

**PONTIFICIA UNIVERSIDAD
CATÓLICA DEL PERÚ
ESCUELA DE POSGRADO**



Fortalecimiento de la capacidad estatal de la Policía Nacional del Perú
para interceptar en tiempo real las comunicaciones por internet

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

Gian Marco Dueñas Chavez

Jonathan Enrique Seña Manguinury

Asesor:

Noam Dante Valentín López Villanes

Lima, 2023

Informe de Similitud

Yo, Noam Dante Valentín López Villanes, docente de la Escuela de Posgrado de la Pontificia Universidad Católica del Perú, asesor del Trabajo de Investigación titulado *“Fortalecimiento de la capacidad estatal de la Policía Nacional del Perú para interceptar en tiempo real las comunicaciones por internet”*, de los autores Gian Marco Dueñas Chávez y Jonathan Enrique Seña Manguinury; dejo constancia de lo siguiente:

-El mencionado documento tiene un índice de puntuación de similitud de 20 %. Así lo consigna el reporte de similitud emitido por el software Turnitin el 13 de setiembre del 2023.

-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, 16 de setiembre del 2023

Apellidos y nombres del asesor / de la asesora: <u>López Villanes, Noam Dante Valentín</u>	
DNI: 45845715	Firma: 
ORCID: 0000-0002-1821-5021	



DEDICATORIA

A los más de 130 mil policías peruanos que día a día entregan su vida con arrojo y pundonor en el apostolado de la función policial, labor muchas veces incomprendida por la sociedad, pero justa por su honor, valores y alto patriotismo.

RESUMEN

El objetivo principal de la presente investigación es describir las brechas tecnológicas en la lucha contra la criminalidad organizada, respecto a la falta de capacidad de la Policía Nacional del Perú para interceptar en tiempo real las comunicaciones por internet en el año 2018 al 2020, identificando y analizando las causas que limitan a las instituciones persecutoras del delito poder controlar la criminalidad durante la intervención de las comunicaciones.

Los avances de la tecnología han abierto muchas ventanas de oportunidad y estas a su vez han sido aprovechadas por elementos antisociales, quienes por su libre albedrío organizan, planean, dirigen, ejecutan y controlan sus actividades criminales por medio o utilizando dispositivos electrónicos teniendo como medio el internet, los cuales en un eventual proceso de investigación penal, dichas interacciones en sus comunicaciones de los elementos criminales no puede ser conocido por la autoridad persecutora del delito, debido a la falta de capacidad estatal de la institución policial, toda vez que realizan comunicaciones por medio de aplicativos móviles y actualmente estas no pueden ser interceptadas en tiempo real por el Departamento de Apoyo Técnico Judicial de la Dirección Antidrogas (DEPATEJUD) de la Policía Nacional del Perú (PNP) “Constelación”, trayendo imputaciones penales débiles que posteriormente generan impunidad.

El presente trabajo de investigación, propone la implementación del Programa “SERPICO”, que consiste en diseñar y formular un instrumento legal que sienta las bases en el Código Procesal Penal y a partir de ello, en un siguiente componente desarrolla el sendero para la gestión de la creación, implementación y articulación de la Unidad Funcional de Registros Remotos de la PNP, quien sería el órgano estatal responsable de la interceptación de las comunicaciones por internet.

PALABRAS CLAVE: Interceptación, comunicaciones, criminalidad, internet, aplicativos, control social.

ABSTRACT

The main objective of this research is to describe the technological gaps in the fight against organized crime, regarding the lack of capacity of the National Police of Peru to intercept in real time Internet communications in the year 2018 to 2020, identifying and analyzing the causes that limit the institutions that persecute the crime to be able to control crime during the intervention of communications.

Advances in technology have opened many windows of opportunity and these, in turn, have been taken advantage of by antisocial elements, who by their free will organize, plan, direct, execute and control their criminal activities through or using electronic devices using the internet, which in a possible criminal investigation process, said interactions in their communications of the criminal elements cannot be known by the authority prosecuting the crime, due to the lack of state capacity of the police institution, since they carry out communications by through mobile applications and currently these cannot be intercepted in real time by the Judicial Technical Support Department of the Anti-Drug Directorate of the National Police of Peru "Constellation", bringing weak criminal charges that subsequently generate impunity.

The present research work proposes the implementation of the "SERPICO" Program, which consists of designing and formulating a legal instrument that lays the foundations in the Criminal Procedure Code and from this, in a following component, develops the path for the management of the creation, implementation and articulation of the Remote Records Unit of the Peruvian National Police, which would be the state body responsible for the interception of Internet communications.

KEY WORDS: Interception, communications, crime, internet, applications, social control.

ÍNDICE

Carátula.....	i
Informe de Similitud.....	ii
Dedicatoria.....	iii
Resumen	iv
Abstract.....	v
Índice	vi
Lista de Tablas.....	viii
Lista de Figuras.....	ix
Introducción	1
CAPITULO I: DEFINICIÓN Y DESCRIPCIÓN DEL PROBLEMA.....	3
1.1. Redacción formal del problema.....	5
1.2. Marco conceptual del problema.....	11
1.2.1. Intervención telefónica o interceptación en tiempo real.....	12
1.2.2. Comunicaciones por internet	14
1.3. Arquitectura del problema	15
1.3.1. Magnitud del Problema	15
1.3.2. Actores en el proceso de investigación de organizaciones criminales	16
1.3.3. Proceso de intervención y grabación en tiempo real de las comunicaciones.....	16
1.3.4. Relación interinstitucional	17
1.3.5. Relación Intrainstitucional	18
1.4. Marco Institucional y normativo relacionado con el problema.....	19
1.4.1. Marco Institucional.....	19
1.4.2. Marco Normativo	22
CAPITULO II: CAUSAS DEL PROBLEMA	30
2.1. Marco teórico	30
2.2. Causas del problema	34

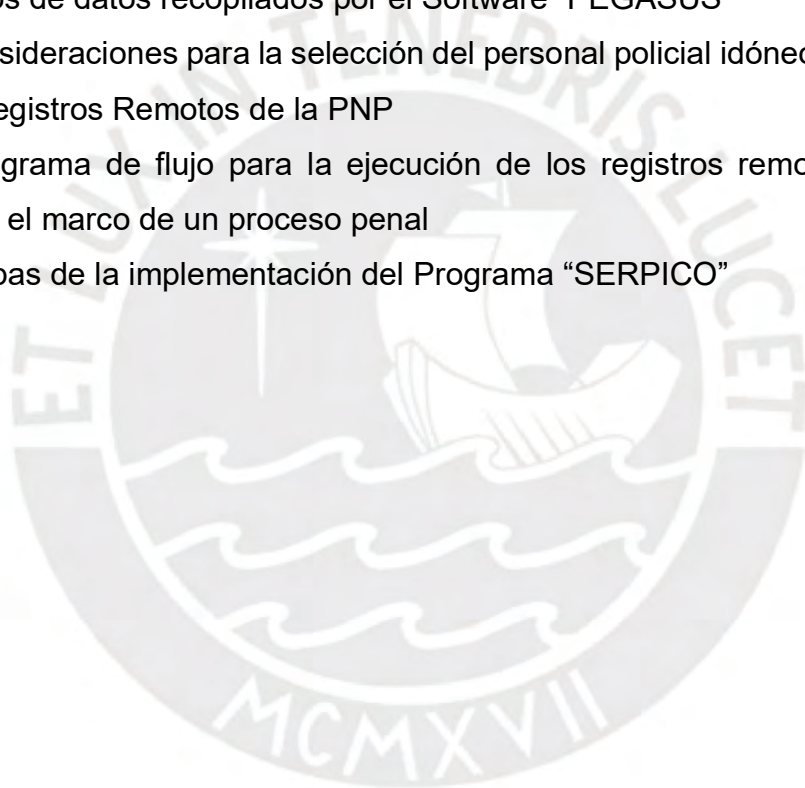
2.2.1. Ausencia de marco normativo específico para las interceptaciones de las comunicaciones por internet	36
2.2.2. Insuficiente colaboración de los Proveedores de Servicios de Internet con la administración de justicia.	37
2.2.3. Insuficiente tecnología para interceptar las comunicaciones encriptadas por medio del internet en el espectro radio eléctrico	39
2.2.4. Insuficiente recurso humano idóneo para las operaciones de interceptación de las comunicaciones.....	42
CAPÍTULO III: DISEÑO DEL PROTOTIPO	45
3.1. Problema reformulado y desafío de la innovación	45
3.2. Experiencias previas para hacer frente al desafío de la innovación.....	47
3.2.1. Implementación del programa Constelación en el año 2009	47
3.2.2. Ley australiana contra el cifrado de las aplicativos móviles.	47
3.2.3. La Ley Orgánica 13/2015 que modifica la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica en España.	48
3.3. Proceso de la conceptualización y prototipado.....	48
3.3.1. Proceso de conceptualización	48
3.3.2. Proceso de prototipado	52
3.4. Concepto y prototipo final de la innovación	55
3.4.1. Concepto final de la innovación	55
3.4.2. Prototipo de alta resolución.....	56
CAPÍTULO IV: ANÁLISIS DE LA DESEABILIDAD, FACTIBILIDAD Y VIABILIDAD DEL PROTOTIPO	84
CONCLUSIONES	90
RECOMENDACIONES	92
REFERENCIAS BIBLIOGRÁFICAS	94
ANEXOS	97
ANEXO 1: MATRIZ DE CONSISTENCIA DE LA ARQUITECTURA DEL PROBLEMA PÚBLICO	97
ANEXO 2: CADENA DE VALOR ASOCIADA.....	98
ANEXO 3: GUÍA DE ENTREVISTA.....	99
ANEXO 4: GUÍA DE GRUPO FOCAL.....	101

LISTA DE TABLAS

TABLA 1: Análisis causal del problema	35
TABLA 2: Estadística de las organizaciones criminales desarticuladas durante el 2018 al 2020 en la DIVIAC PNP	42
TABLA 3: Índice de jerarquización de las causas	45
TABLA 4: Problema reformulado	46
TABLA 5: Desafío de la innovación	46
TABLA 6: Grupo de ideas para el desafío de la innovación	49
TABLA 7: Priorización de ideas para el diseño de la innovación	50
TABLA 8: Descripción del bosquejo del concepto	51
TABLA 9: Primeras impresiones en el testeo del prototipo de innovación	52
TABLA 10 : Descripción del Concepto	55
TABLA 11: Alcances para el diseño y formulación del proyecto de ley del fortalecimiento de la lucha contra el crimen organizado.	57
TABLA 12: Matriz de análisis de viabilidad	85
TABLA 13: Costo de Inversión	87

LISTA DE FIGURAS

FIGURA 1: La simbiosis de la decisión política y la gestión eficaz para lograr la efectiva implementación.	10
FIGURA 2: Las actas de recolección de las interceptaciones telefónicas en las etapas del proceso penal	11
FIGURA 3: Ubicación de la Unidad Funcional de Registros Remotos en el Organigrama de la PNP.	66
FIGURA 4: Estructura orgánica de la Unidad Funcional de Registros Remotos	66
FIGURA 5: Tipos de datos recopilados por el Software “PEGASUS”	69
FIGURA 6: Consideraciones para la selección del personal policial idóneo para la Unidad Funcional de Registros Remotos de la PNP	72
FIGURA 7: Diagrama de flujo para la ejecución de los registros remotos de equipos tecnológicos en el marco de un proceso penal	81
FIGURA 8: Etapas de la implementación del Programa “SERPICO”	83



INTRODUCCIÓN

El Estado peruano en su afán de brindar servicios de seguridad pública cuenta con herramientas legales para ejercer el control social y regular la conducta de sus ciudadanos, evidenciándose que en el control de la criminalidad existen sendas brechas públicas durante los actos de investigación que realizan las entidades estatales persecutoras del delito, pues es la PNP quien ejecuta técnicas especiales de investigación y demás procedimientos especiales en el marco de una investigación penal, dentro de ellas las interceptaciones de las comunicaciones en tiempo real debidamente autorizados por el juez competente.

No obstante, los avances de la tecnología han sido aprovechados por los elementos criminales, quienes pretendiendo estar a la vanguardia del control estatal, organizan, planean, dirigen ejecutan y controlan sus actividades criminales por medio de comunicaciones utilizando el internet, es decir mediante aplicativos móviles como el WhatsApp, Facebook, Instagram, Telegram entre otros, dejando de lado sus comunicaciones por canales convencionales de operadora a operadora, evidenciándose una gran desventaja a las agencias persecutoras del delito por la falta de capacidad estatal de la PNP para interceptar en tiempo real las comunicaciones por internet en el marco de una investigación de carácter penal.

A partir de ello, esta investigación académica establece como objetivo principal describir las brechas públicas que generan las limitaciones de la Institución policial en su afán de perseguir el delito, para posteriormente identificar y analizar las causas que impiden ejecutar las interceptaciones de las comunicaciones por internet, es decir comunicaciones por aplicativo; en ese sentido, la principal hipótesis de la investigación académica es “si logramos interceptar en tiempo real las comunicaciones por internet, se podrán realizar mejores imputaciones y acusaciones penales, para lograr sentencias condenatorias, y así como resultado final tener un eficaz control de la criminalidad”, para ello se realizaron entrevistas a expertos en investigaciones a organizaciones criminales, se analizaron diversas documentales, estadísticas y demás datos cuantitativos.

Producto del análisis de la problemática, se advirtió que la ausencia de un cuerpo normativo específico para la interceptación de las comunicaciones por internet, es la causa principal por la cual no es posible brindar estos servicios públicos; a partir de ello, se postula el desafío de innovación ¿cómo podemos lograr la implementación de un marco normativo específico para las interceptaciones de las comunicaciones por internet? y así fortalecer la capacidad estatal de la PNP para interceptar las comunicaciones desarrolladas en por medio de aplicativos móviles que usan el internet.

Como resultado del proyecto de innovación se ha desarrollado el Programa “SERPICO”, consistente en un primer componente en diseñar y formular un marco legal que fortalezca la lucha contra la criminalidad organizada incorporando un sub capítulo en el Código Procesal Penal referente a los registros remotos, para luego, una vez sentado las bases jurídicas, dar paso al siguiente componente de creación e implementación de la Unidad Funcional de Registros Remotos de la PNP con infraestructura, tecnología y recursos humanos idóneos, dejando pautas para la articulación interinstitucional durante la ejecución de los registros remotos de los equipos tecnológicos en el desarrollo de una investigación penal.

CAPITULO I: DEFINICIÓN Y DESCRIPCIÓN DEL PROBLEMA

La capacidad estatal esta enraizada en la efectividad para la provisión de los servicios públicos correspondientes a salud, educación, seguridad, etc.; o también, en la protección contra amenazas externas, el salvaguardar el orden interno, una administración eficiente y eficaz proveyendo de condiciones necesarias para hacer funcionar el aparato estatal en la prestación de sus servicios públicos.

CEPLAN (2022), hace un tiempo ha determinado que el Perú es uno de los estados en la región latina que evidencia signos de insuficiente capacidad en la puesta en marcha de sus políticas públicas y lineamientos de gestión en todo su espacio territorial, evidenciándose una debilidad estatal o estatalidad incompleta; ahora bien, resulta necesario responder a la pregunta planteada por Dargent (2012), ¿por qué se gesta una brecha entre el cuerpo de la ley y la implementación efectiva?, la respuesta para un mejor análisis está en las dimensiones planteadas por el propio autor, la autonomía y la efectividad, pues la primera conceptualización está relacionada a la ausencia de influencia externa para tomar las decisiones públicas en una agencia estatal, y en la segunda dimensión corresponde a la capacidad para implementar efectivamente las decisiones o como bien las llamó *enforcement*.

Los estados deben brindar servicios básicos, como salud, educación y también seguridad, estableciendo para ello reglas de juego que regulen la conducta de sus cohabitantes, es por ello de acuerdo con Sapolinski (2018), dice que en la inseguridad ciudadana evidentemente se violan estipulaciones de un contrato social, vulnerando sus deberes y atentando contra los derechos de otros. Se precisa ello, toda vez que el Estado, así como brinda los servicios públicos de seguridad, los ciudadanos se encuentran en obligación de cumplir sus deberes como miembros de la sociedad, y ante aquellos que actúen como *depredadores* del orden social, es el Estado, el que, mediante el diseño y formulación de políticas públicas, y su debida gestión de implementación tendrá que regular las conductas antisociales.

Sapolinski (2018) ha calificado a los antisociales como *depredadores de la sociedad*, quienes con sus conductas desviadas del orden social, perpetran hechos criminales atentando contra derechos de otros; asimismo, desde la perspectiva de la seguridad ciudadana existen factores que se profundizan en la criminalidad organizada, dentro de ellos la corrupción y la impunidad, como también fragilidad del Estado con la insuficiente gobernabilidad; sumado a ello, las nuevas tendencias del uso y manejo de la Tecnología de la Información y Comunicaciones (TICs), las cuales han permitido globalizar las organizaciones estatales y no estatales, las formales y no formales, Tapia Pérez (2013) describe que las nuevas herramientas tecnológicas de comunicación nos evidencia que estamos en un mundo globalizado, siendo necesario el uso de las tecnologías para agilizar su vida diaria.

Estas tecnologías vienen siendo aprovechadas no solamente en un mundo globalizado formal, sino también en un mundo paralelo de la informalidad y la criminalidad, más aún aquella de carácter organizada, que es actualmente un fenómeno delictivo y social de altísimo impacto, donde se evidencian factores que propician su aparición como la falta de demanda laboral, sanciones débiles que no conminan la conducta social, entre otros, como también aparecen factores que hacen dificultoso la lucha frontal contra el fenómeno mundial del crimen organizado, como es la corrupción de los funcionarios estatales, falta de procedimientos y en otros casos instrumentos innovadores de investigación que permitan al Estado tener la intromisión legítima para regular conductas de la sociedad.

Ahora bien, está claro que el Estado es quien reclama el ejercicio y control de la violencia legítima, mediante la coerción y la fuerza pública, ello para controlar las conductas disociales de las minorías de la población, y dotar de garantías y seguridad a las mayorías, para que puedan desplegar una vida plena y de paz en un estado de derecho que garantice su desarrollo como ciudadanos de bien, garantice la protección de la propiedad privada y pública, su libertad y hasta su propia vida; esto será posible mediante el diseño y formulación de políticas públicas que permitan minimizar las acciones de los desafiantes y retadores estatales, en sinergia y articulación con la gestión pública, para una efectiva implementación.

1.1. Redacción formal del problema

Dargent Bocanegra (2015) considera un retador a la extensión del crimen patrimonial en las ciudades del Perú, particularmente Lima, haciéndose la precisión que los retadores son los elementos antisociales que bajo la violencia o no, objetan, resisten o enfrentan a la fuerza estatal, en este caso a las políticas públicas en salvaguarda de la seguridad; es en ese sentido, el estado peruano constantemente debe enfrentar diversos desafíos que ponen a prueba su capacidad estatal.

Como bien precisó Dargent Bocanegra (2015), el Estado peruano actualmente no se encuentra en condiciones de responder ante situaciones adversas, especialmente desafíos sorpresivos; no obstante, debe agregarse si el Perú está en capacidad para enfrentar fenómenos antisociales en el mundo globalizado, máxime aquellas que se manifiestan con del uso de las TICS o por medio de este. Según la ONU (2019) las herramientas tecnológicas crearon ventanas de oportunidad para los elementos criminales y trajeron como consecuencia el incremento de la tasa delincencial por el medio virtual y a través de él. Si bien estamos lejos de ser un estado débil y frágil, como los Estados africanos y algunos Latinoamericanos, es evidente nuestra debilidad en el aparato estatal que realiza el tratamiento de la seguridad nacional contra la ciberdelincuencia.

La OEA hizo un aproximado que ciberdelincuencia genera costos de 575 mil millones de dólares al año aproximadamente, monto que representa el 0.5 % del Producto Bruto Interno Mundial y estableció que en América Latina y el Caribe dichos costos superan los 90 mil millones de dólares anuales. En reproche a estos retadores del Estado, el Perú suscribió el “Convenio de Budapest” o el denominado el Convenio de la Ciberdelincuencia, como parte del paquete de instrumentos legales internacionales y el aprovisionamiento de normas nacionales como la Ley N° 30999, que busca regular dicha conducta antisocial perpetrado en el mundo tecnológico y a través de él. *Ley N° 30999, Ley de Ciberdefensa (2019)*.

Miró Llinares (s.f.), explica que el cibercrimen es el comportamiento criminal materializado en el ciberespacio, interactuando y efectuando sus comunicaciones personales por medio de las tecnologías de la información y comunicaciones, pues ahora es el ciberespacio o espectro donde se evidencian comportamientos nuevos, o tradicionalmente ilícitos y que ahora únicamente cambia que se llevan a cabo por medio del internet; producto de tales conductas, la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la PNP, de octubre 2013 a diciembre del 2020, registró 12 169 delitos vinculados a la Ley 30096. El 78% (9515) de las conductas criminales son vinculados al fraude informático, secundado por el delito de suplantación de identidad (13%) y delitos contra datos y sistemas informáticos (6%).

En ese orden de ideas, la *Política Nacional Multisectorial de Lucha Contra El Crimen Organizado 2019-2030* (2019) del Ministerio del Interior (MININTER), muestra que la incidencia de las actividades delictivas perpetradas por grupos criminales ha ido aumentando en el país, según las estadísticas de la PNP entre 2014 y 2018 se registraron 1 507 000 denuncias de víctimas de la delincuencia, de las cuales el 72% tiene relación con delitos vinculados a organizaciones criminales.

Es sabido que los potenciales delincuentes para **planear, organizar y ejecutar sus operaciones criminales constantemente se comunican mediante herramientas tecnológicas (TIC)**, sea mediante llamadas, mensajes o videoconferencias, ello usando las líneas telefónicas de las operadoras que contratan en Perú y por otro lado con aplicativos móviles que se desarrollan mediante el uso del internet; y es justamente que las comunicaciones por internet mediante aplicativos móviles no puede ser interceptado en tiempo real, trayendo como consecuencia que el Estado peruano no ejerza legítimamente su control social, evidenciando su capacidad limitada en afán de garantizar servicios públicos básicos como la seguridad.

En el Perú, las comunicaciones y telecomunicaciones son servicios que vienen ofreciendo diferentes empresas operadoras como: Claro, Entel, Bitel y Movistar, quienes brindan servicios de comunicación telefónica y de internet; tales empresas, se encuentran obligadas a contribuir con la administración de justicia proporcionando reportes telefónicos, geolocalización en tiempo real, mensajes de texto, multimedia, etc.; dichas actuaciones son incorporados como medio probatorios y así contribuyen a establecer responsabilidades en los presuntos autores.

La delincuencia organizada viene innovando sus prácticas criminales, utilizando nuevos canales de comunicación como las llamadas telefónicas, mensajes, video conferencias, las cuales se desarrollan por medio del internet, utilizando aplicativos de redes sociales convencionales como el Whats App, Facebook, Instagram, Telegram entre otras, y es justamente estas comunicaciones por internet que desarrollan los grupos criminales no pueden ser interceptado en tiempo real, en el marco de una investigación penal, por las razones que esta se encuentra alojada en el espacio virtual y los titulares de estas aplicaciones no cuentan con representación legal en Perú, que permita plantear estrategias de política criminal.

La Interceptación de las comunicaciones en tiempo real se encuentra enmarcada en la Ley N° 27697, las cuales son motivadas debidamente para su autorización por la autoridad judicial, *Ley N° 27697 Ley que otorga facultad al Fiscal para La Intervención y Control de Comunicaciones y Documentos privados en caso excepcional (2002)*; sin embargo, los antisociales cuando planean, organizan, ejecutan y controlan sus actos criminales, típicamente lo realizan por medio de un teléfono que facilita su plan criminal, y en la actualidad estos evaden el control de las comunicaciones cuando se practican interceptaciones legales a las líneas telefónicas, toda vez que el planeamiento criminal y su ejecución lo desarrollan por medio del internet y no mediante el servicio telefónico de la operadora; es ahí donde el Estado a la fecha no puede ejercer el control social a tiempo real, pues

no basta que la Unidad de Cooperación Internacional de la Fiscalía de la Nación realice acciones propias a su función obteniendo de esas empresas de telecomunicaciones extranjeras meros reportes históricos que solamente ilustran la ejecución criminal de manera diferida, trayendo como consecuencia imputaciones débiles, carencia de elementos probatorios por falta de elementos periféricos, e identificación de los integrantes de grupos criminales, todo ello concluyéndose en un resultado de impunidad de conductas antisociales gravosas.

Actualmente, la ejecución de una medida judicial para la interceptación de las comunicaciones telefónicas se encuentra a cargo de la PNP, específicamente el Departamento de Apoyo Técnico Judicial (DEPATEJUD), o bien llamado “Constelación”, dependiente de la Dirección Antidrogas (DIRANDRO) de la PNP, esta cuenta con la capacidad para interceptar legítimamente comunicaciones que se desarrollan en el Perú por medio de las operadoras telefónicas de las empresas Bitel, Movistar, Claro y Entel; sin embargo, durante las investigaciones a grupos criminales, los pesquisas advierten que los delincuentes están dejando de comunicarse por medio de este canal convencional, dando paso a uno más innovador y tecnológico, los aplicativos móviles que se desarrollan en el espacio virtual por medio del internet como el Whats App, Facebook, Instagram, Telegram entre otros, retando así a la capacidad estatal de la PNP, representado por el DEPATEJUD “Constelación”.

Esta capacidad limitada o debilidad estatal para garantizar un servicio básico como la seguridad, debe ser estudiada desde diversos enfoques a fin de dar soluciones transversales y sostenibles; ante ello, Altman & Luna (2012) han resaltado que los estados son frágiles cuando los cuerpos estatales no tienen la voluntad política o son débiles para brindar servicios básicos, pues dentro del estudio se tendrán que identificar las brechas más importantes que están aportando a la debilidad del Estado peruano. Tal vez al solucionar dicha brecha y lograr una total intromisión del Estado en la regulación legítima en las interceptaciones en tiempo real de las comunicaciones por internet, pueda ir en contra de intereses de sendos grupos de

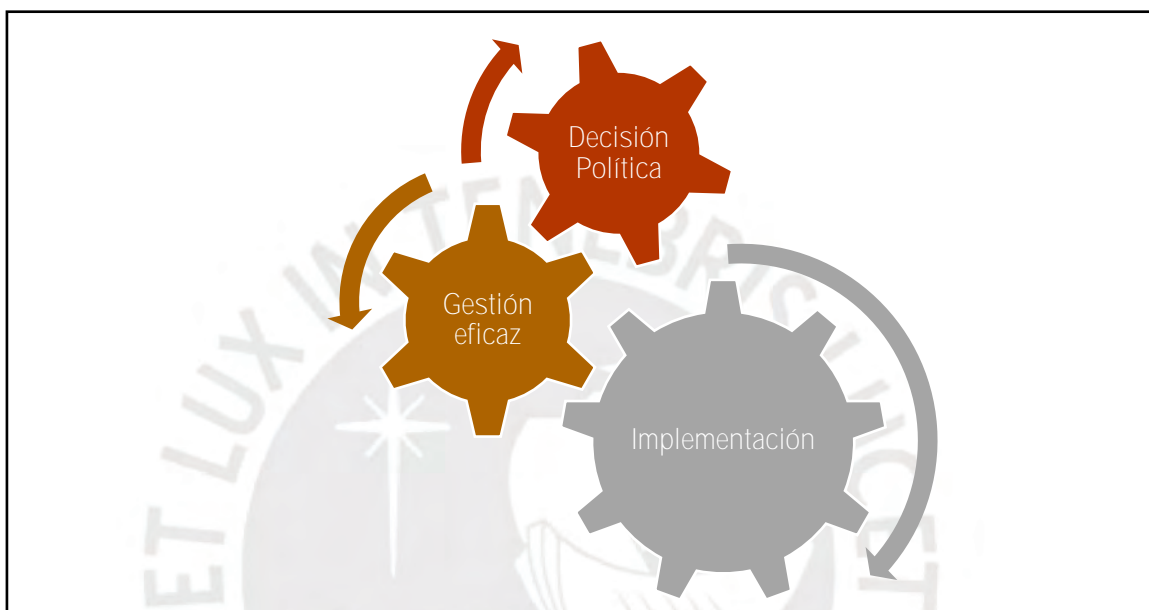
actores estatales que usan estos medios de comunicación o canal para coordinaciones de tipo antisociales y regularlos tal vez no sea políticamente conveniente, que de acuerdo a Holland (2017) lo llamó “*forbearance*”, que no es más que no hacer cumplir la ley de forma intencional o no dictar políticas públicas para este tema, pues la solución a la problemática no solamente requerirá políticas públicas, sino más bien articularse con la gestión pública para una óptima implementación.

Ahora bien, los aplicativos móviles mencionados, si bien es cierto son los más convencionales utilizados actualmente por los ciudadanos de a pie, entre ellos la delincuencia organizada; no obstante, en una posición predictiva estos aplicativos móviles se irán innovando, mejorando o transformando, o más aun, irán apareciendo otros aplicativos móviles más sofisticados, utilizando únicamente códigos para la comunicación y no el número telefónico como medio identificación del comunicante p ej. el aplicativo móvil Zangi, solo requiere acceso a internet y con un código de comunicación otorgado por el receptor podrán establecer contacto en un tiempo limitado, siendo variable dicho código para una nueva comunicación, la particularidad de todas ellas es que requieren de un dispositivo tecnológico con acceso a internet y es donde debe orientarse la búsqueda de alternativas de solución

Es por ello, se considera que dicha brecha pública debe ser tratado con mucho detenimiento y estudio, pues no bastará la adquisición de softwares y hardwares, que cuenten con sistemas para interceptación en tiempo real de las comunicaciones por internet, pues cada aplicativo móvil cuenta con códigos de encriptación único, siendo que una es diferente de la otra, por ello, ante estos desafíos del Estado, esta brecha debe tratarse de manera transversal con soluciones sostenibles , fortaleciendo la capacidad estatal de la PNP, Organismo Supervisor de la Inversión Privada en Telecomunicaciones (OSIPTEL) y el Ministerio de Transportes y Comunicaciones (MTC), en una articulación fuerte entre el diseño y formulación de la política pública y el curso de la gestión eficaz

durante la implementación, en palabras de Tanaka (2021) la política aporta el liderazgo y la voluntad de cambio, debiendo considerarse las complejidades de la gestión para una implementación eficaz.

FIGURA 1: La simbiosis de la decisión política y la gestión eficaz para lograr la efectiva implementación



Fuente: Elaboración propia

En ese sentido, se traza un punto de partida para emprender el proyecto de innovación, dentro de la Política Nacional Multisectorial de Lucha Contra el Crimen Organizado 2019-2030 del Ministerio del Interior, específicamente en OP1 “*Fortalecer la capacidad del estado en la lucha contra las organizaciones criminales*”, con un resultado que permita la interceptación legal de las comunicaciones por internet, para así lograr imputaciones penales debidamente fundamentadas y acusaciones fiscales que establezcan plenamente la conducta criminal de los acusados, evitando la impunidad de implicados de los grupos criminales, todo ello dentro del marco de garantizar la seguridad pública del Estado peruano, cumpliendo el objetivo interestatal del control de la criminalidad, que en palabras de Binder (s.f.) la denomina la persecución penal estratégica, como la

acción articulada de las instituciones en diferentes niveles de gobierno para el control de la conducta criminal.

Pues, es el Ministerio Público y la PNP el binomio interinstitucional que persiguen el delito, quienes al ejecutar una medida de intervención telefónica de los investigados en un proceso penal, estas para que puedan ser consideradas preliminarmente como elementos de convicción y posteriormente medios de prueba en el juicio oral, son materializadas en actas de recolección y control de las comunicaciones, siendo examinada y valorada en todas sus partes por la autoridad jurisdiccional que emitirá sentencia.

FIGURA 2: Las actas de recolección de las interceptaciones telefónicas en las etapas del proceso penal



Fuente: Elaboración propia

1.2. Marco conceptual del problema

Considerando la identificación del problema como: *“Falta de capacidad de la Policía Nacional del Perú para interceptar en tiempo real las comunicaciones por*

internet a nivel nacional durante el periodo 2018-2020”, se advierten términos que deben ser desarrollados para una mejor comprensión del problema público.

1.2.1. Intervención telefónica o interceptación en tiempo real

La libertad de las comunicaciones y el secreto de estas, es un derecho fundamental que convencionalmente es restringido por una autoridad judicial; en algunos otros lugares del mundo como en la Constitución Italiana de 1948 (artículo 15) y en la Constitución española, establecen un presupuesto adicional que se restringen el secreto de las comunicaciones cuando se dispone la suspensión individual de los derechos fundamentales; asimismo, en el caso inglés también se admite al Ministerio del Interior disponga el controlar las comunicaciones, no encontrando claridad en la literatura respecto cuales son los presupuestos para requerir la intervención de las comunicaciones y principalmente el flujo procesal cuando la autorización la expide una autoridad que no es funcionario judicial.

En el Perú, el artículo 2 inciso 10 de la Constitución reconoce la libertad de las comunicaciones y dispone que su secreto solo puede ser levantado por mandato motivado del juez conforme la *Constitución Política Del Perú* (1993), lo que en palabras del Tribunal Constitucional denomina, la “garantía de judicialidad” (STC 1058-2004-AA/TC, FJ 22), para lo cual debe diferenciarse claramente los derechos de la intimidad y la inviolabilidad de la libertad de comunicación.

Sobre el particular, en palabras de Abad (s.f.) si en el desarrollo de una comunicación telefónica esta es grabada por una de ella sin la autorización de a la otra, no se consideraría una vulneración al derecho al secreto de las comunicaciones, sino dicha conducta estaría inmersa en otras conductas típicas, ello de acuerdo con la forma y circunstancias de los hechos, como por ejemplo vulnerándose el derecho a la intimidad.

En nuestro país el Código Procesal Penal es la ley donde se regulan estas medidas limitativas de derechos y que a su vez la Ley N° 30077 ha recogido dicho concepto, considerándola además como una técnica especial de investigación para la lucha contra la criminalidad organizada. *Ley N° 30077 Ley Contra El Crimen Organizado (2013)*. Dicha técnica especial de investigación viene siendo utilizado por los pesquisas policiales y representantes del Ministerio Público para acopiar información de las comunicaciones de integrantes de grupos criminales, fundamentar acusaciones y lograr sentencias condenatorias para evitar su impunidad. El levantamiento del secreto de las comunicaciones, autorizado por la autoridad judicial, convencionalmente da como resultado reportes históricos de llamadas, permite la geolocalización de los teléfonos celulares, como también la intervención y grabación de las llamadas en tiempo real.

La interceptación de las comunicaciones en tiempo real, es una herramienta legal precisada en el Código Procesal Penal, de naturaleza compleja y confidencial, pues se realiza de forma no consentida y desconocida por el investigado. Convencionalmente esta técnica especial de investigación es ejecutada durante la etapa de diligencias preliminares, que por su naturaleza compleja es declarada en secreto, a fin recabar elementos probatorios productos del flujo comunicacional de los investigados y puedan ser ofrecidos posteriormente en el juzgamiento en la teoría del caso que postulará el Ministerio Público.

El cumplimiento de las medidas judiciales que autorizan el levantamiento del secreto de las comunicaciones, en el tipo de intervención telefónica o interceptación en tiempo real, se encuentra a cargo del DEPATEUD de la DIRANDRO PNP, o bien llamado “Constelación”, quienes tienen el monopolio de interceptación de tiempo real de las comunicaciones convencionales en articulación permanente con Representantes del Ministerio Público.

1.2.2. Comunicaciones por internet

Los primeros usos del servicio de internet datan por los años 60, remontándose a los años del desarrollo de las redes de comunicación, creada por los Estados Unidos cuando desarrolla una red exclusivamente militar, con el caso hipotético de ataques rusos, para que pudieran acceder en cualquier momento a su información; hoy en día, la internet se esparció por todo el mundo creando acceso mundial de la información, alterando economías mundiales y simplificando muchas actividades del quehacer diario.

La globalización de los mercados, organizaciones y diversas estructuras formales y no formales, tienen como uno de sus pilares fundamentales el uso del internet, el cual es un medio de creciente importancia, siendo un elemento indispensable para lograr satisfacer las expectativas de sus usuarios.

Según Gamboa & Domenge (2011), los servicios de internet son aquellos que cuentan con características particulares que los hacen diferentes de las demás, con mínimas o casi ninguna interacción humana, diseños precisos e interacciones mediante canales de comunicación virtual, pues este es el medio que ahora los comercios, personas y todas las entidades vienen utilizando para sus interacciones entre sí y externos.

Las comunicaciones por internet son la interacción que realizan las personas, mediante llamadas, mensajes, video conferencias, interactuando por medio de los aplicativos móviles convencionales como el Whats app, facebook, Instagram, telegram entre otros, que usan como canal de comunicación el internet, utilizando dispositivos electrónicos p. ej. teléfonos celulares, tablets, lap top o cualquier otro equipo tecnológico que pueda acceder al internet.

1.3. Arquitectura del problema

El presente proyecto de innovación se desarrolla dentro de la Política Nacional Multisectorial de Lucha Contra el Crimen Organizado 2019-2030 del Ministerio del Interior, específicamente en OP1 “*Fortalecer la capacidad del estado en la lucha contra las organizaciones criminales*”, el cual para lograr su ejecución, corresponde realizar una arquitectura de la investigación que comprende establecer preguntas a las dimensiones que nos ayude a comprender el problema, estableciendo los objetivos y posibles hipótesis, determinando las herramientas como entrevistas, focus group, encuestas, observación y revisión de información que se utilizaran para conocer el problema público. Se han establecido las siguientes dimensiones:

1.3.1. Magnitud del Problema

En esta dimensión corresponde establecer la siguiente interrogante: ¿De qué manera influye la limitación de no poder interceptar en tiempo real las comunicaciones por internet, en la recopilación de elementos de convicción en investigaciones a organizaciones criminales en la División de Investigaciones de Alta Complejidad (DIVIAC) y la División de Investigación de Crimen Organizado de la PNP (DIVINCCO), en el año 2018 al 2020?, el cual nos permitirá conocer como sucede el problema, donde sucede, y debido a que se genera el problema público; lo que se pretende es describir la influencia de la limitación de no poder interceptar en tiempo real las comunicaciones que desarrollan los integrantes de organizaciones criminales mediante el uso del internet; asimismo, permitirá conocer cuáles son los efectos del problema público en la administración de justicia, principalmente en las agencias policiales como la DIVIAC y la DIVINCCO de la PNP, unidades especializadas de investigación que ejecutan convencionalmente técnicas especiales de investigación engarzada con interceptaciones legales de las telecomunicaciones, en las investigaciones a integrantes de organizaciones criminales.

Paralelamente, se recabará información mediante entrevistas y documentales de parte del Departamento de Apoyo Técnico Judicial (DEPATEJUD), el cual es la agencia responsable de gestionar el sistema de intervención de las comunicaciones con mandato judicial y con participación del Ministerio Público, ello para que nos permita evidenciar o diseñar algún indicador que demuestre la falta de capacidad para interceptar en tiempo real las comunicaciones por internet.

1.3.2. Actores en el proceso de investigación de organizaciones criminales

En esta dimensión se estableció la siguiente pregunta: ¿Quiénes son los actores que participan en el proceso de investigación de organizaciones criminales, en el periodo 2018-2020?, el cual permitirá conocer como se engarzan los actores que desarrollan las investigaciones de organizaciones criminales, dichas actuaciones están sujetas a normas procesales, protocolos de actuación y guías de intervención. Los actores de investigación a organizaciones criminales son los pesquisas policiales, el fiscal encargado del caso, analistas de Investigación, el juez de investigación preparatoria y analistas de la DEPATEJUD-DIRANDRO “Constelación”.

Para conocer el desarrollo de su actuación funcional, se realizarán diversas herramientas cualitativas y comprender como las normas procesales, protocolos de actuación y manuales instructivos vienen cumpliéndose en las investigaciones prospectivas que desarrollan el binomio Policía Nacional del Perú y Ministerio Público.

1.3.3. Proceso de intervención y grabación en tiempo real de las comunicaciones

Esta dimensión nos ayudará a comprender el proceso de la interceptación de las comunicaciones, es por ello por lo que se plantea la pregunta: ¿Cómo

se desarrolla las intervenciones y grabaciones de las comunicaciones en tiempo real?, dichas acciones están erguidas en el Código Procesal Penal; no obstante, con mayor especificidad se encuentran en el Protocolo de Actuación Conjunta para la intervención y grabación en tiempo real de las comunicaciones, donde el actor principal es el Juez de Investigación Preparatoria, pues es la autoridad que legalmente autorizará el levantamiento del secreto de las comunicaciones, ello atendiendo el requerimiento fundamentado de la autoridad fiscal; en este proceso, se observará la participación del pesquisa policial, quien podrá tener acceso al contenido de las comunicaciones, siempre y cuando el fiscal del caso lo permita. Para conocer a mayor amplitud esta dimensión se realizarán métodos cualitativos de investigación a los actores principales que participan en el procedimiento de interceptación en tiempo real de las comunicaciones.

1.3.4. Relación interinstitucional

Para conocer esta dimensión, se plantea la siguiente pregunta: ¿Cómo se engarzan las agencias estatales vinculadas a las investigaciones de organizaciones criminales, cuando se gestionan las interceptaciones en tiempo real de las comunicaciones?, dando respuesta a esta interrogante se plantea determinar la forma de articulación de las instituciones relacionadas en la gestión de la interceptación en tiempo real de las comunicaciones por internet, donde se conocerá que las instituciones comprometidas en la gestión del levantamiento del secreto de las comunicaciones va desde la PNP, el Ministerio Público y el Juez de la Investigación Preparatoria.

No obstante, es necesario conocer el rol de la autoridad rectora de las telecomunicaciones, representada por el MTC, quien es la encargada de dar las concesiones para el uso del espectro radioeléctrico donde se encuentra el flujo de todo tipo de comunicaciones, es con este sector donde

se formulan los contratos de concesión a las empresas que brindan servicios de telecomunicación y principalmente los servicios de internet, es por ello que se realizará una revisión de la información documental que es de acceso público, que nos ayude a comprender los términos de la relación contractual en la cesión del uso del espectro radioeléctrico, las obligaciones de las empresas que brindan servicios de internet, la cantidad de concesiones, permisos, autorizaciones o licencias en los servicios de portabilidad, finales o valor añadidos, según corresponda, donde se brindan servicios de internet; asimismo, se realizará la revisión de información que permita conocer las acciones que realiza la autoridad reguladora de las telecomunicaciones, representada por OSIPTEL, ello para evidenciar el rol que cumple en la gestión de la interceptación en tiempo real de las comunicaciones, y principalmente aquellas que se cumplen en las comunicaciones que se desarrollan por el internet.

1.3.5. Relación Intrainstitucional

En esta última dimensión corresponde responder a la siguiente interrogante: ¿Cuáles son los factores que limitan las interceptaciones legales de las comunicaciones por internet en tiempo real en el Departamento de Apoyo Técnico Judicial - DIRANDRO "Constelación"? Como hipótesis general se puede mencionar que los factores más determinantes que limitan las interceptaciones en tiempo real de las comunicaciones por internet son: 1) no contar con los sistemas tecnológicos operativos adecuados, 2) la falta de decisión política para la lucha frontal contra el crimen organizado, 3) la ausencia de mecanismos legales que obliguen a los operadores de las telecomunicaciones a coadyuvar con la administración de justicia, principalmente ante la advertencia de este problema público; para ello, se realizarán métodos cualitativos de investigación, realizando entrevistas a actores que dirijan el DEPATEJUD de la DIRANDRO "Constelación", para que nos ayude a comprender fehacientemente cuales son las brechas que impiden la interceptación de las comunicaciones por internet; asimismo,

determinar si es solo un problema de gestión en la implementación logística de softwares, es un problema de política pública que se encuentra sujeta a decisiones de actores políticos o la ausencia de herramientas legales que permitan a los actores de la persecución penal estratégica.

1.4. Marco Institucional y normativo relacionado con el problema

1.4.1. Marco Institucional

1.4.1.1. Convención de Palermo contra la Delincuencia Transnacional Organizada, ratificada en el Perú el 4 de octubre del 2001, mediante la Resolución Legislativa N° 27527

Este marco normativo internacional orienta a los Estado parte del Convención de Palermo a orientar sus políticas criminales a una lucha frontal contra la delincuencia organizada, mediante el establecimiento de reglas, procedimientos, y sanciones para conductas criminales vinculadas a delitos graves de forma organizada. El objetivo de este instrumento internacional es promover la cooperación para prevenir y combatir más eficazmente la criminalidad organizada internacional. *Resolución Legislativa N° 2752 (2001).*

Asimismo, describe la forma de asistencia judicial entre los Estados que son parte de la Convención de Palermo, la cual esta erguida en la cooperación mutua en sus acciones de administración de justicia, ello facilitando información, elementos de prueba y evaluación de peritos.

1.4.1.2. Política Nacional Multisectorial de Lucha Contra el Crimen Organizado 2019-2030 del Ministerio del Interior -MININTER, aprobado por Decreto Supremo N° 019-2019-IN

En los últimos años se ha evidenciado en el Perú el aumento de la incidencia de las actividades delictivas cometidas por grupos criminales, atentando directamente a la democracia y la seguridad nacional.

En ese sentido se ha dictado la Política Nacional Multisectorial de Lucha Contra el Crimen Organizado 2019-2030 del Ministerio del Interior- MININTER, donde se realiza un diagnóstico del problema público a partir de la identificación de las causas que son: 1) debilidad estatal para combatir el crimen organizado, 2) mercados ilegales nacionales e internacionales; 3) tolerancia a los delitos contra el crimen organizado; y 4) debilidad en la asistencia a víctimas del crimen organizado.

El trabajo de innovación se desarrolla en el fortalecimiento de las capacidades del Estado en la lucha contra las organizaciones criminales, y se advierte lineamientos para una asignación adecuada de los recursos en las instituciones estatales para una gestión eficaz de sus operaciones, del mismo modo busca mejorar la articulación de las entidades públicas vinculadas en la lucha contra el crimen organizado a fin que todas estén orientadas al control de la criminalidad.

1.4.1.3. Informe de Análisis N° 04, Ciberdelincuencia en el Perú: pautas para una investigación fiscal especializada.

Las TICs generaron oportunidades para los elementos criminales,

Incrementando el índice delincencial que se perpetran en el ámbito virtual o utilizando dispositivos electrónicos que se desarrollan en el mundo virtual. Ante ese escenario el Ministerio Público desarrolla un estudio descriptivo sobre la base de información policial y fiscal, para conocer la capacidad estatal y abortar el problema público. *Oficina de Análisis Estratégico Contra la Criminalidad del Ministerio Público (2021)*.

Este documento destaca como un importante elemento normativo el Convenio de Budapest o denominado “Convenio de Ciberdelincuencia”, al cual el Estado peruano se adhiere el 2015, aprobándose el 2019 y entrando en vigor el 01 de diciembre del 2019. Dicho instrumento normativo internacional es generado por los países miembros del Consejo de Europa para luchar contra la ciberdelincuencia.

1.4.1.4. Resolución N° 56/21 sobre la lucha contra la utilización de la tecnología de la información con fines delictivos, aprobada por la Asamblea General de las Naciones Unidas, el 19 de diciembre del 2001.

La Asamblea General de las Naciones Unidas, precisa que los países que son miembros deben velar porque los beneficios de las nuevas tecnologías de la información y comunicación alcancen a toda la sociedad; asimismo, advierten que los avances de la tecnología dieron paso a nuevas posibilidades de actividades delictivas, dando a conocer su orientación y recomendación sobre cada presupuesto. *Asamblea General de las Naciones Unidas (2001)*.

1.4.2. Marco Normativo

1.4.2.1. Constitución Política del Perú de 1993.

Es la ley sobre la cual se rige el derecho, la justicia y las normas del Perú; en su artículo 2°, destaca como un derecho fundamental, el derecho al secreto y a la inviolabilidad de sus comunicaciones y documentos privados.

Es a partir de ella que se desarrolla todo el cuerpo normativo para custodiar la inviolabilidad de las comunicaciones, es también que a partir de ella que se dotan de facultades al sistema de justicia para legalmente conocer el secreto de sus comunicaciones.

1.4.2.2. Código Procesal Penal del 2004 aprobado por Decreto Legislativo N° 957, artículo 230° y 231°.

En estos instrumentos legales se describen los procedimientos que deben regirse cuando se gestione el levantamiento del secreto de las comunicaciones, el cual debe atender irrestrictamente al principio de proporcionalidad, razonabilidad, necesidad e idoneidad, y en la medida que existan suficientes elementos de convicción.

Para conseguir la medida judicial que autorice la interceptación en tiempo real de las comunicaciones, la norma procesal establece como primer presupuesto que debe existir suficientes elementos de convicción, que el delito investigado supere los cuatro años de privación de libertad, asimismo se debe fundamentar que el requerimiento es absolutamente necesario para continuar con las investigaciones, la medida judicial se autorizará con un plazo máximo de 60 días, pudiendo prorrogarse en plazos sucesivos

durante la investigación preparatoria. Código Procesal Penal (2004).

Asimismo, describe que los concesionarios de servicios públicos de telecomunicaciones deberán facilitar la geolocalización de teléfonos móviles y la interceptación en tiempo real de las comunicaciones cuando la autoridad judicial así lo autorice, las 24 horas del día y los 365 días del año. Los concesionarios otorgarán el acceso, la compatibilidad y conexión de su tecnología con los sistemas del DEPATEJUD- DIRANDRO “Constelación” de la PNP; no obstante, cuando los concesionarios renueven o modifiquen sus equipos y software, deberán mantener la compatibilidad con el sistema de interceptación en tiempo real de las comunicaciones de la PNP.

1.4.2.3. Ley N° 27697, Ley que regula el Levantamiento del Secreto de las comunicaciones y sus modificatorias por el Decreto Legislativo N° 991.

La Ley N° 27697, conceptualiza a las comunicaciones en su artículo 2° como: “(...) *cualquier forma de transmisión del contenido del pensamiento, o de una forma objetivada de éste, por cualquier medio (...)*”; por lo que dicha descripción extiende el concepto de comunicarse a aquellas que son realizadas de manera directa entre las personas o que son efectuadas utilizando medios tecnológicos.

La presente ley en su artículo 1° precisa que tiene por finalidad lo siguiente: “(...) *desarrollar legislativamente la facultad constitucional otorgada a los jueces para conocer y controlar las comunicaciones de las personas que son materia de investigación preliminar o jurisdiccional. Solo se podrá hacerse uso de la*

facultad prevista en la presente Ley en los siguientes delitos: secuestro, trata de personas, pornografía infantil, robo agravado, extorsión, tráfico ilícito de drogas, tráfico ilícito de migrantes, asociación ilícita para delinquir, delitos contra la humanidad, atentados contra la seguridad nacional y traición a la patria, peculado, corrupción de funcionarios, terrorismo, delitos tributarios y aduaneros, lavado de activos, otros delitos cuando existan suficientes elementos de convicción que permitan prever que el agente forma parte de una organización criminal.”

Asimismo, la norma en mención destaca en su artículo 2° inciso 5 que: *“El fiscal recolector supervisa la intervención y control de las comunicaciones, que realiza el personal autorizado del Ministerio Público y/o de la Policía Nacional del Perú, con el apoyo técnico de las empresas operadoras de comunicaciones con la finalidad de asegurar la intervención o control de las mismas en tiempo real”*, instrumento normativo que fue el génesis para lograr el acopio del flujo comunicacional de los investigados por delitos graves y fortalecer la teoría del caso durante el proceso penal, con el fin de obtener sentencias condenatorias.

1.4.2.4. Ley N° 27379, Ley que regula las medidas limitativas de derechos en sede preliminar de la investigación penal, modificada por el Decreto Legislativo N° 988.

El presente cuerpo normativo en su artículo 2° desarrolla el procedimiento para el requerimiento y ejecución de medidas limitativas de derechos, esto es: *“1) detención preliminar; 2) impedimento de salida del país o de la localidad en domicilio el investigado o del lugar que se le fije; 3) incautación, apertura, e interceptación de documentos privados, libros contables, bienes y*

correspondencia; 4) embargo u orden de inhibición para disponer o gravar bienes, que se inscribirán en los Registros Públicos cuando correspondan, 5) levantamiento del secreto bancario y de la reserva tributaria; 6) exhibición y remisión de información en poder de instituciones públicas o privadas; 7) allanamiento de inmuebles o lugares cerrados fuera de los casos de flagrante delito o de peligro inminente de su perpetración; y 8) inmovilización de bienes muebles y clausura temporal de locales.” Ley N° 27379, Ley que regula las medidas limitativas de derechos en sede preliminar de la investigación penal (2000).

1.4.2.5. Ley N° 29733, Ley de protección de datos personales.

La presente ley garantiza el derecho fundamental a la protección de los datos personales previsto en la Constitución Política del Perú, a través un adecuado tratamiento en el marco de respeto de los derechos fundamentales.

El mismo instrumento normativo precisa solamente se podrá abrir, incautar e interceptar por mandato judicial las comunicaciones, sistemas informáticos y telecomunicaciones, en con todas las garantías que la ley establece. *Ley 29733 Ley de Protección de Datos Personales (2011).*

1.4.2.6. Ley N° 27336, Ley de Desarrollo de las Funciones y facultades del Organismo Supervisor de Inversión Privada en Telecomunicaciones- OSIPTEL.

El artículo 1° de la Ley N° 27336, describe que es objeto de la presente ley: “definir y delimitar las facultades del Organismo Supervisor de Inversión Privada en Telecomunicaciones

(OSIPTEL), para supervisar y sancionar a personas naturales o jurídicas que prestan servicios públicos de telecomunicaciones (...)”; asimismo, describe las limitaciones respecto al secreto e inviolabilidad de las comunicaciones, las mismas que deben estar enmarcadas en torno al artículo 2 de la Constitución Política del Perú. *Ley N° 27336, Ley de desarrollo de las funciones y facultades del organismo supervisor de inversión privada en telecomunicaciones (2000).*

Por otro lado, este marco legal describe que órgano regulador en cumplimiento de sus funciones puede exigir a las entidades que brindan servicios de telecomunicaciones, la presentación de información relacionada con la facturación, tasación, lugar y fecha de instalación de líneas o circuito, **tráfico entrante y saliente**, y demás que establezca el Reglamento del presente instrumento legal, coligiéndose que OSIPTEL cuenta con las facultades suficientes para solicitar toda la información necesaria, excepto el contenido de las comunicaciones, a las entidades que brindan servicios de telecomunicaciones, incluyendo los servicios de internet.

1.4.2.7. Ley N° 30077, Ley Contra el crimen organizado.

Este cuerpo normativo procesal establece las reglas y procedimientos para una óptima investigación y el proceso que se debe seguir durante la administración de justicia perpetrado por las organizaciones criminales, pudiéndose aplicar según el artículo 3° de la presente ley los siguientes delitos: *“Homicidio calificado- Asesinato, Secuestro, Trata de personas, Violación del secreto de las comunicaciones, Delitos contra el patrimonio, Pornografía infantil, Extorsión, Usurpación, Delitos informáticos,*

Delito contra la propiedad industrial, Delitos monetarios, Tenencia, fabricación, tráfico ilícito de armas, municiones y explosivos, Delitos contra la salud pública, Tráfico Ilícito de drogas, Tráfico Ilícito de migrantes, Delitos ambientales, Delito de marcaje o reglaje, Genocidio, Delitos contra la administración pública, Delito de falsificación de documentos y, Lavado de activos".Ley N° 30077 Ley Contra El Crimen Organizado (2013).

Describe a la intervención de las comunicaciones como una técnica especial de investigación que actúa acorde al código procesal penal, y fija reglas para su aplicación para organizaciones criminales, el cual servirá para que los pesquisas de investigación puedan recoger información adelantada sobre los hechos criminales que se vienen averiguando.

1.2.4.8. Decreto Supremo N° 013-93-TCC, que aprueba el Texto Único Ordenado de la Ley de Telecomunicaciones.

El presente instrumento legal, describe que, para la prestación de los teleservicios o servicios finales de telecomunicaciones públicas, se requerirá contrato de concesión. La concesión de las telecomunicaciones es aquel acto jurídico donde el estado otorga a una persona natural o jurídica las facultades para que esta preste servicios de telecomunicaciones, se perfecciona con un contrato escrito y es aprobado por el titular del sector; la concesión en todos los casos para prestar servicios de telecomunicaciones deben indicar un plan mínimo de expansión, coberturas, el plazo de duración que es 20 años, tarifas y la **garantía que debe otorgar para asegurar el secreto de las comunicaciones**, entre otros, para lo último la empresa operadora que brinda servicios de telecomunicaciones deberán adoptar medidas necesarias que permita salvaguardar el derecho fundamental de la inviolabilidad

de las comunicaciones. *Decreto Supremo N° 013-93-TCC Decreto Supremo Que Aprueba El Texto Único Ordenado de La Ley de Telecomunicaciones (1993).*

1.2.4.9. Decreto Supremo N° 020-2007-MTC, Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones.

Hace una orientación para comprender que una empresa operadora es la persona jurídica o natural que cuenta con contratos de concesión para la explotación de uno o más servicios públicos de telecomunicaciones; asimismo, precisa que el estado es el ente promotor del desarrollo de las TICs, como soporte de la Sociedad Global de la Información; en ese sentido, adoptará medidas necesarias para el crecimiento, expansión, y democratización de uso de las TICs; en ese sentido, se advierte que es el Estado peruano el ente promotor.

El concesionario está obligado a otorgar las garantías que exige el Ministerio de Transportes y Comunicaciones para el cumplimiento de la ley y el contrato de concesión; su incumplimiento, siempre que se consigne explícitamente en el contrato de concesión, será causa de resolución de contrato.

Decreto Supremo N° 020-2007-MTC Texto Único Ordenado Del Reglamento General de La Ley de Telecomunicaciones (2007).

1.2.4.10. Protocolo de Actuación Conjunta de Intervención o grabación de registro de comunicaciones o de otras formas de comunicación aprobado mediante Resolución Administrativa N° 134-2014-CE-PJ.

Este instrumento normativo de naturaleza compleja, uno de los más importantes, establecen las pautas a seguir por la Policía

Nacional del Perú, el Ministerio Público y los Órganos Jurisdiccionales del Poder Judicial, marcando una ruta articulada de las Institución estatales vinculadas durante la intervención de las comunicaciones, ello en la lucha frontal contra la delincuencia y el crimen organizado. Esta interceptación en tiempo real tiene como características principal que no es consentida por los interesados y desconocida por los imputados, esta medida se adopta en el curso de una investigación preliminar de delitos graves, para su gestión se realiza el procedimiento respectivo en los siguientes paso: 1) Informe Policial; 2) Solicitud o requerimiento fiscal; 3) Resolución Judicial (control jurisdiccional); 4) Notificación de la resolución; 5) Ejecución de la medida; 6) Transcripción de las grabaciones; 7) Control o reexamen. *Resolución Administrativa N° 134-2014-CE-PJ (2014).*

Una de las particularidades del presente cuerpo normativo se da en la ejecución de la medida, donde se describe que luego de la notificación de la Resolución Judicial por el Ministerio Público a la DEPATEJUD-DIRANDRO “Constelación”, cumple un rol muy importante el Fiscal Recolector asignado a la sala de “Constelación”, toda vez que es el responsable de supervisar la intervención y control de las comunicaciones; adicionalmente, la gestión de esta interceptación de las comunicaciones se complementan con el apoyo de las empresas operadoras de las telecomunicaciones, pues son ellas que ponen a disposiciones sus sistemas compatibles con los softwares de interceptación en tiempo real.

CAPITULO II: CAUSAS DEL PROBLEMA

En los últimos años, la tecnología ha creado ventanas de oportunidad a la delincuencia, estableciéndose así el cibercrimen; no obstante, esta nueva forma de cometer delitos no solamente aborda aquellas conductas que se comenten usando la tecnología, sino aquellos que usan esta para lograr sus fines. La Ley Orgánica 13/2015 de Modificación de La Ley de Enjuiciamiento Criminal Para El Fortalecimiento de Las Garantías Procesales y La Regulación de Las Medidas de Investigación Tecnológica (2015) en España, advierte que las renovadas formas de delincuencia ligadas al uso de la tecnología pusieron en ese momento la insuficiencia de un cuerpo normativo para tiempos donde la delincuencia pretende estar a la vanguardia, toda vez que los flujos de comunicación generados por los sistemas de comunicación telemática advierten los mecanismos con los cuales se potencia la actividad criminal, pero también proporcionan eficaces instrumentos de investigación al poder estatal en su afán de control social.

De acuerdo con Perea (2017) ha expuesto que los nuevos desafíos del estado como la delincuencia organizada y delincuencia terrorista, deben ser abordados con la utilización de técnicas modernas de investigación, con políticas de encontrarse a la vanguardia de las técnicas delincuenciales, para efectivizar el control de la criminalidad, pues esta se encuentra materializada en el uso de la tecnología como herramienta potencial para el control social, legítima y legalmente para el esclarecimiento de hechos criminales. En ese sentido, López Ruiz (2020) describe que si se pudiese emplear más opciones tecnológicas sería posible resolver delitos violentos o graves en un tiempo muy corto. Es verdad que la tecnología no los es todo, pero sí es un gran aliado que complementa en un punto de partida iniciado por el DEPATEJUD “Constelación” para combatir y evitar los delitos, y ayudar a consolidar como país desarrollado.

2.1. Marco teórico

El programa de Constelación, es dependiente de la DIRANDRO PNP, de acuerdo a López Ruiz (2020) expone que el nacimiento del programa Constelación fue fundamental la cooperación de la Drug Enforcement Administration (DEA) y la

Embajada de los Estados Unidos, toda vez que fue puesto en marcha en un escenario de desconfianza total debido a los casos de escuchas ilegales reveladas por la prensa a fines de los años 90, generando percepción negativa en la población e instituciones del Estado. Hoy en día el programa “Constelación” más que unidad policial es un cúmulo de buenas prácticas, llegando a ser acreditados con el ISO 9001 Certificado del Sistema de Gestión de Calidad, por los procesos realizados y el producto que tiene como agencia estatal de apoyo a la persecución del delito.

No obstante, el programa “Constelación” no cuenta con los recursos necesarios para poder interceptar las comunicaciones por medio del internet; pues, el programa no cuenta con partidas presupuestarias independientes que les permitan ejecutar sus propios lineamientos; máxime, recibe un apoyo constante de la DEA, ello vía cooperación internacional; sin embargo, se advierte que la clase política no ha tomado hasta el momento la debida atención a esta brecha pública que viene limitando el actuar de los funcionarios públicos en investigaciones penales, trayendo como consecuencia el incremento de la impunidad, pues cabe la interrogante: ¿Por qué no se implementa políticas públicas para lograr la interceptación en tiempo real de las comunicaciones por internet?, la respuesta se encuentra en palabras de (Holland, 2017), quien advierte que la clase política muchas veces denota un incumplimiento de la ley de manera intencional ello debido a intereses particulares, pues como se describe en la investigación, las comunicaciones por medio de aplicativos es considerado según la praxis criminal y la sociedad en general, como medios de comunicación pseudo seguros para comunicaciones de carácter altamente privados, demostrándose así con literatura internacional una segunda causa al problema público, que es la falta de atención al problema público por parte de la clase política.

López Ruiz (2020) precisa que Constelación no es una unidad que cumple funciones usuales, su función es muy especial: un error pequeño puede provocar la desestabilización del programa, del comando de la Policía Nacional del Perú,

del gabinete ministerial e incluso del Gobierno, el mismo autor explícitamente dice: *“(...) no podíamos darnos el privilegio de errar, porque luego sería aprovechado por quienes desean quitar esta piedra de su camino, pues cualquier error o exceso será considerado como una mala práctica y mal comparado con los escenarios del espionaje ilegal realizado a finales de los años 90.”*

Por otro lado, el Código Procesal Penal del 2004 en su artículo 230° dice: *“El fiscal, (...) podrá solicitar al Juez de la Investigación Preparatoria la intervención y grabación de comunicaciones telefónicas, radiales, o de otras formas de **comunicación**”*, pues como ha de advertirse el dispositivo legal si aborda el levantamiento del secreto de las comunicaciones, cuando es estrictamente necesario, en el tipo interceptación y de otras formas de comunicación; es ese sentido, haciendo una interpretación extensiva la herramienta legal incluye aquellas que se realizan por medio del internet, precisamente por medio de aplicativos móviles como el Whats App, Facebook, Instagram, Telegram, entre otros; no obstante, el dispositivo legal es muy precario ante la débil capacidad estatal para ejecutar lo dispuesto, pues no basta contar con meras pautas legales producto de la interpretación extensiva de la norma procesal, sino más bien, es necesario diseñar, formular e implementar fórmulas jurídicas de carácter procesal penal que sienten las bases para una óptima recolección de elementos incriminatorios de los grupos criminales, el cual debe estar sujeto a un acompañamiento de políticas de gestión para la implementación de la agencia responsable, los recursos para su financiación en tecnología, infraestructura y demás, como también los procesos que este debe seguir que deben estar estandarizados y automatizados, demostrándose así en la literatura jurídica una segunda causa que es la interpretación extensiva del artículo 231 de Código Procesal Penal, que incrementa los riesgos jurídicos en los procesos penales.

De acuerdo con López Ruiz (2020), expone que la Ley de Telecomunicaciones del Perú y otras normas relacionadas con la prestación de servicios públicos carecen de un capítulo dedicado al apoyo a la justicia, a la seguridad o a la función policial,

como sí ocurre en otros países, es por ello que es necesario para, junto con las empresas que ofrecen algún servicio de telecomunicaciones u otros, optimizar los esfuerzos en la lucha contra la delincuencia y el crimen, pues ha de advertirse una debilidad en la cooperación de las empresas que brindan servicios de telecomunicaciones que – vía contrato- vienen utilizando el espectro radioeléctrico, toda vez que son ellas que no solamente brindan el servicios de llamadas y mensajes, sino también brindan los servicios de internet y gestionan el funcionamiento de los aplicativos móviles, evidenciándose en la literatura nacional una tercera causa que se vincula al problema público, que es la insuficiente colaboración en la administración de justicia de las empresas que ofrecen servicios de telecomunicaciones y otros.

Chipana, Jhoel & López (2019) denomina a las comunicaciones por aplicativos móviles que usan el internet, comunicaciones *App2App* y que la limitación de la interceptación en tiempo real de las comunicaciones en el marco del desarrollo de una investigación limita la búsqueda y el acopio de elementos probatorios para el esclarecimiento de hechos criminales, como también establecer responsabilidades penales a quienes correspondan, puesto que este tipo de flujo comunicacional se canalizan mediante aplicativos móviles que en la actualidad se transmiten y reciben archivos documentales, fotografías, audios, mensajes de texto, llamadas en tiempo real y video llamadas, flujo que no es desarrollado solamente entre dos personas, sino extendiéndose a conferencias grupales utilizando medios tecnológicos entre celulares, tabletas y computadoras; el autor advierte la complejidad para tener acceso al flujo de información pues se realizan usando el internet, máxime en este tipo de comunicación APP2APP, el flujo comunicaciones se realiza únicamente usando como canal el internet de aplicativo a aplicativo, y no como una comunicación convencional que es usuario1 (emisor)-operadora- usuario 2 (receptor).

Para López Ruiz (2020) el entrenamiento de los analistas del Departamento de Apoyo Técnico Judicial “Constelación”, es lo más determinante para el éxito del

programa, pues expone que Constelación trata por todos los medios de mantener a su buen personal, garantizando así la confidencialidad de lo conocido y de la tecnología. Para el autor, tener permanencia de los recursos humanos es un desafío que trae como consecuencia que el personal policial asuma sacrificios de no cumplir aspiraciones en la carrera policial, principalmente porque los indicadores de evaluación para el ascenso son muy generales, elevándose así el costo por consolidar un buen trabajo, haciendo no tan atractiva el puesto permanente para los oficiales y suboficiales que aspiran un ascenso en la carrera, limitando así los recursos humanos debidamente especializados de manera permanente; advirtiéndose en este extremo de la literatura que la parte medular de las interceptaciones telefónicas es la idoneidad del personal policial, por lo que una ausencia de política pública en la carrera de la especialidad en el trabajo de interceptación de las comunicaciones que realiza la DEPATEJUD, incrementa la rotación de personal de oficiales y suboficiales.

En suma, esta es una problemática recientemente generada por el rápido avance de la tecnología y las ventanas de oportunidad creadas y aprovechadas por la criminalidad, y que la literatura internacional como nacional, aun no es tan extensa sobre las interceptaciones de las comunicaciones por internet; sin embargo, de la revisión minuciosa del andamiaje académico, se han advertido las siguientes causas: 1) la falta de atención de la clase política al problema público en cuestión; 2) la interpretación extensiva del artículo 231 de Código Procesal Penal; 3) insuficiente colaboración en la administración de justicia de las empresas que ofrecen servicios de telecomunicaciones y otros; y 4) la ausencia de la una política pública en la carrera policial en el extremo de las labores no convencionales que realizan los analistas del DEPATEJUD “Constelación”.

2.2. Causas del problema

El marco teórico del problema y el trabajo de campo han servido de reflexión para poder identificar y postular cuatro posibles causas a nuestro problema público, siendo las siguientes: 1) ausencia de marco normativo específico para las

interceptaciones de las comunicaciones por internet; 2) insuficiente colaboración de los proveedores de servicios de internet con la administración de justicia; 3) insuficiente tecnología para interceptar las comunicaciones encriptadas por medio del internet en el espectro radio eléctrico; y 4) insuficiente recurso humano idóneo para las operaciones de interceptación de las comunicaciones.

TABLA 1: Análisis causal del problema

Pregunta causal	Objetivos	Hipótesis	Fuentes de dato	Herramientas	Método de análisis
¿Qué genera la falta de capacidad estatal en la Policía Nacional del Perú para interceptar en tiempo real las comunicaciones por internet?	Explicar las causas que generan la falta de capacidad estatal en la Policía Nacional del Perú para interceptar en tiempo real las comunicaciones por internet?	Las causas de la falta de capacidad estatal en la Policía Nacional del Perú para interceptar en tiempo real las comunicaciones por internet son 1) ausencia de marco normativo específico para las interceptaciones de las comunicaciones por internet; 2) insuficiente colaboración de las empresas que brindan servicios por internet con la administración de justicia; 3) falta de implementación de tecnología para interceptar las comunicaciones por medio del internet en el espectro radio eléctrico; y 4) insuficiente recurso humano para las operaciones de interceptación de las comunicaciones.	Policías especialistas en investigación a organizaciones criminales	Entrevistas	Estudio de caso con análisis de información no participante y saturación de respuestas semiestructuradas a entrevistas
			Analistas del DEPATEJUD (Constelación)	Entrevistas	
			Fiscales de Fiscalías Especializadas Contra La Criminalidad Organizada	Entrevistas	
			Funcionarios del Ministerio Público de Transportes y Comunicaciones	Entrevistas/ Revisión de Información	
			Base de datos	Revisión de Información	

Fuente: Elaboración propia

Asimismo, la misma metodología que nos ayuda a postular las causas del problema, también nos permite identificar los efectos que trae cada una de ellas siendo los siguientes: 1) operadores de justicia (Ministerio Público, Poder Judicial y Policía Nacional del Perú) con limitadas herramientas legales para la lucha contra la delincuencia; 2) Insuficientes elementos probatorios para la lucha contra la delincuencia; 3) limitada actuación de la PNP para combatir las organizaciones criminales; y 4) limitada atención y retraso en las operaciones de interceptación en tiempo real, respectivamente.

2.2.1. Ausencia de marco normativo específico para las interceptaciones de las comunicaciones por internet

En el Perú, las comunicaciones son derechos protegidos por la Constitución y esta solamente puede ser vulnerada y conocida por autorización judicial, ello en el marco de una investigación de carácter penal y por delitos únicamente graves, lo cual nos advierte que el derecho al secreto de las comunicaciones no son derechos absolutos, pues se permite la intromisión del Estado en su afán de administrar justicia cuando es estrictamente necesario, en atención y evaluación de principios de proporcionalidad, idoneidad y necesidad; no obstante, la globalización ha incrementado las nuevas formas de comunicación utilizando medios tecnológicos, y más aun siendo aprovechada por elementos criminales, para lo cual el estado no cuenta con marcos normativos explícitos que conceptualicen estas nuevas formas de comunicación por los antisociales, evidenciando la debilidad estatal en la persecución penal estratégica, dejando sin herramientas eficaces y efectivas a los persecutores del delito.

De la revisión del marco normativo de la interceptación legal en tiempo real, se ha podido advertir que el Código Procesal Penal del 2004 en su artículo 230° dice: *“El fiscal, (...) podrá solicitar al Juez de la Investigación Preparatoria la intervención y grabación de comunicaciones telefónicas, radiales, o de otras formas de comunicación”*, pues este dispositivo legal es la fuente para la interceptación en tiempo real de las comunicaciones, y de manera general se establece a las comunicaciones APP2APP, como aquellas otras formas de comunicación; según la práctica del derecho, las normas deben ser explícitas, toda vez que su interpretación extensiva puede causar inconsistencias en los resultados; y es pues esta limitación legal es una causa que limita no solo a los actores de la persecución penal estratégica al encontrarse limitados para formular requerimientos, sino también a los operadores de justicia que en su labor jurisdiccional,

interpretan marcos normativos generales, quedando la autorización judicial de una investigación compleja a criterio de la autoridad jurisdiccional.

Asimismo, si bien el marco procesal penal reconoce la procedibilidad de interceptar en tiempo real otras comunicaciones, como las que se desarrollan por internet, no advierte como se deben desarrollar estas prácticas en el marco de una investigación penal y su articulación con las demás agencias estatales vinculantes, como si lo describe en el caso de interceptaciones en tiempo real de comunicaciones convencionales de operadora a operadora, delegándose la ejecución de la resolución judicial de autorización de interceptación en tiempo real al Departamento de Apoyo Técnico Judicial de la DIRANDRO “Constelación”, estableciéndose protocolos y en un nivel administrativo Directivas Institucionales. En el caso español, la Ley de Enjuiciamiento Criminal reconoce **explícitamente** que las comunicaciones con sesgos criminales que han evolucionado y estas actualmente se desarrollan por medio de herramientas no convencionales utilizando las redes sociales, dotando de mecanismos necesarios para fortalecer su administración de justicia en ese país, como la implementación de softwares de alta tecnología que son de carácter invasivo en los equipos electrónicos de los objetivos.

2.2.2. Insuficiente colaboración de los Proveedores de Servicios de Internet con la administración de justicia.

Estando de acuerdo con López Ruiz (2020) precisa que la Ley de Telecomunicaciones del Perú y otras normas relacionadas con la prestación de servicios públicos carecen de un capítulo dedicado al apoyo de la justicia, a la seguridad o a la función policial, pues el análisis del compendio normativo sobre las telecomunicaciones en el Perú no advierte en ninguna de sus partes la obligatoriedad para con la administración de justicia de las empresas proveedores de servicios de internet, pues es este el pilar por donde se desarrollan las comunicaciones de los aplicativos móviles. Según

la entrevista a los policías especialistas en investigaciones a organizaciones criminales concluyen que las interceptaciones telefónicas es una de las técnicas especiales de investigación más importante y al ejecutar sus operaciones se ven limitados al advertir las comunicaciones por internet de parte de los investigados; aunado a ello, Fiscales de la Fiscalía de Crimen Organizado también concluyen que esta limitación trae como consecuencia que muchos imputados en el curso de una investigación penal, por los elementos de convicción recogidos, no crucen las parcelas de la investigación preparatoria a la acusación fiscal, pese a conocer por medios de inteligencia su participación en las actividades criminales del grupo delictivo, generándose impunidad al no ser incorporados en la acusación fiscal o ser absueltos en la etapa de juicio oral.

Aunado a ello, Oficiales PNP especialistas en investigar a organizaciones criminales y que practican actualmente técnicas especiales de investigación como la interceptación en tiempo real de las comunicaciones, concluyen que los delincuentes cambian frecuentemente el número de su línea telefónica, contando solamente con ella de dos a 15 días, pues para ellos este mecanismo es una manera de burlar las vallas del control estatal, específicamente la capacidad investigativa de los actores de la persecución penal estratégica, pues al contar con otro número telefónico se requiere un nuevo procedimiento de autorización judicial, y más aún la participación diligente de las operadoras telefónicas, siendo un tiempo prudencial para su gestión, tiempo en vacío que es aprovechado para seguir perpetrando sus actividades criminales dichas estructuras delictivas.

Prácticas de Interceptación en tiempo real de las comunicaciones en España, Colombia y Perú, se realizan en alianza a de los Operadores Telefónicos, pues en España la obligatoriedad de su cooperación en la administración de justicia es bajo apercibimiento de su incumplimiento; todo lo contrario, en Perú no se advierte marco normativo alguno de cooperación

con la administración de justicia, más solamente escasos marcos normativos enunciativos y endebles; máxime, los protocolos de interceptación en tiempo real solamente reconocen a las empresas de comunicaciones, más no a los proveedores de servicios de internet, por lo que se requiere que los marcos normativos sean explícitos para una eficaz implementación.

2.2.3. Insuficiente tecnología para interceptar las comunicaciones encriptadas por medio del internet en el espectro radio eléctrico

Las interceptaciones telefónicas se hacen presente con la industria telefónica, y los primeros registros se dieron en Estados Unidos estando a cargo a la Agencia de Seguridad Nacional (NSA), dando sus resultados en la lucha contra el crimen organizado; es por ello, de acuerdo con Ramirez Bustamante (2015), ha destacado que en Estados Unidos, desde hace unos años se han puesto en marcha sistemas de alta tecnología para la intervención telefónica en tiempo real, con gran alcance y cobertura para un seguimiento y vigilancia a nivel nacional e internacional, aprovechando tecnologías vinculadas al internet, puesto que su capacidad de interceptación incluye el flujo comunicacional que se desarrollan a través de aplicativos móviles como el Facebook, WhatsApp, Instagram, Signal entre otros.

El 2001, se ha implementado en España el Sistema de Telecomunicaciones (SITEL), que puso en marcha la implementación de sofisticados sistemas tecnológicos para fortalecer su fuerza estatal en la lucha contra el crimen. Este proyecto tiene cobertura en todo el territorio español, contando para ello un centro de monitorización enlazado con las operadoras telefónicas quienes tienen la obligación de brindar información sobre el flujo comunicacional de los investigados; por otro lado, esta red estatal es trasladada hasta los diferentes puestos de policía a nivel nacional donde se han establecido mecanismos para que la información interceptada y

canalizada a través de los centros de monitorización respecto a audios, videos, imágenes, documentos entre otros, puedan ser reproducidas de manera descentralizada en los puestos policiales

Al respecto, el 2015 mediante una modificación a la Ley de Enjuiciamiento Criminal se destaca el capítulo “La interceptación de las comunicaciones y telemáticas”, se promueve nuevas herramientas tecnológicas para poder realizar el registro remoto de equipos tecnológicos en el marco de una investigación penal y conocer así el flujo comunicacional por aplicativos; pues a nivel mundial se conoce que las comunicaciones por las redes sociales como el Whats App, Facebook, Instagram y muchas otras aplicaciones utilizadas por elementos criminales, se encuentran encriptados de extremo a extremo, siendo inaccesibles para el investigador que persigue conocer legítima y legalmente la información.

Ramírez Bustamante (2015), enfatiza que el rápido avance del desarrollo tecnológico apertura ventanas de oportunidad y ventajas al componente oscuro de la sociedad que es la criminalidad organizada, desafiando el control estatal y poniendo en desventaja la intervención de la fuerza estatal; en la entrevista a un funcionario del Departamento de Apoyo Técnico Judicial “Constelación”, advierte que el programa cuenta con capacidades para interceptar en tiempo real las comunicaciones que se realizan por medio de las cuatro operadoras telefónicas: a) claro; b) movistar; c) entel; y d) bitel; sin embargo, esa capacidad está limitada para las comunicaciones que se desarrollan por medio del internet, pues las comunicaciones estarían encriptadas y requerirían de tecnología superior.

En esa misma línea, otro funcionario del Departamento de Apoyo Técnico Judicial “Constelación”, destaca que las nuevas tendencias criminales, vienen realizando sus flujos comunicacionales usando el internet, mediante el uso de aplicativos como el Whats App, Telegram, Facebook, Signal, o hasta usando comunicaciones por medio de video juegos, por lo que

también dicha unidad se encuentra en constante seguimiento de las nuevas tendencias criminales y proponiendo soluciones para fortalecer sus capacidades, puesto que actualmente esta agencia pública no cuenta con la tecnología para poder interceptar las comunicaciones que se canalizan por medio del internet; demostrándose una ausencia de la capacidad estatal de la Policía Nacional del Perú para ejecutar medidas judiciales que dispongan la interceptación en tiempo real de las comunicaciones por internet y no siendo posible diseñar algún indicador de suficiencia o nivel de capacidad, puesto que evidentemente es una ausencia total de capacidad para el tratamiento de estas comunicaciones no convencionales.

En ese mismo orden de ideas, en la entrevista al Coronel PNP Harvey Julio COLCHADO HUAMANI, especialista en investigar organizaciones criminales destaca que el principal factor que limitan la eficacia en las interceptaciones telefónicas en tiempo real, es la ausencia de tecnología, pues advierte que el programa “Constelación”, que es la unidad encargada de la intervención telefónica, a la fecha solamente intercepta las comunicaciones ordinarias, y no aquellas que se desarrollan por medio de las redes sociales; y es pues así, el programa Constelación ha tenido una evolución desde el 2009, año en que se inició su fundación, contando en un primer momento con 300 líneas y a la fecha ya cuenta con 7000 líneas vigentes para poder interceptar; sin embargo, aún no cuenta con la tecnología suficiente para intervenir el flujo de datos que se desarrollan en el internet los investigados.

Por otro lado, según la División de Investigaciones de Alta Complejidad de la Policía Nacional del Perú, que es una agencia estatal que investiga organizaciones criminales vinculadas a objetivos de alto valor, pone en evidencia que, durante el año 2018, 2019 y 2020, lograron la desarticulación de 89 organizaciones criminales y la detención de 1317 personas, quienes

luego de ejecutar las diligencias preliminares, la autoridad judicial dispuso su detención preliminar, conforme el siguiente detalle:

TABLA 2: Estadística de Organizaciones criminales desarticuladas durante el 2018 al 2020 en la DIVIAC PNP.

	2018	2019	2020	TOTAL
Organizaciones criminales	35	35	19	89
Personas detenidas	655	437	225	1317

Fuente: Elaboración propia en base a la información de la División de Investigaciones de Alta Complejidad de la Policía Nacional del Perú.

De la revisión documental de dichos casos y las entrevistas con los pesquisas quienes cumplen tareas de análisis operativo y estratégico en la División de Investigaciones de Alta Complejidad PNP, se pudo advertir que durante el curso de las investigaciones del 2018 al 2020, las **89 organizaciones criminales evidenciaron durante sus comunicaciones, el uso de aplicativos para la planificación, organización y hasta la ejecución de sus pretensiones delictivas**, es decir el **100%** de las organizaciones criminales investigadas, **evidenciaron interacción criminal usando aplicativos móviles**, el cual debido a la falta de capacidad estatal de la unidad policial que ejecuta las interceptaciones en tiempo real de las comunicaciones, fue imposible en ese momento poder conocer el *iter criminis* de las organizaciones criminales, posicionándolos en una desventaja como entidad persecutora del delito.

2.2.4. Insuficiente recurso humano idóneo para las operaciones de interceptación de las comunicaciones.

López Ruiz (2020) nos advierte que para la implementación del programa Constelación, el insumo principal fue el recurso humano idóneo, pues se

requería personal de alta confiabilidad que guarde la reserva de las comunicaciones que conocería durante las operaciones, para lo cual debían pasar por procesos de inducción y capacitación rigurosos, los cuales en muchos casos de no pasar esos filtros no eran admitidos, debiendo ser incisivos en la selección; también, el responsable del programa Constelación, concluye que el personal policial es el más idóneo y especializado, atendiendo cada uno de cuatro a cinco carpetas de investigación, estando copado la carga laboral de los analistas de Constelación, resultando insuficiente los agentes en esa unidad tan sensible.

La evolución del programa Constelación, a comparación de la región latina, no ha sido mucha, pues en Colombia estas prácticas legales de intervención telefónica inició el 2003, pudiendo intervenir más de 9000 líneas, ello sin considerar que aún se encuentran implementado el programa PUMA (Plataforma Única de Monitoreo y Análisis), con la cual se pretende poder interceptar en tiempo real y previa orden judicial, las comunicaciones por internet, con una capacidad de interceptación de 20 mil medios de comunicación diferentes al mismo tiempo.

Sin embargo, en Perú a la fecha solo se puede intervenir 7000 líneas telefónicas y aquellas comunicaciones por medio de las operadoras; ello nos advierte que más allá de la tecnología, el insumo determinante para esta técnica especial de investigación requiere de un análisis humano, que debe ser el más idóneo y especializado. Según la entrevista al Coronel PNP Harvey Julio COLCHADO HUAMANI, con más de 20 años de experiencia investigando organizaciones criminales, destaca que en el programa Constelación existe un gran déficit de personal, pues cada agente encargado del análisis, tiene a su cargo cuatro a cinco casos, y cada caso aproximadamente de cuatro a cinco líneas telefónicas, por lo que cada analista se hace cargo de unas 20 líneas telefónicas aproximadamente, de

las cuales debe realizar un análisis y comunicar al equipo de investigación tanto al pesquisa policial y el Fiscal encargado del caso.

Al respecto, dichos fundamentos son corroborados por el Coronel PNP Eduardo Frías López, Jefe del Departamento de Apoyo Técnico Judicial de la DIRANDRO “Constelación”, quien destaca que una de las brechas en la gestión realizada en esa unidad de élite policial es el déficit de personal, pues cuentan con capacidad tecnológica para interceptar en tiempo real las comunicaciones que se dan de operadora a operadora móvil, sin embargo, es insuficiente el personal policial idóneo que analizará la información recogida.

Ello nos evidencia que el recurso humano, es muy determinante para fortalecer las prácticas de interceptación en tiempo real de la comunicaciones por internet, y pues de implementarse mecanismos para fortalecer esta técnica especial de investigación, requiere de recursos humanos idóneos y especializados, pues la información requiere de análisis que solamente lo realiza un especialista, más no una máquina o software, pues tiene que valorar la pertinencia y oportunidad de la información que debe ser transmitida a los responsables de la investigación en curso, para que adopten las medidas que correspondan.

CAPÍTULO III: DISEÑO DEL PROTOTIPO

3.1. Problema reformulado y desafío de la innovación

TABLA 3: Índice de jerarquización de las causas

Causas	Dimensiones			Total
	Dimensión 1: Nivel de impacto en el problema	Dimensión 2: Posibilidades de modificación por parte de la organización	Dimensión 3: Se encuentra en el ámbito normativo de la organización desde el cual pretendo generar la intervención	
Ausencia de marco normativo específico para las interceptaciones de las comunicaciones por internet	2	2	2	6
Insuficiente colaboración de los proveedores de servicios de internet con la administración de justicia	0	2	2	4
Insuficiente tecnología para interceptar las comunicaciones encriptadas por medio del internet en el espectro radio eléctrico	1	1	0	2
Insuficiente recurso humano idóneo para las operaciones de interceptación de las comunicaciones	1	1	2	4

Fuente: Elaboración Propia

Después de identificar las causas del problema público en cuestión, según la Tabla N° 04, de la jerarquización de ideas, se advierte que la causa: *“ausencia de marco normativo específico para las interceptaciones de las comunicaciones por internet”*, tiene mayor impacto sobre problema, puesto que ninguna norma legal o marco constitucional describe la evolución de las comunicaciones tecnológicas, y más aún que estas son usadas por elementos antisociales que vienen atentando contra la

seguridad ciudadana, el orden público y el orden interno; es por ello, se requiere de un marco normativo que describa esta brecha pública, que plantee soluciones innovadoras, y muestre como debe implementarse, ello con la finalidad de lograr la interceptación en tiempo real de las comunicaciones por internet.

En ese sentido, la causa elegida para el proyecto de innovación es la causa *“ausencia de marco normativo específico para las interceptaciones de las comunicaciones por internet”*.

TABLA 4: Problema reformulado

Problema	Falta de capacidad estatal de la Policía Nacional del Perú para interceptar en tiempo real las comunicaciones por internet en el año 2018 al 2020.
Causa seleccionada	Ausencia de marco normativo específico para las interceptaciones de las comunicaciones por internet
Problema reformulado	La Policía Nacional del Perú requiere la implementación de un marco normativo específico para las interceptaciones de las comunicaciones por internet, porque actualmente no se puede interceptar en tiempo real las comunicaciones que se desarrollan por este medio.

Fuente: Elaboración propia

El desafío de la innovación que se plantea es: ¿cómo podemos lograr la implementación de un marco normativo específico para las interceptaciones de las comunicaciones por internet?

TABLA 5: Desafío de la innovación

Problema reformulado	La Policía Nacional del Perú requiere la implementación de un marco normativo específico para las interceptaciones de las comunicaciones por internet, porque actualmente no se puede interceptar en tiempo real las comunicaciones que se desarrollan por este medio.
Desafío de innovación	¿Cómo podemos lograr la implementación de un marco normativo específico para las interceptaciones de las comunicaciones por internet?

Fuente: Elaboración propia

3.2. Experiencias previas para hacer frente al desafío de la innovación

3.2.1. Implementación del programa Constelación en el año 2009

El programa “Constelación” se forjó en escenarios adversos donde la sociedad civil tenía mala impresión sobre la interceptación en tiempo real, pues luego de las escuchas ilegales de los años 90 y los Petro audios del 2008, fueron desafíos que la Policía Nacional del Perú con la cooperación de la DEA pudieron superar para lograr implementar la interceptación en tiempo real; ahora, el programa Constelación consiste en un cúmulo de buenas prácticas; cabe precisar para la ejecución de la interceptación legal, se cumplen protocolos con participación del Fiscal, el cual se encuentra adscrito en dicha entidad, convirtiéndose en una entidad multisistémica, llegándose a acreditar con el Certificado del Sistema de Gestión a la Calidad conforme norma ISO 9001:2015, por sus procesos estandarizados y automatizados, y la calidad de sus producto en su gestión de apoyo a la investigación de organizaciones criminales.

3.2.2. Ley australiana contra el cifrado de las aplicativos móviles.

El 2018, Australia aprobó una ley que requeriría que las empresas debiliten su cifrado, una medida que podría repercutir en todo el mundo. Esta medida pública fue dictada por el Parlamento de Australia, el cual consiste en permitir a las agencias de inteligencia y aplicación de la ley de ese país, acceder a las comunicaciones digitales cifradas de extremo a extremos como Whats App, Facebook, entre otras, obligando a debilitar su cifrado por motivos de seguridad pública y derechos humanos.

3.2.3. La Ley Orgánica 13/2015 que modifica la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica en España.

El 2015, España fortaleció sus herramientas persecutoras del delito, implementando el Sistema de Interceptación Legal de las Telecomunicaciones (SITEL), dotando instrumentos legales para la interceptación en tiempo real de las comunicaciones que se desarrollen por aplicativos móviles por medio del internet, más aun aquellas que se encuentran encriptadas, pues implementó un capítulo en la Ley de Enjuiciamiento Criminal de “*registros remotos sobre equipos informáticos*”, donde se precisa que, mediante una autorización judicial se permite la instalación de un software que realice de forma remota y telemática la evaluación a distancia y sin conocimiento del investigado que es titular o usuario del equipo tecnológico, ello en el marco de investigaciones cometidas en el seno de organizaciones criminales, terrorismo, delitos cometidos contra menores, delitos contra la Constitución y delitos cometidos a través de instrumentos informáticos.

3.3. Proceso de la conceptualización y prototipado.

3.3.1. Proceso de conceptualización

Después de conocer las experiencias ya realizadas por actores estatales internacionales respecto al problema público en cuestión, se procede a emplear la técnica de lluvia de ideas para la generación de posibles soluciones, identificándose las siguientes:

- ✓ Revisar el marco procesal penal donde se ubica el problema público, para incorporar o modificar instrumentos legales de ser el caso.

- ✓ Diseño y formulación de un Programa, que realizará las tareas de registros remotos de equipos tecnológicos, que debe depender del DEPATEJUD “Constelación”, de la DIRANDRO.
- ✓ Formulación del plan de implementación del Programa.
- ✓ Implementar Protocolos de Actuación Conjunta Interinstitucional, entre la PNP, Ministerio Público y Poder Judicial, para la puesta en marcha del programa.
- ✓ Selección del personal especializado e idóneo para las tareas para el Programa.
- ✓ Revisión del marco constitucional donde se ubica el problema público, para incorporar o modificar instrumentos legales de ser caso.
- ✓ Implementar tecnología confiable y actualizable al mundo que evoluciona constantemente.
- ✓ Modificar el marco normativo que regula las obligaciones de las empresas de telecomunicaciones y proveedores de servicios de internet.

Ahora se procede a agrupar estas ideas de determinados criterios.

TABLA 6: Grupo de ideas para el desafío de innovación

Grupo de ideas de diseño, formulación e implementación de un Programa	Grupo de ideas respecto a la regulación constitucional	Grupo de ideas respecto a la regulación de las empresas de telecomunicaciones
Revisar el marco procesal penal donde se ubica el problema público, para incorporar o modificar instrumentos legales de ser el caso.	Revisión del marco constitucional donde se ubica el problema público, para incorporar o modificar instrumentos legales de ser caso.	Modificar el marco normativo que regula las obligaciones de las empresas de telecomunicaciones y proveedores de servicios de internet.
Diseño y formulación del Programa “SERPICO”, que realizará las tareas de registros remotos de equipos tecnológicos, que debe depender de la División de Apoyo Técnico Judicial “Constelación”, de la DIRANDRO.		

Formulación del plan de implementación del Programa “SERPICO”.		
Implementar Protocolos de Actuación Conjunta Interinstitucional, entre la Policía Nacional del Perú, Ministerio Público y Poder Judicial, para la puesta en marcha del programa.		
Selección del personal especializado e idóneo para las tareas en el Programa “SERPICO”.		
Implementar tecnología confiable y actualizable al mundo que evoluciona constantemente.		

Por último, se realizará la priorización del grupo de ideas a través de determinados criterios:

TABLA 7: Priorización de ideas para el grupo de ideas para el desafío de innovación

Grupos de ideas	Deseabilidad	Factibilidad	Viabilidad	Impacto	Disrupción	Total
Diseño, formulación e implementación de un Programa	x	x	x	x	x	5
Regulación Constitucional	x	x	-	x	-	3
Regulación de las empresas de Telecomunicaciones	x	x	x	-	-	3

Fuente: Elaboración propia

De este modo, la idea relacionada al diseño, formulación e implementación de un Programa para la interceptación en tiempo real de las comunicaciones por internet es la ganadora del proceso de priorización por lo que en la siguiente etapa se pasará a desarrollar.

TABLA 8: Descripción del bosquejo del concepto

ITEM	CONTENIDO
Denominación de la solución	Diseño, formulación e implementación de un Programa para la interceptación en tiempo real de las comunicaciones por internet.
Población beneficiada de la solución	Departamento de Apoyo Técnico Judicial (DEPATEJUD) de la Policía Nacional del Perú, responsable de la interceptación en tiempo real de las comunicaciones.
Descripción de solución	Diseño y formulación de una fórmula legislativa incorporando instrumentos legales para el <i>registro remoto de equipos tecnológicos</i> , que viabilizará, el diseño y formulación de un Programa que realizará tareas de registros remotos de equipos tecnológicos (celulares), dependiente del DEPATEJUD PNP, el plan de implementación de acuerdo a los recursos disponibles, y el diseño de los protocolos de actuación conjunta interinstitucional entre la Policía Nacional del Perú, Ministerio Público y Poder Judicial.
Descripción breve del beneficio aportado	Este producto permitirá que la Policía Nacional del Perú, cuente con el marco normativo procesal correspondiente para los registros remotos de los equipos tecnológicos, la entidad que estará a cargo, su marco administrativo y el protocolo de actuación interinstitucional, que conllevará al efectivizar la interceptación en tiempo real de las comunicaciones por internet, ello en el marco de una investigación penal.

Fuente: Elaboración propia

La tabla 8 nos muestra que la alternativa de la solución es el Diseño, formulación e implementación de un Programa para la interceptación en tiempo real de las comunicaciones por internet, el mismo que viene complementado con diversas actividades como el desarrollo de protocolos, regulación normativa, implementación de sistemas administrativos entre otros, que se detallaran líneas abajo.

3.3.2. Proceso de prototipado

Se ha procedido a diseñar el producto de la innovación en la presente investigación en el marco del problema de “Falta de capacidad estatal de la Policía Nacional del Perú para interceptar en tiempo real las comunicaciones por internet en el periodo 2018-2020”, donde luego de construir la arquitectura del problema e identificar metodológicamente las causas del problema se escogió el desafío de la innovación siguiente: ¿Cómo podemos lograr la implementación de un marco normativo específico para las interceptaciones de las comunicaciones por internet?, y después de hacer una lluvia de ideas y haber analizado experiencias pasadas, se concluye en el diseño de un PLAN DE IMPLEMENTACIÓN Y EJECUCIÓN DEL PROGRAMA “SERPICO”, que permita solucionar el problema público haciéndolo sostenible en el tiempo, considerando diversas aristas, desde la incorporación de instrumentos legales a la normativa procesal penal, en paralelo con acciones de gestión para su implementación.

La primera versión del PLAN DE IMPLEMENTACIÓN Y EJECUCIÓN denominado “PROGRAMA SERPICO”, fue puesto a consideración de diversos especialistas en la materia de investigación a organizaciones criminales, usuarios finales entre otros, a fin que den sus primeras impresiones y comentarios de mejora a la innovación.

TABLA 9: Primeras impresiones en el testeo del prototipo de innovación

NOMBRES Y APELLIDOS	CARGO	PRIMERAS IMPRESIONES Y DECISIONES
Harvey Julio Colchado Huamaní	Coronel PNP, Jefe de la División de Búsqueda de la	(...) <i>El producto de los registros remotos debe ser entregado al Fiscal y</i>

	DIGIMIN- MININTER. Coordinador General del Equipo Especial de la PNP en apoyo al EFICCOP	<i>únicamente a los pesquisas del equipo de investigación, y no a los agentes de inteligencia.</i>
Edwar Masiel CACHAY DIAZ	Comandante PNP, Participante del XX Programa de Maestría en Ciencias Policiales Administrativas Policiales con mención en inteligencia. Fue responsable del Departamento de Apoyo Técnico Judicial “Constelación”	<i>(...) Si es viable en el factor económico, solo necesitan la aprobación de un proyecto de inversión institucional, programación presupuestal, decisión, voluntad política, planificación y comunicación integral e institucional, sin embargo, es necesario evaluar la ley de protección de datos personales, debido que, en otros países, no está permitido el almacenamiento de los datos personales.</i>
Cinthia Carrillo Cutire	Fiscal Adjunta Provincial de la Fiscalía Especializada Contra la Criminalidad Organizada	<i>(...) El protocolo debe ser lo más preciso posible para tener celeridad durante la ejecución de la medida.</i>

Carlos Martínez García	Capitán PNP en situación actividad, experto en investigaciones contra organizaciones criminales	<i>(...) El proceso de selección del personal policial de la Unidad Funcional Policial que ejecutará la medida, debe ser muy estricto con altos niveles de idoneidad.</i>
------------------------	---	---

Fuente: Elaboración propia.

De la misma manera se ha realizado el focus group con 10 Oficiales con experiencia en investigaciones a organizaciones criminales, quienes al plantear la pregunta “**¿Hasta qué punto es probable que este prototipo sea efectivo para lograr conocer las legal y legítimamente las comunicaciones por internet en tiempo real, de investigados por organización criminal?**”, concluyen que obtener información mediante registros remotos de las organizaciones criminales, les permitiría diligenciar efectivamente las investigaciones que están en curso; asimismo, en otra respuesta concluyen que la voluntad política juega un papel determinante, puesto para el diseño, formulación y promulgación de la norma base para la ejecución del programa y las demás acciones de gestión de su implementación, están sujetas a decisiones de políticos y de la alta dirección; por lo cual indefectiblemente debe buscarse el escenario oportuno para lograr que la problemática sea incorporada a la agenda pública, para que sea admitida y evaluada, aprobando la alternativa de solución propuesta en el presente proyecto de innovación.

3.4. Concepto y prototipo final de la innovación

3.4.1. Concepto final de la innovación

TABLA 10: Descripción del Concepto

ITEM	CONTENIDO
¿Cómo se denomina?	Programa “SERPICO”
¿En qué consiste la solución?	El programa permite que la Policía Nacional del Perú, pueda interceptar en tiempo real las comunicaciones por internet, mediante herramientas de registros remotos a los equipos tecnológicos en el marco de una investigación penal.
¿Para quién es la solución?	Departamento de Apoyo Técnico Judicial (Constelación) de la Policía Nacional del Perú, responsable de la interceptación en tiempo real de las telecomunicaciones.
¿Para qué es la solución?	Para tener mayores elementos probatorios eficaces en el marco de las investigaciones de carácter penal, minimizando la impunidad.
¿Cuáles son los indicadores clave de desempeño (KPI, por sus siglas en ingles) para identificar que la propuesta ha resultado exitosa.	Número de días en las investigaciones de criminalidad organizada hasta la culminación de las diligencias preliminares.
¿Qué valor agrega a los usuarios respecto de lo que hoy existe?	Eficacia y eficiencia en la obtención de elementos probatorios, mediante la interceptación en tiempo real de las comunicaciones por internet
¿Por qué indica que su propuesta es innovadora?	Porque introduce un marco normativo engarzado con mecanismos para su implementación, describiendo los componentes para su creación, implementación y articulación de la Unidad Policial que ejecutará los registros remotos en el marco de las investigaciones a organizaciones criminales.
¿Cuáles son los riesgos asociados a la solución (internos y externos)	El principal riesgo es la falta de voluntad de la clase política o de los decisores para la ejecución del programa “SERPICO”, toda vez que su implementación permitirá obtener información de organizaciones criminales que en la coyuntura actual se han advertido su pertenencia de muchos decisores.

¿Qué impactos positivos tiene la solución en su entorno?	El principal impacto es sustanciar las investigaciones contra organizaciones criminales y a su efectivizar la identificación de nuevos integrantes, deflagrar modo de operación criminal y demás prácticas criminales.
¿Cuáles son las principales acciones de los usuarios?	La Policía Nacional del Perú debe ser capaz de interceptar en tiempo real las comunicaciones por internet.
¿Cuáles son las principales acciones de la organización?	Predisposición y cooperación a nivel normativo, administrativo y presupuestal.
¿Quiénes son sus aliados estratégicos internos?	Policía Nacional del Perú, correspondiente al componente de investigadores, puesto que mediante ellos, conocedores del contexto de la investigación motivarán la ejecución de resoluciones judiciales.
¿Quiénes son sus aliados estratégicos externos?	- Ministerio Público - Poder Judicial

Fuente: Elaboración Propia

3.4.2. Prototipo de alta resolución

A continuación, se presenta el **“PLAN DE IMPLEMENTACIÓN Y EJECUCIÓN DEL “PROGRAMA SERPICO”**, el cual fuera de sus páginas preliminares como I. RESUMEN EJECUTIVO, II. ASPECTOS GENERALES, cuenta con la parte principal respecto a IV. ETAPAS DE LA IMPLEMENTACIÓN DEL PROGRAMA “SERPICO”.

A. PRIMERA ETAPA

PROMULGACIÓN Y PUBLICACIÓN DE LA LEY DEL FORTALECIMIENTO DE LA LUCHA CONTRA EL CRIMEN ORGANIZADO.

La primera etapa del proyecto de innovación consta de implementar con instrumentos legales específicos que regulen las interceptaciones de las comunicaciones por internet, comunicaciones APP2APP, para ello, la

norma legal a implementarse contará con un componente referente a la incorporación del “**SUB CAPÍTULO IV: Registros remotos sobre equipos informáticos**”, en los artículos 234-A, 234-B y 235-C del Código Procesal Penal, conforme al siguiente detalle:

TABLA 11: Alcances para el diseño y formulación del proyecto de ley del fortalecimiento de la lucha contra el crimen organizado.

SUB CAPÍTULO IV: REGISTROS REMOTOS SOBRE EQUIPOS INFORMÁTICOS	
Artículo 234-A.- Presupuestos	<p>1. El juez competente autorizará la utilización e instalación de softwares avanzados, que permitan de forma remota y telemática, la extracción de la información relevante a distancia y sin conocimiento del investigado titular o usuario del dispositivo electrónico, siempre que persiga la investigación de delitos cometidos por organizaciones criminales y organizaciones terroristas.</p> <p>2. La resolución judicial que autorice deberá especificar:</p> <ul style="list-style-type: none"> a. Los dispositivos tecnológicos o parte de los mismos, de donde se conocerá la información y que serán objeto de la medida. b. El alcance de la misma, la forma en la que se procederá al acceso y recolección de los datos o archivos informáticos relevantes para la investigación y el software mediante el que se ejecutará el control de la información. c. Se deberá precisar la Unidad policial que se hará cargo de la ejecución de la medida.

	<p>d. Las medidas que han de adoptarse para salvaguardar los datos almacenados.</p> <p>3. Cuando el personal policial especializado tome conocimiento o tengan razones convincentes para creer que los datos a buscar se encuentran en otro dispositivo tecnológico, pondrán en conocimiento del juez competente dicho hecho, quien podrá autorizar la ampliación correspondiente de la resolución judicial.</p>
Artículo 234-B.- Deber de colaboración.	Los proveedores de servicios de internet están obligados a facilitar a los agentes investigadores la colaboración necesaria para la ejecución de la medida.
Artículo 234-C.- Duración y ejecución de la medida	La medida tendrá una duración máxima 60 días, prorrogable por iguales períodos hasta la culminación de la investigación preliminar. La Policía Nacional del Perú mediante la unidad correspondiente será la encargada de ejecutar dicho acto de investigación, mediante el empleo de tecnología y software correspondiente.

Ahora bien, es imperioso fundamentar la necesidad de gestionar un andamiaje normativo para dotar de bases legales a una nueva herramienta procesal en la búsqueda de las pruebas; en ese sentido, se determinó en el presente proyecto de innovación el diseño y formulación de una ley que fortalezca la lucha contra la criminalidad organizada, incorporando al Código Procesal Penal el **“SUB CAPÍTULO IV: Registros remotos sobre equipos informáticos”** que correspondería al **“Capítulo VII: El Control de las comunicaciones y documentos privados”**, puesto que en dicho apartado solamente describe en sus

articulados la forma de interceptación de comunicaciones por medios convencionales, y en uno de sus extremos extensivamente precisa la intervención de “**otras formas de comunicación**”; no obstante, como bien ya se ha señalado es necesario diseñar normas legales que sean precisas y específicas, máxime aquellas que tienen injerencia en la limitación de derechos fundamentales.

Al respecto, la propuesta legal en concordancia con el cuerpo constitucional normativo, precisa que solamente el Juez será la autoridad que autorice el levantamiento del secreto de las comunicaciones, y en el presente caso correspondería la modalidad de **registro remoto**, ello permitiendo la instalación de un software de manera remota y sin conocimiento del investigado para averiguar adelantadamente la planeación, organización y ejecución de la práctica criminal de las organizaciones estructuradas.

Sobre el particular, si bien la presente propuesta solamente sería ejecutada con autorización judicial, esta se encuentra muy bien alineada a lo dispuesto por nuestra norma constitucional que dice: “*la defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y del estado*”, es por ello la presente norma sentaría bases jurídicas para poder implementar un sistema administrativo que fortalezca el sistema procesal penal en la búsqueda y obtención de las pruebas durante una investigación de criminalidad organizada, toda vez que no es posible crear controversia respecto a un pseudo equilibrio que debería haber entre la forma de obtener pruebas en la investigación criminal con la protección de los derechos fundamentales, puesto que nuestra máximo ordenamiento jurídico dice que es el estado quien debe garantizar la defensa de la persona humana, ello correspondería que debe adoptar medidas diligentes y efectivas para protegerla de entes adversos y desafiantes al estado de tranquilidad y paz de la sociedad,

esto es defenderla de la criminalidad organizada, de aquellas minorías disociales que causan distorsión a la libertad humana, atentan contra su desarrollo y hasta la propia vida de las mayorías de ciudadanos de bien.

En esa línea, la decisión judicial estará condicionada a una evaluación y análisis de necesidad, proporcionalidad e idoneidad, como también a una efectiva fundamentación de hecho y derecho en un primer plano desde el informe policial y luego el requerimiento fiscal, acreditando la necesidad para la investigación para contar con la información de los registros remotos de los equipos tecnológicos de los investigados, descritos y especificados en el requerimiento fiscal. La propuesta normativa, a diferencia del artículo 231 del Código Procesal Penal, es explícito para la autorización de los registros remotos que será aplicable solamente a los equipos de los investigados, no siendo extensible a terceros bajo ninguna circunstancia.

Asimismo, respecto a las conductas criminales que serán materia de evaluación judicial son aquellas vinculadas a organizaciones criminales, en concreto a lo precisado en el artículo 3 de la Ley de Crimen Organizado, esto es: *“1) homicidio calificado- sicariato y la conspiración y el ofrecimiento para el delito de sicariato, de conformidad con los artículos 108, 108-C, 108-D del Código Penal; 2) secuestro, tipificado en el artículo 152 del Código Penal; 3) trata de personas, tipificado en el artículo 153 del Código Penal; 4) Violación del secreto de las comunicaciones, en la modalidad delictiva tipificada en el artículo 162 del Código Penal; 5) delitos contra el patrimonio, en las modalidades delictivas tipificadas en los artículos 186, 189, 195, 196-A y 197 del Código Penal; 6) pornografía infantil, tipificado en el artículo 183-A del Código Penal; 7) extorsión, tipificado en el artículo 200 del Código Penal; 8) usurpación, en las modalidades delictivas tipificadas en los artículos 202 y 204 del Código Penal; 9) delitos informáticos previstos en la ley*

penal; 10) delitos monetarios, en las modalidades delictivas tipificadas en los artículos 252, 253 y 254 del Código Penal; 11) tenencia, fabricación, tráfico ilícito de armas, municiones y explosivos y demás delitos tipificados en los artículos 279, 279-A, 279-B, 279-C y 279-D del Código Penal; 12) delitos contra la salud pública, en las modalidades delictivas tipificadas en los artículos 294-A y 294-B del Código Penal; 13) tráfico ilícito de drogas, en sus diversas modalidades previstas en la Sección II del Capítulo III del Título XII del Libro Segundo del Código Penal; 14) delito de tráfico ilícito de migrantes, en las modalidades delictivas tipificadas en los artículos 303-A y 303-B del Código Penal; 15) delitos ambientales, en las modalidades delictivas tipificadas en los artículos 307-A, 307-B, 307-C, 307-D y 307-E, 310-A, 310-B y 310-C del Código Penal; 16) delito de marcaje o reglaje, previsto en el artículo 317-A del Código Penal; 17) genocidio, desaparición forzada y tortura, tipificados en los artículos 319, 320 y 321 del Código Penal, respectivamente; 18) delitos contra la administración pública, en las modalidades delictivas tipificadas en los artículos 382, 383, 384, 387, 393, 393-A, 394, 395, 396, 397, 397-A, 398, 399, 400 y 401 del Código Penal; 19) delito de falsificación de documentos, tipificado en el primer párrafo del artículo 427 del Código Penal; 20) lavado de activos, en las modalidades delictivas tipificadas en los artículos 1, 2, 3, 4, 5 y 6 del Decreto Legislativo 1106, Decreto Legislativo de lucha eficaz contra el lavado de activos; y 21) en los artículos 153-B, 153-D, 153-F, 153-G, 153-H, 153-I, 153-J, 179, 180, 181 y 181-A del Código Penal.”

Por otro lado, en el cuerpo normativo de las telecomunicaciones, se precisa que debe haber una mera colaboración al estado entre las empresas de brindan servicios de telecomunicaciones, no precisándose una obligatoriedad de parte de estas empresas para con la administración de justicia; es por ello, con la presente propuesta normativa se pretende dotar de bases jurídicas para que a partir de ello,

las empresas de que brindan servicios de telecomunicaciones y en particular las empresas proveedores de servicios de internet sean reguladas por el ente rector, y en estricto estén obligadas a colaborar con la administración de justicia cuando sea necesario, los reglamentos correspondientes del Ministerio de Transportes y Comunicaciones serán los competentes para especificar los puentes con la persecución penal estratégica.

La vulneración legítima y legal de un derecho fundamental, pese a ser necesario, proporcional e idóneo solo debe durar el tiempo estrictamente imprescindible para la averiguación de los hechos que viene perpetrando la organización criminal; se propone que la medida debe ser autorizada por un plazo de 60 días, prorrogables por plazos iguales durante la investigación preliminar, esto toda vez que durante las primeras averiguaciones nos permite encontrar elementos reveladores de la existencia del delito, conocer a sus autores, su modus vivendi y articulación estructural criminal, mediante la utilización de técnicas especiales de investigación complementarias, instrumentos procesales penales innovadores como el secreto de la investigación, entre otras, que son también practicadas durante la etapa preliminar de la investigación, considerada esta como la columna vertebral del proceso penal, pues es esta etapa donde se deben buscar y obtener medios de prueba para que posteriormente permitan crear certeza a la autoridad judicial sobre las conductas criminales de los acusados.

B. SEGUNDA ETAPA

CREACIÓN, IMPLEMENTACIÓN Y ARTICULACIÓN DE LA UNIDAD DE REGISTROS REMOTOS DE LA POLICÍA NACIONAL DEL PERÚ.

1. CREACIÓN DE LA UNIDAD FUNCIONAL DE REGISTROS REMOTOS DE LA POLICÍA NACIONAL DEL PERÚ.

Una vez publicado el instrumento normativo que sienta las bases para gestionar y ejecutar la técnica especial de investigación de “registros remotos”, la Policía Nacional del Perú, mediante la Dirección Nacional de Investigación Criminal de conformidad artículo 99, inciso 2) del Reglamento del Decreto Legislativo N° 1267, Ley de la Policía Nacional del Perú aprobado con Decreto Supremo, precisa que tiene como función: *“Elaborar y proponer al Sub Director General los proyectos normativos destinados a fortalecer el desarrollo funcional, y operativo de las materias especializadas relacionadas con la investigación criminal en el ámbito de su competencia”*; motivo por el cual, deberá promover la creación de la **Unidad Funcional de Registros Remotos de la PNP**, el cual deberá depender del **Departamento de Apoyo Técnico Judicial “CONSTELACIÓN”** de la División de Inteligencia Antidrogas, que a su vez depende de la Dirección Antidrogas de la Policía Nacional del Perú.

La gestión de la creación de la Unidad Funcional en mención, debe regirse a lo establecido en el Decreto Supremo N° 054-2018-PCM que aprueban los “Lineamientos de organización del Estado”, a fin que las agencias estatales se organicen óptimamente de acuerdo al tipo, funciones y competencias, orientadas siempre a satisfacer las necesidades públicas en beneficio de la sociedad y alineado a lo dispuesto en numerales 7.3 y 7.4 del artículo 7, del Decreto

Supremo 054-2018-PCM que establecen que la estructura funcional conglomerada funciones de un programa, proyecto especial, estableciendo líneas de autoridad para una mejor organización, debiendo estructurarse el Manual de Operaciones donde se describirá la estructura funcional y la organización. (Decreto Supremo N° 054-2018-PCM Decreto Supremo Que Aprueba Los Lineamientos de Organización Del Estado, 2018).

También, en la Décima Disposición Complementaria Final del Decreto Supremo N° 054-2018-PCM, modificado con el Decreto Supremo N° 064-2021-PCM, respecto las “Unidades Funcionales”, prescribe que excepcionalmente, es factible conformar una unidad funcional en el interior de un programa o proyecto especial, órgano o unidad orgánica de una entidad estatal, siempre que el volumen de operaciones o recursos se gestione para cumplir con sus funciones de línea o administración interna, así lo justifique, debiéndose establecer las líneas jerárquicas y las responsabilidades de cada organismo.

Guzmán (2020), considera entre tantos a la estrategia, las prioridades institucionales, los recursos, la capacidad operativa y los factores externos que pudiesen afectar el cumplimiento de sus funciones como criterios para un diseño organizacional óptimo y efectivo, pues claro está en el caso en particular, estratégicamente es necesario la creación de esta unidad funcional dependiente del DEPATEJUD, sosteniéndose en su buen prestigio y su calidad de servicio público acreditado, pues dichas agencias tendrían diferente campo funcional; asimismo, por la falta de capacidad estatal de la propia institución policial, es de prioridad institucional la creación de esta agencia pública para que ejecute resoluciones judiciales de registros remotos; en esa misma línea, en los fundamentos del

presente proyecto de innovación se identifica explícitamente los recursos y las capacidades ha tomar en cuenta para la implementación del programa y la puesta en marcha de la Unidad Funcional de Registros Remotos; por último, ha de clarificarse la problemática y crear conciencia en la clase política sobre el rápido avance de practicas criminales usando la tecnología, y urgen desde el estado adoptar medidas más innovativas y efectivas para lograr el control social de las minorías adversas.

La propuesta de creación de la **Unidad Funcional de Registros Remotos de la PNP**, una vez la División de Modernización y Desarrollo Institucional de la Dirección de Planeamiento Institucional de la Policía Nacional del Perú, el Estado Mayor General y el Equipo de Asesoramiento Especial del Comando de Asesoramiento General de la Policía Nacional del Perú, recomienden dar viabilidad y factibilidad a la creación de la citada unidad funcional, esta será aprobada mediante **Resolución de la Comandancia General de la Policía Nacional del Perú**. Un especialista jurídico con más de 20 de años de experiencia en la administración pública, precisa que es imprescindible identificar la prioridad institucional para la creación de una unidad funcional y los efectos que se tendrían interna y externamente en la organización, puesto que la naturaleza de las unidades funcionales es maximizar la especialización y la comunicación.

La Unidad Funcional de Registros Remotos se ubicará en el organigrama de la Policía Nacional del Perú, de la siguiente manera:

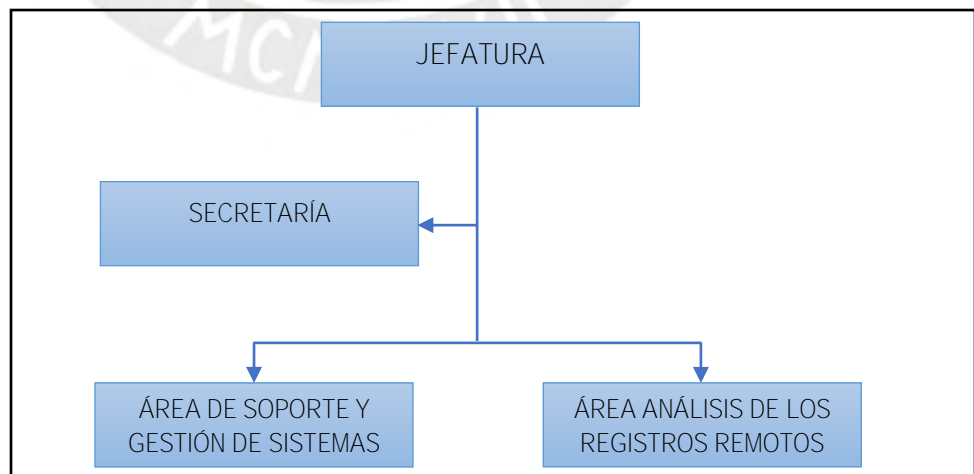
FIGURA 3: Ubicación de la Unidad Funcional de Registros Remotos en el Organigrama de la PNP



Fuente: Elaboración propia

Asimismo, tendrá el siguiente organigrama:

FIGURA 4: Estructura orgánica de la Unidad Funcional de Registros Remotos.



Fuente: Elaboración propia

2. IMPLEMENTACIÓN DE INFRAESTRUCTURA Y RECURSOS

a. INFRAESTRUCTURA

El Departamento de Apoyo Técnico Judicial cederá una sala para el análisis criminal de la intervención mediante registros remotos de equipos tecnológicos, a la Unidad de Registros Remotos de la Policía Nacional del Perú, ello con la finalidad del aprovechamiento de la legitimidad adquirida por el DEPATEJUD-DIRANDRO PNP “Constelación”, respecto al producto que brindan en las interceptaciones en tiempo real de las comunicaciones, contando con la acreditación de alta calidad a sus procesos, el ISO 9001:2015.

Es determinante que la ubicación infraestructural de la nueva Unidad Policial, se encuentre en las mismas instalaciones del DEPATEJUD, pues en este caso monopolizar las interceptaciones en tiempo real de las comunicaciones en general en el citado Departamento, resulta conveniente debido a sus reconocidas buenas prácticas realizadas desde su creación en el año 2009.

b. TECNOLOGÍA

Conforme la literatura internacional, se conoce que la empresa **NSO GROUP**, es una empresa que desarrolla tecnología para ayudar a las agencias gubernamentales a prevenir e investigar delitos de terrorismo, organización criminal y delitos graves, pues es esta empresa propietaria del software **PEGASUS**, que según su propio Manual es una solución de inteligencia cibernética líder en el mundo que permite a las unidades de inteligencia gubernamentales y aquellas entidades de investigación criminal extraer información valiosa de forma

remota y encubierta desde prácticamente cualquier dispositivo móvil.

PEGASUS es un software invisible que se instala en el dispositivo de destino de forma remota con instalación automática, no requiriendo acción alguna por parte del objetivo, teniendo como ventaja no dejar rastro en el dispositivo de destino, en este caso en el dispositivo de destino autorizado judicialmente; luego, este software hace que se extraiga la información del equipo tecnológico del investigado en tiempo real, esto es mensajes, llamadas, videollamadas, mensajes de texto, imágenes, documentos entre otros, que se dan en el flujo comunicacional de investigado con su receptor, transmitiendo este software toda la información de forma segura a una base de datos para su análisis posterior.

Respecto la instalación del software en el dispositivo, a diferencia de los demás productos en el mercado de la ciberseguridad, cuenta con la **instalación remota**, pues basta con un mensaje encubierto de empuje que se envía al dispositivo tecnológico del objetivo este procederá a instalarse de manera automática en equipo del investigado, no requiriendo la cooperación o participación del objetivo p. ej. hacer click en algún enlace, o abrir algún archivo o mensaje, haciéndola totalmente silenciosa e invisible y el objetivo no puede impedirla. Luego de la instalación del software en el dispositivo de destino se logrará la recopilación de una gama de datos:

- (1) Textual: la información que se recopilará corresponde a los mensajes de texto, registro de calendario, correos electrónicos, mensajería instantánea, contactos entre otros.
- (2) Audios: la información que se recopilará corresponde a los audios por llamadas de voz interceptadas en tiempo real,

sonidos ambientales de la grabación del micrófono y otros archivos de audio grabados, **superando el cifrado de los aplicativos de redes sociales utilizados convencionalmente por los objetivos.**

- (3) Visual: la información que se recopilará corresponde a imágenes instantáneas de la cámara, recuperación de fotos y captura de pantalla.
- (4) Ubicación: monitoreo permanente de la ubicación del dispositivo tecnológico.

La variedad de datos que recopila el sistema PEGASUS se muestra en la siguiente figura:

FIGURA 5: Tipos de datos recopilados por el Software “PEGASUS”



Fuente: Elaboración propia en base a la información de la Guía del producto de PEGASUS.

La masiva información que ha de recopilarse una vez instalado el software en el dispositivo de destino, para ver, ordenar, filtrar, consultar y analizar los datos recopilado, PEGASUS incluye herramientas de análisis geográfico para realizar un seguimiento de la ubicación histórica y en tiempo real del objetivo, gestiona grupos de interés, cuenta con herramientas para realizar una búsqueda de términos, nombres, palabras claves, números entre otras opciones.

Ahora bien, una vez que haya culminado en plazo de autorización del registro remoto, el software cuenta con la herramienta de desinstalación, eliminándose y desinstalándose del dispositivo del objetivo, no teniendo ningún efecto en el dispositivo del objetivo.

Respecto a la instalación, la empresa NSO es responsable de implementar y configurar el hardware y software de PEGASUS en las instalaciones de la oficina gubernamental, asegurándose que funcione correctamente.

Las especificaciones del hardware para operar el sistema PEGASUS dependen de la cantidad de agentes virtuales instalados simultáneamente, la cantidad de estaciones de trabajo, la cantidad de datos almacenados y por cuanto tiempo deben almacenarse, teniendo un plazo de 15 semanas para una implementación de la instalación.

Según diversas fuentes de comunicación de España¹ y otros países de Europa, el sistema PEGASUS tendría un costo

¹ <https://elpais.com/espana/2022-04-20/el-cni-pidio-comprar-el-sistema-pegasus-para-espiar-en-el-extranjero.html>

promedio de **seis millones de euros**, y según las informaciones obtenidas recurrentemente requiere actualización de los vectores por la constante actualización de los aplicativos móviles; por ello, es necesario diseñar y formular un proyecto de inversión pública para la adquisición de dicha tecnología expuesta líneas arriba, la cual deberá estar alineada a la Política Nacional Multisectorial de lucha contra el crimen organizado 2019-2030, en el marco del fortalecimiento de las capacidades del estado en la lucha contra las organizaciones criminales.

c. RECURSOS HUMANOS

El personal designado de la Policía Nacional del Perú, perteneciente a la Unidad Funcional de Registros Remotos de la PNP, son seleccionados a través de un procedimiento que incluye entrevista personal, pruebas toxicológicas, pruebas psicológicas, examen médico y prueba del polígrafo, bajo un programa de capacitación y especialización permanente.

El programa debe contener políticas de retención del personal, pues los conocimientos adquiridos por la constante capacitación y su praxis son pilares fundamentales para la operativización del programa “SERPICO”. Considerar que el personal seleccionado tendrá acceso a comunicaciones e información relevante para el caso en investigación, por ello el perfil idóneo para ser parte del componente humano de la Unidad Funcional de Registros Remotos de la PNP es (1) manejo de estrés, (2) experiencia operativa, (3) respeto de leyes, normas y reglas, (4) dominio de herramientas tecnológicas, (5) discreción, (6) confiabilidad y (7) trabajo colaborativo en equipo.

Ahora bien, la selección del personal es uno de los pilares fundamentales para la gestión de cualquier organización pública o privada, por ello es necesario establecer cinco pruebas de evaluación de perfiles para seleccionar a los integrantes más idóneos para el programa.

FIGURA 6: Consideraciones para la selección del personal policial idóneo para la Unidad Funcional de Registros

Remotos de la PNP



Fuente: Elaboración propia

d. GESTIÓN DE LOS PROCESOS INTERNOS

El DEPATEJUD “Constelación” de la DIRANDRO PNP, debido a sus buenas prácticas de trabajo, procedimientos establecidos y articulados con el Ministerio Público, Poder Judicial y demás actores, fue la base para que obtenga el Certificado del Sistema de Gestión de Calidad conforme la norma ISO 9001:2015, por

ello, que es la Unidad de Registros Remotos orgánicamente dependerá de este Departamento especializado en análisis de comunicaciones, para así emular su cultura, buenas prácticas y procesos internos.

Es necesario que la Unidad Funcional de Registros Remotos de la Policía Nacional del Perú, desarrolle la gestión por procesos y se materialice en un manual, donde se especifiquen los procesos estratégicos, procesos misionales u operativos, y cuáles son los procesos de soporte y apoyo, ello permitirá obtener un producto de alta calidad respecto a la información obtenida de los registros remotos, y posteriormente, luego del trabajo articulado con todos los actores, lograr también la Certificación del Sistema de Gestión de Calidad ISO 9001:2015.

Diseñar tales instrumentos, permitirá monitorear y evaluar la gestión de la Unidad de Registros Remotos de la PNP, puesto que será necesario la formulación de indicadores clave que clarifiquen el panorama sobre el estado de la gestión, los recursos y el cumplimiento de su finalidad como Unidad Policial

3. DISEÑO, FORMULACIÓN E IMPLEMENTACIÓN DEL PROTOCOLO DE ACTUACIÓN CONJUNTA INTERINSTITUCIONAL ENTRE LA POLICÍA NACIONAL DEL PERÚ, EL MINISTERIO PÚBLICO Y PODER JUDICIAL PARA LA INTERVENCIÓN O GRABACIÓN MEDIANTE REGISTROS REMOTOS DE EQUIPOS TECNOLÓGICOS.

Posterior a la creación de la Unidad Funcional de Registros Remotos de la PNP dependiente del DEPARTAMENTO DE POLÍTICA Y PLANIFICACIÓN DE LA DIRANDRO, y al haberse implementado el programa con los

recursos logísticos y recursos humanos requeridos, resulta necesario diseñar, formular e implementar el Protocolo de Actuación Conjunta Interinstitucional entre la Policía Nacional del Perú, el Ministerio Público y el Poder Judicial para la intervención o grabación mediante registros remotos de equipos tecnológicos, motivo por el cual a continuación se describen los componentes y consideraciones que deben contener el citado instrumento de gestión para obtener un producto de calidad e incuestionable procesalmente.

ÁMBITO DE APLICACIÓN

La criminalidad organizada viene innovando sus prácticas delictivas, utilizando nuevos canales de comunicación como las llamadas por aplicativo, mensajería instantánea, video conferencias, las cuales se desarrollan por medio del internet, utilizando aplicativos de redes sociales convencionales, y es justamente estas comunicaciones por medio del internet las cuales resulta necesario conocer para una averiguación adelantada en la investigación de delitos graves y aquellos cometidos por organizaciones criminales, recabar las fuentes de prueba y asegurarlas para el proceso.

La interceptación de las comunicaciones en tiempo real, es una herramienta legal precisada en la normativa procesal penal, es de naturaleza compleja y confidencial, pues se realiza de forma no consentida y desconocida por el investigado. Regularmente se ejecuta en el curso de una investigación en etapa de diligencias preliminares por la necesidad de la averiguación adelantada de los hechos en la investigación de delitos graves que puedan servir como elementos de convicción de cargo y posteriormente sirvan como medios de prueba en un escenario de juicio oral.

PROCEDIMIENTO

Paso 1: Informe Policial

La agencia policial que tenga a cargo un expediente de investigación, debe orientar su esfuerzo de búsqueda de información a través de acciones de inteligencia o cualquier otra fuente legítima, ello para obtener datos de identificación tecnológica, esto es números telefónicos, SIM, IMEI, IMSI, dirección IP, correos electrónicos y demás datos que sean aprovechables para individualizar al investigado, y que vengán utilizando equipos tecnológicos durante sus actividades criminales.

La Policía Nacional o el fiscal, cuando sea el caso, verificarán que el número o el dato de identificación del equipo tecnológico usado por el investigado está activo y lo viene usando este, valorando su necesidad, proporcionalidad y legalidad de la medida judicial a solicitar. Se exceptúa los datos obtenidos durante la ejecución de la medida judicial de la intervención de las comunicaciones y de la intervención mediante registros remotos de equipos tecnológicos.

El informe policial deberá contener, los hechos que se viene investigando, el o los delitos atribuidos, las razones de su necesidad, los elementos de convicción, la identidad del equipo tecnológico a intervenir (celular, Tablet, computadora, etc.), la forma de intervención (registro remoto), su alcance (distrito, departamento, en todo el Perú, otros), y su duración como plazo máximo 60 días; deberá precisar que la ejecución de la medida lo realizará la Unidad de Registros Remotos de la Policía Nacional del Perú.

Paso 2: Solicitud o requerimiento fiscal

Recibido el Informe Policial, el Fiscal evaluará si el documento policial está debidamente fundamentado y contiene los datos necesarios. El Fiscal luego de evaluar el informe policial de acuerdo a los presupuestos exigidos por la Ley, y atención a la urgencia en el plazo de 24 horas, formulará el requerimiento correspondiente ante la autoridad judicial, anexando los elementos indiciarios que fundamentan el pedido fiscal. De advertir el Fiscal observaciones en el documento policial, comunicará a la Policía Nacional los motivos de su decisión, requiriendo la debida sustentación con los elementos que resulten necesarios, luego, de considerar pertinente, en un plazo de 24 horas formulará el requerimiento fiscal correspondiente ante la autoridad judicial competente.

El requerimiento fiscal deberá describir el hecho investigado, el delito atribuido que la pena privativa de libertad debe ser superior a cuatro años, cometidos por organizaciones criminales, y organizaciones terroristas, la identidad del equipo tecnológico a intervenir (celular, Tablet, computadora, etc.), la forma de intervención (registro remoto), su alcance (distrito, departamento, en todo el Perú, otros) su duración 60 días; precisar que la ejecución de la medida lo realizará la Unidad de Registros Remotos de la Policía Nacional del Perú.

Paso 3: Resolución Judicial (control jurisdiccional)

El juez competente evaluará el requerimiento fiscal, su debida motivación y si cuenta con los presupuestos establecidos que fundamente su pedido.

La resolución judicial deberá consignar la identificación del dispositivo tecnológico a intervenir (celular, Tablet, computadora, etc.), el investigado o persona vinculada que lo estaría usando, la duración de la medida, disponer la ejecución de la medida sea realizada por la Unidad de Funcional de Registros Remotos de la PNP, deberá indicar que al culminar la ejecución de la medida se comunicará de los resultados obtenidos a la autoridad judicial, para que realice el control respectivo, también deberá precisar que se debe entregar al órgano judicial la información grabada (datos, audios, imágenes, videos, documentos, etc), se debe especificar las obligaciones de los responsables de la Fiscalía y PNP para la ejecución de la medida y la redacción del Acta de Recolección y Control de las comunicaciones con las incidencias que se hayan producido en su desarrollo, para lo cual el acta deberá adjuntar un dispositivo de almacenamiento conteniendo la información obtenida, debidamente lacrado y con la cadena de custodia respectiva. El juez emitirá su decisión en un plazo no mayor de 24 horas.

Paso 4: Notificación de la Resolución

La resolución judicial será notificada al Fiscal que solicitó o requirió la medida con las debidas medidas de seguridad y reserva, pudiendo utilizar medios y herramientas tecnológicas para su debida notificación. La comunicación deberá ser inmediata conforme lo establece el Código Procesal Penal.

Paso 5: Ejecución de la Medida

Una vez que el Fiscal fue notificado con Resolución Judicial que autoriza el registro remoto de equipos tecnológicos,

inmediatamente pone en conocimiento del equipo policial de investigación, solicitando el apoyo de la Unidad Funcional de Registros Remotos de la Policía Nacional del Perú.

En el marco de una mejor articulación y calidad del producto, la Fiscal de la Nación, designará a los Fiscales Titulares necesarios en la Unidad Funcional de Registros Remotos de la PNP, para la administración del componente de gestión de los registros remotos de equipos tecnológicos (aprovisionamiento, ampliación o desactivación de números o cualquier dato de identificación del equipo tecnológico), durante la ejecución de la medida. Las Fiscalías Especializadas y aquellas que se encuentran fuera de Lima que tengan a cargo investigaciones de organizaciones criminales, solicitarán al Fiscal designado como recolector en la Unidad de Registros Remotos, que proceda a aprovisionar los números dispuesto por mandato judicial en el sistema de los registros remotos, remitiendo vía correo institucional la resolución judicial, el cual debe ser legible en todas sus partes, para luego ser entregado directamente al componente de la Unidad de Registros Remotos de la Policía Nacional del Perú para su ejecución.

El Fiscal que requiere la ejecución de la medida, responsable de la investigación, de estimarlo necesario, dispondrá por escrito que la información obtenida en la Unidad Funcional de Registros Remotos de la Policía Nacional del Perú, sea brindada también a un integrante del equipo de la Unidad policial a cargo de la investigación, la cual debe ser las comunicaciones por llamada, audio, video llamada en tiempo real que han de advertirse durante la ejecución de la medida.

El jefe de la Unidad de Registros Remotos de la Policía Nacional del Perú, una vez que reciba la copia certificada de la resolución judicial, que autoriza la intervención de los equipos tecnológicos mediante registros remotos, dispondrá que el personal especializado configure la plataforma y servidores a fin que se proceda a ejecutar la medida judicial.

El personal del Grupo asignado a la intervención de los equipos tecnológicos mediante los registros remotos, bajo la supervisión y control del Fiscal, procederá a formular el Acta correspondiente en cumplimiento de la Resolución Judicial de la información obtenida, referente a grabaciones de llamadas, video llamadas, audios enviados y recibidos, documentos, mensajería instantánea que se adviertan en los aplicativos móviles, las cuales deberán ser grabadas en dispositivos de almacenamiento y posteriormente lacrado, dejándose constancia en el acta en mención, para luego ser entrega al fiscal a cargo de la investigación. Luego de haber vencido el plazo autorizado en la resolución judicial del levantamiento del secreto de las comunicaciones en el tipo de intervención de equipos tecnológicos mediante registros remotos, el Fiscal dispondrá la desactivación de los números, código u otro dato de identificación del equipo tecnológico e informará al Juez dentro de las 24 horas, culminándose de esta manera el procedimiento. Las actas levantadas con la muestra respecto al dispositivo de almacenamiento que contiene la información obtenida, producto de la ejecución de los registros remotos, se incorpora a la investigación para su análisis correspondiente.

Paso 6: Grabación de la información en dispositivos de almacenamiento virtual de las comunicaciones por audio y video, imágenes, documentos y otros,

El fiscal, juntamente con personal de la Unidad Funcional de Registros Remotos, levantará el acta correspondiente sobre la información obtenida, respecto a las comunicaciones por llamada por aplicativo, video llamadas, audios enviados y recibidos, imágenes, documentos y otros, **que deberá ser grabada en dispositivos de almacenamiento virtual para su posterior lacrado y entrega al fiscal a cargo de la investigación.**

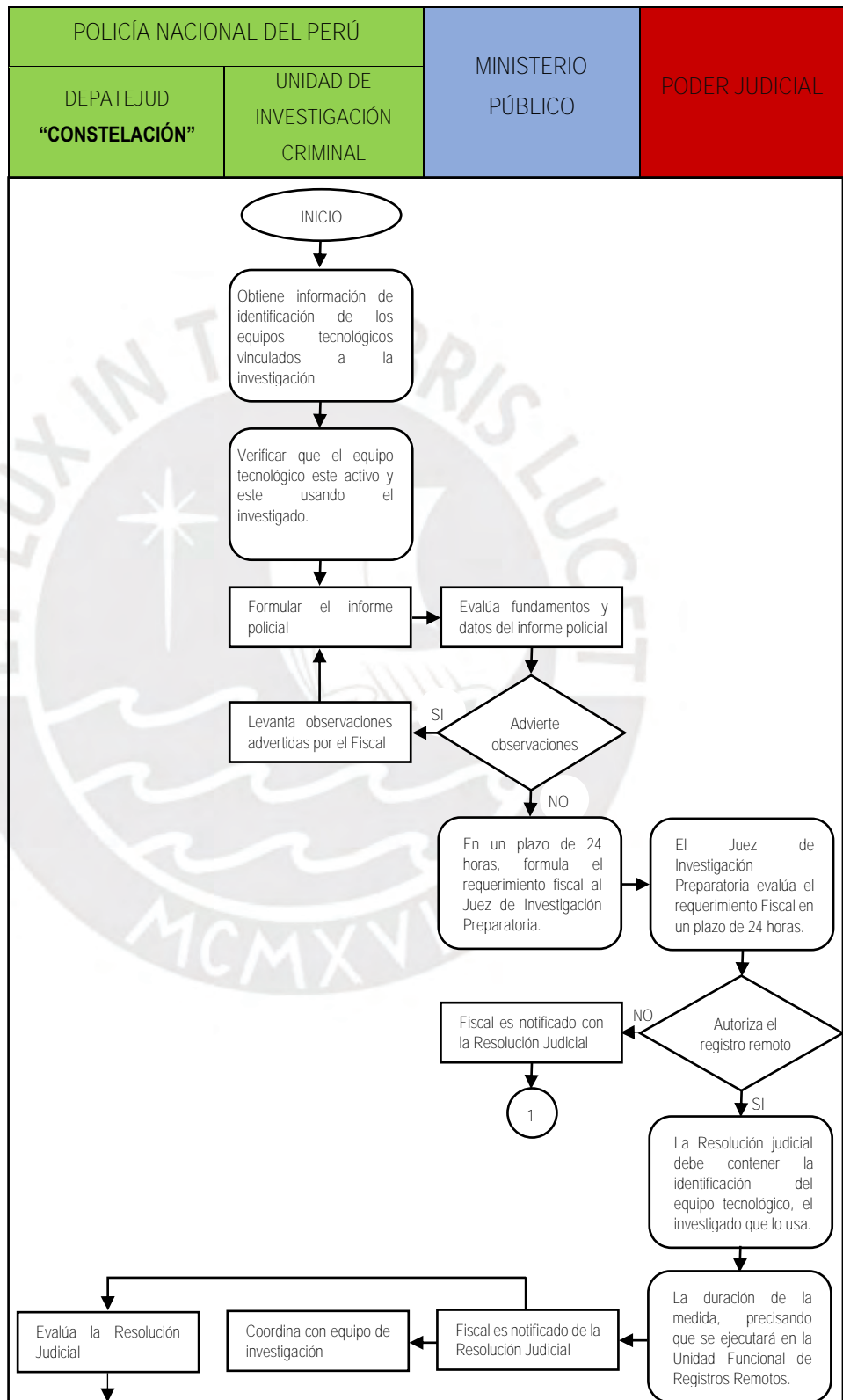
El Fiscal recolector es el responsable de garantizar que la medida cumpla sus fines y está facultado para apartar comunicaciones y demás información no relevante

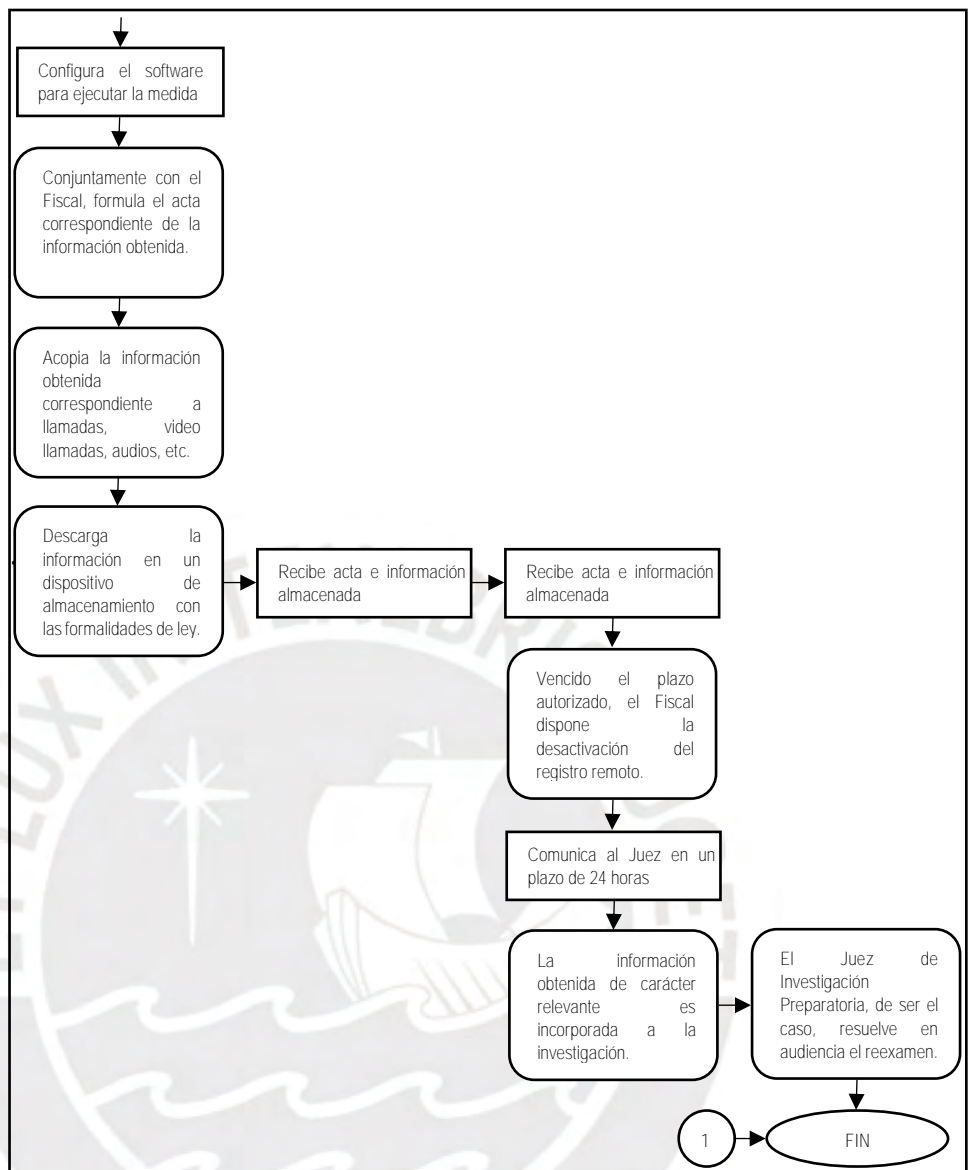
Paso 7: Control o reexamen

Conforme el Código Procesal Penal, en su artículo 231, describe las acciones necesarias para el reexamen judicial, que deberá solicitarse dentro de los tres días de haber sido notificado, el cual se realizará en una audiencia para dicho efecto, donde se observará si el imputado reconoce su propia voz o no entre otras consideraciones, para lo cual deberá estar acompañado de su abogado defensor.

FIGURA 7:

Diagrama de flujo para la ejecución de los registros remotos de equipos tecnológicos en el marco de un proceso penal



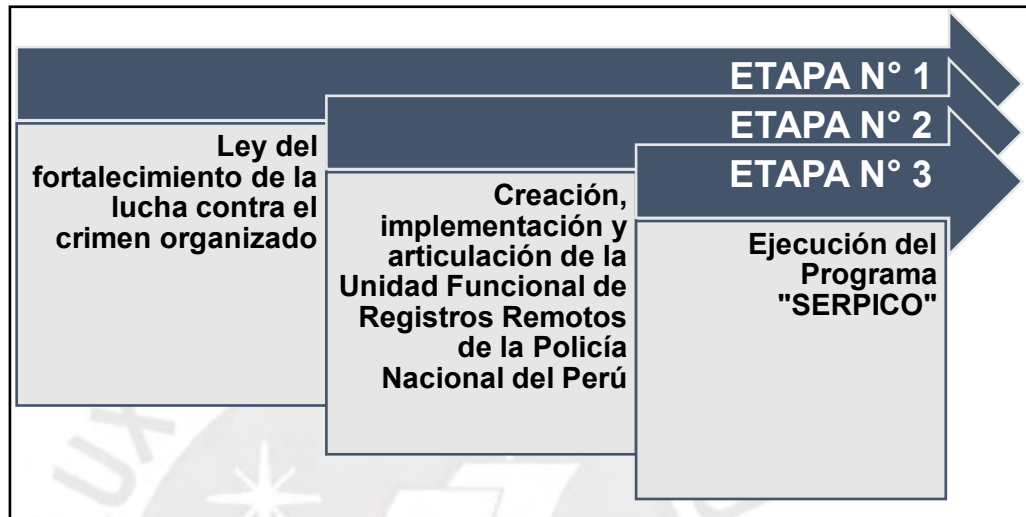


Fuente: Elaboración propia

C. TERCERA ETAPA

EJECUCIÓN DEL PROGRAMA “SERPICO”

FIGURA 8: Etapas de la implementación del Programa “SERPICO”



Fuente: Elaboración propia en base al desarrollo de la investigación.

La presente etapa, es el producto de la articulación de los componentes antes descritos, debiendo ser implementado en el orden desarrollado, puesto que es fundamental primero contar con un marco jurídico procesal para desplegar las gestiones de implementación del programa referente a la creación de la Unidad de Funcional de Registros Remotos de la PNP y su implementación con recursos y tecnología, como también la articulación con los demás actores procesales, en este caso el Ministerio Público y Poder Judicial.

CAPÍTULO IV: ANÁLISIS DE LA DESEABILIDAD, FACTIBILIDAD Y VIABILIDAD DEL PROTOTIPO

4.1. Análisis de la deseabilidad

El prototipo de innovación correspondiente al Plan de Implementación y Ejecución del Programa “SERPICO”, es el resultado de un estudio metodológico para cerrar brechas en la investigación criminal que desarrolla el Ministerio Público y la Policía Nacional del Perú, puesto que, a través del citado programa, que es un cúmulo de componentes, permitirá interceptar en tiempo real las comunicaciones que se desarrollan por aplicativo, es decir APP2APP.

Producto del trabajo de campo, durante las entrevistas a especialistas que ejecutan investigaciones a organizaciones criminales entre policías investigadores y fiscales de crimen organizado, especialistas en interceptaciones de las comunicaciones, pusieron en advertencia la necesidad urgente de implementar sendos instrumentos legales y de gestión que permitan cerrar estas brechas que vienen poniendo en desventaja a la capacidad del estado peruano frente a las practicas innovadoras de la criminalidad organizada, quienes vienen utilizando nuevas tecnologías durante la planificación, organización y ejecución de sus hechos delictivos.

Luego de haber practicado diversas herramientas cualitativas durante el trabajo de campo y el testeo del prototipo, estamos seguros que el Programa “SERPICO”, será recibido positivamente por el Departamento de Apoyo Técnico Judicial “Constelación” fortaleciéndose sus capacidades con la creación, implementación y articulación de la Unidad Funcional de Registros Remotos de la PNP, por las Unidades de Investigación de la PNP que realizan investigaciones de organizaciones criminales, el Ministerio Público a través, el Poder Judicial y claro está a los ciudadanos que día a día son víctimas directas o indirectas de la criminalidad organizada, a partir de la dación de mecanismos legales que regulen su ejecución, puesto que todos esos actores tienen participación durante la gestión

de la interceptación de las comunicaciones por internet mediante los registros remotos.

En la siguiente tabla se observa el análisis de deseabilidad, categorizándose de la siguiente manera:

TABLA 12: Matriz de análisis de viabilidad

Actor	Nivel de Influencia	Nivel de deseabilidad
Investigadores PNP especialistas en criminalidad organizada	Alto	Alto
Fiscales Especializados en Criminalidad Organizada	Alto	Alto
Especialistas en interceptaciones en tiempo real	Alto	Alto
Jueces de Investigación Preparatoria	Medio	Medio

Fuente: Elaboración propia

4.2. Análisis de la factibilidad

El proceso de implementación de la propuesta del prototipo es factible porque genera un panorama de cambio que fortalecerá la capacidad estatal de la Policía Nacional del Perú para interceptar en tiempo real las comunicaciones por internet, y para su funcionamiento se ha considerado reasignar internamente el capital humano que labora en distintas áreas de la Policía Nacional del Perú para especializarlo en la materia, esto con la finalidad de la articulación de los componentes de cada una de las etapas del Programa SERPICO, el cual será a

través de la incorporación de una norma específica fundamental para desplegar las gestiones de implementación del programa a través de la creación de la Unidad de Funcional de Registros Remotos de la PNP con la adquisición de equipos tecnológicos y un sistema que permita dichos registros, indispensable para el desarrollo de las investigaciones en la lucha contra el crimen organizado, permitiendo un trabajo estandarizado y coordinado con los actores procesales, en este caso el Ministerio Público y Poder Judicial.

4.3. Análisis de la viabilidad

El Decreto Legislativo N° 1267 Ley de la Policía Nacional del Perú, destaca en su Título preliminar, artículo II, que: *“La Policía Nacional del Perú es un órgano al servicio de la ciudadanía, que depende del Ministerio del Interior; con competencia administrativa y operativa en el ejercicio de la función policial en todo el territorio nacional, al amparo del artículo 166 de la Constitución Política del Perú”*; en ese último extremo la PNP tiene como finalidad constitucional prevenir, investigar y combatir el crimen organizado, articulándose con el Ministerio Público como un componente más de la persecución penal estratégica.

Asimismo, el Reglamento de la Ley N° 1267 Ley de la Policía Nacional del Perú, aprobado con Decreto Supremo N° 026-2017-IN, precisa en su artículo 99° que: *“La Dirección Nacional de Investigación Criminal es el órgano de línea de la Policía Nacional del Perú, con carácter técnico y sistémico, especializado, normativo y operativo; responsable de planificar, ejecutar, comandar, evaluar y supervisar a nivel nacional las operaciones policiales en materia de lucha contra el terrorismo, antidrogas, medio ambiente, investigación criminal, lavado de activos, trata de personas y tráfico ilícito de migrantes, corrupción, delitos aduaneros, contra los derechos intelectuales, el orden económico, financiero y monetario, y el patrimonio cultural, en el marco de la lucha contra la delincuencia y la criminalidad organizada.”* En ese sentido, la propuesta del prototipo es viable y sostenible

siendo el Ministerio del Interior quien asegura su financiamiento en su implementación y equipamiento al 100%, la Policía Nacional del Perú a través de la Dirección Nacional de Investigación Criminal y su **unidad ejecutora** la Dirección Ejecutiva de Investigación Criminal y Apoyo a la Justicia PNP- DIREICAJ PNP , pues cuenta con la capacidad de gestión para asumir la ejecución de un proyecto inversión para la implementación de la Unidad Funcional de Registros Remotos de la PNP y la adquisición del sistema denominado PEGASUS, herramienta que fortalecerá la capacidad estatal de la Policía Nacional del Perú para interceptar en tiempo real las comunicaciones por internet en la lucha contra el crimen organizado.

TABLA 13: Costo de Inversión

ESTIMACIÓN DE COSTES						
CONCEPTO	CANT.	COSTO UND./ MENSUAL	COSTO TOTAL	CLASIFICADOR	FUENTE DE FINANCIAMIENTO	UNIDAD PRESUPUESTAL
RECURSOS HUMANOS						
Jefe del Programa SERPICO	1	00.0 (Reasignación)	0.00	23.28.11	00. Recursos Ordinarios	Dirección Ejecutiva de Investigación Criminal y Apoyo a la Justicia PNP- DIREICAJ PNP (Recursos Determinados)
Secretaría	1	00.0 (Reasignación)	0.00	21.17.12	00. Recursos Ordinarios	
Área de Soporte y Gestión de Sistemas	5	00.0 (Reasignación)	0.00	23.28.11	00. Recursos Ordinarios	
Área de Análisis de los Registros Remotos	30	00.0 (Reasignación)	0.00	21.17.12	00. Recursos Ordinarios	
SUB TOTAL 1			0.00			
EQUIPAMIENTO						
PC de escritorios (hardware)	22	5,000.00	110,000.00	26.32.31	00. Recursos Ordinarios	DIREICAJ PNP (Recursos Determinados)
Laptops	2	4,000.00	8,000.00	26.31.31	00. Recursos Ordinarios	
Escritorio	22	1,000.00	22,000.00	26.32.22	18. Canon y sobrecanon, regalías, renta de aduanas y participaciones	
Armario	7	500.00	3,500.00	26.32.22	18. Canon y sobrecanon, regalías, renta de	

					aduanas y participaciones	
SUB TOTAL 2			143,500.00			
SISTEMA SOFTWARE						
PEGASUS	1	24,000,000.00	24,000,000.00	26.61.32	19. Recursos por operaciones de crédito	DIREICAJ PNP (Recursos Determinados)
SUBTOTAL 3			24,000,000.00			
PUBLICACIÓN DE INSTRUMENTO NORMATIVO						
Modificación del Código Procesal Penal	1	00.0 (D.S. N° 001-2009-JUS)	0.00	-	-	DIREICAJ PNP (Recursos Determinados)
Creación de la Unidad Funcional de Registros Remotos	1	00.0 (D.S. N° 001-2009-JUS)	0.00	-	-	
SUB TOTAL 4			0.00			
COSTO ESTIMADO TOAL						
SUB TOTAL 1			0.00			
SUB TOTAL 2			143,500.00			
SUB TOTAL 3			24,000,000.00			
SUB TOTAL 4			0.00			
TOTAL			24,143,500.00			DIREICAJ PNP

Fuente: Elaboración propia

La problemática expuesta en los primeros componentes del proyecto de innovación, nos evidencia la existencia de una brecha pública muy determinante en el curso de los procesos penales complejos y de criminalidad organizada, pues tienen efectos en los resultados de percepción y efectividad de la política criminal. Dicha problemática alcanza a todos los ciudadanos en general en el Perú, puesto que son todos ellos quienes son pasibles de ser víctimas de los efectos del crimen organizado, máxime conforme lo expuesto anteriormente según las estadísticas de la PNP entre 2014 y 2018 se registraron 1 507 000 denuncias de víctimas de la delincuencia, de las cuales el **72%** tiene relación con delitos vinculados a organizaciones criminales, incrementándose los índices de inseguridad en el país; ahora bien, en España, Italia y otros países de Europa han implementado sistemas normativos, tecnología y demás instrumentos que son parte de todo un componente, los cuales han permitido interceptar en tiempo real las

comunicaciones por aplicativo a las organizaciones criminales, contando con una capacidad de respuesta ante los retos propios de su seguridad estatal.

Dicha alternativa de solución, identifica claramente el camino que ha de seguirse para su efectiva implementación; ahora bien, actualmente la sociedad clama urgentes políticas públicas de parte de los decisores para el tratamiento de la inseguridad del país, pues esta no permite el desarrollo pleno de los ciudadanos de bien, dado que los desafiantes al estado de derecho constantemente innovan sus prácticas criminales, y el estado peruano en su rol protector y garante de derechos fundamentales de las mayorías, está obligado a limitar derechos fundamentales de aquellas minorías depredadoras del orden social.

En ese contexto, se han especificado claramente las fuentes de financiamiento que sustentarían económicamente el proyecto de innovación; asimismo, actualmente se advierte un clima de inseguridad en el país por los constantes eventos violentos que atentan contra la seguridad de las personas, su propiedad, su libertad y hasta su propia vida, gestándose un escenario político y social oportuno para poder incorporar en la agenda pública la brecha existente en la búsqueda de pruebas al investigar a organizaciones criminales y sus limitaciones que vienen causando impunidad e incrementando el índice delictivo, postulando como principal alternativa de solución el proyecto de innovación propuesto en el presente trabajo académico.

CONCLUSIONES

1. El Estado peruano está sujeto a diversos desafíos y retos, comprendiendo los últimos a los elementos adversos a la sociedad, quienes en forma organizada perpetran actividades criminales, utilizando herramientas tecnológicas de vanguardia para dar rienda a sus pretensiones delictivas, evidenciando la debilidad estatal del Perú, al no contar con mecanismos legales e instrumentos de gestión que permitan luchar contra brechas tecnológicas que atentan contra la sociedad y no permitan un control eficaz de la criminalidad.
2. Los avances de la tecnología han abierto ventanas de oportunidad a diversas actividades de la sociedad, siendo aprovechadas por elementos criminales, el cual utilizando herramientas tecnológicas sincronizadas en internet interactúan por medio de esta y cuando el estado con causa justificada tiene que ejercer su control de la criminalidad, se evidencia la falta de capacidad estatal por parte de las entidades persecutoras del delito al no poder ejecutar sus operaciones para controlar eficazmente la criminalidad, generándose la impunidad como resultado del proceso penal.
3. Se ha evidenciado que en la División de Investigaciones de Alta Complejidad (DIVIAC) de la Policía Nacional del Perú, agencia estatal responsable de la investigación a organizaciones criminales, que en el curso de sus investigaciones del 2018 al 2020 de las 89 organizaciones criminales desarticulares, se evidenciaron en todas ellas el uso de aplicativos virtuales para la planificación, organización y hasta la ejecución de sus pretensiones criminales, precisándose que el 100% de las estructuras delictivas investigadas, interactuaron por medio de aplicativos móviles usando el internet, el cual por la evidente falta de capacidad de estatal de la Policía Nacional del Perú, no se pudo interceptar en tiempo real y por lo tanto no se recogieron elementos de cargo antes sus conductas delictivas, generándose impunidad.

4. La causa principal identificada de la falta de capacidad estatal de la Policía Nacional del Perú para interceptar en tiempo real las comunicaciones por internet es la ausencia de un marco normativo específico que permita ejecutar judicialmente las interceptaciones en tiempo real realizadas mediante los aplicativos móviles, y a partir de esta se puedan realizar gestiones de implementación de sistemas administrativos para su funcionamiento eficaz, toda vez que hasta la fecha se realizan interpretaciones extensivas por parte de los operadores de justicia, lo cuales pueden llevar a cuestionamientos en sus resultados.
5. El desafío de la innovación implementar el Programa “SERPICO”, que tiene como primer componente el diseño y formulación de un cuerpo normativo que permita interceptar en tiempo real las comunicaciones por internet, incorporando un sub capítulo de registros remotos al Código Procesal Penal, decisiones que se encuentran dimensionados y sujetos a la voluntad política; consecuentemente, el segundo componente consta de la creación e implementación de la Unidad de Registros Remotos de la Policía Nacional del Perú que será el organismo responsable de ejecutar medidas judiciales de los investigados integrantes de organizaciones criminales para conocer sus interacciones en aplicativos móviles como WhatsApp, Facebook, Instagram, Telegram entre otros, como también se establecen pautas específicas para la articulación de las entidades estatales vinculadas al procedimiento de registro remoto durante la investigación penal.
6. En el segundo componente se considera la creación de la Unidad Funcional de Registros Remotos de la Policía Nacional del Perú, y se ha establecido que esta debe depender del Departamento de Apoyo Técnico Judicial de la DIRANDRO – PNP “Constelación”, a fin que emule los procedimientos estandarizados y los productos de calidad que brinda en apoyo a la investigación criminal de organizaciones delictivas, pues cuenta con el Certificado del Sistema de Gestión a la Calidad conforme norma ISO 9001:2015.
7. Este proyecto es deseable, factible y viable, en primer lugar porque responde a las necesidades de los investigadores quienes son los principales usuarios y utilizarían

esta herramienta para identificar, ubicar y capturar a integrantes de las organizaciones criminales; asimismo, es viable porque de la voluntad y decisiones políticas y decisiones de gestión pública, podrá generarse un clima de cambio en el control de la criminalidad por parte de las entidades persecutoras del delito; y por último, es viable pues su sostenimiento se encontraría a cargo del Ministerio del Interior encargándose en materia presupuestal para la adquisición e implementación de los recursos e infraestructura.

RECOMENDACIONES

1. La Policía Nacional del Perú mediante el Ministerio del Interior debe convocar a mesas de trabajo técnica a representantes del Ministerio Público, Poder Judicial, Procuraduría, Ministerio de Justicia y Derechos Humano, Colegio de Abogados y demás organismos especialistas en la materia a fin de analizar la problemática planteada y evaluar las alternativas de solución, consensuando un proyecto de ley respecto la incorporación del sub capítulo IV “de los registro remotos” en el Código Procesal Penal y sea enviado al Congreso de la República para su análisis, evaluación y decisión política.
2. Es necesario que la Policía Nacional del Perú, realice actos de sensibilización a los decisores políticos a fin que tomen conciencia sobre la posición de desventaja que se encuentra actualmente las entidades persecutoras del delito en el control de la criminalidad, pues dependerá de la voluntad política para que en primer lugar se admita y aprueba modificaciones legislativas en el Código Procesal Penal y se incorpore instrumentos legales para operativizar los registros remotos durante una investigación penal.
3. Se recomienda a la Policía Nacional del Perú que, mediante sus agencias correspondientes, identifiquen en el desarrollo de sus investigaciones a organizaciones criminales que utilizan canales no convencionales para sus comunicaciones durante sus actividades criminales, a fin de conocer cuales son

aquellos aplicativos seudo seguros que burlan el control de la criminalidad, ello a fin de generar una base datos y tomar decisiones para una gestión eficaz de la investigación criminal.

4. La creación de la Unidad Funcional de Registros Remotos de la Policía Nacional del Perú, deberá ser dependiente del Departamento de Apoyo Técnico Judicial de la DIRANDRO (Constelación), a fin que emule sus buenas prácticas y gestión en apoyo a la investigación de organizaciones criminales, como también sostenerse de su buena reputación que tiene como entidad pública de intervención de las comunicaciones, a fin que se fortalezca su legitimidad por parte de la sociedad y se eviten cualquier controversia durante la ejecución de las resoluciones judiciales.
5. El Ministerio del Interior deberá desplegar recursos presupuestales a la Dirección Ejecutiva de Investigación Criminal y Apoyo a la Justicia, para la adquisición del software “PEGASUS” y demás mobiliario, mediante la formulación de un proyecto de inversión pública, para lograr interceptar en tiempo real las comunicaciones por internet mediante los registros remotos y considerando los demás fundamentos expuestos en el presente trabajo de investigación académica.
6. El personal seleccionado que operativizará los sistemas de la plataforma virtual correspondiente debe cumplir con sendos niveles de idoneidad, evaluar sus referencias, realizar entrevistas personales, pruebas de credibilidad y confianza (polígrafo), examen toxicológico y psicológico, y preferentemente debe haber egresado recientemente de la Escuela de Formación Técnica para que ingrese a conocer información sensible y relevante con un recorrido policial indemne.
7. Las mesas de trabajo técnicas entre los representantes de la Policía Nacional del Perú, Ministerio Público, Poder Judicial, y el Ministerio de Justicia y Derechos Humanos deben concluir su trabajo con la formulación de un Protocolo de Actuación Interinstitucional para la intervención o grabación mediante registros remotos de equipos tecnológicos, a fin de estandarizar y automatizar sus procedimientos durante sus requerimientos, ejecución y control de las medidas judiciales que autoricen el

levantamiento del secreto de las comunicaciones en el extremo de los registros remotos.

REFERENCIAS BIBLIOGRÁFICAS

Abad, S. B. (s.f.). El derecho al secreto de las comunicaciones. Alcances, límites y desarrollo jurisprudencial. *Pensamiento Constitucional Año XVI*, 16.

Altman, D., & Luna, J. P. (2012). Introducción: El Estado latinoamericano en su laberinto. *Revista De Ciencia Política*, 521–544.

Asamblea General de las Naciones Unidas. (2001). *Resolución N° 56/21 sobre lucha contra la utilización de la tecnología de la información con fines delictivos*.

Binder, A. M. (s.f.). *TENSIONES POLÍTICO-CRIMINALES EN EL PROCESO PENAL*.

CEPLAN. (2022). *Capacidad estatal para la entrega de servicios públicos en el Perú: Un análisis exploratorio cuantitativo*. www.ceplan.gob.pe

Chipana, Jhoel; López, J. (2019). ¿Se puede interceptar legalmente las comunicaciones que se hacen a través del WhatsApp? *La Ley El Ángulo Legal de La Noticia*, 1–11.

Código Procesal Penal (2004).

Constitución Política del Perú. (1993).

Dargent Bocanegra, E. (2015). Capacidad de respuesta del Estado en el Perú: Crisis, desafíos y entorno cambiante. *Revista de Ciencia Política y Gobierno*, 2(4), 11–22.

Dargent, E. (2012). *El estado en el Perú: Una agenda de investigación*. Escuela de Gobierno y Políticas Públicas de la Pontificia Universidad Católica del Perú.

Decreto Supremo N° 013-93-TCC Decreto Supremo que aprueba el Texto Único Ordenado de la Ley de Telecomunicaciones. (1993).

Decreto Supremo N° 020-2007-MTC Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones. (2007).

Decreto Supremo N° 054-2018-PCM Decreto Supremo que aprueba los Lineamientos de Organización del Estado. (2018).

Gamboa, M. M., & Domenge, R. (2011). Un modelo de la percepción de la calidad en servicios puros por Internet. Aplicación al sistema de inscripciones en línea en una institución educativa. *Contaduría y Administración. Artículos de Investigación* 11–31.

Guzman, C. (2020). Diseño y estructura de la Administración pública. *Blog Escuela de Posgrado de La Universidad Continental.*

Holland, A. C. (2017). *Forbearance as Redistribution.*

Ley 29733 Ley de protección de datos personales. (2011).

Ley N° 27336 Ley de Desarrollo de las Funciones y facultades del Organismo Supervisor de Inversión Privada en Telecomunicaciones. (2000).

Ley N° 27379 Ley que regula las medidas limitativas de derechos en sede preliminar de la investigación penal. (2000).

Ley N° 27697 Ley que otorga facultad al Fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional. (2002).

Ley N° 30077 Ley Contra el Crimen Organizado. (2013).

Ley N° 30999, Ley de Ciberdefensa. (2019).

Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. (2015). <https://www.boe.es/eli/es/lo/2015/10/05/13>

López Ruiz, L. V. (2020). *Constelación. Prácticas que forjaron sus cimientos.*

Miró Llinares, F. (s.f.). *Delincuencia asociada al uso de las TIC.*

Oficina de Análisis Estratégico Contra la Criminalidad del Ministerio Público. (2021). *Informe de análisis N° 04 Ciberdelincuencia en el Perú: Pautas para una investigación fiscal especializada.*

Perea, L.-B. (2017). Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos. *Revista Internet, Derecho y Político*, 24, 14.

Política Nacional Multisectorial de Lucha Contra el Crimen Organizado 2019-2030. (2019).

Ramirez Bustamante, J. E. (2015). *El sistema de Constelación. Aportes a la lucha contra el crimen desde una perspectiva comparada*.

Resolución Administrativa N° 134-2014-CE-PJ. (2014). *Protocolo de Actuación Conjunta de Intervención o grabación de registro de comunicaciones o de otras formas de comunicación*.

Resolución Legislativa N° 2752. (2001). *Convención de Palermo contra la Delincuencia Transnacional Organizada*.

Sapolinski, J. R. (2018). *Algunas reflexiones sobre el Estado y la seguridad pública* (Vol. 37). <http://orcid.org/0000-0002->

Tanaka, M. (2021). *El desafío del buen gobierno. Intersecciones entre academia, política y gestión pública*.

Tapia Perez, J. (2013). La inseguridad pública: causas y consecuencias. *El Cotidiano* 180, 103–113.

ANEXOS

ANEXO 1: MATRIZ DE CONSISTENCIA DE LA ARQUITECTURA DEL PROBLEMA PÚBLICO

Dimensión de la arquitectura del problema	Preguntas	Objetivos	Hipótesis	Fuentes de dato	Herramientas
Magnitud del Problema	Pregunta 1: ¿De qué manera influyó la limitación de no poder interceptar en tiempo real las comunicaciones por internet, en la recopilación de elementos de convicción en investigaciones a organizaciones criminales en la División de Investigaciones de Alta Complejidad y la División de Investigación de Crimen Organizado de la PNP, en el año 2018 al 2020?	Explicar la influencia de la limitación de no poder interceptar en tiempo real las comunicaciones por internet en la División de Investigaciones de Alta Complejidad y la División de Investigación de Crimen Organizado de la PNP en el año 2018 al 2020, respecto a la recopilación de elementos de convicción en investigaciones a organizaciones criminales?	Se estima que la División de Investigaciones de Alta Complejidad -DIVIAC, logró la desarticulación de 120 veinte organizaciones criminales, logrando identificar, ubicar y capturar a más 2500 personas, estimándose que no se logró acopiar evidencia probatoria para un 50% de investigados. Los aplicativos más convencionales que utilizan los integrantes de organizaciones criminales para sus comunicaciones por internet son el Whats app, messenger, instagram y telegram.	Instructores de caso	Entrevista/ Encuestas
				Fiscales de Crimen Organizado	Entrevista
				Base de datos de la DIVIAC	Revisión de la información
Actores en el proceso de investigación de organizaciones criminales	Pregunta 2: ¿Quiénes son los actores que participan en el proceso de investigación de organizaciones criminales, en el periodo 2018-2020?	Determinar quienes son los actores que participan en el proceso de investigación de organizaciones criminales, el periodo 2018-2020?	Los actores que participan en el proceso de investigación de las organizaciones criminales son los pesquisas policiales, el juez de la investigación preparatoria, el fiscal encargado del caso, analistas de investigación, analistas de la DEPATEJUD "Constelación")	Instructor del caso	Entrevista
				Pesquisas Policiales	Focus Group
				Fiscal encargado del caso	Entrevista
				Analistas de Investigación Analistas de la DEPATEJUD "Constelación"	Focus Group Observación no participante
Proceso de intervención y grabación en tiempo real de las comunicaciones	Pregunta 3: ¿Cómo se desarrolla las intervenciones y grabaciones de las comunicaciones en tiempo real?	Describir el proceso de intervención y grabación en tiempo real de las comunicaciones	El juez, el fiscal, el pesquisas instructor del caso y los analistas de la DEPATEJUD "Constelación", son los encargados de dar cumplimiento a la autorización de interceptación y grabación en tiempo real de las comunicaciones	Instructor de caso	Entrevista
				Fiscal encargado del caso	Entrevista
				Protocolos de Actuación Conjunta para la intervención y grabación en tiempo real de las comunicaciones	Revisión documental
				Analista de la DEPATEJUD-"Constelación"	Entrevista
Relación Interinstitucional	Pregunta 4: ¿Cómo se engarzan las agencias estatales vinculadas a las investigaciones de organizaciones criminales, cuando se gestionan las interceptaciones en tiempo real de las comunicaciones?	Describir la forma de articulación de las agencias estatales que gestionan las interceptaciones en tiempo real de las comunicaciones.	Las instituciones comprometidas en la gestión del levantamiento del secreto de las comunicaciones va desde la Policía Nacional del Perú, el Ministerio Público y el Juez de la Investigación Preparatoria; no obstante, es necesario conocer el rol de la autoridad rectora de las telecomunicaciones (MTC), como el rol de la autoridad reguladora de las telecomunicaciones (OSIPTEL).	Fiscal de Crimen Organizado	Entrevista
				Jefe de la DIVIAC	Entrevista
				Juez de Investigación Preparatoria	Entrevista
				Ministerio de Transportes y Comunicaciones	Revisión de información (Normas, contratos de concesión, licencias, etc.)
				OSIPTEL	Revisión de Información
Relación Intrainstitucional	Pregunta 5: ¿Cuáles son los factores que limitan las interceptaciones legales de las comunicaciones por internet en tiempo real en el Departamento de Apoyo Técnico Judicial - DIRANDRO "Constelación"?	Determinar los factores que limitan las interceptaciones legales de las comunicaciones por internet en tiempo real en el Departamento de Apoyo Técnico Judicial - DIRANDRO "Constelación"	Los factores mas determinantes que limitan las interceptaciones en tiempo real de las comunicaciones por internet son: 1) no contar con los sistemas tecnológicos operativos adecuados, 2) la falta de decisión política para la lucha frontal contra el crimen organizado, 3) la ausencia de mecanismos legales que obliguen a los operadores de las telecomunicaciones a coadyuvar con la administración de justicia.	Jefe del DEPATEJUD-DIRANDRO "Constelación"	Entrevista
				Base de datos de la DEPATEJUD-DIRANDRO "Constelación"	Revisión de la información

Fuente: Elaboración propia

ANEXO 2: CADENA DE VALOR ASOCIADA

INSUMOS	PROCESOS	PRODUCTOS	RESULTADOS ESPERADOS
<ul style="list-style-type: none"> • Marco normativo que regula el levantamiento del secreto de las comunicaciones y telecomunicaciones. • Normas que regulan los contratos con las empresas móviles • Normas que regulan el campo funcional de OSIPTEL • Marco normativo del DEPAJEJUD PNP-Constelación • Normas ISO, que garantizan la calidad de la gestión. • Recursos logísticos, personal. • Base de datos de investigaciones de organizaciones criminales • Sistemas tecnológicos para la interceptación en tiempo real. 	<ul style="list-style-type: none"> • Protocolos Interinstitucionales. • Guías de Intervención, Instructivos. • Manuales de Procedimientos • Técnicas Especiales de Investigación 	<ul style="list-style-type: none"> • Regulación de las aplicaciones que permite comunicaciones por internet. • Eficiencia en la Investigación policial de organizaciones criminales. • Acusaciones penales ricas en elementos probatorias. • Sistemas tecnológicos para la interceptación en tiempo real de las comunicaciones por internet 	<ul style="list-style-type: none"> • Interceptación en tiempo real de las comunicaciones por internet. • Investigación eficiente, que permita fundamentar una acusación penal y lograr posteriores sentencias condenatorias que fortalezcan el control de la criminalidad.

Fuente: Elaboración propia

ANEXO 3: GUÍA DE ENTREVISTA

La entrevista se realizará a un Oficial de la Policía Nacional del Perú mayor de 30 años que labore actualmente investigando organizaciones criminales, con una experiencia mayor de 3 años.

Nombre del entrevistador:

1. Datos Generales

- 1.1. Fecha :
- 1.2. Lugar :
- 1.3. Nombre del entrevistado/a :
- 1.4. Género :
- 1.5. Edad :
- 1.6. Grado :
- 1.7. Tiempo de servicio en la PNP :

2. Datos del servicio

- 1.1 ¿En qué unidad donde presta servicios?
- 1.2
- 1.3 ¿Qué cargo que ocupa en la Unidad PNP?
- 1.4 ¿Describa las actividades laborales que desarrolla?
- 1.5 ¿Cuál es su formación académica en investigación de organizaciones criminales?
- 1.6 ¿Cuál es su experiencia en investigación de organizaciones criminales?
- 1.7 ¿Qué tiempo de capacitación en uso y manejo de herramientas tecnológicas?
- 1.8 ¿Qué Técnicas especiales de investigación viene usando con frecuencia?
- 1.9 ¿Cuáles considera más importantes y necesarias, y cuáles no?

3. Datos de la investigación

- 3.1 ¿Cuánto dura una investigación promedio de organizaciones criminales?
- 3.2 ¿Cómo procesan la información del resultado de la interceptación en tiempo real de las comunicaciones?

- 3.3 ¿Cuáles son las limitaciones que impiden la eficacia en las investigaciones de organizaciones criminales?
- 3.4 ¿Durante su experiencia, ha advertido mediante el resultado de la interceptación en tiempo real de las comunicaciones, que los integrantes de organizaciones criminales se comunican mediante llamadas por internet?
- 3.5 ¿Respecto a la respuesta anterior, ¿cuáles fueron las acciones que adoptó su equipo de investigación?
- 3.6 ¿Qué efectos emocionales causó en su equipo de investigación, la limitación de no contar con la información necesaria cuando los integrantes de las organizaciones criminales se comunicaban por aplicativos mediante el internet?

4. Datos de las instalaciones y los recursos

- 4.1 ¿Cuentan con los recursos logísticos para realizar investigación de organizaciones criminales?
- 4.2 ¿Describa alguna instalación donde se investigan y analizan información de investigaciones a organizaciones criminales?
- 4.3 ¿Existe personal externo que los capacita? ¿Con qué frecuencia?
- 4.3 ¿La velocidad de internet de las instalaciones le permite trabajar de forma cómoda?
- 4.4 ¿Comparten equipos tecnológicos (computadoras, laptops) con otros agentes o cada uno tiene su estación de trabajo?
- 4.5 ¿Los vehículos son suficientes para realizar el trabajo de campo?
- 4.6 ¿Podría mencionar 3 aspectos positivos sobre las instalaciones?
- 4.7 ¿Podría realizar 3 sugerencias para mejorar las instalaciones?
- 4.8 ¿Qué recursos serían necesarios para potenciar las investigaciones contra las organizaciones criminales?

5. Final

- 5.1 ¿Qué recomendaría ante la limitación de no poder interceptar legítimamente las comunicaciones que se desarrollan por internet?
- 5.2 ¿Agregarías alguna pregunta?

ANEXO 4: GUÍA DE GRUPO FOCAL

Objetivos del grupo focal:

Perfil de los participantes: Oficiales de la Policía Nacional del Perú, mayores de 30 años que laboran investigando a organizaciones criminales, con una experiencia mayor de 3 años.

A. Conocimientos básicos

1. ¿Conoce usted qué es una Organización Criminal?
2. ¿Conoce de qué manera pueden usar las Técnicas Especiales de Investigación?

B. Investigación

1. ¿Cuáles son las limitaciones que afrontan al realizar una investigación?
2. ¿Con qué recursos cuentan para realizar una investigación?
3. ¿Suelen tener reconocimientos por su trabajo?

C. Resultado de las investigaciones

1. ¿Considera usted que los equipos de investigación cuenten con el personal adecuado y suficiente?
2. ¿El tiempo para que un agente proceda con la investigación de la denuncia es adecuado? En caso de ser mayor: ¿Por qué sucede eso?
3. ¿Cuál es el rol del Ministerio Público al tomar conocimiento de la limitación de interceptar comunicaciones por internet?

D. Procedimientos

1. ¿Los equipos de investigación de organizaciones criminales son conocedores de los procedimientos y están familiarizados con ellos?
2. ¿Cuál es la técnica especial de investigación más recurrente?
3. ¿Cuál es la técnica especial de investigación menos recurrente?

E. Motivación

1. ¿Se encuentran motivados al realizar sus labores?
2. ¿Consideran trabajan con las herramientas adecuadas?
3. ¿Qué recomendarían para mejorar sus limitaciones generales?