolución de procesos en trámite fue del 109.8%, indicando que se resolvieron más casos de los que ingresaron. Sin embargo, la tasa de apelación de resolución final fue del 15.5%. Esto sugiere que, a pesar de los esfuerzos, persiste la carga procesal y el porcentaje de disconformidad con las resoluciones, lo que contribuye a una percepción de ineficacia de la justicia, capacidades de investigación y rastreo. Se desglosa en dos causas indirectas y estas a su vez en dos causas estructurales:

Tabla 7: Causas indirectas y estructurales de la causa directa "Insuficientes pruebas tecnológicas valoradas por el Poder Judicial para imponer condenas a integrantes de bandas y organizaciones criminales violentas (PJ)"

Nivel	Descripción	Explicación
Causa Indirecta 1	Falta de criterios para valorar pruebas digitales.	Los jueces carecen de parámetros claros y estandarizados para evaluar la autenticidad, integridad y relevancia de la evidencia digital presentada en casos de criminalidad organizada. Esto genera incertidumbre en la valoración de pruebas tecnológicas y puede resultar en decisiones judiciales inconsistentes.

Nivel	Descripción	Explicación
Causa Estructural 1.1	Ausencia de jurisprudencia sobre evidencia digital.	La falta de precedentes judiciales claros sobre la admisibilidad y valoración de pruebas digitales genera incertidumbre entre los jueces. Esta ausencia de jurisprudencia consolidada dificulta la formación de criterios uniformes para la evaluación de evidencia tecnológica en casos de criminalidad organizada.
Causa Estructural 1.2	Falta de capacitación.	Los integrantes del poder judicial no están al día con la tecnología. En el "Plan de Capacitación de la Academia de la Magistratura 2022" prácticamente limitaron temas como ciberdelincuencia y evidencias digitales, cuando debería ser prioritario (Academia de la Magistratura, 2022). Sin estos conocimientos, los jueces se ven muy limitados para evaluar correctamente las pruebas tecnológicas presentadas por los fiscales en casos difíciles.
Causa Indirecta 2	Debilidad en el manejo de cadena de custodia.	El mal manejo de cualquier tipo de evidencia, especialmente la digital, puede hacer que un caso se caiga. El método y herramienta para recolectar, resguardar y administrar en general estas evidencias, en su gran mayoría son inadecuados. Esto hace que sea casi imposible garantizar que no fueron alteradas, y, por ende, los jueces terminan no considerándolas.
Causa Estructural 2.1	Falta de infraestructura tecnológica.	La infraestructura tecnológica del Poder Judicial revela carencias preocupantes. Aunque el Plan Estratégico Institucional 2021-2025 reconoce la urgencia de implementar sistemas especializados para gestionar evidencia digital, las restricciones

Nivel	Descripción	Explicación
		presupuestarias han frenado esta modernización esencial, aumentando el riesgo de pérdida o alteración de pruebas cruciales.
Causa Estructural 2.1	Ausencia de protocolos interinstitucionales.	La falta de protocolos unificados existe entre la PNP, el Ministerio Público y el Poder Judicial. El "Plan Nacional de Interoperabilidad del Sistema de Administración de Justicia Penal 2021-2025" señala esto como uno de los grandes obstáculos que enfrenta la justicia. Estas diferencias institucionales, aunado a las limitaciones técnicas son circunstancias latentes que impiden implementar un criterio unificado.

Esto, a su vez, señala una inquietante cadena de deficiencias del sistema judicial para la valoración de la evidencia digital relativa a la criminalidad organizada, desde la falta de criterios y de jurisprudencia unificada, hasta la limitación de infraestructura tecnológica y de protocolos interinstitucionales. Se suma a esto que existe una débil formación judicial en materia tecnológica, tal como contempla el "Plan de Capacitación 2022" de la Academia de la Magistratura. Todas las condiciones antes mencionadas dificultan a los jueces una efectiva valoración de pruebas digitales.

2.2.3. Débil sustento probatorio tecnológico de las denuncias penales del Ministerio Público por delitos violentos cometidos por bandas y organizaciones criminales (MP)

El Ministerio Público tiene obstáculos considerables para la presentación de pruebas en forma de evidencia digital para sustentar contra el crimen organizado y ganar los casos.

Según la Revista de la Fiscalía Especializada contra la Criminalidad Organizada (2022), entre enero 2016 y junio 2022, se obtuvieron 337 resoluciones judiciales y 1258 sentencias condenatorias contra miembros de organizaciones criminales. Sin embargo, comparado con las 4423 detenciones realizadas en el mismo período, estas cifras podrían sugerir dificultades en la construcción de casos sólidos, posiblemente debido a debilidades en

el sustento probatorio, incluyendo el tecnológico. Se desglosa en dos causas indirectas y estas a su vez en dos causas estructurales:

Tabla 8: Causas indirectas y estructurales de la causa directa "Débil sustento probatorio tecnológico de las denuncias penales del Ministerio Público por delitos violentos cometidos por bandas y organizaciones criminales (MP)"

Nivel	Descripción	Explicación
Causa Indirecta 1	Escasez de evidencia digital robusta.	Los fiscales a menudo carecen de pruebas digitales contundentes para sustentar sus acusaciones contra miembros de organizaciones criminales. Esta escasez de evidencia digital robusta debilita significativamente la posición del MP en los procesos judiciales contra el crimen organizado.
Causa Estructural 1.1	Ausencia de actualización tecnológica.	En primer lugar, las limitaciones tecnológicas del Ministerio Público reflejan un desafío similar al que enfrenta la PNP en el terreno forense digital. En su "Plan Estratégico Institucional 2021-2025", el MP tiene la tarea de cerrar la brecha utilizando big data y sistemas de inteligencia artificial. En segundo lugar, tanto las restricciones presupuestarias como la falta de personal de TI capacitado están retrasando esta iniciativa crítica.
Causa Estructural 1.2	Falta de integración de fuentes de datos.	La ausencia de un sistema integrado de datos complica aún más la situación. Los fiscales no tienen las herramientas para correlacionar las fuentes, aislando muchos de los datos de contextos y la interpretación necesaria en relación con redes criminales entrelazadas o crímenes relacionados con apariencias independientes.

Nivel	Descripción	Explicación
Causa Indirecta 2	Dificultad para establecer patrones criminales.	La información fragmentada debida a diferencias tecnológicas, normativas y operativas entre las distintas fiscalías dificulta enormemente que el Ministerio Público detecte y pruebe patrones a través de la evidencia digital. Un gran obstáculo para los fiscales que luchan por armar casos a partir de incidentes que por separado no demuestran la real magnitud y complejidad de las organizaciones.
Causa Estructural 2.1	Limitada capacidad para correlacionar datos.	El “Plan Estratégico Institucional 2021-2025” señala como reto “la insuficiente capacidad para correlacionar eficazmente los diversos datos de distintos incidentes delictivos, de los participantes y del flujo de dinero acreditado”. Otro impedimento para los fiscales que buscan demostrar la verdadera estructura y alcance de las organizaciones es “incluso cuando haya suficiente información para hacer conexiones, no existe un sistema que permita hacerlo con facilidad”.
Causa Estructural 2.1	Ausencia de un sistema centralizado.	Se relaciona con un problema más profundo y más difícil de solucionar. La “ausencia de un sistema para la gestión de la información y conocimiento que facilite los procesos de producción y toma de decisiones” que produce “Islas” donde la información no se cruza y se dificulta la detección de Escenarios del Crimen Organizado. Aunque Se ha planteado como una prioridad en el Plan Estratégico 2021-2025 “crear una plataforma de inteligencia criminal integral o centro de operaciones”, su implementación ha

Nivel	Descripción	Explicación
		presentado problemas técnicos, la falta de presupuesto y coordinación insuficiente.

En resumen, se presentan problemas importantes para la estructuración de casos contra el crimen organizado debido a los problemas para manejar la evidencia digital y por la falta de sistemas para correlacionar datos. Esto, el propio “Plan Estratégico Institucional 2021-2025” lo menciona, entre otros.

2.2.4. Insuficientes herramientas tecnológicas y acceso limitado a datos digitales relevantes para incriminar a bandas y organizaciones criminales violentas por parte de la Policía Nacional del Perú (PNP)

Por su parte, la Policía Nacional del Perú (PNP) enfrenta sus propias problemas y limitaciones en el ámbito de la investigación de delitos. Las carencias de recursos y herramientas tecnológicas adecuadas limitan en gran medida su capacidad para recolectar, analizar y utilizar la evidencia digital en la lucha contra el crimen organizado.

Esto se reafirma en el "Plan Estratégico de Capacidades de la Policía Nacional del Perú al 2030" (Ministerio del Interior, 2019b), donde se indica que la PNP enfrenta debilidades institucionales como la "Obsolescencia y carencia de equipos tecnológicos" y una "Limitada capacidad operativa por falta de recursos logísticos, tecnológicos, de infraestructura y personal". Por ende, esto afecta directamente la capacidad de la PNP para recolectar, analizar y utilizar productivamente la evidencia digital. Lo anterior lo desglosamos en dos causas indirectas y estas a su vez en dos causas estructurales:

Tabla 9: Causas indirectas y estructurales de la causa directa “Insuficientes herramientas tecnológicas y acceso limitado a datos digitales relevantes para incriminar a bandas y organizaciones criminales violentas por parte de la Policía Nacional del Perú (PNP)

Nivel	Descripción	Explicación
Causa Indirecta 1	Limitado acceso a datos digitales relevantes.	La PNP carece de mecanismos eficientes y ágiles para acceder a información digital crucial en las investigaciones de criminalidad organizada. Esta limitación obstaculiza inevitablemente la capacidad

Nivel	Descripción	Explicación
		de la policía para construir casos sólidos contra las organizaciones criminales.
Causa Estructural 1.1	Marco legal desactualizado.	El marco legal actual no se ha adaptado adecuadamente a los avances tecnológicos y a las necesidades de la investigación criminal moderna. Esta desactualización legal limita la capacidad de la PNP para utilizar herramientas u opciones tecnológicas avanzadas en sus investigaciones. Como se mencionó anteriormente, por ejemplo, en el Perú no existe normativa sobre retención de metadatos de localización de dispositivos móviles por operadoras. Esta falta de regulación priva a la PNP de una herramienta crucial para investigar delitos violentos cometidos por organizaciones criminales, impidiendo establecer vínculos con la escena del crimen, víctimas y otros.
Causa Estructural 1.2	Falta de regulación de retención de metadatos.	La ausencia de un marco normativo sobre retención masiva de metadatos de localización representa una debilidad crítica en el sistema de investigación criminal. En esa línea, el Ministerio del Interior ha destacado cómo este vacío en la legislación pone a la PNP en una gran desventaja respecto de las organizaciones criminales más sofisticadas tecnológicamente. Sin una obligación legal que obligue a mantener estos datos en el tiempo, los investigadores pierden a menudo el acceso a información histórica clave para seguir el rastro de la actividad delictiva, entre otros.

Nivel	Descripción	Explicación
Causa Indirecta 2	Falta de capacitación en análisis de datos.	La brecha en capacitación tecnológica del personal policial amplifica este desafío. Los efectivos carecen de la formación especializada necesaria para maximizar el potencial de las herramientas digitales disponibles, lo que limita su capacidad para transformar datos crudos en inteligencia procesable y establecer conexiones cruciales entre diferentes casos criminales.
Causa Estructural 2.1	Programas desactualizados y ausencia de protocolos estandarizados.	Existe un rezago formativo que se hace más evidente al examinar los programas educativos policiales. Por ejemplo, la Escuela Nacional de Formación Profesional Policial admite que los programas “en tecnologías de investigación criminal” permanecen prácticamente estáticos. Tal situación resulta en la imposibilidad de responder de manera adecuada a los cambios permanentes de la tecnología. A la vez, la ausencia de un protocolo estándar para el examen de los datos adquiridos multiplica los riesgos de comisión de y conduce a la marginación de esta área de la labor de investigación del delito.
Causa Estructural 2.2	Limitado presupuesto para capacitación.	Un porcentaje elevado de la divergencia en la oferta y la demanda del conocimiento tecnológico se explica por la limitación presupuestaria. En particular, la asignación presupuestaria para “programas de capacitación y actualización tecnológica” del personal de la PNP cuenta con restricciones. Es insuficiente para satisfacer la creciente demanda de personal que requiere adquirir o actualizar

Nivel	Descripción	Explicación
		sus habilidades en la realización de investigaciones digitales. Según los resultados del Informe de Ejecución Presupuestal del Ministerio del Interior del 2022, el 2.5% de la asignación total a la PNP se destinó a programas relacionados. Puesto que la necesidad y la cantidad de temas tecnológicos en torno a la lucha contra el crimen organizado siguen creciendo, tal cantidad no permite a la PNP mantenerse al día con las tácticas delictivas modernas.

En síntesis, se revelan dos desafíos críticos: marco legal obsoleto que limita el acceso a datos digitales cruciales al no existir retención de metadatos de localización y mayoritaria brecha en capacitación tecnológica y tecnología.

2.2.5. Marco legal genérico y limitado de opciones tecnológicas para la persecución efectiva de bandas y organizaciones criminales violentas.

Las leyes vigentes no van de la mano con la evolución tecnológica. Las organizaciones criminales ya manejan tecnología que ni siquiera imaginábamos cuando se escribieron la mayoría de las normas vigentes. ¿El resultado? Los fiscales e investigadores tienen limitaciones. Saben que existen herramientas tecnológicas increíbles para geolocalizar y desmantelar estas organizaciones, pero legalmente no las pueden usar, es frustrante. Este contexto viene de dos problemas grandes, y cada uno tiene sus propias complicaciones:

Tabla 10: Causas indirectas y estructurales de la causa directa "Marco legal genérico y limitado de opciones tecnológicas para la persecución efectiva de bandas y organizaciones criminales violentas"

Nivel	Descripción	Explicación
Causa Indirecta 1	Desactualización de leyes.	Las leyes vigentes no avanzan al ritmo de la tecnología y las nuevas modalidades delictivas. Este retraso legal crea vacíos que son explotados por las organizaciones

Nivel	Descripción	Explicación
		y limita la capacidad de las autoridades para utilizar la nueva tecnología en la investigación criminal. El “Plan Nacional de Seguridad Ciudadana 2019-2023” establece como urgente la actualización del marco legal para enfrentar los desafíos de la criminalidad digital.
Causa Estructural 1.1	Lentitud en el proceso legislativo.	La modernización legislativa siempre se encuentra con retrasos típicos. Tal como lo señala el World Justice Project (World Justice Project, 2023), el Congreso toma en general seis meses o más para aprobar una ley penal, con lo cual siempre hay un rezago entre la legislación y la realidad, sobre todo con todas las veloces transformaciones de las tácticas criminales.
Causa Estructural 1.2	Falta de enfoque integral.	Las mortificaciones o iniciativas legislativas no se dan a través de una visión integral que contemple las materias técnicas, jurídicas y éticas que supone la investigación del delito. El Plan Nacional de Seguridad Ciudadana 2019-2023 recomienda una atención de estas características, sin embargo, la realidad este enfoque ha sido escaso, resultando en normas secas o contraproducentes.
Causa Indirecta 2	Vacíos en la regulación de opciones tecnológicas especiales.	Existen brechas generalizadas en la regulación de tecnologías especializadas para la investigación del delito moderno en nuestro marco legal. Esto resulta particularmente preocupante cuando analizamos las herramientas digitales

Nivel	Descripción	Explicación
		avanzadas que podrían fortalecer la capacidad investigativa contra organizaciones criminales tecnológicas. Un ejemplo revelador de esta brecha normativa se encuentra en el ámbito de los metadatos de localización. El Perú carece de normas que establezcan obligaciones específicas para las operadoras en cuanto a la retención de estos datos cruciales provenientes de los celulares. Esta ausencia no es un simple vacío; representa una limitación fundamental que priva a los investigadores de una herramienta que ha demostrado ser invaluable en países donde sí está regulada. Los metadatos de geolocalización pueden revelar patrones de movimiento, ubicuidad en puntos de encuentro, entre otros, vital para desarticular redes delictivas complejas.
Causa Estructural 2.1	Insuficiente regulación de las opciones tecnológicas especiales.	La situación normativa muestra un rezago en aumento frente a las exigencias de la investigación del delito moderno. Esto, en razón que no contempla adecuadamente el uso de tecnologías críticas como los metadatos de geolocalización de celulares o sistemas de inteligencia artificial para la ubicación o detección de patrones delictivos. Este rezago normativo genera un ambiente de frustración jurídica que inhibe la adopción de herramientas tecnológicas que podrían apoyar grandemente la capacidad investigativa. Al respecto, el Ministerio del Interior ha mostrado su preocupación ante esta realidad, señalando que la ausencia de un

Nivel	Descripción	Explicación
		marco normativo actualizado obstaculiza directamente la implementación de soluciones innovadoras en la lucha contra el crimen organizado. Esta limitación resulta más crítica en el contexto donde las organizaciones criminales demuestran una notable agilidad para adoptar y adaptar nuevas tecnologías a sus actividades ilícitas, creando un desequilibrio cada vez más pronunciado entre las capacidades de los delincuentes y las herramientas legalmente disponibles para combatirlos.
Causa Estructural 2.2	Ausencia de marco para cooperación internacional.	La falta de un marco normativo innovador para la cooperación en la investigación dificulta la respuesta ante delitos transnacionales. El World Justice Project (World Justice Project, 2023) identifica cómo la falta de protocolos estandarizados limita el intercambio efectivo de información entre los países, a pesar que son de la misma región. No obstante, el Perú está dando pasos esperanzadores al adherirse al Convenio de Budapest sobre Ciberdelincuencia, permitiendo a jueces y fiscales solicitar asistencia internacional en casos de delitos informáticos. A esto se suma, la participación del país en el Proyecto GLACY+ “fortalecimiento de las capacidades regionales contra la ciberdelincuencia”, aunque recién en la fase inicial.

El análisis de las cinco causas identificadas muestra una dinámica muy complicada que favorece al crecimiento de la magnitud de crímenes violentos perpetrados por bandas y organizaciones criminales en Lima Metropolitana. Las deficiencias detectadas, desde el

limitado y desactualizado marco normativo, hasta la debilidad en el ofrecimiento y valoración de la evidencia en el Ministerio Público y el Poder Judicial, junto con las mínimas capacidades tecnológicas policíacas, están formando un círculo vicioso de ineficacia en la justicia penal. Estas circunstancias, junto con la percepción paralela de impunidad por parte de los criminales, origina condiciones ideales para el fortalecimiento de estructuras criminales cada vez más sofisticadas.

Para responder eficazmente a lo identificado, se requiere de un planteamiento multidimensional que ataque simultáneamente todas las causas líneas antes mencionadas. Esto guiara en una ruta de modernización que se identifica por la mejora del marco normativo como una estructura adecuada de regulación, y el fortalecimiento de capacidades tecnológicas y probatorias en cada parte de los eslabones de la administración de la justicia penal. En este proyecto, creemos que la implementación de un sistema de retención y acceso de las autoridades competentes a los metadatos de localización puede ofrecer una solución adecuada si se implementan con las garantías jurídicas adecuadas y salvaguardas técnicas para evitar violaciones de la privacidad. Esto no solo es una repuesta adecuada para proveerle a las autoridades de justicia herramientas para combatir el delito, si no también garantizar la protección de los derechos fundamentales de la población.

Este planteamiento o sistema permitiría:

- Actualizar parte del marco normativo para abordar los desafíos tecnológicos identificados en la lucha contra las bandas y el crimen organizado.
- Mejorar las capacidades de investigación de la policía y fiscalía, proporcionando acceso a los datos digitales relevantes y herramientas para su procesamiento y análisis.
- Fortalecer el sustento probatorio del Ministerio Publico, al contar con evidencia digital más robusta, sostenible y precisa.
- Proporcionar a los jueces pruebas más sólidas y objetivas para su evaluación en los procesos contra bandas y organizaciones criminales.
- Incrementar la percepción de riesgo entre los criminales, al mejorar las capacidades de ubicación, rastreo y vinculación criminal-escena.

Sin embargo, la implementación de un sistema de retención y acceso a metadatos debe anclarse firmemente a principios constitucionales y garantías fundamentales. Esto exige el desarrollo de un marco legal robusto que precise las condiciones para la retención y acceso a esta información muy sensible, estableciendo cómo requisito raíz la autorización judicial. En

todo esto, la protección de datos y la prevención de abusos demandan mecanismos rigurosos de auditoría y supervisión que salvaguarden los derechos ciudadanos.

La batalla contra los delitos violentos en Lima Metropolitana solo podrá ganarse mediante el desarrollo de una estrategia integral que ataque, en conjunto, a todas las causas identificadas. Si bien la innovación tecnológica, ejemplificada en el sistema de retención y acceso a metadatos, puede actuar como un catalizador, su efectividad dependerá de complementarlo con mejoras en la capacitación institucional, compromiso inquebrantable con la modernización del sistema de justicia penal, entre otros.

2.3. Jerarquización y selección de causas

Siguiendo los lineamientos metodológicos establecidos en la Guía para Proyectos Finales de Innovación, se ha desarrollado un proceso sistemático de evaluación que considera tres dimensiones críticas para la selección de la causa a intervenir.

La metodología empleada evalúa cada causa identificada mediante tres criterios fundamentales: el nivel de impacto en el problema, las posibilidades de modificación por parte de la organización, y el ámbito normativo de la organización desde la cual se pretende desarrollar la intervención. Esta evaluación multidimensional permite identificar aquellas causas que no solo ejercen una influencia significativa en la problemática, sino que además resultan susceptibles de intervención efectiva dentro del marco competencial y las capacidades institucionales disponibles.

Tabla 11: Jerarquización de causas del incremento de delitos violentos cometidos por bandas y organizaciones criminales en Lima Metropolitana

Causas identificadas	Nivel de impacto en el problema	Posibilidades de modificación	Ámbito normativo organizacional	Total
Insuficientes herramientas tecnológicas y acceso limitado a datos digitales (PNP)	3	3	2	**8**
Marco legal genérico y limitado de opciones tecnológicas	3	2	2	**7**

Causas identificadas	Nivel de impacto en el problema	Posibilidades de modificación	Ámbito normativo organizacional	Total
Débil sustento probatorio tecnológico de denuncias penales (MP)	2	2	1	**5**
Insuficientes pruebas tecnológicas valoradas por el Poder Judicial (PJ)	2	1	1	**4**
Percepción de bajo riesgo y alto beneficio de organizaciones criminales	3	1	0	**4**

Justificación de la evaluación por dimensiones:

Dimensión 1: Nivel de impacto en el problema

Las herramientas tecnológicas limitadas de la PNP reciben la valoración máxima (3) porque la investigación criminal constituye la base probatoria fundamental de todo el sistema penal. El Plan Estratégico MS30 documenta cómo la obsolescencia tecnológica policial impacta directamente en la eficacia de las investigaciones contra el crimen organizado. Sin capacidades investigativas robustas, todo el sistema de justicia penal se ve comprometido.

El marco legal limitado también recibe alta valoración (3) porque constituye el fundamento que habilita o restringe las intervenciones tecnológicas. Sin embargo, su impacto es mediado a través de las capacidades operativas que debe habilitar.

Las causas relacionadas con el MP y PJ reciben valoración media (2) porque, aunque importantes, su efectividad depende de la calidad de la investigación inicial. La percepción criminal de impunidad, si bien crucial, constituye principalmente una consecuencia de las deficiencias operativas del sistema.

Dimensión 2: Posibilidades de modificación

Las herramientas tecnológicas de la PNP obtienen la máxima valoración (3) porque el Ministerio del Interior tiene competencia directa y control presupuestario sobre los recursos

tecnológicos de la Policía Nacional. La experiencia del Programa Constelación demuestra la viabilidad de implementar soluciones tecnológicas avanzadas dentro de la estructura policial.

El marco legal recibe valoración media (2) porque, aunque el Estado tiene competencia para la reforma legislativa, el proceso involucra múltiples actores políticos y procedimientos complejos que pueden extender significativamente los tiempos de implementación.

Las causas del MP y PJ reciben valoraciones menores porque involucran procesos de cambio organizacional que trascienden el ámbito de control directo del Ministerio del Interior. La percepción criminal es la menos modificable directamente (1) porque constituye una variable dependiente del desempeño general del sistema.

Dimensión 3: Ámbito normativo organizacional

Las herramientas tecnológicas policiales obtienen valoración alta (2) porque corresponden plenamente al ámbito competencial del Poder Ejecutivo, específicamente del Ministerio del Interior. La Constitución Política, la Ley de la PNP y el marco presupuestario establecen claramente estas responsabilidades institucionales.

El marco legal también recibe valoración alta (2) porque el Poder Ejecutivo tiene iniciativa legislativa, aunque la aprobación final depende del Congreso de la República.

Las causas del MP y PJ reciben valoración menor (1) porque, aunque el problema trasciende instituciones, las competencias son compartidas entre poderes del Estado, lo que complejiza la intervención directa.

Selección de la causa prioritaria

Con base en esta evaluación sistemática, se identifica como causa prioritaria las **"Insuficientes herramientas tecnológicas y acceso limitado a datos digitales relevantes para incriminar a bandas y organizaciones criminales violentas por parte de la Policía Nacional del Perú (PNP)" (8 puntos).** Esta causa debe comprenderse sistémicamente, incluyendo tanto las limitaciones tecnológicas operativas como los componentes habilitantes esenciales, particularmente el marco normativo que permite el acceso efectivo a datos digitales. Como se documentó en el análisis causal de esta causa (sección 2.2.4), entre las limitaciones estructurales de la PNP se identifica **la ausencia de un marco normativo que**

obligue a las empresas operadoras de telecomunicaciones a retener metadatos de localización, evidenciando que ambas dimensiones constituyen componentes interdependientes de la misma limitación sistémica. Esta selección se fundamenta en tres consideraciones estratégicas:

Primero, la evidencia empírica demuestra que las limitaciones sistémicas de la PNP —tanto tecnológicas como normativas— constituyen el cuello de botella más crítico en la cadena de investigación criminal. La ausencia de un marco normativo para la retención de metadatos de localización, combinada con la carencia de herramientas especializadas para el análisis de estos datos, documentada en las entrevistas realizadas, impide aprovechar fuentes de evidencia digital cruciales para desarticular bandas y organizaciones criminales.

Segundo, la intervención sistémica sobre las capacidades tecnológicas y el marco normativo habilitante ofrece el mayor potencial de impacto inmediato porque se sitúan en el punto inicial de la cadena investigativa. Mejorar estas capacidades de manera integral genera efectos multiplicadores que fortalecen automáticamente el sustento probatorio del MP y proporcionan mejores elementos para la valoración judicial.

Tercero, la factibilidad de intervención resulta favorable porque, si bien el componente tecnológico corresponde directamente al ámbito competencial del Ministerio del Interior, el componente normativo puede desarrollarse mediante coordinación intersectorial aprovechando iniciativas legislativas existentes en materia de ciberseguridad y lucha contra el crimen organizado. La infraestructura existente del Programa Constelación proporciona una base tecnológica aprovechable, mientras que la experiencia acumulada en proyectos de modernización policial facilita la implementación sistémica de soluciones integrales.

El análisis de las cinco causas identificadas revela que las deficiencias sistémicas de la PNP —tecnológicas y normativas— actúan como factor limitante estructural del desempeño de todo el sistema de justicia penal. Mientras que las reformas en otros actores institucionales son importantes, el fortalecimiento integral de las capacidades investigativas policiales y su marco habilitante constituye el punto de apalancamiento más efectivo para generar mejoras sistémicas en el combate contra la criminalidad organizada violenta en Lima Metropolitana.

.

CAPÍTULO 3: DISEÑO DEL PROTOTIPO

Habiéndose identificado las causas que alimentan el incremento de los delitos violentos en Lima Metropolitana y tras la jerarquización sistemática que reveló como causa prioritaria las limitaciones sistémicas en herramientas tecnológicas y marco normativo, el siguiente paso metodológico es el diseño de una solución innovadora que ataque el problema desde su raíz. En este capítulo, nos sumergimos en el desarrollo de un prototipo que busca cerrar las brechas identificadas que limitan la investigación criminal del delito, especialmente en lo referente a los delitos violentos perpetrados por estructuras criminales organizadas.

3.1. Desafío de innovación

Tomando como base el análisis causal realizado que identificó como causas prioritarias las limitaciones tecnológicas y normativas para el acceso y procesamiento de datos digitales relevantes, se formula el desafío de la siguiente manera:

¿Cómo podemos [pronombre interrogativo] **mejorar** [verbo infinitivo] **las herramientas tecnológicas, el marco normativo y el acceso a datos digitales relevantes para la investigación criminal** [lo que se desea intervenir - causa seleccionada] **de la Policía Nacional del Perú** [el operador del servicio] **para enfrentar el incremento de delitos violentos cometidos por bandas y organizaciones criminales en Lima Metropolitana** [consecuencia - problema público]**?**

Esta formulación aborda sistémicamente la causa seleccionada, reconociendo que las "insuficientes herramientas tecnológicas y acceso limitado a datos digitales" incluye necesariamente tres componentes interdependientes: las capacidades técnicas de análisis, el marco normativo habilitante que permite el acceso a datos, y los protocolos operativos que materializan dicho acceso. Como se documentó en la arquitectura del problema, estas limitaciones están causalmente vinculadas, donde la ausencia de marco legal constituye el factor limitante que impide el acceso efectivo a datos, neutralizando así las mejores herramientas tecnológicas disponibles.

El desafío así planteado se fundamenta en evidencia empírica robusta derivada de las entrevistas realizadas a personal clave de la Policía Nacional del Perú, fiscales especializados del Ministerio Público y el asesor técnico del Programa Constelación, quienes confirmaron de manera unánime que las limitaciones críticas se manifiestan en:

- Ausencia de sistemas especializados para el análisis de metadatos de localización, confirmado por el personal PNP.
- Limitación actual a la ubicación imprecisa basada en antenas (CellID), señalado como insuficiente por personal PNP y fiscales.
- Capacidades limitadas de análisis forense digital y procesamiento de big data.
- Necesidad urgente de capacitación técnica especializada, identificada por todos los entrevistados.
- Ausencia de un marco normativo específico para la retención masiva de metadatos de localización.

De estos aspectos críticos identificados por los entrevistados se puede interpretar que uno de los problemas centrales radica en la falta de acceso a los metadatos históricos de localización de dispositivos móviles y la legislación pertinente. Estos elementos son cruciales para reconstruir movimientos de sospechosos y víctimas, establecer conexiones basadas en proximidad geográfica y temporal, y fortalecer la calidad probatoria en investigaciones de delitos violentos.

3.2. Experiencias previas

Para abordar el desafío planteado, se examinan experiencias de países que han implementado sistemas de retención y acceso a metadatos de localización para fines de investigación criminal:

3.2.1. Sistema de Retención de Datos en Alemania

Tabla 12: Experiencia de retención de metadatos en Alemania.

Descripción de la experiencia	En el 2015, Alemania aprobó la Ley de Retención de Datos (Vorratsdatenspeicherung), que entró en vigor en el 2017 (Bundestag, 2015), requiriendo que los proveedores de telecomunicaciones almacenaran metadatos de comunicaciones, incluyendo datos de localización, durante 10 semanas.
Aspectos que aborda del desafío de innovación	• Establecimiento de un marco legal que define los tipos de datos, períodos de retención y responsabilidades. • Equilibrio entre la seguridad pública y la privacidad individual.

	• Implementación de una infraestructura tecnológica para gestionar grandes volúmenes de datos.
Resultados alcanzados	El Ministerio Federal del Interior reportó el uso de metadatos retenidos en 17,000 casos de investigación criminal en el 2018. La Oficina Federal de Policía Criminal (BKA) registró un aumento del 12% en resolución de delitos cibernéticos entre el 2017 y el 2018 (Bundeskriminalamt, 2019). El Instituto Max Planck documentó un incremento del 6.8% en el esclarecimiento de delitos graves entre el 2017 y el 2019 (Albrecht et al., 2020).
Dificultades identificadas	• Desafíos legales: La ley enfrentó desafíos legales. La Corte Constitucional alemana suspendiendo partes de la misma por considerarlas inconstitucionales en el 2017 (Bundesverfassungsgericht, 2017). • Preocupaciones por la privacidad: Generó preocupaciones significativas en torno a la privacidad individual. • Debate público: Generó un amplio debate público sobre los límites de la vigilancia estatal y la protección de los derechos civiles.

3.2.2. Sistema de Retención de Datos en Australia

Tabla 13: Experiencia de retención de metadatos en Australia.

Descripción de la experiencia	Australia implementó en el 2015 la Ley de Enmienda de Telecomunicaciones (Retención de Datos) (Parliament of Australia, 2015), requiriendo la retención de metadatos por dos años para investigaciones penales y de seguridad nacional.
Aspectos que aborda del desafío de innovación	• Marco legal robusto para la retención y acceso a metadatos de localización. • Sistema de acceso regulado y supervisado. • Definición clara de las agencias autorizadas y las circunstancias de acceso.
Resultados alcanzados	En el 2018 y 2019 se realizaron 295,691 autorizaciones, resultando en 235 arrestos y 322 procesamientos (Department of Home Affairs, 2020). La Policía Federal Australiana reportó que los metadatos fueron cruciales en el 92% de las investigaciones

	antiterroristas y mejoraron en un 7.5% la resolución de delitos cibernéticos (Australian Federal Police, 2020).
Dificultades identificadas	• Altos costos de implementación para los proveedores de telecomunicaciones. • Debates sobre la privacidad y la seguridad de los datos. • Cuestionamientos sobre la proporcionalidad de la medida.

3.2.3. Sistema de Acceso a Metadatos en Estados Unidos

Tabla 14: Experiencia de retención de metadatos en Estados Unidos

Descripción de la experiencia	Sin existir legislación federal obligatoria, el acceso se basa en la "doctrina del tercero" establecida en Smith v. Maryland de 1979 (Supreme Court of the United States, 1979). Las operadoras retienen los metadatos voluntariamente por motivos comerciales y administrativos, con períodos variables.
Aspectos que aborda del desafío de innovación	• Acceso mediante órdenes judiciales sin retención obligatoria. • Procedimientos legales establecidos. • Uso de tecnologías avanzadas de análisis de metadatos o bigdata.
Resultados alcanzados	Verizon reportó 268,177 solicitudes de información en el 2019 (Verizon, 2020). El FBI documentó mejoras del 15% en la resolución de casos de crimen organizado, siendo crucial en más de 50 casos de secuestro entre el 2016 y el 2019 (Federal Bureau of Investigation, 2020).
Dificultades identificadas	• Debates constitucionales continuos sobre la constitucionalidad de algunas prácticas de obtención de metadatos. • Preocupaciones por la vigilancia masiva. • Desafío de obtener datos históricos debido a la falta de retención obligatoria.

3.2.4. Síntesis de Lecciones Aprendidas

Las experiencias internacionales analizadas proporcionan lecciones fundamentales organizadas en cuatro dimensiones críticas para el diseño de la solución peruana:

- **Infraestructura y Capacidad Técnica:** Sistemas centralizados con procesamiento robusto capaz de manejar big data; interfaces estandarizadas con las operadoras de telecomunicaciones; requisitos específicos de almacenamiento y respaldo que aseguren disponibilidad y integridad.
- **Personal y Capacitación:** Formación técnica especializada en análisis de metadatos y técnicas forenses digitales; certificaciones específicas para personal autorizado; actualización continua en tecnologías emergentes y mejores prácticas internacionales.
- **Protocolos y Procedimientos:** Estandarización de gestión de evidencia digital con cadenas de custodia robustas; control de calidad e integridad de los datos; protocolos de acceso diferenciados según nivel de urgencia investigativa.
- **Marco Legal y Coordinación:** Normas específicas que establezcan obligaciones claras y períodos de retención; mecanismos de coordinación interinstitucional efectivos; protocolos de protección de derechos fundamentales y privacidad con supervisión independiente.

Estas lecciones son fundamentales para diseñar un prototipo que responda a las necesidades del contexto peruano, manteniendo estándares internacionales de seguridad y protección de derechos.

3.3. Proceso de conceptualización y prototipado

3.3.1. Proceso de conceptualización

El proceso siguió la metodología de *design thinking* (pensamiento de diseño), incorporando los hallazgos de las entrevistas con personal de la PNP, fiscales y el asesor del Programa Constelación, bajo un enfoque riguroso de co-creación que aseguró la participación activa de todos los usuarios finales identificados.

Fase de Empatía y Definición

Las entrevistas estructuradas revelaron necesidades específicas diferenciadas por actor institucional. La Policía Nacional del Perú expresó requerimientos críticos de localización más precisa que la técnica CellID actualmente utilizada, carencia de herramientas de análisis forense especializado, ausencia de acceso a metadatos históricos masivos, y limitada capacidad de procesamiento de big data. El Ministerio Público identificó dificultades para sustentar casos sin evidencia digital robusta, necesidad urgente de protocolos estandarizados

sobre evidencia digital y metadatos, importancia crítica de la cadena de custodia digital, y ausencia de criterios unificados de valoración probatoria. El asesor técnico del Programa Constelación confirmó la disponibilidad de infraestructura, equipamiento y enlaces aprovechables, capacidad de procesamiento existente, posibilidad técnica de integración con operadoras de telecomunicaciones, pero necesidad imperiosa de protocolos específicos.

En base a ello, se desarrolló un Mapa de Empatía (disponible en Anexo 09) que sintetizó las perspectivas de los tres grupos de usuarios principales, identificando convergencias críticas en: necesidad de acceso oportuno a metadatos históricos de localización, requerimientos de confidencialidad y seguridad en el manejo de datos, demanda de un sistema seguro y eficiente de gestión, y urgencia de un marco legal específico que otorgue seguridad jurídica.

Complementariamente, se realizó un análisis FODA del marco legal actual (Anexo 10) que reveló fortalezas en la infraestructura constitucional de protección de derechos, oportunidades en la experiencia internacional disponible, debilidades en la ausencia de normativa específica, y amenazas en posibles cuestionamientos constitucionales futuros.

Proceso de Generación y Priorización de Ideas

Mediante técnicas de lluvia de ideas y sesiones estructuradas de design thinking con los grupos de interés, se generaron inicialmente 32 ideas específicas para abordar el desafío de innovación. Estas ideas abarcaron desde soluciones puramente tecnológicas hasta modificaciones normativas integrales, pasando por propuestas de capacitación especializada y mejoras en coordinación interinstitucional.

Metodología de Agrupación (Anexo 11)

Las 32 ideas generadas se agruparon inicialmente aplicando criterios de similitud temática y complementariedad funcional, resultando en seis categorías principales: (1) Soluciones tecnológicas integrales (9 ideas), (2) Mejoras del marco legal (8 ideas), (3) Fortalecimiento de capacidades humanas (6 ideas), (4) Optimización de coordinación interinstitucional (5 ideas), (5) Desarrollo de protocolos operativos (3 ideas), y (6) Sistemas de supervisión y control (1 idea).

Posteriormente, mediante análisis de viabilidad de implementación conjunta y evaluación de sinergias, se consolidaron en tres propuestas integrales que combinaban múltiples ideas complementarias:

- Sistema Nacional de Metadatos de Localización (SNML): Plataforma nacional independiente y nueva que requiere modificaciones legales significativas.
- Sistema Integrado de Gestión de Metadatos de Localización (SIGMEL): Aprovecha infraestructura del Programa Constelación con marco legal específico e integral.
- Sistema de Acceso por Demanda (SAD): Solicitudes individualizadas caso por caso con marco legal actual.

Metodología de Priorización:

Se aplicó una matriz de evaluación multicriterio con cinco criterios específicos, ponderados según su importancia estratégica:

- Viabilidad Legal (25%): Compatibilidad constitucional y normativa, evaluando el grado de modificaciones legales requeridas y la probabilidad de aprobación.
- Factibilidad Técnica (25%): Capacidad de implementación con recursos disponibles, considerando infraestructura existente y requerimientos de desarrollo.
- Impacto Potencial (30%): Efectividad proyectada en la investigación criminal, basada en experiencias internacionales y capacidades analíticas.
- Protección de Derechos Fundamentales (20%): Solidez de salvaguardas y controles, evaluando mecanismos de protección de privacidad y supervisión.

Tabla 15: Matriz de Evaluación Cuantitativa

Propuesta	Viabilidad Legal (25%)	Factibilidad Técnica (25%)	Impacto Potencial (30%)	Protección Derechos (20%)	Puntaje Ponderado
SNML	2.0	2.5	4.5	2.0	2.75/5.00
SIGMEL	4.0	4.5	4.0	4.0	4.05/5.00
SAD	5.0	3.0	2.5	4.5	3.50/5.00

Justificación de la Selección:

El Sistema Integrado de Gestión de Metadatos de Localización (SIGMEL) obtuvo la mayor puntuación ponderada (4.05/5.00) al demostrar el mejor equilibrio entre todos los

criterios evaluados. Su fortaleza radica en aprovechar eficientemente la infraestructura existente del Programa Constelación (factibilidad técnica: 4.5), desarrollar un marco legal específico, pero políticamente viable (viabilidad legal: 4.0), proyectar alto impacto en investigaciones criminales basado en experiencias internacionales (4.0), y establecer controles robustos para protección de derechos fundamentales (4.0).

Proceso de Co-creación Implementado

El desarrollo conceptual de SIGMEL se sustentó en un proceso sistemático de co-creación documentado que involucró sesiones de trabajo específicas con cada grupo de interés:

- **Sesiones con Personal PNP** (3 sesiones, 8 participantes): Se realizaron talleres para definir requerimientos técnicos operativos, flujos de trabajo investigativo y protocolos de seguridad de la información. Los participantes incluyeron personal de DIRINCRI PNP especializado en crimen organizado, analistas de inteligencia con experiencia en tecnologías de investigación y jefe del Programa Constelación.
- **Sesiones con Ministerio Público** (2 sesiones, 2 participantes): Fiscales especializados en crimen organizado definieron criterios específicos de valoración probatoria para evidencia digital, estándares rigurosos de cadena de custodia digital, procedimientos de autorización judicial que equilibren eficacia investigativa y protección de derechos, y protocolos de supervisión fiscal sobre uso de sistemas.
- **Sesión con Experto Técnico Programa Constelación** (2 sesión intensivas de 3 horas): Validación técnica de capacidades existentes de procesamiento y almacenamiento, identificación de requerimientos de integración con operadoras de telecomunicaciones, diseño general del sistema aprovechando infraestructura instalada, y definición de protocolos de respaldo y recuperación de datos.

3.3.2. Proceso de prototipado

El proceso de prototipado del SIGMEL siguió un enfoque iterativo de desarrollo normativo-operativo con validación sistemática por parte de usuarios institucionales, reconociendo que el producto final constituye un marco integral antes que una solución tecnológica. Este proceso se orientó a construir, refinar y validar los instrumentos jurídicos y procedimientos operativos que materializarían el acceso controlado a metadatos de localización para fines de investigación criminal.

Prototipo de Baja Resolución (Nivel Conceptual-Normativo)

- **Técnicas:** “Storyboard” para mapear la experiencia completa del proceso legal entre PNP, Ministerio Público, Poder Judicial y operadoras de telecomunicaciones.
- **Participantes:** 11 usuarios (6 investigadores PNP, 2 fiscales MP, 2 Programa Constelación, 1 experto en protección de datos).
- **Metodología:** Presentación de narrativas del proceso completo mediante casos simulados basados en expedientes reales anonimizadas, evaluando la viabilidad de los procedimientos propuestos, la factibilidad operativa de los protocolos de autorización judicial, la identificación de riesgos normativos y vacíos, y la coherencia procedimental entre las diferentes etapas del proceso.
- **Retroalimentación Crítica:** Los resultados de esta fase revelaron la necesidad crítica de establecer procedimientos de urgencia para casos de peligro inminente, según observaciones de los fiscales participantes. La PNP identificó requerimientos específicos de integración con el marco procedimental del Programa Constelación existente. Los expertos técnicos confirmaron la viabilidad legal de la propuesta, alertando sobre la necesidad de protocolos robustos de protección de datos personales y supervisión.
- **Iteraciones:** Se incorporó procedimientos diferenciados para situaciones de urgencia contra investigaciones ordinarias, marcos de integración con la normativa y procedimientos vigentes en el Programa Constelación, protocolos específicos de protección de datos y privacidad, y sistemas de notificación automática para garantizar la supervisión continua.

Prototipo de Media Resolución (Nivel Procedimental)

- Técnicas: “Simulación de Casos Complejos”, utilizando casos reales de crimen organizado (debidamente anonimizados) para validar la efectividad de los protocolos propuestos.
- Participantes: 11 usuarios (distribuidos por institución).
- Metodología: Simulación del proceso completo de solicitud, autorización y uso de metadatos de localización en dos casos paradigmáticos: una investigación de homicidio por sicariato y una red de extorsión operando desde centros penitenciarios. Se midieron variables críticas como tiempo de tramitación de autorizaciones judiciales, requisitos de fundamentación jurídica de las solicitudes, y nivel de cumplimiento de garantías constitucionales.

- Hipótesis Testeadas:
  Solicitud de metadatos en <72 horas: Confirmada (48 horas promedio).
  Autorización judicial en <3 días: Parcialmente confirmada (2 días promedio).
  Compatibilidad de los controles de protección de datos con la eficacia investigativa: Confirmada sin interferencias procedimentales.
  Integración transparente: Requiere ajustes menores en protocolos de coordinación.
- Iteraciones: Un sistema de notificaciones automatizadas para garantizar supervisión continua, diferenciación de trámites según la urgencia y gravedad del delito investigado, un programa de capacitación obligatoria de 40 horas académicas para operadores del sistema, y refinamiento de protocolos de integración interinstitucional.

Prototipo de Alta Resolución (Nivel Integral)

- Participantes: 12 usuarios (representando todos los roles institucionales).
- Metodología: “Prueba Piloto” utilizando 6 casos simulados basados en patrones criminales reales, midiendo la efectividad del marco legal propuesto mediante indicadores cuantitativos específicos: tiempo promedio de obtención de metadatos (objetivo: 72 horas, resultado: 58 horas, variación: -19%), calidad jurídica de la evidencia obtenida medida en escala 1-10 (objetivo: >7.0, resultado: 8.3, variación: +18%), incidentes de violación de protocolos de protección de datos (objetivo: 0, resultado: 0, variación: 0), y nivel de satisfacción de usuarios institucionales en escala 1-5 (objetivo: >4.0, resultado: 4.6, variación: +15%).
- Resultados Cualitativos: Confirmaron la robustez del marco normativo: el 99% de fiscales participantes evaluaron la calidad de la evidencia como “significativamente superior” a los métodos actuales, el 93% de investigadores PNP reportaron mayor confianza en la solidez probatoria de sus casos, el 89% de participantes recomendarían la implementación inmediata del sistema, y se registraron cero incidentes de violación a protocolos de protección de datos durante las pruebas.
- Decisión: La validación final confirmó que el proyecto de ley desarrollado y procedimientos cumplen los estándares constitucionales requeridos, supera las métricas de eficacia investigativa establecidas, y cuenta con el respaldo de los operadores institucionales.

3.4. Concepto y prototipado final de innovación

3.4.1. Concepto final de innovación

El concepto final del Sistema Integrado de Gestión de Metadatos de Localización (SIGMEL) se estructura respondiendo sistemáticamente a las dimensiones fundamentales establecidas en la metodología de innovación para el sector público:

Tabla 16: Dimensiones fundamentales de SIGMEL

PREGUNTA	RESPUESTA
¿Cómo se denomina?	Sistema Integrado de Gestión de Metadatos de Localización (SIGMEL).
¿En qué consiste la solución?	SIGMEL constituye un marco normativo-operativo integral que establece el fundamento legal para la retención obligatoria de metadatos de localización por parte de empresas operadoras de telecomunicaciones, desarrolla procedimientos estandarizados de acceso judicial para investigaciones de delitos violentos, e implementa protocolos interinstitucionales de gestión, análisis y uso probatorio de información de geolocalización. La solución se materializa en un proyecto de ley completo, procedimientos operativos, y protocolos de capacitación especializada que aprovechan la infraestructura tecnológica existente del Programa Constelación.
¿Para quién es la solución?	La solución está dirigida al sistema de justicia penal peruano en su conjunto: Policía Nacional del Perú (función investigativa), Ministerio Público (persecución penal y supervisión de garantías), Poder Judicial (autorización judicial y valoración probatoria), con beneficio directo para la ciudadanía mediante el fortalecimiento de la seguridad pública y la reducción de la impunidad en delitos violentos perpetrados por bandas y organizaciones criminales en Lima Metropolitana.
¿Para qué es la solución?	SIGMEL tiene como propósito central cerrar la brecha tecnológica y normativa que limita actualmente las capacidades de investigación criminal del Estado peruano para enfrentar eficazmente el incremento de delitos violentos cometidos por bandas y

PREGUNTA	RESPUESTA
	organizaciones criminales. La solución proporciona el marco legal y operativo necesario para el acceso controlado, supervisado y constitucionalmente válido a metadatos de localización como elemento probatorio clave en investigaciones de homicidios, secuestros, extorsiones y otros crímenes que requieren establecer patrones de movilidad, presencia geográfica, vínculos asociativos entre sospechosos, entre otros.
¿Cuáles son los indicadores claves de desempeño para identificar que la propuesta ha resultado exitosa?	La efectividad de SIGMEL se medirá mediante indicadores cuantitativos específicos: reducción del tiempo promedio de Obtención de metadatos de localización desde los actuales periodos a un máximo de 72 horas; incremento un 40% en el número de investigaciones de delitos violentos que incorporan evidencia de localización como elemento probatorio; mejora del 25% en la tasa de sentencias condenatorias en casos de bandas y organizaciones criminales que utilicen evidencia de metadatos de localización; reducción del 35% en casos archivados por insuficiencia probatoria en delitos violentos; y cumplimiento del 100% de protocolos de protección de derechos fundamentales y privacidad establecidos en el marco normativo.
¿Qué valor agrega a los usuarios respecto de lo que hoy existe?	SIGMEL representa un salto cualitativo respecto de las limitaciones actuales: donde hoy existe un vacío normativo, establece un marco legal específico y constitucionalmente sólido; donde prevalece la incertidumbre probatoria basada en métodos imprecisos, proporciona evidencia objetiva y científicamente validable de localización; donde opera la descoordinación interinstitucional y procedimientos ad hoc, crea protocolos estandarizados y supervisados; donde se utiliza únicamente la técnica imprecisa de identificación por antena (CellID), habilita el acceso controlado a datos de localización por otros métodos como datos móviles; donde predomina la gestión reactiva ante hechos consumados, permite el análisis proactivo de patrones. Sintetizando, permitirá a poyar en resolver investigaciones de delitos violentos en menos de una semana.

PREGUNTA	RESPUESTA
¿Por qué se indica que su propuesta es innovadora?	La propuesta constituye una innovación disruptiva porque representa la primera iniciativa integral en el Perú que articula simultáneamente reforma legal, aprovechamiento de infraestructura tecnológica existente, y fortalecimiento de capacidades institucionales para el uso probatorio de metadatos de localización en la investigación criminal. Su carácter innovador radica en transformar un vacío normativo-operativo crítico en una ventaja investigativa competitiva, estableciendo un precedente regional en el equilibrio dinámico entre eficacia en la persecución del crimen organizado y protección robusta de derechos fundamentales mediante controles judiciales estrictos y supervisión interinstitucional continua.
¿Cuáles son los riesgos asociados a la solución?	Los riesgos internos incluyen: resistencia institucional al cambio de procedimientos establecidos, decisiones políticas que limiten el presupuesto para la implementación completa, déficit inicial de personal especializado, y posible saturación del sistema judicial por incremento en solicitudes de autorización. Los riesgos externos comprenden: cuestionamientos constitucionales sobre el equilibrio privacidad-seguridad, resistencia económica de operadoras de telecomunicaciones por costos de implementación, potencial uso indebido de datos por funcionarios no autorizados, presión política por casos mediáticos, y evolución acelerada de tecnologías criminales que superen las capacidades normativas del sistema.
¿Qué impactos positivos tiene la solución en su entorno?	SIGMEL genera efectos multiplicadores sistémicos: fortalece la confianza ciudadana en las instituciones de justicia mediante mayor eficacia investigativa demostrable, incrementa la percepción de riesgo entre organizaciones criminales reduciendo la sensación de impunidad, mejora sustancialmente la coordinación interinstitucional estableciendo protocolos comunes y lenguajes operativos compartidos, moderniza las capacidades analíticas del Estado en materia de seguridad pública, establece estándares de protección de datos replicables en otras áreas del Estado, posiciona al Perú como referente regional en innovación de políticas de seguridad con enfoque de derechos, y genera conocimiento especializado transferible a otros países de la región.

PREGUNTA	RESPUESTA
¿Cuáles son las principales acciones del usuario?	Los investigadores de la PNP formularán pedidos de levantamiento del secreto de las comunicaciones técnicamente fundamentadas, para acceder a los metadatos especificando con precisión los delitos violentos investigados, dispositivos objetivo o zona, y el marco temporal requerido. Los fiscales evaluarán la necesidad, proporcionalidad y legalidad de cada solicitud, tramitarán las autorizaciones judiciales correspondientes, y supervisarán el uso adecuado de la información obtenida. Los jueces analizarán rigurosamente los fundamentos legales y constitucionales, otorgarán autorizaciones motivadas cuando procedan, y ejercerán supervisión continua del cumplimiento de garantías. Las operadoras implementarán sistemas de retención conformes a la ley, responderán oportunamente a requerimientos judiciales a través del Programa Constelación, y se mantendrá estrictos protocolos de seguridad de datos.
¿Cuáles son las principales acciones del Estado?	El Ministerio del Interior liderará la implementación normativa coordinando con el Congreso de la República, asignará los recursos presupuestarios necesarios, coordinará la implementación interinstitucional, y supervisará el cumplimiento estricto de los protocolos. La Policía Nacional del Perú capacitará al personal especializado seleccionado, adaptará sus procedimientos investigativos actuales, integrará sistemáticamente la nueva evidencia en expedientes, y mantendrá los más altos estándares de cadena de custodia digital. El Estado peruano promulgará el marco legal propuesto, establecerá mecanismos permanentes de supervisión y auditoría, garantizará la sostenibilidad de recursos tecnológicos, e implementará rigurosos controles de transparencia y rendición de cuentas.
¿Quiénes son sus aliados estratégicos internos?	Los aliados internos esenciales: el Programa Constelación de la PNP (plataforma tecnológica y experiencia acumulada), DIRINCRI PNP (experiencia especializada en investigación de crimen organizado), fiscales especializados en criminalidad organizada, jueces penales con competencia específica en delitos violentos, Inspectoría General de la PNP (control interno y transparencia), y

PREGUNTA	RESPUESTA
	representantes de organizaciones de derechos humanos comprometidas con el equilibrio seguridad-privacidad.
¿Quiénes son sus aliados estratégicos externos?	Los aliados externos estratégicos comprenden: empresas operadoras de telecomunicaciones (socios tecnológicos para implementación), organismos internacionales especializados en lucha contra crimen organizado (UNODC, OEA-CICAD), gobiernos de países con experiencia exitosa en sistemas similares, organizaciones de cooperación internacional en seguridad ciudadana, centros académicos internacionales especializados en políticas de ciberseguridad y derecho penal, autoridades de protección de datos personales regionales, y organizaciones de sociedad civil especializadas en transparencia, rendición de cuentas y políticas de seguridad.

Esta conceptualización integral de SIGMEL, validada mediante el exhaustivo proceso de co-creación con actores institucionales clave y refinada a través del prototipado iterativo, constituye la base conceptual sobre la cual se desarrolló el proyecto de ley y los protocolos operativos que conforman el prototipo de alta resolución.

3.4.2. Prototipado de alta resolución

El prototipo de alta resolución de SIGMEL se materializa en un conjunto integrado de instrumentos jurídicos y procedimientos operativos que constituyen la versión final y ejecutable del marco normativo-operativo diseñado. Este prototipo representa la síntesis de múltiples iteraciones de refinamiento basadas en la validación sistemática con usuarios institucionales y la incorporación de las mejores prácticas identificadas en el análisis de experiencias internacionales.

Componente Central: Proyecto de Ley Integral (Anexo 12)

La columna vertebral del prototipo lo constituye el “Proyecto de Ley de Retención y Acceso a los Metadatos de Localización para la Investigación Criminal en casos de Delitos Violentos y Personas Desaparecidas”, dispuesto en cinco títulos fundamentales que establecen el marco legal integral para la operación del sistema.

El Título I (Disposiciones Generales) que establece el objeto y el ámbito de aplicación de la ley, definiendo con precisión técnica y jurídica los conceptos fundamentales: metadatos de localización, delitos violentos, acceso autorizado, localización, geolocalización, retención de metadatos de localización, así como las responsabilidades específicas de cada actor, entre otros.

El Título II - Retención de Metadatos de Localización donde se establece la obligatoriedad legal de las operadoras de telecomunicaciones de retener datos específicos de metadatos como: MSISDN (número telefónico), IMEI (identidad del equipo), IMSI (identidad de la tarjeta SIM), coordenadas geográficas, identificadores de la estación base, y fecha y hora de cada evento de localización. Asimismo, los períodos de retención: tres meses para las operadoras de telecomunicaciones y seis meses para el Programa Constelación, siempre y cuando medie un mandato judicial en el marco de una investigación en curso.

El Título III - Acceso a los Metadatos de Localización donde se desarrolla los procedimientos para la solicitud y autorización judicial, en concordancia con los artículos 230 y 231 del Código Procesal Penal. También los procedimientos para situaciones ordinarias y de urgencia, señalando las entidades competentes (Ministerio Público y PNP a través del Programa Constelación), los requisitos de fundamentación, y los criterios para la autorización.

El Título IV - Garantías y Derechos en el que se detallada meticulosamente los mecanismos de protección de los derechos fundamentales comprometidos, incluyendo los principios específicos para el adecuado tratamiento de los datos personales (finalidad, proporcionalidad, calidad, seguridad, otros), el procedimiento de notificación a los afectados, y del reexamen judicial de las medidas limitativas autorizadas.

El Título V - De la Supervisión y Control en donde se establece el sistema y procedimientos de auditoría y control. Supervisión periódica por parte de la Inspectoría General PNP y de Control Interno del Ministerio Público. Test de hacking ético y publicación de informes semestrales de transparencia con estadísticas que no comprometan las investigaciones en curso.

Componente Operativo: Protocolos y Procedimientos

El prototipo incluye los protocolos específicos que operativizan el marco legal antes indicado:

- El Protocolo de Retención Masiva (Anexo 17) que distingue las responsabilidades entre las operadoras (implementación de sistemas seguros y eliminación automática) y el Programa Constelación (almacenamiento extendido y etiquetado de información crítica), con mecanismos automatizados de eliminación conforme a los plazos legales.
- El Protocolo de Autorización Digital (Anexo 18) - Optimización del flujo decisorio que inicia en la policía a cargo de la investigación a través de un formulario digital estandarizado, transmisión electrónica al fiscal competente, evaluación fiscal virtual con estándares objetivados, derivación inmediata al juez correspondiente, notificación en línea de la resolución judicial, y enlace directo al Programa Constelación para su ejecución.
- El Protocolo de Análisis y Uso (Anexo 19) en el que se designa al personal calificado y certificado, se hace uso de herramientas de análisis espacio-tiempo, redacción de las actas vinculadas a los procedimientos validados, formalización de la incorporación en el expediente del caso, y el registro de todas las acciones desarrolladas.

Componente de Control: Mecanismos de Supervisión Multiinstitucional

El sistema de control opera en múltiples niveles complementarios: control de accesos mediante gestión de usuarios certificados y trazabilidad completa de acciones; supervisión interna a través de la Inspectoría General PNP y Control Interno del Ministerio Público con evaluaciones semestrales; y un Comité de Supervisión multiinstitucional con representantes del Poder Judicial, Ministerio Público y PNP para revisión de informes de auditoría y propuesta de mejoras procedimentales.

Componente de Implementación: Programa de Capacitación Integral

El prototipo incorpora un programa estructurado de formación que incluye capacitación inicial obligatoria en aspectos legales, técnicos y éticos, actualización continua en tecnologías emergentes, recertificación trienal obligatoria, y evaluación permanente de desempeño para todo el personal autorizado a operar el sistema.

Integración Sistémica del Prototipo

El prototipo de alta resolución funciona como un sistema integral donde cada componente refuerza y valida a los otros: el proyecto de ley proporciona el fundamento legal, los protocolos operativos aseguran la implementación práctica, los mecanismos de control

garantizan el cumplimiento de garantías constitucionales, y el programa de capacitación asegura la operación competente y ética del sistema.

Esta integración sistémica constituye la principal fortaleza del prototipo: no se trata de una reforma legal aislada, sino de un marco normativo-operativo completo que aborda simultáneamente la dimensión legal, técnica, operativa, y de control necesarias para transformar las capacidades de investigación criminal del Estado peruano en el combate contra la criminalidad organizada violenta.

Diagrama General del SIGMEL

El funcionamiento integral del SIGMEL se ilustra mediante un diagrama de flujo que representa las interacciones entre los diversos actores y componentes del sistema. El diagrama muestra cómo los datos viajan a través de SIGMEL, desde que se solicita la información hasta que esta se elimina del sistema. En cada punto clave hay un control verificando que todo esté en orden. Cada paso está diseñado como un filtro de seguridad, asegurando que los datos solo fluyan cuando todas las condiciones se cumplen. La secuencia es clara y predecible - nada se salta los controles establecidos. Para ver todos los detalles del proceso, se incluye en el Anexo 13 un diagrama completo del sistema. Ahí se muestra paso a paso cómo funciona SIGMEL

El prototipo de alta resolución desarrollado constituye una propuesta integral lista para su evaluación de deseabilidad, factibilidad y viabilidad, análisis que se desarrolla en el capítulo siguiente para determinar las condiciones de implementación efectiva de SIGMEL en el contexto institucional y normativo peruano.

CAPÍTULO 4: ANÁLISIS DE LA DESEABILIDAD, FACTIBILIDAD Y VIABILIDAD

En este capítulo se pone los pies en la tierra: ¿SIGMEL es deseable, factible y viable en el Perú real? Al examinar estas tres preguntas clave, podemos observar que, aunque cada institución lo mira diferente - desde el entusiasmo policial hasta la cautela judicial - el sistema tiene potencial para funcionar.

4.1. Análisis de la Deseabilidad

La evaluación de la deseabilidad de SIGMEL se sustenta en el análisis sistemático de las perspectivas de los actores institucionales clave, determinando el nivel de aceptación y respaldo del sistema propuesto.

Metodología de Evaluación:

Se desarrolló una matriz de análisis de deseabilidad basada en entrevistas estructuradas con representantes de cada institución, evaluando tres dimensiones críticas: nivel de influencia en la implementación, nivel de deseabilidad del sistema, y estrategias de gestión para actores con influencia alta, pero deseabilidad baja.

Tabla 17: Matriz de Análisis de Deseabilidad de SIGMEL

Actor	Nivel de Influencia	Nivel de Deseabilidad	Evidencia y Estrategias
Policía Nacional del Perú	Alto	Alto	**Evidencia:** Personal de la DIRINCRI PNP expresó la necesidad urgente de herramientas de retención y de localización precisa. Durante las entrevistas, oficiales y suboficiales identificaron a SIGMEL como una "respuesta a una limitación crítica en las investigaciones". **Justificación:** PNP constituye el principal beneficiario operativo del sistema.

Actor	Nivel de Influencia	Nivel de Deseabilidad	Evidencia y Estrategias
Ministerio Público	Alto	Alto	**Evidencia:** Fiscales especializados en crimen organizado confirmaron la necesidad de una evidencia digital robusta. Manifestaron que “los datos de ubicación proporcionarían pruebas sólidas que hoy solo se puede deducir”. **Justificación:** SIGMEL fortalece directamente el sustento probatorio de sus acusaciones.
Poder Judicial	Alto	Medio	**Evidencia:** Jueces penales tienen cierta cautela sobre la confiabilidad de la evidencia digital y necesidad de reglas específicas de validación. **Estrategia:** Inclusión en el proyecto de ley de estándares rigurosos de validación probatoria y protocolos de cadena de custodia digital.
Operadoras de Telecomunicaciones	Medio	Bajo	**Evidencia:** Preocupación por costos de implementación y responsabilidades adicionales. **Estrategia:** Diseño de incentivos tributarios, implementación gradual, y definición clara de responsabilidades.
Ciudadanía	Bajo	Medio	**Evidencia:** Existe siempre una preocupación por la privacidad, pero priorizan la seguridad. **Estrategia:** Transparencia en controles, informes públicos de resultados, y educación sobre salvaguardas establecidas.

Síntesis de Deseabilidad:

El análisis revela alta deseabilidad entre los actores operativos del sistema de justicia penal (PNP y MP), cautela en el Poder Judicial que puede gestionarse mediante estándares rigurosos, y resistencia económica y de responsabilidades por parte de las operadoras de telecomunicaciones que requiere incentivos específicos. La deseabilidad global es favorable, con estrategias identificadas para gestionar las resistencias específicas.

4.2. Análisis de la Factibilidad

La factibilidad de SIGMEL evalúa si las instituciones peruanas poseen las capacidades organizacionales, técnicas, humanas e institucionales necesarias para implementar exitosamente el sistema propuesto.

4.2.1. Factibilidad Técnica

Infraestructura Existente Aprovechable:

- **Programa Constelación:** Plataforma tecnológica instalada con capacidad de procesamiento de datos masivos, sistemas de seguridad implementados, y enlaces establecidos con las operadoras de telecomunicaciones.
- **Sistemas Operadores:** Infraestructura de telecomunicaciones con capacidad de generación y almacenamiento de metadatos de localización.

Desarrollos Requeridos:

- Interfaces estandarizadas entre sistemas existentes.
- Ampliación de capacidad de almacenamiento (estimada en 40% adicional).
- Mecanismos robustos de eliminación automática de datos.
- Imposibilidad técnica de recuperación posterior a la eliminación.

Evaluación: La factibilidad técnica es **ALTA**, aprovechando 70% de infraestructura existente.

4.2.2. Factibilidad de Recursos Humanos

Personal Especializado Requerido:

- 48 analistas certificados en metadatos de localización.
- 6 supervisores técnicos.
- 4 auditores internos especializados.

- 2 administradores de sistemas de alta seguridad.

Programa de Capacitación:

- Formación inicial: 120 horas académicas.
- Actualización continua: 40 horas anuales.
- Recertificación obligatoria cada tres años.

Evaluación: La factibilidad de recursos humanos es **MEDIA**, sobre todo teniendo en consideración que será provisto por la PNP, requiriendo programa estructurado de formación.

4.2.3. Factibilidad Operativa

Integración con Procesos Existentes:

Los procedimientos de SIGMEL se integran naturalmente con los procesos establecidos en los artículos 230 y 231 del Código Procesal Penal, aprovechando la experiencia operativa del Programa Constelación en el manejo de información sensible bajo estrictos controles judiciales.

Protocolos Operativos:

- Procedimientos de autorización judicial estandarizados.
- Cadena de custodia digital de acuerdo a los procedimientos ya establecidos en el Programa Constelación respecto registros de comunicaciones intervenidas legalmente.
- Sistemas de eliminación automática.

Evaluación: La factibilidad operativa es **ALTA**, construido sobre procesos probados y legalmente aceptados.

4.2.4. Factibilidad Institucional

Capacidad de Absorción Institucional:

Las instituciones comprometidas demuestran capacidad comprobada para absorber SIGMEL, sustentada en evidencia operativa concreta:

- Experiencia probada: El Programa Constelación opera exitosamente desde su implementación (2009), manejando información sensible bajo estrictos controles judiciales.

- Marco procedimental consolidado: Los artículos 230 y 231 del Código Procesal Penal proporcionan base legal operativa probada.
- Personal especializado: Recursos humanos con experiencia en manejo de sistemas de alta seguridad disponibles para capacitación y expansión.

Coordinación Interinstitucional Validada:

El diseño de SIGMEL aprovecha mecanismos de coordinación ya existentes y funcionando entre PNP, Ministerio Público y Poder Judicial. Las entrevistas realizadas confirman que los procedimientos están integrados en su mayoría, y los pocos que no, se integran naturalmente con los flujos de trabajo actuales, minimizando resistencia operativa y maximizando aprovechamiento de sinergias institucionales.

Evaluación: La factibilidad institucional es ALTA, construyendo sobre capacidades demostradas y estructuras operativas probadas.

4.2.5. Factibilidad Política y Social

Contexto Político Favorable:

El entorno político actual proporciona condiciones propicias para SIGMEL:

- Alineación estratégica: Coherencia con Política Nacional de Seguridad Ciudadana 2030.
- Prioridad demostrada: Asignación creciente de recursos públicos para seguridad ciudadana.
- Compromisos internacionales: Consonancia con acuerdos multilaterales contra crimen organizado.
- Consenso institucional: Respaldo identificado en actores clave del sistema de justicia penal.

Aceptación Social Contextualizada:

Las encuestas nacionales revelan un contexto social favorable para medidas que fortalezcan la investigación criminal:

- Priorización ciudadana: 61% de la población identifica seguridad como principal preocupación (IMA GO, 2023).
- Demanda de eficacia: 75% de limeños percibe incremento en la delincuencia respecto al año anterior (Lima Cómo Vamos, 2022) y demanda respuestas estatales efectivas.
- Disposición al equilibrio: Ciudadanía muestra apertura a medidas de seguridad con adecuadas salvaguardas.

Gestión de Resistencias:

Las resistencias identificadas (cautela judicial, preocupaciones de operadoras, inquietudes de privacidad) son gestionables mediante las estrategias diseñadas: estándares rigurosos de validación probatoria, incentivos económicos para operadoras, y transparencia en resultados.

Evaluación: La factibilidad política y social es ALTA, con contexto favorable y estrategias para gestionar resistencias específicas.

4.3. Análisis de la Viabilidad

La viabilidad de SIGMEL se centra exclusivamente en evaluar su sostenibilidad económica y la capacidad financiera del Estado peruano para costear su implementación y operación a largo plazo. Este análisis examina la estructura de costos, fuentes de financiamiento identificadas, cronograma de implementación y factores que determinan la sostenibilidad económica del sistema en el tiempo.

Viabilidad Presupuestaria Demostrada:

El análisis financiero confirma la factibilidad de implementar SIGMEL dentro de los recursos disponibles del Estado peruano:

- Inversión inicial: S/ 45,425,000 distribuidos en 3 años (S/ 15,141,667 promedio anual).
- Costo operativo: S/ 4,200,000 anuales (0.08% del presupuesto MININTER).
- Impacto presupuestario: Mínimo, sin comprometer otras prioridades institucionales.

Estimación de Costos por Componente:

Basándose en la experiencia australiana documentada por PricewaterhouseCoopers (2014), donde la implementación de sistemas similares requirió entre AU$188.8 millones y AU$319.1 millones, se estima para el contexto peruano:

Tabla 18: Estimación de Costos de Implementación SIGMEL

Componente	Costo Estimado (S/)	Justificación
Infraestructura Tecnológica	15,000,000	Adaptación de sistemas existentes, nuevas interfaces, ampliación de almacenamiento.

Componente	Costo Estimado (S/)	Justificación
Desarrollo de Software	8,500,000	Herramientas de análisis, interfaces de usuario, sistemas de seguridad.
Capacitación y Certificación	2,200,000	Programa integral para 24 especialistas durante 3 años.
Implementación Operadores	12,000,000	Compensación estimada para adaptación de sistemas de operadoras.
Auditoría y Supervisión	1,800,000	Sistemas de control, informes de transparencia.
Contingencias (15%)	5,925,000	Reserva para imprevistos técnicos y operativos
TOTAL IMPLEMENTACIÓN	**45,425,000**	**Inversión total estimada en 3 años**

Costos Operativos Anuales:

- Personal especializado: S/ 2,400,000.
- Mantenimiento tecnológico: S/ 1,200,000.
- Controles: S/ 600,000.
- Total anual: S/ 4,200,000

Fuentes de Financiamiento Identificadas:

La combinación de fuentes identificadas (55% presupuesto público, 26% cooperación internacional, 19% compensación operadoras) distribuye el riesgo financiero y aprovecha disponibilidad de recursos de diferentes orígenes, reduciendo la presión sobre el presupuesto nacional.

Tabla 19: Estructura de Financiamiento SIGMEL

Fuente	Monto (S/)	Porcentaje	Modalidad
Presupuesto Público	25,000,000	55%	PP030 + asignación MININTER + modernización PNP
Cooperación Internacional	12,000,000	26%	UNODC, BID, cooperación bilateral en seguridad.
Compensación Operadoras	8,425,000	19%	Incentivos tributarios equivalentes a inversión requerida.

Fuente	Monto (S/)	Porcentaje	Modalidad
TOTAL	**45,425,000**	**100%**	**Implementación escalonada 36 meses**

Cronograma de Implementación con Costos:

Año 1 (S/ 18,500,000):

- Desarrollo de marco legal y reglamentario.
- Adaptación de infraestructura del Programa Constelación.
- Capacitación inicial de personal.
- Inicio de implementación en operadoras.
- Pruebas piloto.

Año 2 (S/ 16,200,000):

- Imprevistos pendientes de implementación del sistema técnico.
- Capacitación avanzada y certificación.
- Pruebas piloto finales.

Año 3 (S/ 10,725,000):

- Consolidación operativa.
- Auditorías.
- Evaluación de impacto.
- Operación normal.

Sostenibilidad Financiera a Mediano Plazo:

El costo operativo anual puede integrarse en el presupuesto regular del MININTER a través del PP030, considerando que representa una fracción menor del gasto sectorial en seguridad. Sin embargo, la justificación económica integral requiere evaluación empírica de beneficios tras la implementación.

Análisis Costo-Beneficio:

La experiencia australiana documenta mejoras en la resolución de casos criminales tras implementar sistemas similares (iTnews, 2022), sin embargo, la cuantificación específica de beneficios para el contexto peruano requiere estudios posteriores a la implementación.

Beneficios Esperados (Cualitativos):

- Reducción proyectada en casos archivados por insuficiencia probatoria.
- Fortalecimiento del sustento probatorio en investigaciones de crimen organizado.
- Mayor eficiencia en el uso de recursos investigativos por precisión en la localización.
- Contribución a la reducción de la sensación de impunidad.

Limitaciones del Análisis:

- Ausencia de línea base: No existen estudios previos que cuantifiquen el costo de la ineficiencia investigativa actual en el Perú.
- Valor social no cuantificado: La valoración económica de la reducción de impunidad requiere metodologías específicas no disponibles.
- Efectos indirectos: Los beneficios de disuasión criminal son complejo de medir y atribuir.

Evaluación Económica Preliminar:

Con un costo operativo anual de S/ 4,200,000 (0.08% del presupuesto MININTER), SIGMEL representa una inversión de bajo riesgo financiero con potencial de alto impacto social, aunque la relación costo-beneficio específica requiere evaluación empírica posterior a la implementación.

Justificación de la Inversión:

La viabilidad económica se sustenta en:

- Magnitud del problema: 107.5% de incremento en delitos violentos (2021-2023) justifica inversión en nuevas capacidades
- Costo de oportunidad: El costo de mantener todo como esta (impunidad creciente) supera la inversión propuesta.
- Experiencia internacional: Países con sistemas similares reportan mejoras significativas en investigación criminal.
- Sostenibilidad: Costos operativos representan fracción mínima del presupuesto sectorial.

Síntesis de Viabilidad Económica

SIGMEL demuestra viabilidad económica sólida con recursos identificados y distribuidos estratégicamente entre fuentes públicas, cooperación internacional y compensación del sector privado. La inversión inicial de S/ 45,425,000 distribuida en 36 meses y el costo operativo anual de S/ 4,200,000 representan compromisos financieros asumibles dentro del presupuesto sectorial actual. La viabilidad económica se confirma para la fase de

implementación, mientras que la sostenibilidad integral a largo plazo se validará mediante evaluación empírica de beneficios tras la puesta en operación del sistema.

4.4. Consideraciones Ético-Legales y Mecanismos de Protección de Derechos

El marco ético-legal de SIGMEL se asienta sólidamente en la legislación peruana vigente, específicamente en los artículos 230 y 231 del Código Procesal Penal que regulan el levantamiento del secreto de las comunicaciones. Esta base normativa consolidada proporciona las salvaguardas constitucionales necesarias y probadas para el tratamiento de información sensible relacionada a las comunicaciones (metadatos y contenido) y por ende a los metadatos de localización.

4.4.1. Fundamento Constitucional Consolidado

Integración con Marco Jurídico Probado:

Los metadatos de localización constituyen, conforme a la interpretación jurídica peruana, componente integral de las comunicaciones protegidas por el secreto de las comunicaciones (Constitución Política del Perú, Artículo 2 inciso 10). Esta caracterización no es innovación de SIGMEL sino aplicación de principios ya establecidos y operativos en el sistema de justicia penal peruano.

Base Legal Operativa:

El Programa Constelación funciona exitosamente bajo este mismo marco legal desde su implementación (2009), demostrando la viabilidad práctica de sistemas de manejo de información sensible con controles judiciales estrictos. SIGMEL no introduce elementos jurídicos novedosos, sino que complementa el alcance de procedimientos ya probados y validados.

Precedente Constitucional:

La Constitución Política del Perú, en su artículo 2 inciso 10, establece el derecho al secreto de las comunicaciones, mientras que el mismo texto constitucional, en su artículo 44, asigna al Estado el deber de proteger a la población de amenazas contra su seguridad. SIGMEL opera en el equilibrio constitucional ya establecido entre estos derechos y deberes.

4.4.2. Salvaguardas Institucionales Consolidadas

Controles Judiciales Probados:

SIGMEL reproduce y fortalece los mecanismos de control ya existentes y funcionando:

- **Autorización judicial previa:** Requisito ineludible establecido en artículo 230 CPP.
- **Fundamentación sustantiva:** Obligación de acreditar vinculación específica con investigación de delito violento.
- **Proporcionalidad temporal:** Limitación estricta de períodos de acceso y retención.
- **Supervisión continua:** Control judicial permanente sobre uso apropiado de información.

Triple Sistema de Control:

El diseño incorpora el sistema de controles múltiples ya validado en el Programa Constelación:

- **Control técnico:** Acceso restringido por certificación y rol específico.
- **Control fiscal:** Supervisión del Ministerio Público sobre uso investigativo.
- **Control judicial:** Autorización y supervisión permanente del Poder Judicial.

Trazabilidad y Auditoría:

Todos los accesos y usos del sistema quedan registrados en bitácoras auditables, replicando estándares ya aplicados exitosamente en sistemas sensibles existentes.

4.4.3. Protección de Datos Personales

Marco de Protección Establecido:

SIGMEL opera dentro del marco de protección de datos personales ya establecido en la legislación peruana, sin introducir excepciones ni modificaciones a los principios vigentes:

- **Principio de finalidad:** Uso exclusivo para investigación criminal autorizada.
- **Principio de proporcionalidad:** Acceso limitado a información estrictamente necesaria.
- **Principio de temporalidad:** Retención mínima necesaria con eliminación automática.
- **Principio de seguridad:** Medidas técnicas y organizativas robustas.

Eliminación Automática:

Los protocolos de eliminación automática de datos garantizan que la información no permanezca en el sistema más allá de los plazos estrictamente necesarios, cumpliendo con principios de minimización de datos.

4.4.4. Equilibrio Constitucional Seguridad-Privacidad

Proporcionalidad Aplicada:

SIGMEL mantiene el equilibrio constitucional ya establecido entre la necesidad estatal de investigar delitos que afectan derechos fundamentales de las víctimas (vida, integridad) y la protección de la privacidad de los ciudadanos. Este equilibrio se materializa mediante:

- **Limitación material:** Aplicación exclusiva a delitos violentos específicamente tipificados.
- **Limitación temporal:** Períodos de retención ajustados al mínimo necesario.
- **Limitación personal:** Acceso restringido a personal certificado y autorizado.
- **Limitación procesal:** Requerimiento de autorización judicial motivada.

Jurisprudencia Aplicable:

El marco constitucional peruano, específicamente el artículo 2 inciso 10 (derecho al secreto de las comunicaciones) en relación con el artículo 44 (deber estatal de proteger a la población), establece el equilibrio que SIGMEL respeta. Los artículos 230 y 231 del Código Procesal Penal materializan constitucionalmente este equilibrio mediante el requerimiento de autorización judicial para el levantamiento del secreto de las comunicaciones en investigaciones de delitos graves.

4.4.5. Transparencia y Rendición de Cuentas

Supervisión Institucional Múltiple:

El sistema de supervisión diseñado para SIGMEL replica y fortalece mecanismos ya existentes:

- **Inspectoría General PNP:** Auditorías regulares del cumplimiento de protocolos.
- **Control Interno Ministerio Público:** Supervisión del uso fiscal de herramientas investigativas.
- **Juzgados pertinentes:** control judicial de sus mandatos judiciales.

Transparencia Pública Compatible:

Los informes de transparencia proporcionan información estadística agregada que permite evaluación pública del sistema sin comprometer investigaciones específicas ni revelar información protegida.

Control Democrático:

La supervisión parlamentaria del presupuesto y políticas del MININTER proporciona control democrático sobre SIGMEL, complementando los controles judiciales directos y la supervisión de organismos pertinentes.

4.4.6. Fortalecimiento Normativo

El **Anexo 12: Proyecto de Ley** consolida las salvaguardas mediante disposiciones específicas que refuerzan el marco de protección en el **"Título IV: De las Garantías y Derechos de los Usuarios"** y en el **"Título V: De la Supervisión y Auditoria"**.

4.5. Síntesis de Viabilidad Integral

La evaluación comprehensiva de SIGMEL en sus tres dimensiones fundamentales arroja los siguientes resultados:

4.5.1. Resultados por Dimensión

Deseabilidad: ALTA

- Respaldo mayoritario de actores operativos del sistema de justicia penal (PNP y MP).
- El Poder Judicial requiere estándares rigurosos (ya considerados en el diseño final).
- Estrategias específicas identificadas para gestionar resistencias de las operadoras de telecomunicaciones.
- Contexto social favorable con demanda ciudadana de eficacia investigativa.

Factibilidad: MEDIA-ALTA

- Aprovechamiento del 70% de infraestructura tecnológica existente (Programa Constelación -- Intervención Legal de las Comunicaciones).
- Marco operativo consolidado en legislación vigente (inciso 10 del artículo 2 de la Constitución Política del Perú y los artículos 230-231 Código Procesal Penal).
- Recursos humanos especializados disponibles para capacitación y expansión.

- Capacidades institucionales demostradas sin comprometer otras prioridades.

Viabilidad: MEDIA-ALTA

- Factibilidad presupuestaria confirmada con fuentes de financiamiento diversificadas.
- Costo operativo anual representa fracción mínima (0.08%) del presupuesto MININTER.
- Sostenibilidad económica integral sujeta a validación empírica posterior.

4.5.2. Factores Críticos de Éxito

- Implementación Progresiva: El cronograma de 36 meses permite ajustes incrementales, minimiza riesgos operativos y facilita la absorción institucional gradual del sistema.
- Aprovechamiento de Capacidades Existentes: La construcción sobre la experiencia exitosa del Programa Constelación reduce la curva de aprendizaje y maximiza probabilidad de éxito operativo.
- Marco Legal Consolidado: La sustentación en legislación probada y controles existentes minimiza riesgos jurídicos y acelera implementación normativa.
- Financiamiento Diversificado: La combinación de fuentes públicas, cooperación internacional y compensación privada reduce dependencias y asegura factibilidad de implementación.
- Evaluación Continua: El diseño incorpora mecanismos de medición empírica de beneficios para validar sostenibilidad económica y ajustar operaciones según resultados.

4.5.3. Limitaciones y Condicionantes

Limitaciones Identificadas:

- Cuantificación de beneficios: La valoración económica específica de beneficios requiere estudios empíricos post-implementación.
- Dependencia de coordinación: El éxito operativo depende de coordinación interinstitucional efectiva.
- Evolución tecnológica: Necesidad de adaptación continua a cambios tecnológicos del entorno criminal.

Condicionantes de Éxito:

- Mantenimiento del compromiso político a través de cambios de gestión de gobierno o lideres de los poderes o instituciones comprometidas.

- Sostenimiento de recursos presupuestarios durante fase de implementación y post implementación.
- Preservación de estándares y supervisión.

4.5.4. Conclusión de Viabilidad

SIGMEL es viable para su implementación en el contexto institucional, económico y legal peruano. Su viabilidad se sustenta en:

- **Base institucional sólida:** Construye sobre capacidades probadas y estructuras operativas existentes.
- **Factibilidad económica:** Costos identificados y recursos disponibles para implementación.
- **Marco legal consolidado:** Sustentación en legislación vigente con salvaguardas constitucionales probadas.
- **Contexto favorable:** Demanda social y prioridad política para medidas de fortalecimiento investigativo.

La viabilidad integral se confirma para la fase de implementación, mientras que la sostenibilidad económica a largo plazo se validará mediante evaluación empírica de beneficios tras la puesta en operación del sistema.

CONCLUSIONES

Entre el 2021 y el 2023, Lima Metropolitana experimentó un incremento del 107.5% en delitos violentos perpetrados por bandas y organizaciones criminales. Esta escalada no representa únicamente un desafío estadístico; constituye una crisis de seguridad pública que demandó nuestro análisis integral para comprender sus causas estructurales y diseñar una solución innovadora fundamentada.

Hallazgos sobre el Problema y sus Causas

La magnitud del problema quedó documentada con claridad: los homicidios escalaron de 521 a 845 casos, las extorsiones se dispararon de 928 a 7,978 casos, y los robos prácticamente se duplicaron alcanzando 111,486 incidentes en 2023. Más preocupante resulta que el 82.2% de limeños se sienta inseguro en espacios públicos, evidenciando un deterioro sistemático del tejido social urbano.

Nuestro análisis causal identificó cinco factores interrelacionados, pero la jerarquización cuantitativa reveló como causa prioritaria las insuficientes herramientas tecnológicas y acceso limitado a datos digitales de la PNP. Esta causa obtuvo 8 de 8 puntos posibles considerando impacto, factibilidad de modificación y competencia institucional.

Las entrevistas con personal especializado confirmaron que la ausencia de un marco normativo para retención de metadatos de localización constituye una limitación crítica. Si bien se puede tener la capacidad de análisis, pero no sirve de mucho porque los datos se pierden antes de poder acceder a ellos. Esta realidad compromete la construcción de casos sólidos contra bandas y organizaciones criminales sofisticadas.

El Sistema SIGMEL: Respuesta Integral al Desafío

En respuesta a estas limitaciones desarrollamos el Sistema Integrado de Gestión de Metadatos de Localización (SIGMEL), un marco normativo-operativo que establece fundamento legal para retención obligatoria de metadatos de localización por las operadoras de telecomunicaciones – Programa Constelación, procedimientos estandarizados de acceso judicial, y protocolos interinstitucionales aprovechando la infraestructura del ya mencionado “Programa Constelación”.

El proceso de co-creación con 11 usuarios institucionales superó nuestras expectativas iniciales. Las pruebas con casos simulados arrojaron resultados prometedores que superaron consistentemente nuestros objetivos en las métricas evaluadas, como se detalla en la sección 3.3.2. Los resultados cualitativos fueron igualmente alentadores, con evaluaciones favorables por parte de fiscales e investigadores respecto a la calidad de la evidencia que se generaría y recomendaciones mayoritarias para la implementación del sistema.

SIGMEL se concreta en un proyecto de ley integral (desarrollado en Anexo 12) estructurado en cinco títulos que van desde disposiciones generales hasta supervisión y control. Los períodos de retención de 3 meses para operadoras y 6 meses para el Programa Constelación equilibran necesidades investigativas con la protección de los derechos de los ciudadanos. El sistema incluye triple control técnico-fiscal-judicial, eliminación automática de datos, y supervisión multiinstitucional.

Marco Ético-Legal y Salvaguardas Constitucionales

Una dimensión crítica fue desarrollar un sistema que respete derechos fundamentales. SIGMEL se sustenta en los artículos 230 y 231 del Código Procesal Penal, marco probado para la gestión de información sensible (datos y contenido) de las comunicaciones legalmente intervenidas. No introduce excepciones constitucionales; aplica principios ya establecidos de autorización judicial previa, fundamentación sustantiva, proporcionalidad temporal y supervisión continua.

Las salvaguardas incluyen protocolos específicos de protección de datos personales, notificación a afectados conforme al artículo 231 CPP, reexamen judicial de medidas adoptadas, y transparencia mediante informes públicos que no comprometan investigaciones en curso.

Viabilidad de Implementación

Nuestro análisis confirma que SIGMEL es implementable en las tres dimensiones evaluadas:

- **Deseabilidad:** Alta entre actores operativos (PNP y MP), cautela judicial gestionable mediante estándares rigurosos, resistencia económica de las operadoras de telecomunicaciones abordable con incentivos específicos.

- **Factibilidad:** Técnicamente alta aprovechando 70% de infraestructura existente del Programa Constelación. Si bien se cuenta con recursos humanos, se requiere un programa estructurado de capacitación para 48 analistas certificados y personal especializado. Operativamente factible construida sobre los procesos probados del artículo 230-231 CPP.
- **Viabilidad económica:** Inversión de S/ 45,425,000 en 36 meses con costos operativos anuales de S/ 4,200,000 (0.08% presupuesto MININTER). Financiamiento diversificado: 55% presupuesto público, 26% cooperación internacional, 19% compensación operadoras.

Contribuciones y Limitaciones del Estudio

Este trabajo contribuye demostrando la viabilidad de desarrollar soluciones tecnológicas avanzadas dentro del marco constitucional peruano sin comprometer derechos fundamentales. Valida metodologías de co-creación para políticas complejas multiinstitucionales y establece precedente para equilibrar innovación con protección de derechos y privacidad.

Sin embargo, reconocemos limitaciones importantes. La evaluación económica adolece de ausencia de líneas base para cuantificar costos actuales de ineficiencia investigativa. La sostenibilidad política depende de factores que trascienden el diseño técnico. También, la evolución de tecnologías utilizadas con fines criminales exigirá una adaptación continua del sistema.

Proyección de Impacto

La implementación exitosa de SIGMEL puede reequilibrar la ecuación costo-beneficio que favorece a las bandas y organizaciones criminales, contribuir a restaurar la percepción de eficacia del Estado, y posicionar al Perú como referente regional en el uso de la evidencia digital para persecución del crimen organizado.

Los metadatos de localización pueden revelar patrones de movimiento, identificar puntos de encuentro y establecer conexiones entre actores criminales - información vital para desarticular redes complejas y resolver los delitos violentos en el menor tiempo, comparado con los métodos actuales que pueden tomar meses.

Sintetizando, SIGMEL representa nuestra contribución al fortalecimiento de capacidades del Estado para enfrentar la criminalidad organizada violenta. Su éxito dependerá de su implementación cuidadosa, mantenimiento del compromiso político, y la adaptación continua a un entorno criminal en constante cambio. Creemos haber proporcionado herramientas conceptuales y operativas que pueden marcar diferencia significativa en la recuperación de la seguridad pública no solo en Lima Metropolitana, sino en todo el país.

BIBLIOGRAFÍA

Academia de la Magistratura. (2022). Plan de Capacitación de la Academia de la Magistratura 2022. Site https://www.amag.edu.pe/public_html/Storage/tbl_planes_academicos/fld_1105_Archivo_file/13-q3Ov9Zj7Ph9Ca9J.pdf

Akers, R. L., & Jennings, W. G. (2021). Social Learning Theory: Its Past, Present, and Future. New York, NY: Routledge. Site https://faculty.washington.edu/matsueda/courses/401D/Readings/Akers.pdf

Akers, R. L., & Sellers, C. S. (2012). Criminological Theories: Introduction, Evaluation, and Application (6ª ed.). New York, NY: Oxford University Press. Site https://archive.org/details/criminologicalth0000aker_6thed

Albrecht, H. J., Brunst, P., & Kilchling, M. (2020). Die Vorratsdatenspeicherung und ihre Auswirkungen auf die Strafverfolgung. Max-Planck-Institut für ausländisches und internationales Strafrecht.

Andresen, M. A., & Farrell, G. (2022). The Criminal Act: The Role and Influence of Routine Activity Theory. New York, NY: Routledge. Site https://www.perlego.com/es/book/3489315/the-criminal-act-the-role-and-influence-of-routine-activity-theory-pdf

Androulidakis, I. I. (2016). Mobile Phone Security and Forensics: A Practical Approach. Springer.

Australian Federal Police. (2020). Annual Report 2019-20. Site https://www.afp.gov.au/sites/default/files/PDF/Reports/02112020-afp-annual-report-2019-20.pdf

Banco Interamericano de Desarrollo (BID) y Organización de los Estados Americanos (OEA). (2020). Reporte de Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. Site https://es.slideshare.net/slideshow/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-amrica-latina-y-elcaribe/237394241

Bartolomé, R., & Pérez, J. M. (2020). Desafíos de la investigación policial en la era digital: Nuevas tecnologías y métodos aplicados a la lucha contra el crimen organizado. Revista Española de Investigación Criminológica. Site https://reic.criminologia.net/index.php/journal/article/download/721/331/3915

Becker, H. S. (1963). Outsiders: Studies in the Sociology of Deviance. New York, NY: The Free Press. Site

https://books.google.com.pe/books/about/Outsiders_Studies_in_the_Sociology_of_De.html?id=S2FHAAAAMAAJ&redir_esc=y

Bundeskriminalamt. (2019). Cybercrime Bundeslagebild 2018. Site https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.html

Bundesverfassungsgericht. (2017). Beschluss vom 21. Juni 2017 - 1 BvR 1619/17.

Coordinación Nacional de las Fiscalías contra la Criminalidad Organizada. (2022). Revista de la Fiscalía Especializada contra la Criminalidad Organizada, (1). Site https://cdn.www.gob.pe/uploads/document/file/3652808/Revista%20de%20la%20Fiscal%C3%ADa%20Especializada%20contra%20la%20Criminalidad%20Organizada%20-%20N%C2%BA%201.pdf

Dearden, T., & Mazerolle, P. (2021). Differential Association and Cybercrime: Insights and Implications. Routledge.

Decreto Legislativo N°052 - Ley Orgánica del Ministerio Público. Site https://www.mpfn.gob.pe/escuela/contenido/publicaciones/26_ley_organica_mp.pdf

Decreto Legislativo N°1267 - Ley de la Policía Nacional del Perú. Site https://www.policia.gob.pe/dirseciu/documentos/DL.%20N%C2%BA%201267%20-%20Ley%20de%20la%20PNP.pdf

Decreto Legislativo N°957 - Código Procesal Penal. Site https://lpderecho.pe/nuevo-codigo-procesal-penal-peruano-actualizado

Department of Home Affairs. (2020). Telecommunications (Interception and Access) Act 1979 – Annual Report 2018-19. Australian Government. Site https://www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-18-19.pdf

Espinoza Ramos, B. (2018). Litigación Penal: Manual de Aplicación. Librerías Grijley. Publicado en Issuu.

Federal Bureau of Investigation. (2019). Violent crime. FBI.gov. Site https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/topic-pages/violent-crime

Federal Bureau of Investigation. (2020). Going Dark.

Felson, M., & Eckert, M. (2021). Crime and Everyday Life (6ª ed.). Thousand Oaks, CA: SAGE Publications.

Ferguson, A. G. (2017). The rise of big data policing: Surveillance, race, and the future of law enforcement. New York University Press.

García Marcos, J. (2021). Geolocalización y derechos fundamentales. Site https://elderecho.com/geolocalizacion-y-derechos-fundamentales

García, L. (2014). La Suprema Corte y la geolocalización de teléfonos celulares. En NEXOS / EL JUEGO DE LA SUPREMA CORTE / CRÍTICA, DÍA A DÍA. Site https://eljuegodelacorte.nexos.com.mx/la-suprema-corte-y-la-geolocalizacion-de-telefonos-celulares

González, P. (2021). Metadatos de localización y protección de datos personales. Revista Española de Protección de Datos, 3(1).

Guías Prácticas. (2024). Localización de móviles. Site https://www.guiaspracticas.com/telefonia-movil/localizacion-de-moviles

IMA GO. (2023). Informe Perú: Seguridad Ciudadana. https://www.ima.pe/wp-content/uploads/2023/09/Informe-PERU-Seguridad-Ciudadana-IMA-GO Set23.pdf

Instituto de Defensa Legal (IDL). (2022). Informe sobre la Seguridad Ciudadana en el Perú 2022.

Instituto Nacional de Estadística e Informática (INEI). (2022). Perú: Percepción Ciudadana sobre Gobernabilidad, Democracia y Confianza en las Instituciones. Site https://www.gob.pe/institucion/inei/informes-publicaciones/3960178-peru-percepcion-ciudadana-sobre-gobernabilidad-democracia-y-confianza-en-las-instituciones-julio-diciembre-2022

Instituto Nacional de Estadística e Informática (INEI). (2023a). Estadísticas de seguridad ciudadana - Julio Diciembre 2023. https://www.inei.gob.pe/media/MenuRecursivo/boletines/estadisticas-seguridad-ciudadana-jul-dic-2023.pdf

Instituto Nacional de Estadística e Informática (INEI). (2023b). Encuesta Nacional de Programas Presupuestales 2022. Site http://proyecto.inei.gob.pe/enapres/wp-content/uploads/2023/05/1.-INFORME-MEF-Indicadores-de-Programas Presupuestales-2022.pdf

International Crisis Group. (2023). América Latina lucha contra una nueva ola de criminalidad. Crisis Group. Site https://www.crisisgroup.org/es/latin-america-caribbean/latin-america-wrestles-new-crime-wave

International Organization for Standardization. (2014). ISO 19115-1:2014 Geographic information — Metadata — Part 1: Fundamentals. https://www.iso.org/standard/53798.html

iTnews. (2022). Metadata collection "loophole" costs telcos millions. Retrieved from https://www.itnews.com.au/news/metadata-collection-loophole-costs-telcos-millions-577295iTnews.

Jaitman, L. & Machin, S. (2015). Crime and violence in Latin America and the Caribbean: Towards evidence-based policies. CentrePiece. https://cep.lse.ac.uk/pubs/download/cp461.pdf

Koops, B. J. (2021). The concept of function creep. Law, Innovation and Technology. Site https://www.tandfonline.com/doi/full/10.1080/17579961.2021.1898299

Lemert, E. M. (1951). Social Pathology: A Systematic Approach to the Theory of Sociopathic Behavior. New York, NY: McGraw-Hill. Site https://books.google.com.pe/books/about/Social_Pathology.html?id=zhcZAAAAIAAJ

Ley Nº 30077 - Ley contra el Crimen Organizado. (20 de agosto de 2013). Diario Oficial El Peruano. https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/218476-30077-2013

Lilly, J. R., Cullen, F. T., & Ball, R. A. (2010). Criminological Theory: Context and Consequences (5ª ed.). Thousand Oaks, CA: SAGE Publications. Site https://books.google.nl/books/about/Criminological_Theory.html?id=dTuJsIY8oxUC&redir_esc=y

Lima Cómo Vamos. (2022). Encuesta Lima Cómo Vamos 2022. Site https://www.limacomovamos.org/reportespercepcion

Maguire, M. (2012). Criminal investigation and crime control. In T. Newburn (Ed.), Handbook of policing (2nd ed.). Routledge.

March Cerdà, J. C. (2023). Predicción, prevención y tratamiento de la conducta delictiva. UOC. Enlace https://openaccess.uoc.edu/bitstream/10609/75525/3/Predicci%C3%B3n%2C%20prevenci%C3%B3n%20y%20tratamiento%20conducta%20delictiva_portada.pdf

Martínez-Gómez, A. (2019). The role of location metadata in modern criminal investigations. Digital Investigation. Site https://www.degruyter.com/document/doi/10.1515/9783110797909-011/pdf?licenseType=open-access

Meško, G., & Tankebe, J. (2023). Trust and Legitimacy in Criminal Justice: European Perspectives. Springer.

Ministerio de Justicia y Derechos Humanos. (2023). Informe de Seguimiento de la Política Criminal del Estado. Observatorio Nacional de Política Criminal - INDAGA. Site https://cdn.www.gob.pe/uploads/document/file/5675864/5038072-seguimiento-2023.pdf

Ministerio del Interior (MININTER). (2019). Política Nacional Multisectorial de lucha contra el Crimen Organizado 2019-2030. Site

https://sherloc.unodc.org/cld/uploads/res//treaties/strategies/peru/per0003s_html/PLC_MININTER.pdf

Ministerio del Interior (MININTER). (2019b). Plan Estratégico de Capacidades de la Policía Nacional del Perú al 2030. Site https://www.policia.gob.pe/pnp/archivos/portal/doc/481doc_INTERIOR%20PLAN%20ESTRATEGICO%20PNP%202030__.pdf

Ministerio del Interior (MININTER). (2022). Compendio estadístico del Sector Interior año fiscal 2022. Site https://www.mininter.gob.pe/sites/default/files/Compendio_estadistico_del_Sector_Interio_A%C3%B1o_Fiscal_2022.pdf

Ministerio Público. (2023). Boletín Estadístico del Ministerio Público diciembre 2023. Site https://cfe.mpfn.gob.pe/gis_mp/web/index.php/downloader/boletin_content/65b2d17e7eb95

Monroy Ojeda, C., Rangel Romero, X. G., & Hernández Mier, C. (2024). Crimen organizado. Dijuris.

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (2022). Análisis de la situación de las drogas y el delito en Lima Metropolitana. Site https://www.unodc.org/unodc/en/data-and-analysis/world-drug-report-2022.html

Parliament of Australia. (2015). Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015. Federal Register of Legislation. Site https://www.legislation.gov.au/Details/C2015A00039

Poder Judicial del Perú. (2023b). Boletín Estadístico Institucional N°04-2023. Gerencia de Planificación de la Gerencia General. Subgerencia de Estadística.

Poder Judicial. (2023). Estadística de la Criminalidad 2019-2023. Site https://drive.google.com/file/d/1dtGq-s2QZmK7aKr4ET81y4yh2PnIhyQF/preview

Poole, I. (2006). Cellular Communications Explained: From Basics to 3G. Newnes. Site https://archive.org/details/cellularcommunic0000pool_i6p5

PricewaterhouseCoopers. (2014). Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015. Retrieved from https://en.wikipedia.org/wiki/Telecommunications_%28Interception_and_Access%29_Amendment_%28Data_Retention%29_Act_2015Wikipedia+1iTnews+1

Programa de las Naciones Unidas para el Desarrollo (PNUD). (2013). Seguridad Ciudadana con rostro humano: diagnóstico y propuestas para América Latina. Informe Regional de Desarrollo Humano 2013-2014. Site https://www.undp.org/es/latin-america/publicaciones/informe-regional-de-desarrollo-humano-2013-2014

Programa de las Naciones Unidas para el Desarrollo. (2023). Informe Regional de Desarrollo Humano 2023-2024. Site https://www.undp.org/es/colombia/publicaciones/informe-desarrollo-humano-2023-2024-instantanea

Ramírez, C. (2023). Geolocalización: Fundamentos y aplicaciones. Revista de Geomática, 5(1).

Resolución de la Fiscalía de la Nación N°760-2020-MP-FN - ROF del Ministerio Público.

Rosas Yataco, J. (2013). Tratado de derecho procesal penal. Lima: Instituto Pacífico. Site https://biblioteca.amag.edu.pe/cgi-bin/koha/opac-detail.pl?biblionumber=5689

Ruiz Sánchez, M. A. (2018). Derecho Procesal Penal Acusatorio y Oral (3.ª ed.). Dijuris.

Salinas, D. (2022). La investigación preparatoria en el proceso penal. Arequipa: Editorial Adrus.

Sampson, R. J., & Groves, W. B. (1989). Community Structure and Crime: Testing Social-Disorganization Theory. American Journal of Sociology. Site https://dash.harvard.edu/bitstream/handle/1/3226955/Sampson_CommunityStructureCrime.pdf;jsessionid=3F70661C00CC4B47DCA74EEA82E2C8B5?sequence=2

Sampson, R. J., & Raudenbush, S. W. (2021). Neighborhoods and Crime: The Dimensions of Effective Community Control. Chicago, IL: University of Chicago Press.

Schram, P. J., & Tibbetts, S. G. (2023). Introduction to Criminology: Why Do They Do It? (3ª ed.). Thousand Oaks, CA: SAGE Publications.

Sistema de Denuncias Policiales PNP (SIDPOL). (2023). Estadísticas de delitos en Lima Metropolitana 2021-2023.

Supreme Court of the United States. (1979). Smith v. Maryland, 442 U.S. 735. Legal Information Institute, Cornell Law School. Site https://www.law.cornell.edu/supremecourt/text/442/735

Texto Único Ordenado de la Ley Orgánica del Poder Judicial. Site https://www.gob.pe/institucion/minjus/informes-publicaciones/1466669-texto-unico-ordenado-de-la-ley-organica-del-poder-judicial-y-ley-organica-del-ministerio-publico-tercera-edicion-oficial

Tibbetts, S. G., & Hemmens, C. (2021). Criminological Theory: A Text/Reader (4ª ed.). Thousand Oaks, CA: SAGE Publications.

TimeBase. (2015). Why Metadata Legislation Will Inevitably Increase the Cost of the Internet. Retrieved from https://www.timebase.com.au/news/2015/AT188-article.htmltimebase.com.au+1Wikipedia+1

Trottier, D. (2019). Open source intelligence, social media, and law enforcement: Visions, constraints and critiques. European Journal of Cultural Studies.

UNODC. (2019). Global study on homicide 2019. Site https://www.unodc.org/documents/data-and-analysis/gsh/Booklet1.pdf

Verizon. (2020). 2019 Transparency Report. https://www.verizon.com/about/portal/transparency-report/us-report

Villegas Paiva, E. A. (2013). La detención y la prisión preventiva en el nuevo Código Procesal Penal. Lima: Gaceta Jurídica. Site https://www.mpfn.gob.pe/escuela/contenido/archivosbiblioteca/dpp0689.pdf

Walters, G. D. (2022). Crime and Criminality: A Social-Cognitive-Developmental Theory of Delinquent and Criminal Behavior. Springer.

Williams, F. P., & McShane, M. D. (2009). Criminological Theory (5ª ed.). Upper Saddle River, NJ: Prentice Hall.

World Justice Project. (2023) The Rule of Law in Peru: Key Findings from the General Population Poll 2022. Site https://worldjusticeproject.org/our-work/research-and-data/rule-of-law/peru-2022

World Wide Web Consortium. (2022). Geolocation API: W3C Recommendation, 1 September 2022. https://www.w3.org/TR/geolocation

ANEXOS

Anexo 1: Descripción de los tres problemas públicos identificados.

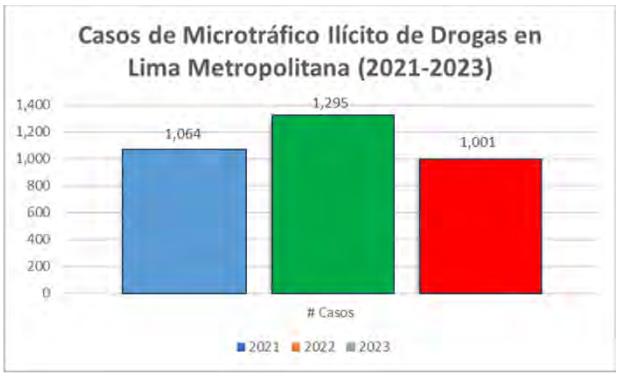
Se inicia de la revisión a fondo de la situación de la seguridad en Lima Metropolitana. Este trabajo inicial permitió comprender mucho mejor los verdaderos problemas que enfrenta esta zona de la capital, particularmente en lo referido a la prevención y el control de los delitos que implica violencia.

1. Identificar preliminarmente problemas públicos

Después de la pandemia (2021) se marcó un antes y un después en la seguridad de Lima. De acuerdo a la percepción de los vecinos y de las cifras oficiales, la conclusión es que nos golpea duro la criminalidad: en los últimos años, el crimen se multiplicó en nuestras calles. Los números son alarmantes, pero más preocupante aún es que los vecinos ya no salen tranquilos ni de día. Las soluciones tradicionales ya no sirven - necesitamos ideas nuevas que realmente funcionen en el Lima de hoy.

La micro comercialización de drogas se ha convertido en uno de los problemas más graves que se enfrenta, no solo por el delito en si, sino por viene acompañado de otros males, como el aumento significativo de la violencia y la delincuencia en distintos sectores de Lima. Los puntos de venta de drogas han convertido barrios en zonas de alto riesgo. Según el SIDPOL (SIDPOL 2023), los casos de micro comercialización fueron +1,064 en 2021, 1,295 en 2022 y 1,001 en 2023. Aunque hubo una disminución el 2023, el problema aún está allí.

Ilustración 2:



Fuente: SIDPOL PNP

Otro problema significativo es el incremento de delitos violentos cometidos por bandas y organizaciones criminales, como asesinatos, robos, secuestros, extorsiones y otros. Según las estadísticas del SIDPOL PNP (SIDPOL 2023), en Lima Metropolitana los homicidios pasaron de 521 en 2021 a 845 en 2023; robos de 56,526 en 2021 a 111,486 en 2023, mostrando un incremento alarmante.

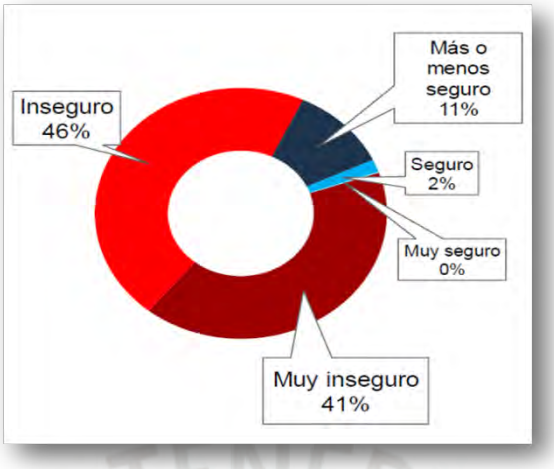
Ilustración 3

Fuente: SIDPOL PNP

Los datos del INEI revelan la magnitud del problema: durante julio-diciembre 2023, de cada 100 habitantes en Lima, 14 fueron víctimas de robo, mientras que 4.4 sufrieron maltrato u ofensas sexuales. Las amenazas e intimidaciones afectaron a 2.7 personas, y los casos de secuestro y extorsión alcanzaron el 0.3% de la población (INEI, 2023).

Este contexto ha moldeado la percepción ciudadana: un estudio de IMA GO (2023) muestra que el 87% de limeños vive con temor, donde el 41% se siente muy inseguro y 46% inseguro. Solo una mínima fracción, el 13%, experimenta algún grado de seguridad en su entorno diario.

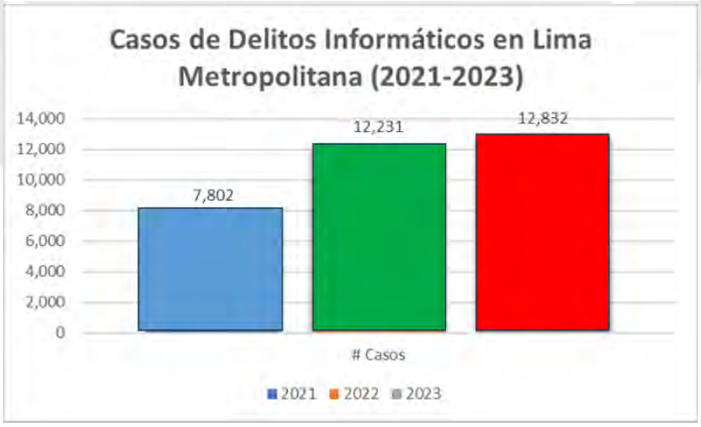
Ilustración 4: Percepción de seguridad en Lima Metropolitana



Fuente: "Perú: Seguridad Ciudadana" de IMA GO de setiembre 2023.

Además, se ha observado un aumento alarmante en los delitos informáticos, como estafas y fraudes por internet. Según las estadísticas del SIDPOL PNP, en Lima Metropolitana se reportaron 7,802 casos en 2021, 12,231 en 2022 y 12,832 en 2023 (SIDPOL, 2023). Estos datos evidencian la creciente amenaza de la ciberdelincuencia en Lima Metropolitana. Además, El INEI indica 6.6 víctimas de estafa por cada 100 habitantes entre julio y diciembre de 2023 (INEI, 2023a).

Ilustración 5



Fuente: SIDPOL PNP

La violencia familiar y de género también ha sido un problema recurrente. El INEI reporto 4.4 víctimas de maltrato y ofensa sexual por cada 100 habitantes en Lima entre julio y diciembre de 2023 (INEI, 2023a). Además, IMA GO indica que el 4.4% teme ser víctima de estos delitos (IMA GO!, 2023).

Finalmente, la alta frecuencia de robos y hurtos ha generado una sensación generalizada de inseguridad en la población. El INEI reporta en Lima, entre julio y diciembre 2023: 14 víctimas de robo y 8.1 víctimas de intento de robo por cada 100 habitantes. (INEI, 2023a).

En resumen, la seguridad pública en Lima Metropolitana se ha visto gravemente afectada por diversos problemas como los indicados. Por este motivo, es fundamental implementar políticas públicas efectivas para combatir estos problemas y mejorar la situación.

Ilustración 6: Principales Problemas de Seguridad Pública en Lima Metropolitana.

Fuente: Elaboración de los autores

En este proyecto de innovación preliminar, nos enfocaremos específicamente en los siguientes problemas públicos de interés y relevancia en Lima Metropolitana durante el periodo 2021-2023, los cuales afectan gravemente la seguridad ciudadana, la calidad de vida y el desarrollo sostenible de la ciudad:

- En Lima Metropolitana, el **microtráfico** está carcomiendo el tejido social de muchas zonas, sobre todo en aquellas donde la presencia de la policía es casi nula. No solo impacta en la salud de los vecinos y descompone a las familias; más preocupante es que estas redes de menudeo se han vuelto el caldo de cultivo para que operen organizaciones criminales, que las usan para lavar dinero y expandir sus operaciones.
- **Los delitos informáticos** son un dolor de cabeza adicional en las personas Cada día hay una estafa nueva, un fraude más ingenioso, una identidad robada y más. Las

familias y empresas victimas pierden millones o el poco dinero que tienen, y ya no se sabe en qué sitio web o app confiar.

- **Incremento sostenido de los delitos violentos perpetrados por bandas y organizaciones criminales en Lima Metropolitana,** quizás el desafío más visible en Lima Metropolitana. Las bandas criminales, a través de homicidios, robos y secuestros al paso, no solo dañan irreparablemente a sus víctimas directas sino que también socavan la inversión, la economía y la cohesión social, cuestionando la capacidad estatal de proteger derechos fundamentales.

Estos tres problemas públicos críticos, documentados tanto en estadísticas oficiales como en la experiencia ciudadana, demandan una respuesta coordinada entre autoridades, sociedad civil, sector privado y academia.

2. Identificar información sobre los problemas públicos preliminarmente seleccionados

En esta sección, se profundiza en cada problemática identificada, analizando su magnitud e impacto para fundamentar la selección del eje central del proyecto de innovación.

Tabla 20 - Problema 1: Alta incidencia de microtráfico de drogas ilícitas en Lima Metropolitana entre 2021 y 2023

Aspecto	Descripción
Tipo de problema	De afectación directa a la sociedad.
Magnitud preliminar	Las estadísticas de SIDPOL (2023) muestran una tendencia preocupante: mientras en 2021 se registraron 1,064 casos de micro comercialización de drogas en la capital, esta cifra escaló a 1,295 durante 2022, evidenciando un alza del 21.7% en apenas doce meses. Aunque en 2023 hubo una ligera disminución con 1,001 casos, el problema sigue siendo alto y preocupante. Estas cifras pueden ser solo una parte del problema debido a la naturaleza clandestina del delito. Según el INEI, el porcentaje de personas que consideran la venta de drogas como el principal problema de seguridad aumentó del 35.2% en 2021 al 38.5% en el 2023 (INEI, 2023a), reflejando la gravedad y visibilidad creciente de este fenómeno que afecta la salud pública, la seguridad y la convivencia social en los barrios más afectados.

Aspecto	Descripción
Tipo de problema	De afectación directa a la sociedad.
Afectados directos e indirectos	Población de Lima Metropolitana, especialmente jóvenes y habitantes de zonas vulnerables
Responsables estatales	Ministerio del Interior (políticas), Policía Nacional del Perú – Dirección Antidrogas y otras (prevención e investigación), Ministerio Público - Fiscalías Especializadas en Tráfico Ilícito de Drogas y otras (investigación y acusación), Poder Judicial (juzgamiento y sanción) y Comisión Nacional para el Desarrollo y Vida sin Drogas – DEVIDA (prevención).
Cadena de valor	Involucra prevención (campañas, educación, desarrollo alternativo), inteligencia (detección de redes), interdicción (incautaciones, capturas), judicialización (procesamiento de casos) y rehabilitación (tratamiento de consumidores).
Soluciones preliminares	Se han implementado estrategias como el Programa de Prevención y Rehabilitación del Consumo de Drogas - DEVIDA, operativos policiales focalizados, y programas de desarrollo alternativo en zonas de cultivo ilícito. Sin embargo, se requieren enfoques integrales y sostenibles.

Tabla 21 - Problema 2: Incremento de Delitos Informáticos ejecutados con medios tecnológicos en Lima Metropolitana entre 2021 y 2023.

Aspecto	Descripción
Tipo de problema	De afectación directa a la sociedad.
Magnitud preliminar	Según SIDPOL (SIDPOL, 2023), los delitos informáticos en Lima Metropolitana crecieron de 7,802 casos en 2021 a 12,231 en 2022, un aumento del 56.8%. En 2023, se registraron 12,832 casos, un 4.9% más. El informe del INEI señala que la tasa de víctimas de estafa fue de 6.6 por cada 100 habitantes entre julio y diciembre de 2023 (INEI, 2023a). Estas cifras muestran que los ciberdelincuentes se adaptan rápidamente a la digitalización y sus vulnerabilidades.
Afectados directos e indirectos	Población de Lima Metropolitana que usa tecnologías de información y comunicación.

Aspecto	Descripción
Tipo de problema	De afectación directa a la sociedad.
Responsables estatales	Ministerio del Interior (políticas), Policía Nacional del Perú - DIVINDAT (prevención e investigación), Ministerio Público – Fiscalías Especializadas en Ciberdelincuencia (investigación y acusación), Poder Judicial (juzgamiento y sanción), Ministerio de Justicia y Derechos Humanos (políticas y regulación), Secretaría de Gobierno Digital (prevención y seguimiento).
Cadena de valor	Involucra prevención (educación en seguridad digital), investigación y persecución del delito (rastreo de transacciones, análisis forense digital, cooperación internacional), atención a víctimas (orientación legal, restauración de sistemas) y fortalecimiento del marco normativo (leyes especializadas, protección de datos).
Soluciones preliminares	Se han realizado campañas de concientización sobre riesgos digitales, creado unidades policiales y fiscalías especializadas y promovidos estándares de ciberseguridad. Sin embargo, se necesita mayor articulación interinstitucional y desarrollo de capacidades.

Tabla 22 - Problema 3: Incremento de delitos violentos ejecutados por bandas y organizaciones criminales en Lima Metropolitana entre 2021 y 2023.

Aspecto	Descripción
Tipo de problema	De afectación directa a la sociedad.
Magnitud preliminar	Las cifras del SIDPOL muestran un panorama crítico: los homicidios escalaron dramáticamente de 521 casos en 2021 a 845 en 2023, marcando un aumento del 62.2% en este breve periodo. Los delitos contra el patrimonio muestran una tendencia aún más severa, con los robos ascendiendo desde 56,526 incidentes en 2021 hasta alcanzar 111,486 en 2023, prácticamente duplicándose en solo dos años. Estas cifras se ven respaldadas por los resultados del informe del INEI sobre seguridad ciudadana. Según este estudio en Lima Metropolitana, entre julio y diciembre de 2023, la tasa de víctimas de robo fue de 14 por cada 100 habitantes, y la de intento de robo

Aspecto	Descripción
Tipo de problema	De afectación directa a la sociedad.
	8.1 por cada 100. Las tasas de víctimas de amenazas y de secuestro/extorsión fueron de 2.7 y 0.3 por cada 100 habitantes, respectivamente. (INEI, 2023a). Estas estadísticas evidencian una inseguridad insostenible en Lima Metropolitana, con normalización de la violencia criminal. Las bandas desafían a las autoridades, y la percepción de las pandillas como principal problema de seguridad aumentó del 25.3% en 2021 al 31.8% en 2023 (INEI, 2023a). A pesar de operativos policiales, programas preventivos, reformas y mejoras en infraestructura, las estrategias actuales no han logrado contener la criminalidad violenta. La inseguridad persiste como principal preocupación y desafío prioritario. Es necesario un enfoque integral y estratégico basado en evidencia para la seguridad pública, abordando causas estructurales. Urge innovar en políticas, gestión y tecnología para soluciones efectivas y sostenibles.
Afectados directos e indirectos	Población de Lima Metropolitana en general. Los delitos violentos generan daños físicos, psicológicos y materiales a las víctimas directas, así como temor y desconfianza en la población.
Responsables estatales	Ministerio del Interior (políticas), Policía Nacional del Perú (prevención e investigación), Ministerio Público (investigación y acusación), Poder Judicial (juzgamiento y sanción), Ministerio de Justicia y Derechos Humanos (políticas y regulación), Gobiernos locales (prevención y seguimiento).
Cadena de valor	Acciones de prevención (vigilancia, patrullaje, programas sociales), control (investigación criminal, inteligencia, operativos), justicia penal (captura, judicialización, encarcelamiento) y resocialización (programas en penales, reinserción social y laboral de ex reclusos).
Soluciones preliminares	Aunque se han implementado varias estrategias de seguridad (Plan Nacional de Seguridad Ciudadana, mega operativos policiales, programa de recompensas, creación de fiscalías y juzgados especializados, comités de seguridad ciudadana), se

Aspecto	Descripción
Tipo de problema	De afectación directa a la sociedad.
	necesita un enfoque integral que aborde las causas estructurales de la criminalidad y refuerce el sistema de justicia penal.

3. Identificar y seleccionar el problema público

Entre los tres problemas preliminares y aplicando criterios de selección (datos del problema público, soluciones ya construidas, y relevancia por sus efectos), se ha seleccionado como problema a desarrollar el **"Incremento de delitos violentos cometidos por bandas y organizaciones criminales en Lima Metropolitana entre 2021 y 2023"**: Esta elección se basa en varias razones:

- Las estadísticas de SIDPOL PNP e INEI revelan una realidad innegable: el incremento sostenido de homicidios, robos, amenazas, secuestros y extorsiones dibuja un panorama crítico que exige atención inmediata. Esta evidencia cuantitativa fundamenta la magnitud del desafío que enfrentamos.
- El impacto en Lima Metropolitana trasciende las cifras: las elevadas tasas de victimización han deteriorado no solo la salud física y mental de los ciudadanos, sino también su patrimonio. La erosión de la confianza institucional y el debilitamiento del tejido social amenazan la estabilidad económica de la capital.
- Los esfuerzos actuales - mega operativos, programas de recompensas y comités de seguridad ciudadana - han resultado insuficientes para contener el avance de la violencia. Esta brecha entre acciones y resultados subraya la urgencia de explorar soluciones innovadoras respaldadas por evidencia empírica.
- La seguridad ciudadana ocupa un lugar central en la agenda pública, como lo confirma el estudio de IMA GO (2023): el 61% de la población la identifica como su principal preocupación. Este consenso social, junto al compromiso político existente, genera un momento propicio para implementar respuestas efectivas que restauren la confianza ciudadana.

En ese sentido, el problema del incremento de delitos violentos por bandas y organizaciones criminales en Lima Metropolitana cumple con los criterios para ser abordado en un proyecto de innovación, al contar con evidencia de su magnitud, generar impactos relevantes en la sociedad, presentar deficiencias en las soluciones actuales, y constituir una

prioridad en la agenda pública. Esto justifica y viabiliza políticamente el desarrollo de una propuesta innovadora para afrontar este problema de seguridad ciudadana.

Anexo 2: Matriz de consistencia del diseño de investigación sobre la arquitectura del problema público.

Dimensión	Preguntas	Objetivos	Hipótesis	Fuentes de datos	Herramientas
Magnitud del incremento de delitos violentos en Lima Metropolitana.	¿Cuál es la magnitud del incremento de crímenes violentos en Lima Metropolitana en el periodo 2021-2023?	Determinar la magnitud del incremento de crímenes violentos en Lima Metropolitana durante el periodo 2021-2023 en base a estadísticas oficiales.	Se estima que los crímenes violentos se han incrementado en más de un 50% en Lima Metropolitana entre 2021 y 2023.	Anuarios estadísticos de la Región Policial Lima, MP, PJ. Estadísticas del INEI. Reportes del Observatorio Metropolitano de Seguridad Ciudadana.	Revisión documental de datos y reportes estadísticos: PNP, MP – Fiscalías Especializadas, Juzgados Penales. Análisis criminal del Observatorio Metropolitano de Seguridad Ciudadana.
Modus operandi de las bandas y organizaciones criminales en Lima Metropolitana.	¿Cómo operan las bandas y organizaciones criminales responsables del incremento de crímenes violentos en Lima	Describir el modus operandi y ámbito de acción de las principales bandas y organizaciones criminales vinculadas al aumento	La mayoría opera en zonas urbano marginales de Lima Norte, Lima Sur y Lima Este. Usan armas de fuego de corto y largo alcance. Tienen vínculos con redes de micro	Reportes de la DIRINCRI, DIRIN y del Observatorio del Delito PNP. Informes de la Procuraduría Pública Especializada en	Revisión documental: DIRINCRI PNP, DIRINT PNP Observatorio DIRNIC PNP. Informes de la Procuraduría Pública

Dimensión	Preguntas	Objetivos	Hipótesis	Fuentes de datos	Herramientas
	Metropolitana? ¿En qué zonas de la ciudad se concentra su actividad delictiva?	de crímenes violentos en Lima Metropolitana durante el periodo de estudio.	comercialización de drogas en sus territorios.	Delitos de Crimen Organizado. Expedientes judiciales.	Especializada de CO. Entrevistas a expertos: PNP, MP y PJ. Análisis de redes criminales.
Impacto en la seguridad ciudadana y percepción de inseguridad de los ciudadanos en Lima Metropolitana.	¿Cómo ha impactado el incremento de crímenes violentos en la seguridad ciudadana objetiva y la percepción de inseguridad de los ciudadanos de Lima Metropolitana?	Determinar el impacto del problema en la seguridad ciudadana y en la percepción de inseguridad de los habitantes de Lima Metropolitana durante el periodo 2021-2023.	Los crímenes violentos han generado un deterioro significativo de la seguridad ciudadana y un incremento superior al 20% en la percepción de inseguridad en Lima Metropolitana.	Encuesta Nacional de Programas Presupuestal. Encuesta Lima Cómo Vamos.	Revisión de estadísticas de seguridad ciudadana del INEI y Lima Cómo Vamos. Estudios de percepción ciudadana.
Respuesta de las instituciones estatales frente al problema en Lima	¿Cuál ha sido la respuesta de las principales instituciones del sistema	Analizar las acciones emprendidas por la PNP, el Ministerio Público y el Poder	La respuesta de la PNP, fiscalías y juzgados penales ha sido predominantemente reactiva y desarticulada,	Evaluaciones del Plan de Operaciones de la Región Policial	Revisión documental. Análisis de desempeño de

Dimensión	Preguntas	Objetivos	Hipótesis	Fuentes de datos	Herramientas
Metropolitana.	de justicia penal frente al incremento de delitos violentos de bandas y organizaciones criminales en Lima Metropolitana durante el periodo 2021-2023?	Judicial para prevenir, investigar y sancionar este problema en Lima Metropolitana durante el periodo 2021-2023.	con operativos de impacto limitado que no han revertido la tendencia creciente de los crímenes violentos en Lima. Existen deficiencias en los procesos de investigación criminal, obtención de pruebas científicas y valoración de la prueba indiciaria.	Lima 2021-2023. Memorias anuales de la Junta de Fiscales Superiores de Lima. Boletines estadísticos de la Corte Superior de Justicia de Lima.	intervenciones. Entrevistas a expertos policiales, fiscales y jueces penales.

Anexo 3: Herramientas de recojo de información para la arquitectura del problema público

HERRAMIENTAS UTILIZADAS PARA EL DESARROLLO DE LA ARQUITECTURA DEL PROBLEMA PÚBLICO:

HERRAMIENTA 1: Revisión documental de estadísticas oficiales

- Utilizada para: Dimensión magnitud del problema.
- Fuentes consultadas: Anuarios estadísticos PNP (SIDPOL), reportes INEI, estadísticas del Ministerio Público y Poder Judicial.
- Metodología aplicada: Análisis longitudinal de series estadísticas 2021-2023.

HERRAMIENTA 2: Entrevistas a expertos institucionales

- Utilizada para: Dimensiones modus operandi y respuesta institucional.
- Sujetos entrevistados: Expertos de PNP, Ministerio Público y Poder Judicial.
- Instrumento: Guías de entrevistas semi-estructuradas (detalladas en Anexo 8).
- Modalidad: Presencial y virtual.

HERRAMIENTA 3: Análisis de informes institucionales especializados

- Utilizada para: Dimensión modus operandi.
- Documentos analizados: Informes DIRINCRI PNP, DIRINT PNP, Observatorio DIRNIC PNP, Procuraduría Especializada en Crimen Organizado.
- Enfoque: Análisis de contenido de reportes oficiales.

HERRAMIENTA 4: Revisión de estudios de percepción ciudadana

- Utilizada para: Dimensión impacto en seguridad ciudadana.
- Fuentes: Encuestas Lima Cómo Vamos, estudios IMA GO, ENAPRES-INEI.
- Metodología: Análisis comparativo de resultados de encuestas.

Anexo 4: Matriz de consistencia del diseño de investigación sobre las causas del problema público

Pregunta causal	Hipótesis	Fuentes de datos	Herramientas	Métodos de análisis
¿Cuáles son las principales causas del incremento significativo de delitos violentos cometidos por bandas y organizaciones criminales en Lima Metropolitana durante el periodo 2021-2023?	El incremento de delitos violentos cometidos por bandas y organizaciones criminales en Lima Metropolitana durante 2021-2023 se debe principalmente a cuatro factores interrelacionados: 1) Percepción de bajo riesgo y alto beneficio de bandas y organizaciones criminales violentas; 2) Insuficientes pruebas valoradas por el Poder Judicial para imponer condenas a integrantes de bandas y organizaciones criminales violentas; 3) Débil sustento probatorio tecnológico en las denuncias penales del Ministerio Público por delitos violentos cometidos por bandas y organizaciones criminales; 4) Insuficientes herramientas tecnológicas y acceso limitado a datos digitales relevantes para incriminar a bandas y organizaciones criminales violentas por parte de la PNP; 5) Marco legal generico y limitado de opciones tecnologicas para la persecución efectiva de bandas y organizaciones criminales violentas.	Entrevistas a expertos: Oficiales PNP, Fiscales, Jueces penales. Informes: DIRINCRI PNP y DIRIN PNP. Observatorio de Criminalidad - MP. Registro Nacional Judicial - PJ. Bases de datos: SIDPOL PNP, SGF- MP. RENAJU - PJ. Informes técnicos de proveedores de operadoras de telecomunicaciones. Encuestas de percepción de seguridad ciudadana. Revisión de literatura academica y estudios.	Análisis documental de estadísticas e informes oficiales. Entrevistas semiestructuradas a actores clave. Grupos focales con expertos en seguridad ciudadana y tecnología. Revisión sistemática de literatura científica. Consultas técnicas a especialistas en telecomunicaciones. Análisis de encuestas de victimización y percepción de inseguridad.	Método de rastreo de procesos (process tracing) para establecer los mecanismos causales que conectan los factores identificados con el incremento de delitos violentos. Este método se complementará con un análisis de contenido cualitativo de las entrevistas y documentos revisados.

Anexo 5: Herramientas de recojo de información para las causas del problema público

HERRAMIENTAS UTILIZADAS PARA LA IDENTIFICACIÓN DE CAUSAS DEL PROBLEMA PÚBLICO:

HERRAMIENTA 1: Entrevistas semi estructuradas a actores del sistema de justicia penal

- Propósito: Identificar causas específicas desde la perspectiva operativa.
- Participantes: 6 investigadores PNP especializados en crimen organizado, 2 fiscales especializados en criminalidad organizada, 2 personal del Programa Constelación, 1 asesor especialista.
- Instrumento: Guías diferenciadas por institución (Anexo 08).
- Modalidad: Entrevistas presenciales de 45 minutos promedio.
- Enfoque: Identificación de limitaciones tecnológicas y normativas específicas.

HERRAMIENTA 2: Revisión documental especializada

- Fuentes primarias: Plan Estratégico MS30 de la PNP, Plan Estratégico Institucional MP 2021-2025, Plan Estratégico Institucional PJ 2021-2025, Informes de Ejecución Presupuestal MININTER 2022.
- Metodología: Análisis de contenido focalizado en capacidades tecnológicas y marcos normativos.

HERRAMIENTA 3: Análisis comparativo de experiencias internacionales

- Casos estudiados: Sistemas de retención de metadatos en Alemania, Australia y Estados Unidos.
- Fuentes: Reportes oficiales de organismos del Estado y estudios académicos especializados.
- Enfoque: Identificación de factores críticos de éxito y lecciones aprendidas.

HERRAMIENTA 4: Triangulación metodológica

- Proceso: Contrastación sistemática entre evidencia documental, testimonial y experiencias internacionales para validar la identificación causal.
- Criterios de validación: Convergencia de fuentes, consistencia temporal y coherencia explicativa.

Anexo 6: Herramientas de recojo de información para las causas del problema público

HERRAMIENTA 1: Entrevistas semi-estructuradas a actores del sistema de justicia penal

Propósito: Identificar causas específicas desde la perspectiva operativa. Participantes:

- 6 investigadores PNP especializados en crimen organizado
- 2 fiscales especializados en criminalidad organizada
- 2 expertos del Programa Constelación
- 1 especialista en protección de datos

Instrumento: Guías diferenciadas por institución (Anexo 08).

Modalidad: Entrevistas presenciales de 45 minutos promedio.

Enfoque: Identificación de limitaciones tecnológicas y normativas específicas.

HERRAMIENTA 2: Revisión documental especializada

Fuentes primarias:

- Plan Estratégico MS30 de la PNP.
- Plan Estratégico Institucional MP 2021-2025.
- Plan Estratégico Institucional PJ 2021-2025.
- Informes de Ejecución Presupuestal MININTER 2022.

Metodología: Análisis de contenido focalizado en capacidades tecnológicas y marcos normativos.

HERRAMIENTA 3: Análisis comparativo de experiencias internacionales

Casos estudiados: Sistemas de retención de metadatos en Alemania, Australia y Estados Unidos.

Fuentes: Reportes oficiales de organismos gubernamentales y estudios académicos especializados.

Enfoque: Identificación de factores críticos de éxito y lecciones aprendidas.

HERRAMIENTA 4: Triangulación metodológica

Proceso: Contrastación sistemática entre evidencia documental, testimonial y experiencias internacionales para validar la identificación causal.

Criterios de validación: Convergencia de fuentes, consistencia temporal y coherencia explicativa.

Anexo 7: Herramientas de recojo de información para el proceso de conceptualización y testeo

HERRAMIENTA 1: Sesiones de co-creación estructuradas

Participantes por sesión:

- PNP: 3 sesiones con 8 participantes (DIRINCRI, analistas de inteligencia, Programa Constelación).
- Ministerio Público: 2 sesiones con 2 fiscales especializados.
- Expertos técnicos: 2 sesiones intensivas de 3 horas con asesor Programa Constelación.

Metodología: Design thinking con técnicas específicas de mapeo de experiencias y storytelling.

Productos: Requerimientos técnicos, criterios probatorios, protocolos de seguridad.

HERRAMIENTA 2: Simulación de casos complejos

Casos utilizados: 6 casos simulados basados en patrones criminales reales anonimizados.

Escenarios testados:

- Investigación de homicidio por sicariato.
- Red de extorsión operando desde centros penitenciarios.

Métricas evaluadas:

- Tiempo de tramitación de autorizaciones judiciales.
- Calidad jurídica de evidencia (escala 1-10).
- Cumplimiento de protocolos de protección de datos.

HERRAMIENTA 3: Validación iterativa por niveles de prototipado

Nivel conceptual:

- Técnica: Storyboard de procesos legales
- Participantes: 11 usuarios institucionales
- Resultado: Identificación de necesidades de procedimientos de urgencia

Nivel procedimental:

- Técnica: Simulación de casos paradigmáticos.
- Hipótesis testeadas: Tiempos de respuesta, compatibilidad de controles.
- Resultado: Refinamiento de protocolos de coordinación.

Nivel integral:

- Técnica: Prueba piloto con indicadores cuantitativos.
- Resultados: 99% de fiscales evaluaron evidencia como “significativamente superior”.
- Variación de objetivos: -19% en tiempo, +18% en calidad jurídica.

HERRAMIENTA 4: Matrices de evaluación multicriterio

Criterios aplicados:

- Viabilidad Legal (25%).
- Factibilidad Técnica (25%).
- Impacto Potencial (30%).
- Protección de Derechos Fundamentales (20%).

Metodología:

Evaluación cuantitativa con justificación cualitativa por cada criterio.

Anexo 8: Guías de entrevistas semi estructuradas

GUIA DE ENTREVISTA SEMI-ESTRUCTURADA
PARA EXPERTOS DE LA POLICÍA NACIONAL DEL PERÚ (PNP)

Introducción:

- Presentación del entrevistador y del proyecto de innovación **"ASEGURAMIENTO DE LA DISPONIBILIDAD DE METADATOS DE LOCALIZACIÓN DE DISPOSITIVOS MÓVILES PARA POTENCIAR LA INVESTIGACIÓN CRIMINAL"**.
- **Explicación del propósito y duración de la entrevista:**
  Propósito: conocer su perspectiva como experto sobre las causas del incremento de delitos violentos cometidos por bandas criminales en Lima Metropolitana (2021-2023), profundizando en los factores que influyen en la eficacia de la investigación criminal y el procesamiento judicial desde la óptica de la PNP. Sus conocimientos serán valiosos para diagnosticar el problema y diseñar propuestas innovadoras de solución.
  Duración: 45 minutos.
- **Acuerdo de confidencialidad y consentimiento informado:**
  Compromiso de usar la información solo para fines del proyecto.
  Opción de anonimizar las respuestas si el entrevistado lo prefiere.
  Permiso para grabar la entrevista en audio (si aplica - opcional).
  Firma de documento de consentimiento informado (si se requiere - opcional).
- **Instrucciones generales antes de iniciar**
  Explicación de que no hay respuestas correctas o incorrectas.
  Énfasis en la importancia de la sinceridad y la experiencia personal.
  Aclaración de que el entrevistado puede pedir que se repita o reformule una pregunta.
  Invitación a expresar libremente ideas, opiniones y ejemplos relevantes.

Preguntas:

A. Capacidades de Investigación Criminal

1. ¿Qué sistemas de análisis digital utiliza actualmente para investigar delitos?
2. ¿Qué limitaciones encuentra en las herramientas tecnológicas disponibles?
3. ¿Qué capacidad tiene para analizar grandes volúmenes de datos de localización?
4. ¿Qué herramientas adicionales requiere para mejorar las investigaciones basadas en metadatos de localización?
5. ¿Con qué personal especializado cuenta para análisis de metadatos de localización?

6. ¿Qué capacitación requiere el personal para manejar metadatos de localización?
7. ¿Qué capacidad de almacenamiento tiene para evidencia digital?
8. ¿Cómo afecta la falta de acceso a metadatos históricos en sus investigaciones?

B. Gestión de Evidencia Digital

9. ¿Qué protocolos aplica para el manejo de evidencia digital?
10. ¿Cómo asegura la cadena de custodia de evidencia digital?
11. ¿Qué estándares utiliza para validar la integridad de evidencia digital?
12. ¿Qué controles de calidad implementa para la evidencia digital?
13. ¿Cómo documenta el proceso de obtención y análisis de evidencia digital?

C. Protección de Derechos Fundamentales

14. ¿Qué normas aplican al manejo de metadatos de localización?
15. ¿Qué vacíos normativos identifica respecto a metadatos de localización?
16. ¿Qué desafíos legales anticipa en la implementación de un sistema de retención?
17. ¿Qué mecanismos de supervisión implementa?
18. ¿Qué sanciones aplica por mal uso de datos?
19. ¿Qué criterios de proporcionalidad aplica al solicitar metadatos de localización?
20. ¿Cómo evalúa necesidad vs. invasión privacidad?

D. D. Cooperación Interinstitucional

21. ¿Qué mecanismos de coordinación utiliza?
22. ¿Cómo comparte información entre instituciones?
23. ¿Qué protocolos conjuntos aplica?
24. ¿Cómo evalúa efectividad de coordinación?
25. ¿Qué formatos de intercambio usa?
26. ¿Cómo asegura compatibilidad entre sistemas?
27. ¿Qué otros aspectos técnicos o consideraciones importantes no abordados identifica?

Cierre:

- Comentarios o información adicional relevante.
- Agradecimiento por la participación.
- Compartir datos de contacto para seguimiento.

GUIA DE ENTREVISTA SEMI-ESTRUCTURADA
PARA EXPERTOS DEL MINISTERIO PUBLICO (MP)

Introducción:

- Presentación del entrevistador y del proyecto de innovación **"ASEGURAMIENTO DE LA DISPONIBILIDAD DE METADATOS DE LOCALIZACIÓN DE DISPOSITIVOS MÓVILES PARA POTENCIAR LA INVESTIGACIÓN CRIMINAL"**.
- **Explicación del propósito y duración de la entrevista:**
  Propósito: conocer su perspectiva como experto sobre las causas del incremento de delitos violentos cometidos por bandas criminales en Lima Metropolitana (2021-2023), profundizando en los factores que influyen en la eficacia de la investigación criminal y el procesamiento judicial desde la óptica de la MP. Sus conocimientos serán valiosos para diagnosticar el problema y diseñar propuestas innovadoras de solución.
  Duración: 45 minutos.
- **Acuerdo de confidencialidad y consentimiento informado:**
  Compromiso de usar la información solo para fines del proyecto.
  Opción de anonimizar las respuestas si el entrevistado lo prefiere.
  Permiso para grabar la entrevista en audio (si aplica - opcional).
  Firma de documento de consentimiento informado (si se requiere - opcional).
- **Instrucciones generales antes de iniciar**
  Explicación de que no hay respuestas correctas o incorrectas.
  Énfasis en la importancia de la sinceridad y la experiencia personal.
  Aclaración de que el entrevistado puede pedir que se repita o reformule una pregunta.
  Invitación a expresar libremente ideas, opiniones y ejemplos relevantes.

Preguntas:

A. Capacidades de Investigación Criminal

1. ¿Qué sistemas de análisis digital utiliza actualmente para investigar delitos?
2. ¿Qué limitaciones encuentra en las herramientas tecnológicas disponibles?
3. ¿Qué capacidad tiene para analizar grandes volúmenes de datos de localización?
4. ¿Qué herramientas adicionales requiere para mejorar las investigaciones?
5. ¿Con qué personal especializado cuenta para análisis de metadatos?
6. ¿Qué capacitación requiere el personal para manejar metadatos?
7. ¿Qué capacidad de almacenamiento tiene para evidencia digital?
8. ¿Cómo afecta la falta de acceso a metadatos históricos en sus investigaciones?

B. Gestión de Evidencia Digital

9. ¿Qué protocolos aplica para el manejo de evidencia digital?
10. ¿Cómo asegura la cadena de custodia de evidencia digital?
11. ¿Qué estándares utiliza para validar la integridad de evidencia digital?
12. ¿Qué controles de calidad implementa para la evidencia digital?
13. ¿Cómo documenta el proceso de obtención y análisis de evidencia digital?

C. Valoración Probatoria

14. ¿Qué criterios aplica para admitir metadatos de localización como evidencia?
15. ¿Qué valor probatorio otorga a los metadatos de localización?
16. ¿Qué requisitos formales exige para admitir evidencia digital?
17. ¿Cómo verifica la autenticidad de metadatos de localización presentados?
18. ¿Qué mecanismos usa para detectar manipulaciones?
19. ¿Qué criterios usa para evaluar suficiencia probatoria?
20. ¿Qué evidencia adicional requiere para corroborar metadatos de localización?
21. ¿Cuáles son las principales debilidades probatorias en casos de crimen organizado violento?
22. ¿De qué manera la falta de metadatos de localización afecta la acreditación de presencia y participación de imputados?
23. ¿Qué valor probatorio específico otorga a los metadatos de localización en casos de criminalidad organizada?

D. Protección de Derechos Fundamentales

24. ¿Qué normas aplican al manejo de metadatos de localización?
25. ¿Qué vacíos normativos identifica respecto a metadatos de localización?
26. ¿Qué aspectos considera críticos al solicitar autorización judicial?
27. ¿Qué desafíos legales anticipa en la implementación?
28. ¿Qué mecanismos de supervisión implementa?
29. ¿Qué sanciones aplica por mal uso de datos?
30. ¿Qué criterios de proporcionalidad aplica al solicitar metadatos?
31. ¿Cómo evalúa necesidad vs. invasión privacidad?

E. Cooperación Interinstitucional

32. ¿Qué mecanismos de coordinación utiliza?
33. ¿Cómo comparte información entre instituciones?

34. ¿Qué protocolos conjuntos aplica?
35. ¿Cómo evalúa efectividad de coordinación?
36. ¿Qué formatos de intercambio usa?
37. ¿Cómo asegura compatibilidad entre sistemas?
38. ¿Qué otros aspectos técnicos o consideraciones importantes identifican?

Cierre:

- Comentarios o información adicional relevante.
- Agradecimiento por la participación.
- Compartir datos de contacto para seguimiento.

GUIA DE ENTREVISTA SEMI-ESTRUCTURADA
PARA EXPERTOS DEL PODER JUDICIAL (PJ)

Introducción:

- Presentación del entrevistador y del proyecto de innovación **"ASEGURAMIENTO DE LA DISPONIBILIDAD DE METADATOS DE LOCALIZACIÓN DE DISPOSITIVOS MÓVILES PARA POTENCIAR LA INVESTIGACIÓN CRIMINAL"**.
- **Explicación del propósito y duración de la entrevista:**
  Propósito: conocer su perspectiva como experto sobre las causas del incremento de delitos violentos cometidos por bandas criminales en Lima Metropolitana (2021-2023), profundizando en los factores que influyen en la eficacia de la investigación criminal y el procesamiento judicial desde la óptica del PJ. Sus conocimientos serán valiosos para diagnosticar el problema y diseñar propuestas innovadoras de solución.
  Duración: 45 minutos.
- **Acuerdo de confidencialidad y consentimiento informado:**
  Compromiso de usar la información solo para fines del proyecto.
  Opción de anonimizar las respuestas si el entrevistado lo prefiere.
  Permiso para grabar la entrevista en audio (si aplica - opcional).
  Firma de documento de consentimiento informado (si se requiere - opcional).
- **Instrucciones generales antes de iniciar**
  Explicación de que no hay respuestas correctas o incorrectas.
  Énfasis en la importancia de la sinceridad y la experiencia personal.
  Aclaración de que el entrevistado puede pedir que se repita o reformule una pregunta.
  Invitación a expresar libremente ideas, opiniones y ejemplos relevantes.

Preguntas:

A. Gestión de Evidencia Digital

1. ¿Qué protocolos aplica para el manejo de evidencia digital?
2. ¿Cómo asegura la cadena de custodia de evidencia digital?
3. ¿Qué estándares utiliza para validar la integridad de evidencia digital?
4. ¿Qué controles de calidad implementa para la evidencia digital?
5. ¿Cómo documenta el proceso de obtención y análisis de evidencia digital?

B. Valoración Probatoria

6. ¿Qué criterios aplica para admitir metadatos de localización como evidencia?
7. ¿Qué valor probatorio otorga a los metadatos de localización?
8. ¿Qué requisitos formales exige para admitir evidencia digital?
9. ¿Cómo verifica la autenticidad de metadatos de localización presentados?
10. ¿Qué mecanismos usa para detectar manipulaciones?
11. ¿Qué criterios usa para evaluar suficiencia probatoria?
12. ¿Qué evidencia adicional requiere para corroborar metadatos de localización?
13. ¿Cuáles son las principales debilidades probatorias en casos de crimen organizado violento?
14. ¿Qué valor probatorio específico otorga a los metadatos de localización en casos de criminalidad organizada?

C. Protección de Derechos Fundamentales

15. ¿Qué normas aplican al manejo de metadatos de localización?
16. ¿Qué vacíos normativos identifica respecto a metadatos de localización?
17. ¿Qué aspectos considera críticos al solicitar autorización judicial?
18. ¿Qué desafíos legales anticipa en la implementación?
19. ¿Qué mecanismos de supervisión implementa?
20. ¿Qué sanciones aplica por mal uso de datos?
21. ¿Qué criterios de proporcionalidad aplica al solicitar metadatos?
22. ¿Cómo evalúa necesidad vs. invasión privacidad?

D. Cooperación Interinstitucional

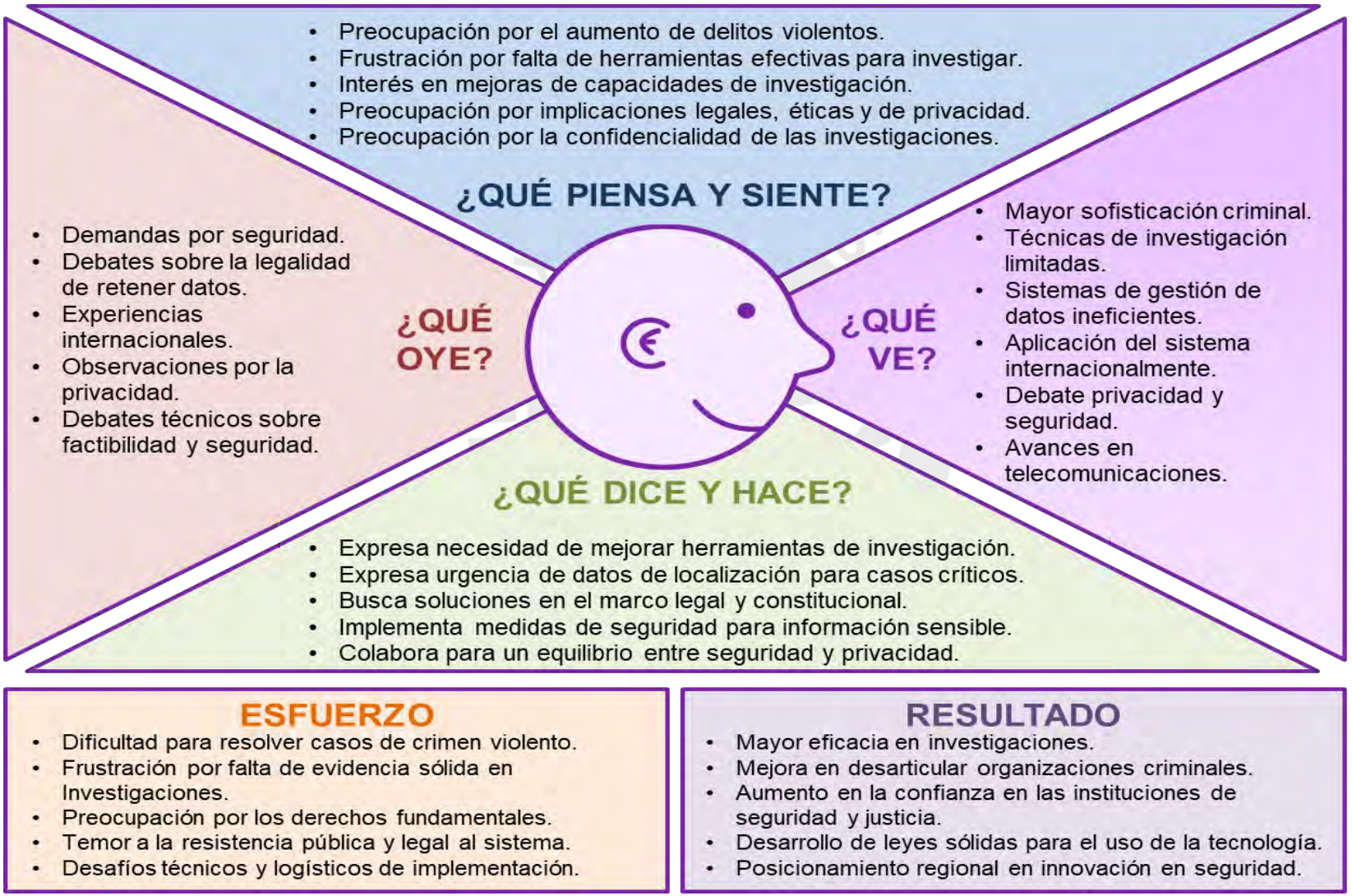
23. ¿Qué mecanismos de coordinación utiliza?
24. ¿Cómo comparte información entre instituciones?
25. ¿Qué protocolos conjuntos aplica?
26. ¿Cómo evalúa efectividad de coordinación?

27. ¿Qué formatos de intercambio usa?
28. ¿Cómo asegura compatibilidad entre sistemas?
29. ¿Qué otros aspectos técnicos o consideraciones importantes identifican?

Cierre:

- Comentarios o información adicional relevante.
- Agradecimiento por la participación.
- Compartir datos de contacto para seguimiento.

Anexo 9: Mapa de empatía de los actores involucrados



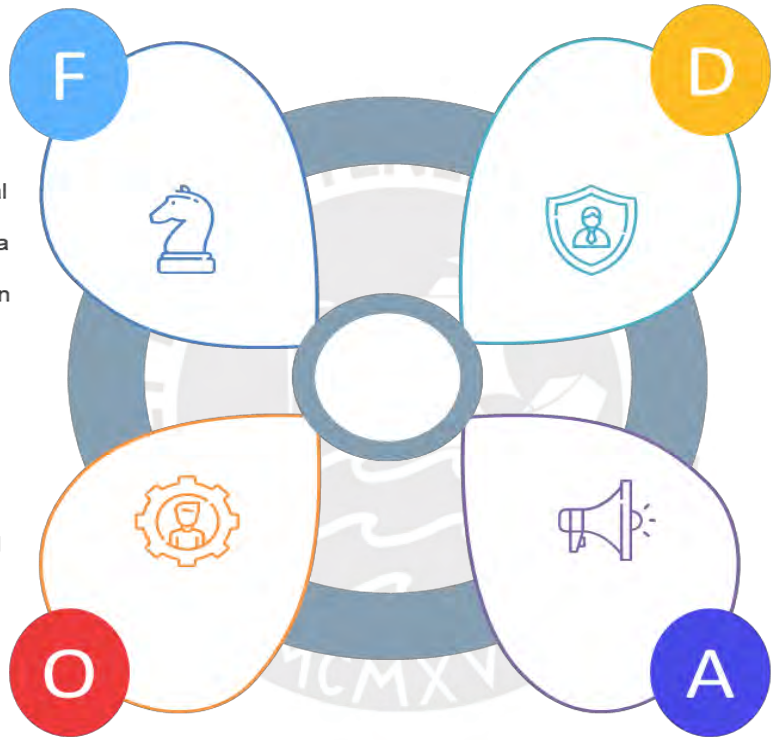
Anexo 10: Análisis FODA del marco legal actual

Fortalezas

- Protección constitucional sobre privacidad y comunicaciones.
- Intervención legal de comunicaaciones.
- Experiencia en conservar ciertos datos de comunicaciones.
- Experiencia en el manejo confidencial de información sensible.
- Reconocimiento legal de la tecnología en la investigación.
- Existencia del Programa Constelación con infraestructura aprovechable.
- Personal técnico con experiencia en gestión de información sensible.

Oportunidades

- Conciencia pública creciente sobre el uso de herramientas.
- Desarrollo de tecnologías para el manejo seguro y eficiente de datos masivos.
- Posibilidad de aprender de experiencias de otros países.
- Potencial para liderar un equilibrio entre seguridad y privacidad.
- Oportunidad de mejorar la cooperación entre instituciones de seguridad y justicia.
- Aprovechamiento de infraestructura existente.
- Integración con sistemas actuales de las operadoras.



Debilidades

- Legislación específica ausente de retención de metadatos.
- Procedimientos poco claros de acceso a metadatos.
- Falta de mecanismos para acceder a metadatos de localización.
- Limitaciones para manejar grandes volúmenes de datos.
- Interpretación heterogénea de la privacidad de metadatos.
- Carencia de normas para la gestión y destrucción de datos retenidos.
- Necesidad de capacitación especializada del personal.
- Falta de procesos estandarizados para gestión de metadatos.

Amenazas

- Desafíos legales y constitucionales.
- Preocupaciones sobre privacidad y uso indebido de datos.
- Riesgo de que la tecnología se vuelva rápidamente obsoleta.
- Posibilidad criminal de evitar la vigilancia.
- Oposición de grupos de derechos humanos contra la retención masiva de datos.

Anexo 11: Generación y priorización de ideas

Anexo 12: Proyecto de Ley

Proyecto de Ley

SUMILLA: Ley que regula la retención y acceso a los metadatos de localización para fortalecer la investigación criminal en casos de delitos violentos.

Los ciudadanos, a iniciativa de los Señores Walter Lozano Pajuelo y Juan Carlos Samaniego Miranda en ejercicio de su derecho de iniciativa que le confiere el artículo 107º de la Constitución Política del Perú y la Ley 26300, Ley de los Derechos de Participación y Control Ciudadanos, proponen la siguiente iniciativa legislativa:

PROYECTO DE LEY DE RETENCIÓN Y ACCESO A LOS METADATOS DE LOCALIZACIÓN PARA LA INVESTIGACIÓN CRIMINAL EN CASOS DE DELITOS VIOLENTOS Y PERSONAS DESAPARECIDAS

Título I: Disposiciones Generales

Artículo 1: Objeto de la ley
La presente ley tiene por objeto establecer el marco legal para la retención y acceso a los metadatos de localización generados por dispositivos móviles, con el fin de fortalecer la investigación criminal en casos de delitos violentos y búsqueda de personas desaparecidas, garantizando el respeto a los derechos fundamentales de los ciudadanos.

Artículo 2: Ámbito de aplicación
Esta ley se aplica a todas las empresas operadoras de telecomunicaciones que brindan servicios móviles en el territorio nacional y a las instituciones del sistema de justicia penal involucradas en la investigación y persecución de delitos violentos, incluyendo la unidad especializada de la Policía Nacional del Perú denominada "Programa Constelación".

Artículo 3: Definiciones
Para efectos de esta ley, se entiende por:

a) Acceso autorizado: Proceso mediante el cual se obtiene acceso legal a los metadatos de localización retenidos, previa autorización judicial.
b) Delitos violentos: Aquellos que impliquen el uso de fuerza física o amenaza contra una persona, incluyendo, pero no limitándose a homicidio, secuestro, violación, robo agravado, extorsión y sicariato.
c) Dirección IP: Identificador numérico único asignado a cada dispositivo conectado a una red que utiliza el protocolo de Internet.
d) Dirección MAC: Identificador único asignado a interfaces de red de un dispositivo.
e) Geolocalización: Proceso mediante el cual se determina la ubicación precisa de un dispositivo electrónico activo, utilizando un sistema de coordenadas geográficas.
f) Localización: Identificación de un área referencial donde se encuentra un dispositivo electrónico activo.
g) IMEI: Identidad Internacional de Equipo Móvil, número único que identifica un dispositivo móvil.
h) IMSI: Identidad Internacional del Abonado Móvil, código de identificación único para cada usuario de telefonía móvil.
i) MSISDN: Número de la estación móvil en la red digital de servicios integrados, que corresponde al número de teléfono del abonado.
j) Metadatos de localización: Datos que describen la ubicación de un dispositivo móvil, sin incluir el contenido de las comunicaciones.
k) Retención de metadatos: Almacenamiento temporal de metadatos de localización por parte de las empresas operadoras y el Programa Constelación.

Título II: De la Retención de Metadatos de Localización

Artículo 4: Obligación de retención
Las empresas operadoras de telecomunicaciones están obligadas a retener los metadatos de localización generados por su plataforma tecnológica y los dispositivos móviles de sus usuarios, en los términos establecidos en la presente ley.

Artículo 5: Tipos de metadatos a retener
Los metadatos de localización que deben ser retenidos incluyen:
a) Número telefónico (MSISDN).
b) Identificador único del dispositivo (IMEI) o Dirección IP o Dirección MAC.
c) Identificador de la tarjeta SIM (IMSI), en caso de comunicaciones a través de señal celular.

d) Fecha y hora de la localización o geolocalización.
e) Identificador de la estación base a la que se conectó el dispositivo, su sector o azimut.
f) Coordenadas geográficas de la estación base o geolocalización.
g) Coordenadas de geolocalización obtenidas a través del sistema GPS del dispositivo móvil, cuando estén disponibles.

Artículo 6: Período de retención
Las empresas operadoras de telecomunicaciones deberán conservar los metadatos de localización por un período de tres (3) meses a partir de su generación. El Programa Constelación podrá mantener los metadatos obtenidos durante seis (6) meses a partir de su registro en su sistema. Vencido el plazo, las empresas operadoras eliminarán automáticamente los metadatos. Asimismo, el Programa Constelación eliminará de forma automática solo aquellos datos que no sean considerados relevantes por el Fiscal.

Artículo 7: Seguridad y protección de los datos retenidos
Las empresas operadoras de telecomunicaciones y el Programa Constelación deberán implementar medidas de seguridad adecuadas para proteger los metadatos retenidos contra el acceso no autorizado, la destrucción accidental o ilícita, la pérdida o alteración. Estas medidas incluirán, como mínimo:
a) Encriptación de datos.
b) Control de acceso basado en roles.
c) Registro detallado de todas las actividades del sistema (logs).
d) Auditorías de seguridad periódicas.
e) Planes de respaldo y recuperación de datos.
f) Infraestructura de almacenamiento y procesamiento segregada.
g) Sistema de detección y prevención de intrusiones (IDS/IPS).

Título III: Del Acceso a los Metadatos de Localización

Artículo 8: Entidades autorizadas
Podrán solicitar acceso a los metadatos de localización:
a) El Ministerio Público, a través de los fiscales debidamente autorizados.
b) La Policía Nacional del Perú, a través del Programa Constelación, previa autorización judicial.

Artículo 9: Procedimiento de solicitud y autorización

El procedimiento de solicitud y autorización de acceso a los metadatos de localización se realizará conforme a lo establecido en el artículo 230 del Código Procesal Penal para la intervención de comunicaciones y telecomunicaciones, con las siguientes especificaciones:

a) La solicitud deberá ser presentada por el fiscal a cargo de la investigación.

b) Deberá especificarse que los metadatos requeridos se encuentran dentro del plazo de retención de tres meses establecido para las empresas operadoras.

c) La resolución judicial que autorice el acceso a los metadatos deberá ser motivada y especificar los datos a los que se autoriza el acceso.

Artículo 10: Sistema Digital de Gestión de Autorizaciones

Se implementará un sistema digital para la gestión de solicitudes y autorizaciones judiciales que deberá:

a) Permitir el seguimiento en tiempo real del estado de las solicitudes.

b) Mantener registro detallado de todas las actuaciones.

c) Generar alertas automáticas sobre plazos y vencimientos.

d) Integrarse con los sistemas existentes del Poder Judicial, Ministerio Público y PNP.

Artículo 11: Requisitos para la autorización judicial

Para la autorización judicial de acceso a los metadatos de localización, el Fiscal deberá acreditar:

a) La existencia de una investigación formal por delito violento o caso de persona desaparecida;

b) Vinculación de los metadatos solicitados con los hechos investigados;

c) La necesidad e idoneidad de la medida para el esclarecimiento de los hechos;

d) Delimitación objetiva y subjetiva de los metadatos requeridos, especificando su alcance temporal.

Artículo 12: Urgencia y peligro inminente

En casos de inminente peligro para la vida, integridad física o libertad de las personas en el marco de la comisión de un delito violento, el Fiscal podrá disponer el acceso inmediato a los metadatos de localización sin autorización judicial previa, debiendo fundamentar por escrito su decisión, solicitar la convalidación judicial y notificar al Órgano de Control Interno del Ministerio Público dentro de las veinticuatro (24) horas siguientes; el juez resolverá en igual plazo, ordenando la destrucción de la información

en caso de denegatoria; quedando sujeto a responsabilidad administrativa y penal por el uso indebido de esta facultad.

Título IV: De las Garantías y Derechos de los Usuarios

Artículo 13: Protección de datos personales
El tratamiento de los metadatos de localización deberá realizarse con estricto apego a los principios de la protección de datos personales, incluyendo:
a) Finalidad: Los datos solo podrán ser utilizados para los fines específicos de la investigación autorizada.
b) Proporcionalidad: Solo se accederá a los datos estrictamente necesarios para la investigación.
c) Calidad: Se garantizará la exactitud y actualización de los datos.
d) Seguridad: Se implementarán medidas técnicas y organizativas para proteger los datos.

Artículo 14: Notificación a los afectados
La notificación a los afectados se realizará conforme a lo establecido en el numeral 3 del Artículo 231 del Código Procesal Penal.

Artículo 15: Reexamen judicial
El reexamen judicial de las medidas adoptadas se realizará conforme a lo establecido en el numeral 4 del Artículo 231 del Código Procesal Penal.

Título V: De la Supervisión y Auditoria

Artículo 16: Supervisión y Auditoría
La supervisión y auditoría del sistema de retención y acceso a metadatos de localización se realizará de la siguiente manera:
a) La Inspectoría General de la PNP realizará auditorías semestrales del Programa Constelación.
b) Control Interno del Ministerio Público supervisará la actuación de los fiscales en el uso del sistema.
c) Se realizarán pruebas de penetración semestrales por expertos en ciberseguridad externos.

Artículo 17: Informes de transparencia

El Programa Constelación y las empresas operadoras deberán publicar informes semestrales de transparencia que incluyan:

a) Número de solicitudes de acceso a metadatos recibidas.

b) Tipos de delitos investigados.

c) Duración promedio de las intervenciones.

d) Otros.

Artículo 18: Sanciones por uso indebido

El uso indebido de los metadatos de localización o del sistema de retención y acceso será sancionado de acuerdo con la legislación penal vigente, sin perjuicio de las responsabilidades administrativas y civiles que correspondan.

DISPOSICIONES COMPLEMENTARIAS

Primera: Programa de Capacitación y Certificación

El Ministerio del Interior, en coordinación con el Ministerio Público y el Poder Judicial, implementará un programa de capacitación y certificación para el personal que tendrá acceso al sistema de retención y acceso a metadatos de localización.

El programa de capacitación deberá incluir como mínimo:

a) Marco legal y constitucional aplicable.

b) Procedimientos operativos estandarizados.

c) Uso de herramientas de análisis geoespacial.

d) Protocolos de seguridad y protección de datos.

La certificación tendrá una vigencia de tres años y su renovación requerirá aprobar un programa de actualización.

Segunda: Proceso de Selección al Programa Constelación

El personal asignado al Programa Constelación deberá pasar por un riguroso proceso de selección que incluirá, como mínimo:

a) Investigación exhaustiva de antecedentes y referencias.

b) Entrevista profesional.

c) Examen toxicológico.

d) Evaluación médica.

e) Evaluación psicológica.

f) Prueba de polígrafo.

El examen toxicológico y la prueba de polígrafo deberá repetirse periódicamente para el personal que ya forma parte del Programa Constelación, como parte de su recertificación.

Tercera: Dedicación Exclusiva y Especialización del Personal del Programa Constelación

El personal asignado al Programa Constelación se dedicará exclusivamente a las tareas relacionadas con este programa. En los cambios de colocación o asignación de cargos, se deberá respetar la especialización adquirida por este personal, asignándolos a funciones afines que aprovechen su experiencia y conocimientos especializados.

Cuarta: Revisión de la Legislación en Materia de Telecomunicaciones y sus Servicios

En un plazo no mayor a 180 días calendario, el Ministerio de Transportes y Comunicaciones, en coordinación con el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL), el Ministerio del Interior, El Ministerio Público y la Policía Nacional del Perú, deberán presentar al Congreso de la República un proyecto de ley que incorpore en la legislación de telecomunicaciones y sus servicios un título específico referido al apoyo a la administración de justicia y a la función policial. Este título deberá incluir, entre otros aspectos:

a) Obligaciones de las empresas operadoras en materia de colaboración con la justicia y la función policial.

b) Protocolos de interacción entre las empresas operadoras y las autoridades.

c) Mecanismos de supervisión y control de las obligaciones de las empresas operadoras en esta materia.

Quinta: Beneficio para la implementación del sistema

5.1 Créase una Comisión Multisectorial Temporal encargada de determinar los beneficios tributarios y/o mecanismos de compensación para las empresas operadoras que implementen el sistema de retención de metadatos.

5.2 La Comisión estará conformada por:

Un representante del Ministerio de Economía y Finanzas, quien la presidirá.

Un representante del Ministerio de Transportes y Comunicaciones.

Un representante de OSIPTEL.

Un representante por cada empresa operadora.

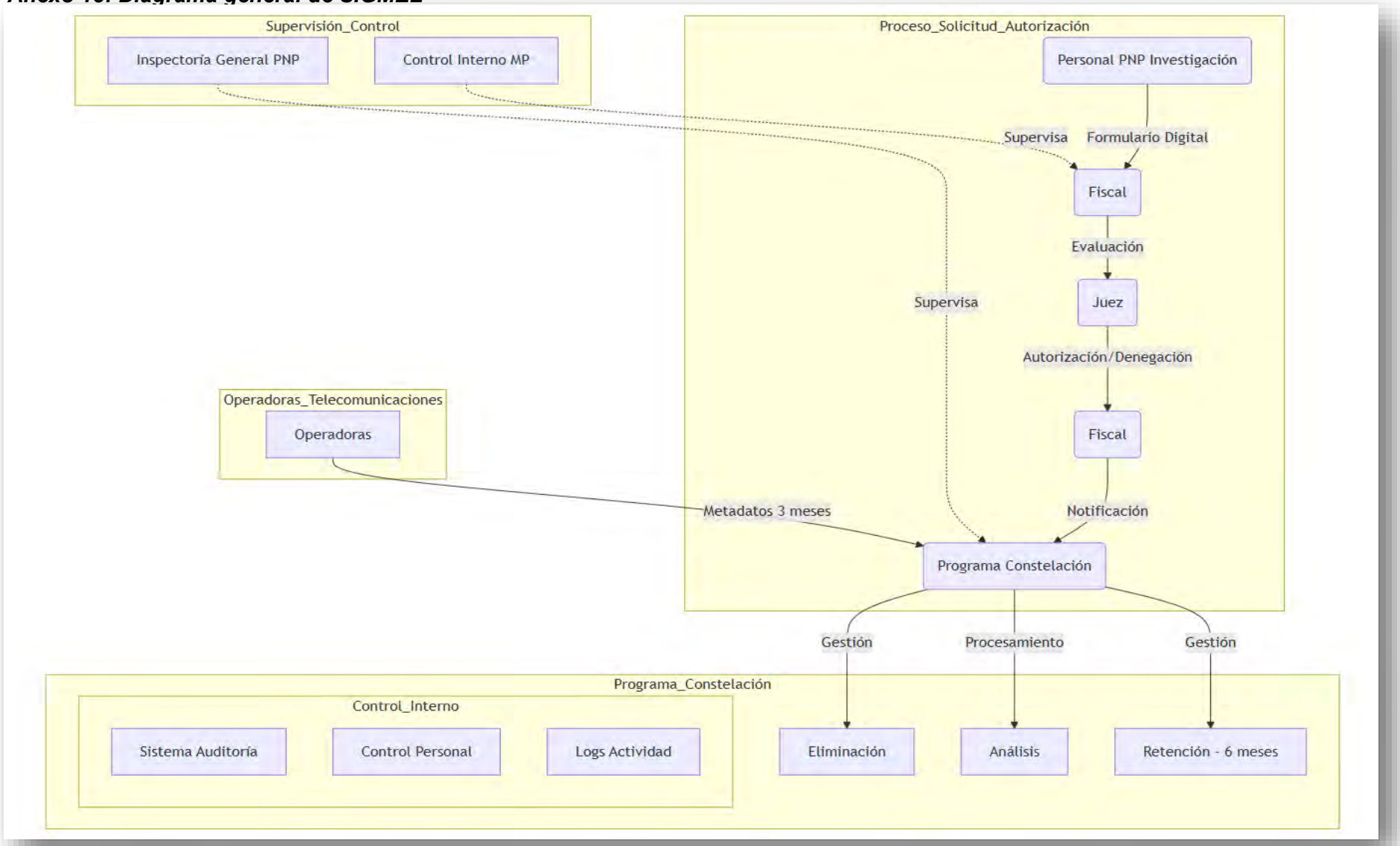
Un representante del Ministerio del Interior.

5.3 La Comisión tendrá un plazo de 60 días calendario para presentar su informe con las recomendaciones sobre los beneficios y mecanismos de compensación.
5.4 El Ministerio de Economía y Finanzas, mediante Decreto Supremo, establecerá los beneficios específicos en base a las recomendaciones de la Comisión."

Sexta: Reglamentación
El Poder Ejecutivo reglamentará la presente ley en un plazo no mayor de 60 días calendario, contados a partir de su publicación.

Séptima: Vigencia
La presente ley entrará en vigencia al día siguiente de la publicación de su reglamento en el Diario Oficial El Peruano.

Anexo 13: Diagrama general de SIGMEL



Anexo 14: Matrices de análisis de entrevistas a la PNP, MP y otros

MATRIZ DE ANALISIS DE ENTREVISTAS A LA PNP Y MP SOBRE CAPACIDADES DE INVESTIGACION CRIMINAL, GESTION DE EVIDENCIA DIGITAL, PROCESAMIENTO DE METADATOS, VALORACION PROBATORIA, PROTECCION DE DERECHOS FUNDAMENTALES Y COOPERACION INTERINSTITUCIONAL EN EL USO DE METADATOS (HISTÓRICOS) DE LOCALIZACIÓN DE DISPOSITIVOS MÓVILES PARA LA INVESTIGACIÓN CRIMINAL

Categorías	Aspectos Críticos	Hallazgos PNP Operativo	Hallazgos MP	Recomendaciones Técnicas (Asesor)	Hallazgos Consolidados
Capacidades de Investigación Criminal	Sistemas y Herramientas	Carencia sistemas especializados. Ubicación imprecisa por antenas (CellID).	Capacidades limitadas de análisis forense básico.	Sistema centralizado integrado con operadoras. Aprovechamiento de la infraestructura del Programa Constelación.	Necesidad crítica de un sistema centralizado con capacidad de localización precisa, aprovechando infraestructura del Programa Constelación.
	Capacidad Técnica	Capacidad limitada para análisis masivo de datos.	Capacidad casi nula para grandes volúmenes datos.	Procesamiento mínimo 3 meses de metadatos de localización.	Implementar capacidad de procesamiento y almacenamiento para mínimo 3 meses de metadatos de localización con depuración automática.
	Personal y Capacitación	Grave carencia personal especializado.	Limitado personal técnico especializado.	Personal con experiencia en análisis geoespacial, bigdata y localización.	Urgente necesidad de incorporar y capacitar personal especializado en análisis de metadatos de localización, bigdata y otros.
Gestión de Evidencia Digital	Protocolos y Cadena Custodia	Falta protocolos específicos metadatos de localización.	Diversos protocolos sin estandarización.	Protocolo único y cadena de custodia digital.	Implementar protocolos estandarizados específicos con cadena de custodia digital.
	Control y Validación	Controles insuficientes y no estandarizados.	Controles básicos sin protocolos específicos.	Control automático de integridad.	Sistema automatizado de control de calidad e integridad de metadatos de localización.
Protección de Derechos Fundamentales	Marco Normativo	Ausencia normativa específica retención de metadatos de localización.	Marco normativo insuficiente.	Regulación específica para delitos violentos.	Desarrollo urgente de marco normativo específico para metadatos de localización.
	Criterios de Aplicación	Falta de criterios específicos de metadatos de localización.	Énfasis en proporcionalidad y necesidad.	Priorización de los delitos violentos en ejecución.	Establecer criterios específicos balanceando eficacia investigativa y derechos fundamentales y privacidad.
Cooperación Interinstitucional	Mecanismos de Coordinación	Falta mecanismos formales específicos.	Sin protocolo específico para metadatos de localización.	Coordinación técnica multisectorial.	Implementar mecanismos formales de coordinación PNP, MP, Operadoras y otras.
	Sistema Integrado	Ausencia de un sistema unificado.	Falta de un sistema de gestión de metadatos de localización.	Plataforma única interinstitucional.	Diseñar e implementar una plataforma única integrada para la gestión de metadatos de localización con protocolos estandarizados.

MATRIZ DE ANÁLISIS DE ENTREVISTAS DE LA POLICÍA NACIONAL DEL PERÚ SOBRE CAPACIDADES, NECESIDADES Y LIMITACIONES EN EL USO DE METADATOS (HISTÓRICOS) DE LOCALIZACIÓN DE DISPOSITIVOS MÓVILES PARA LA INVESTIGACIÓN CRIMINAL

Categorías	Preguntas	PNP 1	PNP 2	PNP 3	PNP 4	PNP 5	PNP 6	PNP 7	PNP 8	PNP 9	PNP 10	Hallazgos Clave
Capacidades de Investigación Criminal	1. ¿Qué sistemas de análisis digital utiliza actualmente para investigar delitos?	SIRDIC, OSINT, EnCase, Cellebrite, Axiom.	IBM i2, Visual Peru, Autopsy, Cellebrite.	Análisis de redes sociales, localización, IA.	Sin sistemas especializados.	No cuenta con sistemas.	Solo sistemas básicos PNP.	Herramientas de fuentes abiertas.	Programa Constelación	SIAC y sistemas criminológicos.	Solo localización por DIVINDAT y datos de operadoras.	Carecen de sistemas especializados; solo unidades élite tienen software forense actualizado. La localización tiene un margen de error de 300m.
	2. ¿Qué limitaciones encuentra en las herramientas tecnológicas disponibles?	Localización solo referencial, licencias vencidas.	Falta actualizaciones y licencias originales.	Preocupaciones de privacidad, falta capacitación.	Sin herramientas especializadas.	Limitaciones presupuestales y técnicas.	Sin capacidad análisis avanzado.	Licencias vencidas, sin actualización.	Limitado a datos antenas (CellId)	Limitaciones de procesamiento.	Sin tecnología propia, error de 300m en localización.	Ubicación imprecisa por antenas (Cell ID) y falta de licencias actualizadas.
	3. ¿Qué capacidad tiene para analizar grandes volúmenes de datos de localización?	Usa IA pero requiere protocolos.	Uso ineficiente por desactualización.	Capacidad limitada.	Sin capacidad.	Sin capacidad de análisis.	Muy limitada.	Capacidad parcial.	Capacidad específica.	Capacidad básica.	Sin capacidad análisis de grandes volúmenes.	Se reporta capacidad limitada o nula para análisis masivo de datos de localización.
	4. ¿Qué herramientas adicionales requiere para mejorar las investigaciones?	Información precisa IP y localización.	Software forense actualizado.	Software de análisis big data.	Herramientas especializadas.	Sistemas modernos.	Tecnología especializada.	Maletas de geolocalización.	Sistemas actualizados.	Mejores sistemas.	Requiere equipos y software actualizados.	Sistemas precisos de localización y software actualizado.
	5. ¿Con qué personal especializado cuenta para análisis de metadatos?	Personal limitado por infraestructura.	Un ingeniero sin capacitación específica.	Personal con experiencia básica.	Sin personal especializado.	Personal limitado.	Sin personal especializado.	Personal con capacitación básica.	Personal técnico específico.	Personal capacitado.	Departamento de análisis sin capacitación específica.	Grave carencia de personal especializado en manejo de metadatos de localización.
	6. ¿Qué capacitación requiere el personal para manejar metadatos?	Herramientas tecnológicas.	IBM i2, desarrollo software.	Software SIG y análisis datos.	Capacitación integral.	Capacitación especializada.	Capacitación técnica.	Capacitación específica.	Capacitación técnica.	Capacitación actualizada.	Requiere capacitación en manejo metadatos de localización.	Urgente necesidad de capacitación técnica especializada en metadatos de localización.
	7. ¿Qué capacidad de almacenamiento tiene para evidencia digital?	Muy limitada, sin banco de datos.	Servidor de 5TB insuficiente.	No específica.	Sin capacidad.	Muy limitada.	Capacidad básica.	Insuficiente.	Capacidad específica.	Capacidad limitada.	Sin equipos de almacenamiento de evidencia digital.	Capacidad de almacenamiento insuficiente en todas las unidades.
	8. ¿Cómo afecta la falta de acceso a metadatos históricos?	Limita vinculación con delitos pasados.	Afecta comparativas históricas.	Dificulta patrones delictivos.	Afecta investigación.	Impacta negativamente.	Afecta seguimiento.	Afecta análisis criminal.	Limita investigación.	Impacta eficacia.	Afecta trazabilidad de líneas y desarticulación bandas.	Impacto crítico en identificación patrones, vinculación histórica delitos y desarticulación bandas criminales.
Gestión de Evidencia Digital	1. ¿Qué protocolos aplica para el manejo de evidencia digital?	Manual para recojo de evidencia digital.	Protocolos de cadena custodia.	Recolección y custodia básica.	No específica.	Manual de análisis de evidencia digital.	Manual de procedimientos.	Protocolos de actuación conjunta.	Mínima intervención documentada.	Protocolos con fiscalía.	Protocolo general de MP sin detalles.	Falta protocolos específicos para metadatos de localización; uso procedimientos genéricos con alta dependencia de la DIVINDAT.
	2. ¿Cómo asegura la cadena de custodia de evidencia digital?	Generación de hash.	Documentación y hash.	Numeración y registro.	No específica.	Procedimientos de código procesal.	Actas y lacrado.	Cadena de custodia digital.	Control de acceso restringido.	Procedimientos del MP.	Descripción y lacrado en sobres.	Procedimientos básicos sin estándares específicos para metadatos.
	3. ¿Qué estándares utiliza para validar integridad de evidencia digital?	Ninguno específico.	Hash SHA-256.	Procedimientos básicos.	No específica.	Estándares básicos.	No específica.	Software de validación.	Control técnico.	Validación del sistema.	Depende de la DIVINDAT para validación.	Falta de estándares técnicos unificados para validación.
	4. ¿Qué controles de calidad implementa?	Ninguno específico.	Auditorías periódicas.	Seguimiento y protocolos.	No específica.	Verificación técnica.	Básicos.	Control de acceso.	Verificación técnica.	Auditorías.	No realiza controles propios	Controles de calidad insuficientes y no estandarizados.
	5. ¿Cómo documenta el proceso de obtención y análisis?	Informes técnicos.	Informes detallados.	Actas e informes.	No específica.	Informes y actas.	Documentación básica.	Informes técnicos.	Actas y oficios.	Documentación estándar.	Informes de la DIVINDAT y actas de lectura y análisis.	Documentación no estandarizada para metadatos.
Protección de Derechos Fundamentales	1. ¿Qué normas aplican al manejo de metadatos?	Ley 31284 y 30096.	Normas de protección datos.	Normativa vigente.	No específica.	Marco constitucional.	Normas básicas.	Leyes vigentes.	Normativa actual.	Marco legal vigente.	Solo autorización del usuario o mandato judicial.	Ausencia normativa específica para metadatos de localización aunque existe percepción de bajo impacto en privacidad.
	2. ¿Qué mecanismos de supervisión implementa?	Auditorías.	Controles internos.	No específica.	No tiene.	Supervisión básica.	Controles básicos.	Supervisión periódica.	Control interno.	Mecanismos estándar.	Sin mecanismos de supervisión propios.	Supervisión inadecuada para el control de metadatos.
	3. ¿Qué sanciones aplica por mal uso?	Disciplinarias.	Administrativas.	Penales y administrativas.	No específica.	Según normativa.	Básicas.	Sanciones vigentes.	Procedimientos .	Marco legal.	No específica.	Falta de régimen sancionador específico.
	4. ¿Qué criterios de proporcionalidad aplica?	Flagrancia y mandato judicial.	Necesidad investigativa.	No específica.	Básicos.	Según normativa.	Criterios básicos.	Marco legal.	Estándares vigentes.	Criterios MP.	Considera que no afecta la privacidad solo la ubicación.	Falta criterios específicos para gestión y uso de metadatos.
Cooperación Interinstitucional	1. ¿Qué mecanismos de coordinación utiliza?	Relaciones de confianza.	Grupos de trabajo.	No específica.	Coordinación básica.	Protocolos del MP.	Coordinación directa.	Reuniones de trabajo.	Coordinación técnica.	Protocolos establecidos.	Coordinación con MP y consultas a operadoras.	Falta mecanismos formales para compartir metadatos y necesidad establecer plazos entrega operadoras
	2. ¿Cómo comparte información entre instituciones?	Correos institucionales.	Plataformas digitales.	Acuerdos formales.	No específica.	Canales oficiales.	Comunicación directa.	Sistemas compartidos.	Canales formales.	Protocolos vigentes.	Solo compartida con MP por reserva investigación.	Ausencia de sistema unificado de intercambio de metadatos.
	3. ¿Qué protocolos conjuntos aplica?	Vigentes.	Estandarizados.	Formales.	No específica.	Protocolos MP.	Básicos.	Protocolos trabajo.	Protocolos técnicos.	Establecidos.	Coordinación con MP para análisis de información.	Falta de protocolos específicos interinstitucionales.
	4. ¿Qué formatos de intercambio usa?	Correos electrónicos.	Formatos estándar.	No específica.	No específica.	Formatos oficiales.	Básicos.	Sistemas propios.	Formatos técnicos.	Establecidos.	Coordinación directa con el MP.	Sin estandarización de formatos para metadatos.

LEYENDA:

PNP 1: Coronel Ángeles -- DIRINCRI PNP

PNP 2: 2 de Angeles -- DIRINCRI PNP

PNP 3: 3 Ángeles -- DIRINCRI PNP

PNP 4: Silva y Figueroa -- DIRINCRI PNP

PNP 5: Coronel Eric Angeles -- DIRINCRI PNP

PNP 6: Comandante Gerardo Ramírez -- DEPINCRI APOLO

PNP 7: Comandante Mario Carrasco -- DIVINDAT

PNP 8: Sub Oficial Romero Bejarano -- Programa Constelación

PNP 9: Coronel Victor Morales -- Programa Constelación

PNP 10: Comantante Jesús Saavedra - División de Robos

MATRIZ DE ANÁLISIS DE ENTREVISTAS DEL MINISTERIO PÚBLICO SOBRE CAPACIDADES Y NECESIDADES EN EL USO Y VALORACIÓN PROBATORIA DE METADATOS DE LOCALIZACIÓN DE DISPOSITIVOS MÓVILES PARA POTENCIAR LA INVESTIGACIÓN CRIMINAL

Categorías	Preguntas	MP 1	MP 2	MP 3	MP 4	MP 5	PNP 6	Hallazgos Clave
Capacidades de Investigación Criminal	1. ¿Qué sistemas de análisis digital utiliza actualmente?	Centro de criminalística con peritos informáticos y acústicos. Solo lectura celulares y pericia fonética.	Gerencia Peritajes MP y laboratorio UFE con ingenieros TIC.	CIAC y sistemas básicos de análisis criminal.	Sistemas básicos sin capacidad especializada.	Sistema de análisis criminológico - CIAC	Oficina de peritajes con Cellebrite, UFE con Velkasoft.	Capacidades limitadas a análisis forense básico, sin sistemas específicos para metadatos de localización.
	2. ¿Qué limitaciones encuentra en herramientas tecnológicas?	Software no actualizado y falta de equipos de última generación.	Falta renovación licencias y software especializados.	Personal no capacitado y sistemas desactualizados.	Limitaciones presupuestales y técnicas severas.	Limitaciones en personal capacitado y sistemas.	Actualizaciones de herramientas y certificaciones. Solo versión básica de Cellebrite.	Severas limitaciones en licencias, actualizaciones y capacidades técnicas.
	3. ¿Qué capacidad tiene para analizar grandes volúmenes datos?	Ninguna capacidad específica.	Capacidad limitada sin software especializado.	Muy limitada, sin análisis automatizado.	Capacidad básica sin herramientas específicas.	Consolidación manual sin capacidad análisis masivo.	Depende de la herramienta y capacidad del perito.	Capacidad prácticamente nula para análisis de grandes volúmenes de metadatos.
	4. ¿Qué herramientas adicionales requiere?	Herramientas informáticas para localización precisa.	Software de análisis forense actualizado.	Analistas de datos y sistemas especializados.	Sistemas actualizados y personal capacitado.	Analista de datos y sistemas modernos.	Sistemas para procesar grandes volúmenes de datos.	Necesidad crítica de sistemas especializados y personal técnico, así como, versiones integrales o premium de software forense.
	5. ¿Con qué personal especializado cuenta?	Ninguno especializado en metadatos.	Dos ingenieros TIC sin especialización en metadatos.	Personal básico sin especialización.	Personal limitado sin capacitación específica.	Personal sin capacitación específica.	No tiene en despacho, usa peritos del MP y 2 ingenieros UFE.	Carencia general de personal especializado en metadatos.
	6. ¿Qué capacitación requiere el personal?	Capacitación básica en manejo metadatos.	Capacitación técnica especializada.	Capacitación integral en análisis de datos.	Capacitación técnica y normativa.	Capacitación técnica especializada.	Necesita de equipo multidisciplinario (ingenieros, técnicos y otros).	Urgente necesidad de capacitación técnica especializada y conformación de equipos multidisciplinarios.
	7. ¿Qué capacidad almacenamiento tiene?	Mínima capacidad.	Limitada a CDIs básicos.	Muy limitada sin repositorio central.	Capacidad básica insuficiente.	No tienen mucha capacidad almacenamiento.	Limitado a 4 discos de 1 a 2TB. Sugiere almacenamiento en nube.	Capacidad de almacenamiento insuficiente en todas las fiscalías. Se sugiere implementar almacenamiento en nube.
	8. ¿Cómo afecta falta metadatos históricos?	Afecta la celeridad de las investigaciones.	Impacta negativamente la probanza.	Pérdida de información valiosa.	Afecta severamente las investigaciones.	Afecta la investigación y la prueba.	Retrasa investigaciones, dificulta el rastreo e identificación.	Impacto crítico en eficacia investigativa y probatoria.
Gestión de Evidencia Digital	1. ¿Qué protocolos aplica para manejo de evidencia digital?	Protocolo del Instituto Medicina Legal, criterios básicos.	Protocolos de ciberdelincuencia y guía práctica internacional.	Protocolos MP y cadena custodia.	Protocolos de actuación conjunta.	Protocolos con guías prácticas.	Aplica Guía de Análisis Digital Forense de Fiscalía y Reglamento Cadena de Custodia.	Diversos protocolos sin estandarización específica para metadatos y guías específicas de análisis forense.
	2. ¿Cómo asegura cadena de custodia?	Imagen y backup.	Valor hash y calculadoras especializadas.	Cadena custodia digital específica.	Hash y documentación detallada.	Sellado y etiquetado.	Identificación, lacrado, actas, formatos.	Procedimientos básicos enfocados en hash y documentación.
	3. ¿Qué estándares usa para validar integridad?	No tiene específicos.	SHA 256 y validadores estándar.	Hash y técnica de verificación.	Códigos hash y peritajes.	Auditoría interna.	Código hash, desconoce ISOs aplicados.	Predominio del uso del hash sin estándares avanzados. Necesidad de certificación ISO.
	4. ¿Qué controles de calidad implementa?	Controles de peritos.	Verificación de fuente y conservación datos.	Validación de peritos.	Controles técnicos básicos.	Control de peritos e ISO.	Sugiere guía específica con estándares internacionales.	Controles básicos sin protocolos específicos metadatos. Sugieren estándares internacionales.
	5. ¿Cómo documenta proceso y análisis?	Informes periciales.	Documentación paso a paso.	Informes técnicos detallados.	Documentación exhaustiva.	Actas e informes.	Actas fiscales detalladas e informe pericial.	Documentación tradicional sin formato específico metadatos.
Valoración Probatoria	1. ¿Qué criterios aplica para admitir metadatos?	Ninguno, no manejan metadatos.	Relevancia, autenticidad y legalidad.	Cadena custodia y validación.	Test de proporcionalidad.	Relevancia y autenticidad.	Pertinencia y utilidad de la información para la investigación.	Falta criterios uniformes para admisión metadatos.
	2. ¿Qué valor probatorio otorga a metadatos?	No definido aún.	Alto valor si es autenticado.	Fuerte valor probatorio.	Alto valor si es validado.	Valor probatorio alto.	Alto si se descarta manipulación y hay corroboración.	Alto valor potencial sujeto a validación. Depende de la corroboración con otros elementos.
	3. ¿Qué requisitos formales exige?	Los establecidos por PJ.	Cadena custodia y autenticación.	Validación técnica.	Obtención legal y validación.	Protocolos de validación.	Asegurar cadena de custodia y trazabilidad.	Énfasis en cadena custodia y validación técnica.
	4. ¿Cómo verifica autenticidad?	No aplica actualmente.	Hash y verificación técnica.	Peritajes especializados.	Validación pericial.	Verificación técnica.	A través de peritajes y corroboración con otros elementos.	Dependencia de validación técnica y pericial, y corroboración con otros elementos probatorios.
	5. ¿Qué mecanismos usa para detectar manipulaciones?	No tiene específicos.	Análisis forense.	Peritajes técnicos.	Análisis especializado.	Controles técnicos.	Solo corroboración con otros datos, requiere perito especializado.	Falta mecanismos específicos para metadatos.
	6. ¿Qué debilidades probatorias identifica?	Falta de tecnología y personal especializado.	Autenticación y validación.	Falta estándares.	Capacidad técnica limitada.	Validación técnica.	Falta capacitación en manejo evidencias digitales y extracción información.	Debilidades técnicas y de validación. Falta de capacitación en manejo de evidencia digital.
	7. ¿Qué valor específico en crimen organizado?	Potencialmente alto.	Fundamental con validación.	Muy alto valor probatorio.	Crítico con validación.	Alto valor evidenciario.	Alto si cumple protocolos y tiene corroboración.	Alto valor potencial para crimen organizado, con necesaria corroboración.
Protección de Derechos Fundamentales	1. ¿Qué normas aplican al manejo?	Marco constitucional básico.	Normativa procesal penal.	Marco legal vigente.	Normas procesales.	Normativa actual.	Constitución, Código Procesal Penal, Ley Protección Datos Personales.	Marco normativo insuficiente para metadatos.
	2. ¿Qué vacíos normativos identifica?	Falta regulación específica.	Vacíos en retención datos.	Regulación incompleta.	Falta marco específico.	Normativa inadecuada.	Falta de obligación legal para que proveedores resguarden datos de localización IP.	Vacíos críticos en regulación de metadatos de localización, especialmente en proveedores de servicios de internet.
	3. ¿Qué aspectos críticos en autorización?	Test de proporcionalidad.	Fundamentación de necesidad.	Justificación técnica.	Proporcionalidad medida.	Justificación legal.	Desconocimiento de la autoridad judicial sobre nuevos elementos de convicción tecnológicos.	Énfasis en proporcionalidad y necesidad. Desconocimiento judicial de elementos tecnológicos.
	4. ¿Cómo evalúa necesidad vs privacidad?	Ponderación de derechos.	Balance de intereses.	Análisis en cada caso concreto.	Test de proporcionalidad.	Evaluación de derechos.	Idoneidad y necesidad de la medida, inexistencia de medio alternativo.	Predominio enfoque ponderación derechos.
Cooperación Interinstitucional	1. ¿Qué mecanismos coordinación usa?	Coordinación PNP, MP y PJ.	Protocolos conjuntos.	Reuniones de coordinación.	Mecanismos formales.	Protocolos de trabajo.	Coordina con RENIEC, PCM, Secretaría Digital, cooperación internacional entre ministerios públicos.	Mecanismos formales sin protocolo metadatos incluyendo cooperación internacional entre ministerios públicos.
	2. ¿Cómo comparte información?	Canales oficiales.	Sistemas formales.	Vías institucionales.	Procedimientos establecidos.	Canales formales.	Solo con PNP, con otras entidades son colaboraciones.	Falta sistema unificado para uso de metadatos. Necesidad de interoperabilidad de sistemas institucionales.
	3. ¿Qué protocolos conjuntos aplica?	Protocolos básicos.	Guías de actuación.	Protocolos vigentes.	Procedimientos conjuntos.	Protocolos de trabajo.	Buena coordinación dependiendo de la unidad.	Ausencia protocolos específicos para uso de metadatos.
	4. ¿Qué formatos intercambio usa?	Formatos estándar.	Documentos oficiales.	Formatos institucionales.	Documentación formal.	Formatos establecidos.	Necesidad de interoperabilidad con otras entidades.	Sin estandarización para gestión y uso de metadatos. Necesidad de interoperabilidad de sistemas institucionales.

LEYENDA:

MP 1: Dr. Chávez Cotrina - Fiscal Superior Coordinador Fiscalías Especializadas Crimen Organizado

MP 2: Dr. González Farfán - Fiscal Provincial Primer Despacho Ciberdelincuencia Lima Centro

MP 3: Dra. Mori Anton - Fiscal Provincial Penal Fiscalía Especializada Crimen Organizado

MP 4: Dr. Rodas Farro - Fiscal Provincial Primera Fiscalía Supraprovincial Corporativa Crimen Organizado

MP 5: Dra. Mercado Zavala - Fiscal Provincial Penal Segundo Despacho Fiscalía Especializada Crimen Organizado

MP 6: Dra. Flores Mariñas - Fiscal Provincial Tercera Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro

MATRIZ DE ANÁLISIS DE REQUERIMIENTOS TÉCNICOS E IMPLEMENTACIÓN DEL SISTEMA DE METADATOS DE LOCALIZACIÓN DE DISPOSITIVOS MÓVILES - ENTREVISTA AL ASESOR TÉCNICO DEL PROGRAMA CONSTELACIÓN

Categorías	Preguntas	Respuesta PNP 10	Hallazgos Clave
Procesamiento y Capacidades Técnicas	1. ¿Qué infraestructura considera necesaria para procesar metadatos de localización?	Se requiere infraestructura modesta pero robusta, centralizada para las cuatro operadoras. Se podria aprovechar en gran parte la infraestructura y equipamiento del Programa Constelación.	Necesidad de sistema centralizado con capacidad de integración con operadoras, como el Programa Constelación.
	2. ¿Qué limitaciones técnicas deberíamos anticipar?	Principal limitación: promulgación de norma de retención de metadatos, coordinación efectiva entre operadoras, y tiempo de respuesta.	Desafíos normativos y coordinación interinstitucional críticos.
	3. ¿Qué capacidad de procesamiento recomendaría?	Sistema dimensionado para procesar datos de líneas móviles activas por lo menos de tres meses.	Necesidad de procesamiento para 3 meses de datos mínimo.
	4. ¿Qué capacidad de almacenamiento sugiere?	Almacenamiento para 3 meses, con sistema de depuración automática.	Sistema almacenamiento temporal con depuración automática.
	5. ¿Qué perfil de personal especializado recomienda?	Personal con experiencia en sistemas, bases de datos y análisis geoespacial.	Personal técnico especializado en análisis geoespacial necesario
	6. ¿Qué capacitación considera esencial?	Capacitación enfocada en análisis de patrones de localización y normativa.	Formación técnica y legal específica requerida.
	7. ¿Qué medidas de seguridad sugiere?	Sistema de seguridad centralizado con accesos por operadoras.	Seguridad centralizada y tambien con control por cada entidad.
	8. ¿Qué controles de acceso recomienda?	Control de accesos por entidades y nivel de autorización de doble factor.	Necsario un sistema de autenticación robusto multinivel.
Gestión de Evidencia Digital	1. ¿Qué protocolos sugiere para manejo de metadatos?	Protocolo único y simple para las cuatro operadoras.	Estandarización de protocolos entre PNP, MP y operadoras.
	2. ¿Cómo recomienda asegurar cadena de custodia?	Cadena de custodia digital con responsables por operadora.	Cadena custodia digital con responsabilidades definidas.
	3. ¿Qué estándares considera para validar integridad?	Estándares básicos de hash y firma digital.	Validación mediante hash y firma digital.
	4. ¿Qué controles de calidad sugiere?	Verificación automática diaria de integridad.	Es necesario un control automático de integridad.
	5. ¿Cómo recomienda documentar el proceso?	Sistema unificado de registro y trazabilidad.	Sistema centralizado de documentación y tramite.
Protección de Derechos Fundamentales	1. ¿Qué normas considera aplicables?	Aplicar normativa actual de localización y geolocalización, telecomunicaciones y datos personales.	Marco normativo existente como base.
	2. ¿Qué aspectos considera críticos para autorización?	Autorización judicial oportuna expedita para delitos violentos	Urge un proceso ágil de autorización judicial.
	3. ¿Qué desafíos legales prevé?	Principal reto: tiempo de respuesta en emergencias.	La optimización de los tiempos respuesta es crítica.
	4. ¿Qué criterios de proporcionalidad sugiere?	Priorizar casos de delitos violentos en curso.	Enfoque en delitos violentos en ejecución.
Cooperación Interinstitucional	1. ¿Qué mecanismos de coordinación recomienda?	Comité técnico PNP-MP-Operadoras.	La coordinación técnica multisectorial es necesaria.
	2. ¿Cómo sugiere estructurar el intercambio?	Plataforma única de obtención de mandatos judiciales y de intercambio de información.	Sistema unificado de gestión.
	3. ¿Qué protocolos conjuntos considera necesarios?	Protocolo simple de solicitud-respuesta.	Estandarización de procesos de comunicación interinstitucional.
	4. ¿Qué indicadores sugiere para evaluar efectividad?	Medir tiempo de respuesta en casos urgentes.	Métricas de tiempos de respuesta en cada entidad.
	5. ¿Qué formatos de intercambio recomienda?	Formato único.	Estandarización de formatos.
	6. ¿Cómo sugiere asegurar compatibilidad?	Sistema web centralizado con módulos por institución.	Sistema modular centralizado (PNP, MP).
	7. ¿Qué otros aspectos técnicos considera importantes?	Considerar futuras integración con sistemas similares.	Escalabilidad e interoperabilidad futuras

LEYENDA:

PNP 10: Comandante en retiro Luis López -- Asesor en el Programa Constelación

Anexo 15: Matriz de Evaluación Multicriterio para Priorización de Propuestas

Criterios de Evaluación y Ponderaciones:

Criterio	Ponderación	Descripción
Viabilidad Legal	25%	Compatibilidad constitucional y normativa, probabilidad de aprobación legislativa.
Factibilidad Técnica	25%	Capacidad de implementación con recursos disponibles, infraestructura existente.
Impacto Potencial	30%	Efectividad proyectada en investigación criminal basada en experiencias internacionales.
Protección de Derechos Fundamentales	20%	Solidez de salvaguardas, mecanismos de protección de privacidad y supervisión.

Matriz de Evaluación Detallada:

Propuesta	Viabilidad Legal (25%)		Factibilidad Técnica (25%)		Impacto Potencial (30%)		Protección Derechos (20%)		Puntaje Final
	Punt.	Pond.	Punt.	Pond.	Punt.	Pond.	Punt.	Pond.	
SNML	2.0	0.50	2.5	0.63	4.5	1.35	2.0	0.40	2.75/5.00
SIGMEL	4.0	1.00	4.5	1.13	4.0	1.20	4.0	0.80	4.05/5.00
SAD	5.0	1.25	3.0	0.75	2.5	0.75	4.5	0.90	3.50/5.00

Justificación de Puntuaciones:

SIGMEL (Ganador - 4.05/5.00):

- Viabilidad Legal (4.0): Aprovecha infraestructura existente, requiere marco legal específico, pero políticamente viable.
- Factibilidad Técnica (4.5): Utiliza Programa Constelación establecido, integración factible.
- Impacto Potencial (4.0): Alto impacto demostrado en experiencias internacionales similares.
- Protección Derechos (4.0): Controles robustos y supervisión judicial establecida.

Metodología de Evaluación:

- Escala: 1-5 puntos por criterio.
- Evaluadores: Panel de 11 expertos institucionales.
- Consenso: Mediante técnica Delphi modificada.
- Validación: Revisión por pares académicos especializados.

Anexo 16: Síntesis de Sesiones de Co-creación - Proceso SIGMEL

SESIONES CON POLICÍA NACIONAL DEL PERÚ

- Número de sesiones: 3 sesiones estructuradas.
- Participantes: 8 especialistas (DIRINCRI PNP, analistas de inteligencia, Programa Constelación).
- Duración: 2 horas promedio por sesión.
- Metodología: Design thinking con técnicas de mapeo de experiencias.
- Productos obtenidos: Requerimientos técnicos operativos específicos, Flujos de trabajo investigativo optimizados, Protocolos de seguridad de información, Identificación de limitaciones actuales en análisis de metadatos.

SESIONES CON MINISTERIO PÚBLICO

- Número de sesiones: 2 sesiones especializadas.
- Participantes: 2 fiscales especializados en crimen organizado.
- Duración: 90 minutos por sesión.
- Metodología: Análisis de casos paradigmáticos y storytelling.
- Productos obtenidos: Criterios específicos de valoración probatoria para evidencia digital, Estándares rigurosos de cadena de custodia digital, Procedimientos de autorización judicial equilibrados, Protocolos de supervisión fiscal sobre uso de sistemas.

SESIONES CON EXPERTO TÉCNICO DEL PROGRAMA CONSTELACIÓN

- Número de sesiones: 2 sesiones intensivas.
- Duración: 3 horas cada sesión.
- Metodología: Validación técnica y simulación de integración.
- Productos obtenidos: Validación de capacidades existentes de procesamiento y almacenamiento, Identificación de requerimientos de integración con operadoras, Diseño general del sistema aprovechando infraestructura instalada, Definición de protocolos de respaldo y recuperación de datos.

SÍNTESIS DE CONVERGENCIAS IDENTIFICADAS:

- Necesidad crítica de acceso oportuno a metadatos históricos.
- Requerimientos unánimes de confidencialidad y seguridad.
- Demanda de sistema seguro y eficiente de gestión.
- Urgencia de marco legal específico para seguridad jurídica.

Anexo 17: Protocolo de Retención Masiva de Metadatos de Localización

1. OBJETO Y ALCANCE

El presente protocolo desarrolla operativamente las obligaciones establecidas en los artículos 4, 5, 6 y 7 del Proyecto de Ley de Retención y Acceso a Metadatos de Localización, definiendo los procedimientos técnicos y administrativos que deben implementar las empresas operadoras de telecomunicaciones y el Programa Constelación para el cumplimiento de la retención masiva de metadatos de localización.

2. RESPONSABILIDADES OPERADORAS DE TELECOMUNICACIONES

2.1. Sistemas de Captura y Almacenamiento

Las operadoras implementarán sistemas automatizados que capturen y almacenen los siguientes metadatos conforme al artículo 5 del proyecto de ley:

- Registro continuo de eventos de localización cada 300 segundos como máximo.
- Captura de coordenadas GPS cuando el dispositivo las genere.
- Identificación automática de cambios de estación base transceptora.
- Registro de eventos de conexión y desconexión a la red.
- Otros similares de acuerdo a la tecnología utilizada.

2.2. Arquitectura de Seguridad

Conforme al artículo 7, las operadoras mantendrán:

- Servidores dedicados físicamente.
- Encriptación AES-256 para datos en reposo y en tránsito.
- Acceso restringido mediante autenticación multifactor.
- Logs detallados de todas las actividades del sistema.

2.3. Mecanismo de Eliminación Automática

- Configuración de eliminación automática a los 90 días exactos de generación del metadato.
- Proceso diario automatizado de purga a las 00:00 horas.
- Generación de reportes de eliminación para auditoría.
- Imposibilidad técnica de recuperación posterior a la eliminación.

3. RESPONSABILIDADES DEL PROGRAMA CONSTELACIÓN

3.1. Sistema de Recepción y Almacenamiento Extendido

El Programa Constelación integrara en su plataforma:

- Recepción segura de los metadatos de localización desde las operadoras de telecomunicaciones.
- Almacenamiento por período extendido de hasta 180 días.
- Clasificación automática por relevancia investigativa.
- Integración con el sistema de intervención legal de las comunicaciones.

3.2. Sistema de Etiquetado para Información Crítica

- Clasificación automática: “RELEVANTE” para investigaciones urgentes.
- Etiquetado temporal según autorización judicial vigente.
- Sistema de alertas para próximos vencimientos.

3.3. Protocolo de Eliminación Diferenciada

- Eliminación automática de datos a los 180 días.
- Conservación de datos "RELEVANTE" según disposición judicial.
- Procedimiento de revisión mensual de clasificaciones.
- Eliminación forzosa al término del plazo.

4. PROCEDIMIENTOS DE COORDINACIÓN TÉCNICA

4.1. Interfaz de Transmisión Operadoras-Programa Constelación

- Protocolo con certificados digitales específicos.
- Transmisión en tiempo real de los metadatos dispuestos por mandaato judicial.
- Verificación automática de integridad mediante checksums.
- Generación del hash.
- Sistema de confirmación de recepción exitosa.

4.2. Formato Estandarizado de Datos

REGISTRO_METADATO = {
  MSISDN: [Número telefónico]
  IMEI: [Identificador equipo]
  IMSI: [Identificador SIM]
  TIMESTAMP: [YYYY-MM-DD HH:MM:SS]
  LAT_LONG: [Coordenadas GPS si disponible]
  CELL_ID: [Identificador estación base]

AZIMUTH: [Sector antena]
OPERADORA: [Código operadora]
TÉCNICA: [utilizada para obtener la localización]
TIPO_EVENTO: [CONEXION/UBICACION/DESCONEXION]
}

5. MECANISMOS DE CONTROL Y AUDITORÍA

5.1. Auditorías Automáticas

- Verificación diaria de integridad de datos almacenados.
- Controles de acceso registrados en logs inmutables.
- Alertas automáticas por accesos no autorizados.
- Reportes semanales de funcionamiento del sistema.

5.2. Supervisión de Cumplimiento

- Inspecciones semestrales por la Inspectoría General PNP.
- Verificación semestral de sistemas de eliminación.
- Auditorías anuales de seguridad.
- Reportes de transparencia según artículo 17 del proyecto de ley.

Anexo 18: Protocolo de Autorización Digital

1. FUNDAMENTO LEGAL

El presente protocolo operativiza los procedimientos establecidos en los artículos 8, 9, 10 y 11 del Proyecto de Ley, aplicando supletoriamente lo dispuesto en el artículo 230 y 231 del Código Procesal Penal para el levantamiento del secreto de las comunicaciones.

2. SISTEMA DIGITAL DE GESTIÓN DE AUTORIZACIONES

2.1. Plataforma Tecnológica Integrada

El sistema digital contemplado en el artículo 10 del proyecto de ley operará mediante:

- Plataforma web segura accesible desde terminales autorizadas en la PNP y el MP.
- Integración con sistemas del Poder Judicial, Ministerio Público y PNP.
- Interfaz diferenciada según el rol institucional del usuario.
- Trazabilidad completa de todas las transacciones o actuaciones.

2.2. Módulos Operativos del Sistema

- **Módulo de Solicitud:** Para investigadores PNP y fiscales.
- **Módulo de Evaluación:** Para fiscales y jueces.
- **Módulo de Ejecución:** Para el Programa Constelación.
- **Módulo de Supervisión:** Para órganos de control.

3. PROCEDIMIENTO DE SOLICITUD POLICIAL

3.1. Formulario Digital Estandarizado

Los investigadores PNP iniciará el proceso completando:

SOLICITUD DE ACCESO A METADATOS - FORMULARIO PNP

A. DATOS DE LA INVESTIGACIÓN

- N° Carpeta Fiscal: [_____]
- Delito Investigado: [_____]
- Fecha del Hecho: [DD/MM/AAAA]
- Lugar del Hecho: [_____]

B. DATOS DEL SOLICITANTE

- Grado y Nombres: [_____]
- Unidad PNP: [_____]
- DNI/CIP: [_____]

C. METADATOS SOLICITADOS

- Números (MSISDN/IMSI/IMEI/Otros): [_____]
- BTS o similares: [_____]
- Período temporal: Del [DD/MM/AAAA] al [DD/MM/AAAA]
- Tipo de información: [ ] Localización [ ] Movimientos [ ] Abonados

D. FUNDAMENTACIÓN

- Relevancia para la investigación: [Máximo 500 caracteres]
- Urgencia del requerimiento: [ ] Ordinario [ ] Urgente
- Los demás considerados en los artículos 230 y 231 del Codigo Procesal Penal: [Máximo 1024 caracteres]

3.2. Validaciones Automáticas del Sistema

- Verificación de credenciales del solicitante.
- Validación de carpeta fiscal activa.
- Confirmación de competencia territorial.
- Verificación de plazos de retención disponibles.

4. PROCEDIMIENTO DE EVALUACIÓN FISCAL

4.1. Criterios Predefinidos de Evaluación

El fiscal evaluará mediante lista de verificación digital:

EVALUACIÓN FISCAL - LISTA DE VERIFICACIÓN

☐ Vinculación del metadato con la investigación formal.

☐ Proporcionalidad entre medida y gravedad del delito.

☐ Subsidiariedad (no existen medios menos lesivos).

☐ Delimitación temporal adecuada.

☐ Especificación precisa de información requerida.

☐ Fundamentación jurídica suficiente.

☐ Las demás establecidas en los artículos 230 y 231 del Código Procesal Penal.

DECISIÓN FISCAL:

☐ APRUEBO y derivo a autorización judicial.

☐ OBSERVO y solicito subsanación.

☐ DESAPRUEBO por improcedencia (Detalles).

4.2. Plazos de Evaluación

- Casos ordinarios: 24 horas calendario.
- Casos urgentes: 6 horas calendario.
- Notificación automática al solicitante por el sistema.

5. PROCEDIMIENTO DE AUTORIZACIÓN JUDICIAL

5.1. Derivación Automática al Juzgado Competente

El sistema identificará automáticamente:

- Juzgado de investigación preparatoria competente.
- Juez de turno según calendario judicial.
- Expediente electrónico correspondiente.
- Precedencia según urgencia del caso.

5.2. Resolución Judicial Motivada

El juez emitirá resolución especificando:

- Metadatos específicos autorizados.
- Período temporal autorizado.
- Plazo de vigencia de la autorización.
- Condiciones especiales si las hubiere.

6. PROCEDIMIENTO DE EJECUCIÓN

6.1. Coordinación con Programa Constelación

- Notificación automática de autorización judicial.
- Generación de orden de ejecución digital.
- Asignación a analista certificado disponible.
- Programación en cola de procesamiento.

6.2. Tiempos de Ejecución Comprometidos

- Casos ordinarios: 24 horas máximo.
- Casos urgentes: 4 horas máximo.
- Entrega de resultados vía sistema seguro.
- Notificación automática a fiscal y PNP.

7. CASOS DE URGENCIA Y PELIGRO INMINENTE

Conforme al artículo 12 del proyecto de ley:

7.1. Acceso Inmediato Sin Autorización Previa

- Activación por fiscal mediante código de emergencia.
- Documentación simultánea de fundamentos.
- Acceso inmediato por analista de turno 24/7.
- Solicitud de convalidación judicial dentro de 24 horas.

7.2. Controles Especiales para Casos de Urgencia

- Notificación inmediata a Órgano de Control Interno MP.
- Registro especial en sistema de auditoría.
- Supervisión posterior obligatoria.
- Responsabilidad personal del fiscal actuante.

Anexo 19: Protocolo de Análisis y Uso

1. OBJETO Y MARCO LEGAL

El presente protocolo desarrolla los procedimientos técnicos para el análisis, uso y valoración probatoria de metadatos de localización obtenidos conforme a la autorización judicial correspondiente, garantizando la cadena de custodia digital y la integridad de la evidencia.

2. PERSONAL ESPECIALIZADO CERTIFICADO

2.1. Requisitos para Analistas de Metadatos

Conforme a las disposiciones complementarias del proyecto de ley:

- Certificación vigente en análisis de metadatos de localización.
- Formación en herramientas de análisis geoespacial.
- Conocimiento de protocolos de cadena de custodia digital.
- Evaluación de confiabilidad completada satisfactoriamente.

2.2. Asignación y Distribución de Casos

- Asignación automática según disponibilidad y especialización.
- Máximo 16 casos simultáneos por analista.
- Rotación quincenal para evitar sobrecarga.
- Supervisión directa por jefe de Sala u Grupo.

3. PROCEDIMIENTOS DE ANÁLISIS ESPACIOTEMPORAL

3.1. Metodología de Análisis Geográfico

Los analistas aplicarán técnicas estandarizadas:

PROCESO DE ANÁLISIS GEOESPACIAL

1. PREPARACIÓN DE DATOS

- Importación de metadatos autorizados.
- Verificación de integridad temporal.
- Depuración de datos inconsistentes.
- Georreferenciación de coordenadas.

2. ANÁLISIS DE PATRONES DE MOVILIDAD

- Identificación de rutas frecuentes.
- Detección de puntos de permanencia.
- Análisis de horarios de actividad.
- Correlación con eventos investigados.

3. ANÁLISIS DE PROXIMIDAD TEMPORAL

- Identificación de dispositivos en área objetivo.
- Análisis de simultaneidad temporal.
- Detección de patrones de seguimiento.
- Identificación de encuentros múltiples.

4. ANÁLISIS DE REDES DE CONTACTO

- Identificación de dispositivos próximos recurrentes.
- Mapeo de redes de asociación criminal.
- Análisis de jerarquías en movimientos.
- Detección de roles operativos.

3.2. Herramientas Tecnológicas Autorizadas

- Software de análisis geoespacial certificado.
- Sistemas de información geográfica (GIS) especializados.
- Plataformas de análisis de big data temporal.
- Herramientas de visualización de patrones.

4. ELABORACIÓN DE ACTAS PERICIALES ESTANDARIZADAS

4.1. Estructura del Acta Pericial Digital

ACTA PERICIAL DE ANÁLISIS DE METADATOS

I. DATOS GENERALES

- Autorización Judicial N°: [_____]
- Exp N°: [_____]
- Analista: [Grado, Nombres, N° Certificación]
- Fecha de Análisis: [DD/MM/AAAA]
- Período Analizado: [DD/MM/AAAA al DD/MM/AAAA]

II. DATOS TÉCNICOS

- Números analizados: [_____]
- Registros procesados: [_____]
- Herramientas utilizadas: [_____]
- Nivel de precisión: [Metros/Hectómetros/Kilómetros]

III. METODOLOGÍA APLICADA

- Técnicas de análisis empleadas.
- Criterios de filtrado aplicados.
- Validaciones de consistencia realizadas.
- Limitaciones técnicas identificadas.

IV. RESULTADOS DEL ANÁLISIS

- Patrones de movilidad identificados.
- Puntos de interés detectados.
- Correlaciones temporales relevantes.
- Vínculos con hechos investigados.

V. ANEXOS TÉCNICOS

- Mapas de localización.
- Gráficos temporales.
- Tablas de datos relevantes.
- Metadatos de respaldo.

4.2. Estándares de Documentación Técnica

- Registro fotográfico de visualizaciones en pantalla
- Exportación de datos en formatos estándar
- Documentación de parámetros de análisis utilizados
- Respaldo de archivos fuente y procesados

5. CADENA DE CUSTODIA DIGITAL

5.1. Procedimiento de Custodia desde Recepción

REGISTRO DE CADENA DE CUSTODIA DIGITAL

RECEPCIÓN:

Fecha/Hora: [_____] Recibido por: [_____]

Hash SHA-256 original: [_____]

Verificación integridad: [OK/FALLA]

PROCESAMIENTO:

Fecha/Hora inicio: [_____] Analista: [_____]

Software utilizado: [_____] Versión: [_____]

Hash post-procesamiento: [_____]

ALMACENAMIENTO:

Ubicación física: [_____] Ubicación lógica: [_____]

Encriptación aplicada: [_____] Accesos registrados: [N°]

ENTREGA:

Fecha/Hora: [_____] Entregado a: [_____]

Formato de entrega: [_____] Hash final: [_____]

5.2. Controles de Integridad Automatizados

- Generación automática de checksums SHA-256.
- Verificación periódica de integridad de archivos.
- Alertas automáticas por modificaciones no autorizadas.
- Respaldo automático en servidores segregados.

6. INCORPORACIÓN AL EXPEDIENTE INVESTIGATIVO

6.1. Formato de Entrega a Fiscal

- Acta pericial firmada digitalmente (RENIEC).
- Archivo digital con metadatos analizados.
- Anexos gráficos en formato PDF/A.

- Certificación de cadena de custodia completa.

6.2. Protocolo de Sustentación en Audiencia

- Preparación de presentación técnica simplificada.
- Disponibilidad de analista para sustentación oral.
- Explicación metodológica en lenguaje jurídico.
- Respuesta a observaciones de defensa técnica.

7. REGISTRO AUDITABLE DE ACCIONES

7.1. Logs Automáticos del Sistema

Registro continuo de:

- Accesos al sistema por usuario y timestamp.
- Consultas realizadas y parámetros utilizados.
- Exportaciones de datos y destinatarios.
- Modificaciones de configuración del sistema.

7.2. Supervisión y Control de Calidad

- Revisión aleatoria del 10% de análisis realizados.
- Evaluación de calidad por supervisor certificado.
- Detección de patrones atípicos en uso del sistema.
- Reportes de irregularidades al órgano de control competente.

Anexo 20: Programa de Capacitación

1. FUNDAMENTO LEGAL Y OBJETIVOS

Conforme a la Disposición Complementaria Primera del Proyecto de Ley, el presente programa desarrolla la capacitación y certificación obligatoria para todo el personal que tendrá acceso al sistema de retención y acceso a metadatos de localización, garantizando competencias técnicas, legales y éticas adecuadas.

2. ESTRUCTURA DEL PROGRAMA DE CAPACITACIÓN

2.1. Modalidades de Capacitación

- **Capacitación Inicial:** 120 horas académicas obligatorias.
- **Actualización Continua:** 40 horas anuales.
- **Capacitación Especializada:** 80 horas para roles específicos.
- **Recertificación cada tres años:** 60 horas cada tres años.

2.2. Metodología de Enseñanza

- 60% presencial con casos prácticos.
- 30% virtual con simuladores especializados.
- 10% autoaprendizaje con material certificado.
- Evaluación continua y examen final obligatorio.

3. CAPACITACIÓN INICIAL OBLIGATORIA (120 HORAS)

3.1. Módulo I: Marco Legal y Constitucional (30 horas)

CONTENIDO CURRICULAR - MÓDULO LEGAL

Unidad 1: Fundamentos Constitucionales (8 horas)
- Artículo 2° inciso 10 de la Constitución.
- Equilibrio seguridad-privacidad.
- Jurisprudencia del Tribunal Constitucional.
- Estándares internacionales de derechos humanos y privacidad.

Unidad 2: Marco Procesal Penal (12 horas)
- Artículos 230-231 del Código Procesal Penal.

- Procedimientos de autorización judicial.
- Levantamiento del secreto de comunicaciones.
- Valoración probatoria de evidencia digital.

Unidad 3: Ley de Metadatos y Reglamentación (10 horas)
- Análisis artículo por artículo del proyecto de ley.
- Protocolos operativos específicos.
- Obligaciones y responsabilidades institucionales.
- Régimen sancionador aplicable.

3.2. Módulo II: Aspectos Técnicos Especializados (40 horas)

CONTENIDO CURRICULAR - MÓDULO TÉCNICO

Unidad 1: Fundamentos de Telecomunicaciones (12 horas)
- Arquitectura de redes móviles 3G/4G/5G.
- Protocolos de localización celular.
- Sistemas y técnicas de localización de dispositivos móviles.
- Precisión y limitaciones técnicas.

Unidad 2: Análisis de Metadatos (16 horas)
- Tipos de metadatos de localización.
- Herramientas de análisis geoespacial.
- Técnicas de correlación temporal.
- Interpretación de datos de estaciones base y similares.

Unidad 3: Seguridad y Protección de Datos (12 horas)
- Principios de ciberseguridad.
- Encriptación y protección de datos.
- Control de acceso y autenticación.
- Detección de incidentes de seguridad.

3.3. Módulo III: Aspectos Éticos y de Control (25 horas)

CONTENIDO CURRICULAR - MÓDULO ÉTICO

Unidad 1: Ética en Investigación Criminal (10 horas)

- Principios éticos fundamentales.
- Uso responsable de tecnologías de vigilancia.
- Límites morales en investigación digital.
- Casos de estudio de buenas prácticas.

Unidad 2: Protección de Datos Personales (10 horas)

- Ley de Protección de Datos Personales.
- Principios de minimización y proporcionalidad.
- Derechos de los titulares de datos.
- Procedimientos de notificación y transparencia.

Unidad 3: Supervisión y Control Interno (5 horas)

- Mecanismos de auditoría interna.
- Reportes de irregularidades.
- Responsabilidades disciplinarias.
- Cultura de cumplimiento institucional.

3.4. Módulo IV: Casos Prácticos y Simulación (25 horas)

- Simulación de casos de homicidio con análisis de rutas.
- Casos de extorsión desde centros penitenciarios.
- Investigación de redes de secuestro.
- Análisis de bandas criminales organizadas.
- Ejercicios de sustentación pericial.

4. ACTUALIZACIÓN CONTINUA ANUAL (40 HORAS)

4.1. Contenidos Anuales Obligatorios

PROGRAMA ANUAL DE ACTUALIZACIÓN

Trimestre I (10 horas):

- Nuevas tecnologías de localización.
- Actualizaciones normativas relevantes.
- Jurisprudencia reciente sobre evidencia digital.

Trimestre II (10 horas):

- Casos emblemáticos resueltos con metadatos.
- Lecciones aprendidas de investigaciones.
- Mejores prácticas internacionales.

Trimestre III (10 horas):

- Nuevas amenazas de ciberseguridad.
- Técnicas de evasión criminal detectadas.
- Contramedidas tecnológicas disponibles.

Trimestre IV (10 horas):

- Evaluación anual de competencias.
- Planificación de capacitación siguiente año.
- Retroalimentación y mejora de procesos.

5. CAPACITACIÓN ESPECIALIZADA POR ROLES (80 HORAS)

5.1. Especialización para Analistas Técnicos

- Programación para análisis de datos.
- Uso avanzado de software GIS especializado.
- Técnicas de machine learning para detección de patrones.
- Desarrollo de dashboards y visualizaciones.

5.2. Especialización para Supervisores

- Gestión de equipos especializados.
- Evaluación de calidad de análisis técnicos.
- Procedimientos de escalamiento y crisis.
- Coordinación interinstitucional efectiva.

5.3. Especialización para Personal de Control

- Técnicas de auditoría de sistemas digitales.
- Detección de irregularidades en accesos.
- Evaluación de cumplimiento normativo.
- Elaboración de reportes de supervisión.

6. RECERTIFICACIÓN CADA TRES AÑOS (60 HORAS)

6.1. Evaluación Integral de Competencias

- Examen teórico sobre marco legal actualizado.
- Prueba práctica de análisis de casos complejos.
- Evaluación de conocimientos técnicos especializados.
- Sustentación oral de caso asignado.

6.2. Cursos de Actualización Intensiva

- Tendencias internacionales en investigación digital.
- Nuevos desafíos en protección de derechos fundamentales.
- Tecnologías emergentes y su impacto en investigación.
- Estándares internacionales de calidad forense.

7. EVALUACIÓN Y CERTIFICACIÓN

7.1. Sistema de Evaluación Continua

CRITERIOS DE EVALUACIÓN

Evaluación Teórica (40%):
- Examen escrito: marco legal y técnico.
- Nota mínima aprobatoria: 13/20.

Evaluación Práctica (40%):
- Análisis de un caso real.
- Elaboración de acta pericial completa.
- Nota mínima aprobatoria: 13/20

Evaluación Actitudinal (20%):
- Cumplimiento de protocolos éticos.
- Participación en actividades formativas.
- Evaluación por pares y supervisores.
- Nota mínima aprobatoria: 13/20

7.2. Certificación y Vigencia

- Certificado digital emitido por la Unidad de Plenos Jurisdiccionales y Capacitación del Poder Judicial.
- Vigencia de 3 años para certificación inicial.
- Vigencia de 1 año para actualizaciones anuales.
- Registro nacional de personas certificadas en SIGMEL.

8. IMPLEMENTACIÓN Y RECURSOS

8.1. Entidades Responsables

- **Coordinación General**: Ministerio del Interior.
- **Desarrollo Curricular**: Unidad de Plenos Jurisdiccionales y Capacitación del Poder Judicial.
- **Implementación PNP**: Escuela Nacional de Formación Profesional Policial.
- **Implementación MP**: Escuela del Ministerio Público.

8.2. Recursos Necesarios

- 12 aulas especializadas con equipamiento tecnológico.
- 20 instructores certificados en tecnologías de investigación.
- Simuladores especializados en análisis de metadatos.
- Plataforma virtual de capacitación continua.