MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
METROPOLITANA SANTIAGO DE CALI
GRUPO TECN DE LA INFORMACIÓN Y LAS COMUNICACIONES MECAL

No. GS-2026-0 1 6 3 6 7 GUDES - GUTIC - 20.1

Santiago de Cali, 2 9 ENE 2026

ALCALDÍA DE SANTIAGO DE CALI
No. 2026-4173010-014123-2
Asunto: REMITE PROYECTOS DE IN VERSION
Fecha Radicado 29/01/2026 04:35:56
Usuario Radicador CATALINA ROSERO Folios
Destino SECRETARÍA DE SEGURIDAD Y JUSTICIA
Remitente (CIU) MINISTERIO DE DEFENSA N ID. 800141397
Visite Nuestra Pagina - http://www.cali.gov.co
Santiago de Cali (Valle del Cauca) Cam Torre Alcaldía Línea 195
20264173010014123 2

Doctor
ÁLVARO ALEJANDRO EDER GARCÉS
Alcalde de Santiago de Cali
Avenida 3N 8N-58 barrio Granada
Santiago de Cali - Valle del Cauca

Asunto: envío proyectos de inversión POAI 20[illegible]

Cordial saludo, de manera atenta me permito enviar a su despacho, los proyectos de inversión priorizado en el Plan Operativo Anual de Inversiones vigencia 2026, de la secretaria de Seguridad y Justicia, Alcaldía Distrital de Santiago de Cali, aprobado en Comité de Orden Público realizado el 03 de diciembre de 2025, mediante Acta No 4161.040.3.2.582, direccionado a garantizar el servicio de policía y cumplir las estrategias de Convivencia y seguridad ciudadana, así:

No	PROYECTOS DE INVERSIÓN 2026	DESCRIPCIÓN
1	Adquisición del servicio de voz y datos para dispositivos PDA y líneas telefónicas de comandantes con inclusión de equipo móvil celular por valor de $2.364.000.000.	Suministra servicio de voz y datos para las PDA, líneas celular y fortalecer la atención de motivos de Policía.
2	Adquirir equipos de cómputo con licenciamiento para las estaciones de Policía que prestan su servicio en el Distrito Especial de Santiago de Cali por valor de $157.500.000.	Adquisición de computadores All IN ONE y paquete ofimático.

Atentamente,

Coronel **ANDRÉS ARIAS BUITRAGO**
Comandante Policía Metropolitana Santiago de Cali (E)

Elaboró: SC. URIEL GUTIERREZ RENGIFO
MECAL - GESTER

Revisó: IJ. YAMIT ARVEY NARVÁEZ RAMÍREZ
MECAL - GUTIC

Revisó: CT. DUVAN CASANOVA VASCO
MECAL - GUTIC

Fecha de elaboración: 28/01/2026
Ubicación: C:\\mis documentos\informes 2026

Calle 21 1N-65, barrio El Piloto
Teléfono I.P: 882-6171
mecal.gester-jef@policia.gov.co
www.policia.gov.co

INFORMACIÓN PÚBLICA

Página: 1 de 26	DIRECCIONAMIENTO ESTRATÉGICO	POLICÍA NACIONAL
Código: 1DE-FR-0051		
Fecha: 02-07-2024	**FORMULACIÓN DE PROYECTOS Y PROGRAMAS EN LA POLICÍA NACIONAL**	
Versión: 1		

FECHA	29 ENE 2026
UNIDAD QUE LO PRESENTA	Policía Metropolitana Santiago de Cali - Grupo de Tecnologías de la Información y las Comunicaciones.
NOMBRE DEL PROYECTO	ADQUISICIÓN DEL SERVICIO DE VOZ Y DATOS PARA DISPOSITIVOS PDA Y LÍNEAS TELEFÓNICAS DE COMANDANTES, CON INCLUSIÓN DE EQUIPO MÓVIL CELULAR.
LÍNEA DE INVERSIÓN	[ ] Infraestructura [ ] Adquisición de predios [ ] Estudios y diseños [ ] Construcción [ ] Ampliación [ ] Adecuación [ ] Mantenimientos [ ] Movilidad [ ] Terrestre [ ] Aérea [ ] Fluvial [ ] Mantenimiento aeronáutico [ ] Armamento [ ] Intendencia [X] Tecnología y comunicaciones [ ] Política educativa [ ] Programas de prevención [ ] Bienestar social y familia [ ] Sanidad [ ] Otros ¿Cuál? [ ]
ENTIDAD A LA QUE VA DIRIGIDO	Alcaldía Distrital Santiago de Cali – Valle del Cauca. [x] Nacional [ ] Internacional
PRESUPUESTO TOTAL	$ 2.364.000.000,00
COFINANCIACIÓN	[ ] Sí [x] NO
FASES DEL PROYECTO	[x] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ] Mas de 5
DURACIÓN DEL PROYECTO	Doce (12) meses.

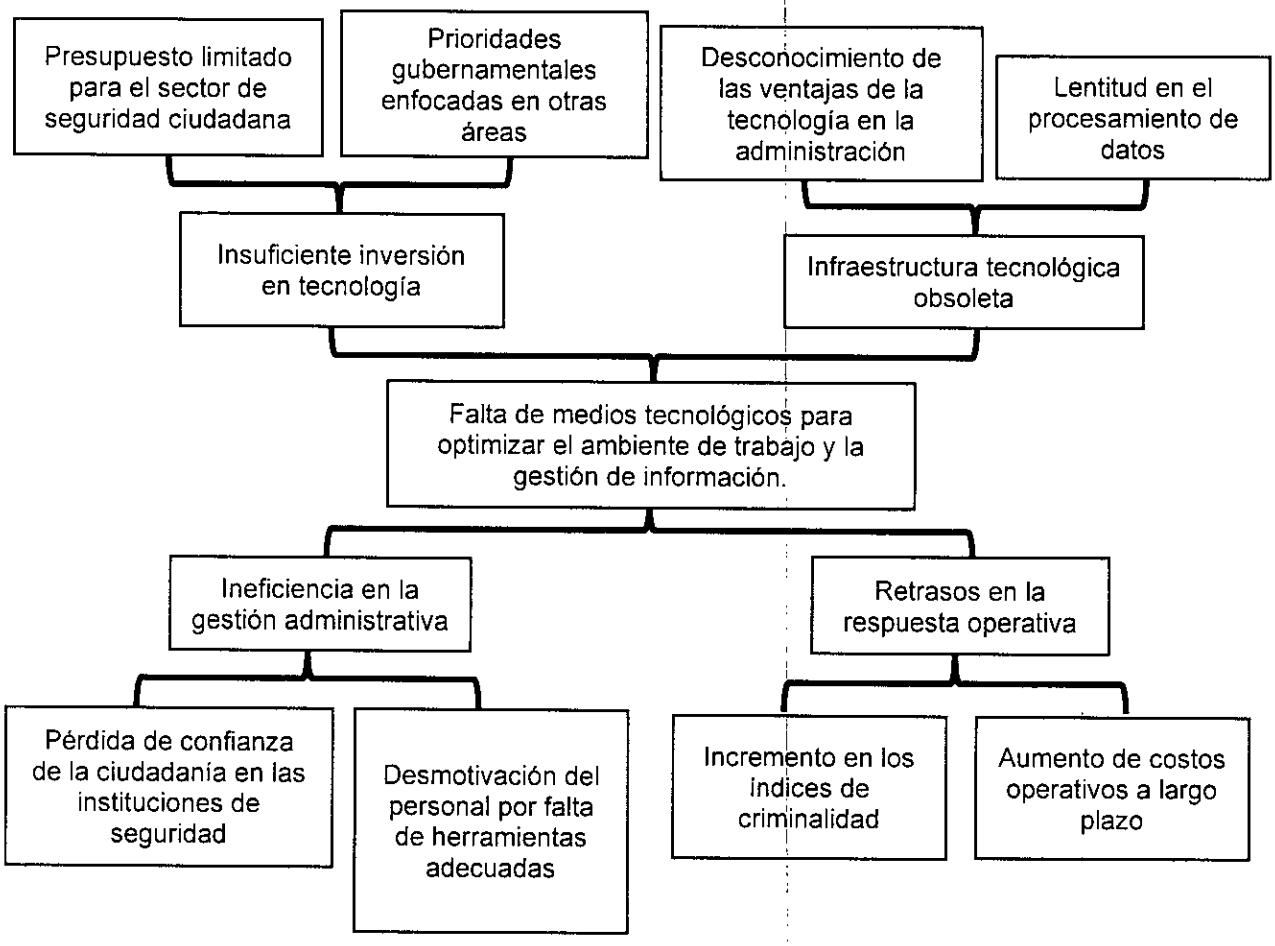
1. ANÁLISIS DEL PROBLEMA

La ciudad de Santiago de Cali enfrenta una serie de desafíos significativos en términos de seguridad, con delitos de alto impacto que pueden afectar la vida diaria de sus habitantes. Entre los principales desafíos se encuentra la prevención de los homicidios, los hurtos, las lesiones personales y el microtráfico de drogas. Estos delitos no solo generan un ambiente de inseguridad, sino que también afectan la percepción de la ciudad a nivel nacional.

Para abordar estos problemas, es esencial implementar estrategias de prevención basadas en experiencias exitosas de otras ciudades como involucrar a la comunidad en programas de prevención del delito y promoción de la convivencia pacífica también es crucial, mejorar la infraestructura urbana, asegurando una buena iluminación en las calles y mejorando los espacios públicos, puede reducir las oportunidades de delitos. Además, implementar programas educativos y de empleo para jóvenes en riesgo puede reducir su vulnerabilidad y ofrecerles alternativas positivas.

El problema de seguridad en Cali es complejo y multifacético, pero con un enfoque integral que combine recursos adecuados, justicia eficiente y participación comunitaria, es posible reducir la incidencia de delitos y mejorar la calidad de vida de sus habitantes. La colaboración entre el gobierno, las fuerzas de seguridad y la comunidad es esencial para lograr un cambio significativo y duradero.

1. ARBOL DE PROBLEMAS



2. DESCRIPCIÓN DEL PROBLEMA

Santiago de Cali, una de las principales ciudades de Colombia, enfrenta serios desafíos en términos de seguridad pública. La ciudad ha sido testigo de la materialización de los delitos de alto impacto, que incluyen homicidios, hurtos, lesiones personales y microtráfico de drogas. Estos delitos no solo afectan la seguridad física de los ciudadanos, sino que también generan un ambiente de miedo e incertidumbre que impacta negativamente en la calidad de vida y el desarrollo económico de la región.

Los homicidios son uno de los problemas más graves, con una alta tasa de asesinatos que coloca a Cali entre las ciudades más violentas del país a pesar de la reducción de casos gracias a los esfuerzos de la Policía Nacional y los demás organismos de seguridad. Los hurtos, tanto a personas como a propiedades, son frecuentes y afectan a una amplia gama de la población, desde residentes hasta visitantes. Las lesiones personales, a menudo resultado de conflictos interpersonales y violencia doméstica, también son una preocupación significativa.

El microtráfico de drogas es otro problema crítico que contribuye a la inseguridad en la ciudad. Este fenómeno no solo alimenta otros delitos, como los homicidios y los hurtos, sino que también tiene un impacto devastador en las comunidades, especialmente en los jóvenes que son reclutados por las redes de narcotráfico.

La falta de recursos adecuados para las fuerzas de seguridad, incluyendo tecnología obsoleta y equipos insuficientes, limita la capacidad operativa de la policía para responder de manera efectiva a estos desafíos. Además, el sistema de justicia enfrenta problemas como la insuficiencia de jueces y fiscales y el hacinamiento en las cárceles, lo que dificulta la administración de justicia y la rehabilitación de los delincuentes.

A continuación, se expone el componente delictivo y los comportamientos contrarios a la convivencia que atienden diariamente los policías en servicio en el Distrito Especial Santiago de Cali, para lo cual es de gran importancia evitar el aumento de estos índices principalmente en aquellas situaciones en que se genera un aumento de la afluencia de público, para lo cual es importante apoyar el servicio con el aumento de las unidades policiales en servicio que permita cumplir con las expectativas de los ciudadanos al momento de salvaguardar sus derechos y libertades.

COMPORTAMIENTO DELICTIVO 2024- 2025 METROPOLITANA DE CALI

A continuación, se presenta la infografía delictiva que ha impactado el Distrito de Santiago de Cali, durante el año 2024 en comparación al 31 de diciembre de 2025, de delitos como el homicidio, hurtos en todas sus modalidades, lesiones personales entre otros, así:

Tipo de Delito		2024	2025	Variación Dif.	Variación %
HOMICIDIO INTENCIONAL		889	987	98	11,02%
FEMINICIDIOS		9	5	-4	-44,44%
LESIONES PERSONALES		4.378	4.054	-324	-7,4%
MODALIDADES DE HURTO	PERSONAS	20.951	16.522	-4.429	-21,1%
	RESIDENCIAS	1.207	905	-302	-25,0%
	COMERCIO	1.749	1.596	-153	-8,7%
	AUTOMOTORES	1.537	1.300	-237	-15,4%
	MOTOCICLETAS	2.889	3.264	375	13,0%
	ENTIDADES FINANCIERAS	2	2	0	0,0%
	ABIGEATO	1	0	-1	-100,0%
	CELULARES	9.217	6.769	-2.448	-26,6%
	BICICLETAS	403	337	-66	-16,4%
	CABLE DE COBRE	102	232	130	127,5%
	TOTAL	38.058	30.927	-7.131	-18,7%
MODALIDADES DE SECUESTRO	SIMPLE	1	1	0	0,0%
	EXTORSIVO	10	12	2	20,0%
	TOTAL	11	13	2	18,2%
EXTORSIÓN		451	418	-33	-7,3%
VIOLENCIA INTRAFAMILIAR		6.290	5.916	-374	-5,9%
PIRATERIA		1			
TERRORISMO		3	18	15	500,0%
DELITOS SEXUALES		1.086	1.264	178	16,4%

El análisis comparativo de los delitos entre los años 2024 y 2025 evidencia cambios significativos en la dinámica criminal, lo que justifica la necesidad de implementar estrategias integrales de seguridad. En primer lugar, se observa un incremento preocupante en los **homicidios intencionales**, que pasaron de 889 casos en 2024 a 987 en 2025, representando un aumento del **11,02%**. Este comportamiento indica una tendencia al alza en la violencia letal, lo que demanda acciones urgentes para fortalecer la prevención y la capacidad de respuesta de las autoridades.

Por otro lado, los **feminicidios** muestran una disminución del **44,44%**, pasando de 9 a 5 casos. Aunque esta reducción es positiva, el fenómeno sigue siendo crítico por su impacto social y la necesidad de garantizar la protección de las mujeres. De manera similar, las **lesiones personales** disminuyeron en un **7,4%**, lo que podría reflejar avances en la mediación de conflictos, pero aún representan más de 4.000 casos, lo que exige programas de convivencia y educación ciudadana.

En cuanto a las **modalidades de hurto**, se evidencia una reducción global del **18,7%**, pasando de 38.058 a 30.927 casos. Sin embargo, el análisis detallado revela comportamientos diferenciados: mientras el hurto a personas disminuyó en un **21,1%** y el hurto de celulares en un **26,6%**, el hurto de cable de cobre aumentó en un alarmante **127,5%**, y el hurto de motocicletas creció un 13%. Estos incrementos sugieren la necesidad de estrategias focalizadas en delitos asociados a infraestructura y movilidad, que afectan directamente la economía y la seguridad urbana.

Otro aspecto crítico es el **secuestro**, que, aunque mantiene cifras bajas, aumentó en un **18,2%**, especialmente en su modalidad extorsiva. Asimismo, los delitos de **terrorismo** presentan un incremento desproporcionado del **500%**, pasando de 3 a 18 casos, lo que constituye una alerta roja para la seguridad nacional y la estabilidad social. Finalmente, los **delitos sexuales** aumentaron en un **16,4%**, lo que evidencia la urgencia de fortalecer políticas de protección a la integridad física y psicológica de las personas, especialmente de poblaciones vulnerables.

En síntesis, aunque algunos indicadores muestran avances, el incremento en delitos de alto impacto como homicidios, terrorismo, delitos sexuales y hurto de cable de cobre plantea la necesidad de un proyecto orientado a la **prevención, control y mitigación del riesgo delictivo**, mediante estrategias tecnológicas, campañas educativas y fortalecimiento institucional. Este proyecto permitirá reducir la incidencia delictiva, mejorar la percepción de seguridad y garantizar el bienestar ciudadano.

COMPORTAMIENTO OPERATIVO 2024- 2025 METROPOLITANA DE CALI

Descripción		2024	2025	Variación Dif.	Variación %	Ver
Capturas	Orden Judicial	1.762	1.850	88	5,0%	
	En Flagrancia	3.786	4.659	873	23,1%	
	Total	5.548	6.509	961	17,3%	
Vehículos Recuperados	Automotores	303	325	22	7,3%	
	Motocicletas	909	1.356	447	49,2%	
	Total	1.212	1.681	469	38,7%	
Droga Incautada (kilogramos)	Cocaína	113	37	-76	-67,4%	
	Heroína	0	0	0	0,0%	
	Base de coca	22	13	-9	-40,6%	
	Bazuco	5	12	7	135,3%	
	Marihuana	9.414	3.648	-5.766	-61,3%	
	Total	9.554	3.710	-5.844	-61,2%	
Armas Incautadas	Con Permiso	379	264	-115	-30,3%	
	Sin Permiso	818	1.013	195	23,8%	
	Total	1.197,0	1.277	80	6,68%	
Casos en Mercancías	Recuperada (Sin Vehículos)	886	934	48	5,4%	
	Incautada (Sin Armas de Fuego)	1.728	2.330	602	34,8%	
	Total	2.550	3.179	629	24,7%	

El análisis comparativo entre los años 2024 y 2025 revela cambios significativos en los indicadores operativos, lo que justifica la necesidad de fortalecer las estrategias de seguridad y control. En primer lugar, las **capturas totales** aumentaron un **17,3%**, pasando de 5.548 en 2024 a 6.509 en 2025, con un incremento de 961 casos. Este crecimiento se explica principalmente por el aumento del **23,1% en capturas en flagrancia** (de 3.786 a 4.659), mientras que las capturas por orden judicial crecieron un **5%**. Este comportamiento refleja una mayor efectividad en la reacción inmediata ante delitos, pero también evidencia la persistencia de conductas delictivas que requieren acciones preventivas.

En cuanto a la **recuperación de vehículos**, se observa un incremento del **38,7%**, pasando de 1.212 a 1.681 unidades. El aumento más significativo se presenta en motocicletas, con un **49,2%** (de 909 a 1.356), mientras que los automotores crecieron un **7,3%**. Este dato indica que el hurto de vehículos sigue siendo un problema relevante, especialmente en motocicletas, lo que demanda estrategias focalizadas en control y vigilancia.

Por otro lado, la **droga incautada** muestra una disminución alarmante del **61,3%**, pasando de 9.554 kg en 2024 a 3.710 kg en 2025. La marihuana, que representaba la mayor proporción, cayó un **61,3%**, mientras que la cocaína disminuyó un **67,4%** y la base de coca un **40,6%**. Aunque esta reducción podría interpretarse como una menor circulación, también puede reflejar limitaciones en la capacidad operativa para detectar cargamentos, lo que exige reforzar la inteligencia y la cooperación interinstitucional.
En relación con las **armas incautadas**, se registra un aumento del **6,68%**, pasando de 1.197 a 1.277 unidades. Las armas sin permiso crecieron un **23,9%**, mientras que las armas con permiso disminuyeron un **30,3%**, lo que indica un mayor control sobre la tenencia ilegal, pero también la necesidad de fortalecer campañas de desarme y regulación.

Finalmente, los **casos en mercancías** (recuperadas e incautadas) aumentaron un **24,7%**, pasando de 2.550 a 3.179, lo que refleja avances en la protección del comercio y la economía local. Este incremento es positivo, pero también evidencia la magnitud del problema del contrabando y hurto de mercancías.

3. ANÁLISIS DE INVOLUCRADOS

Mapa de Actores

	Posición frente al proyecto			
Actores	**Beneficiarios**	**Oponentes**	**Afectados**	**Financiadores**
Alcaldía Distrital Santiago de Cali				X
Comunidad zona urbana y rural	X			
Policía Metropolitana Santiago de Cali	X			

4. ALINEACIÓN ESTRATÉGICA

Plan Estratégico Institucional 2023 – 2026:

- Contribuir a la afectación de las organizaciones multi crimen, economías ilícitas, finanzas criminales y lucha contra el cibercrimen.
- Implementar el nuevo modelo servicio de Policía orientado a las personas
- Fortalecer el servicio de Policía para atender población de especial protección constitucional
- Contribuir a la protección del ambiente y el desarrollo sostenible
- Potencializar el desarrollo humano y calidad de vida para el Policía y su familia

Política de Defensa, Seguridad y Convivencia Ciudadana:

Objetivo
Proveer condiciones de seguridad y protección para la vida y patrimonio

- Abordar el problema mundial de las drogas
- Avanzar en la seguridad urbana
- Fortalecer la seguridad de los grupos poblacionales en situación de vulnerabilidad

Objetivo
Fortalecer la Fuerza Pública

- Fortalecer el Talento Humano
- Legitimidad de la Fuerza Pública (Transparencia – DDHH, Género)
- Policía y Transformación Policial más humana

Objetivo
Proteger el medio ambiente

- Contribuir a la Gestión del Cambio Climático y Protección al Medio Ambiente

5 RV

Plan Nacional de Desarrollo:

Seguridad humana y justicia social

- Transformación de la Policía Nacional para responder a los propósitos de la vida y generar las condiciones para la paz total
- Estrategia de articulación nación territorio para la convivencia y seguridad ciudadana

Plan Distrital de Desarrollo Municipal:

Metas de Producto Sector de Seguridad y Convivencia Ciudadana
Estrategia: Implementar el Plan Integral de Seguridad y Convivencia Ciudadana

Plan Integral de Seguridad y Convivencia Ciudadana:

Eje 3: Cali con autoridad para la disrupción del crimen
Componente: Fortalecimiento al control institucional del territorio
Subcomponente: Fortalecimiento de la fuerza pública y agencias de seguridad y justicia

MACRO ESTRATEGIA DISTRITAL DE SEGURIDAD

- CALI UNIDAD POR LA SEGURIDAD

De igual manera se encuentra alineado, con el Macroplan Metropolitano de Seguridad, diseñado para continuar con la consolidación de la Policía Nacional en la Metropolitana Santiago de Cali, con el fin de garantizar la seguridad y convivencia ciudadana a los habitantes de Santiago de Cali, poniendo las capacidades de todos los horizontes institucionales, enfocados en el talento humano, tecnología, medios logísticos, entre otros, así:

- Soportada en 3 actores estratégicos, comunidad, autoridades y policía

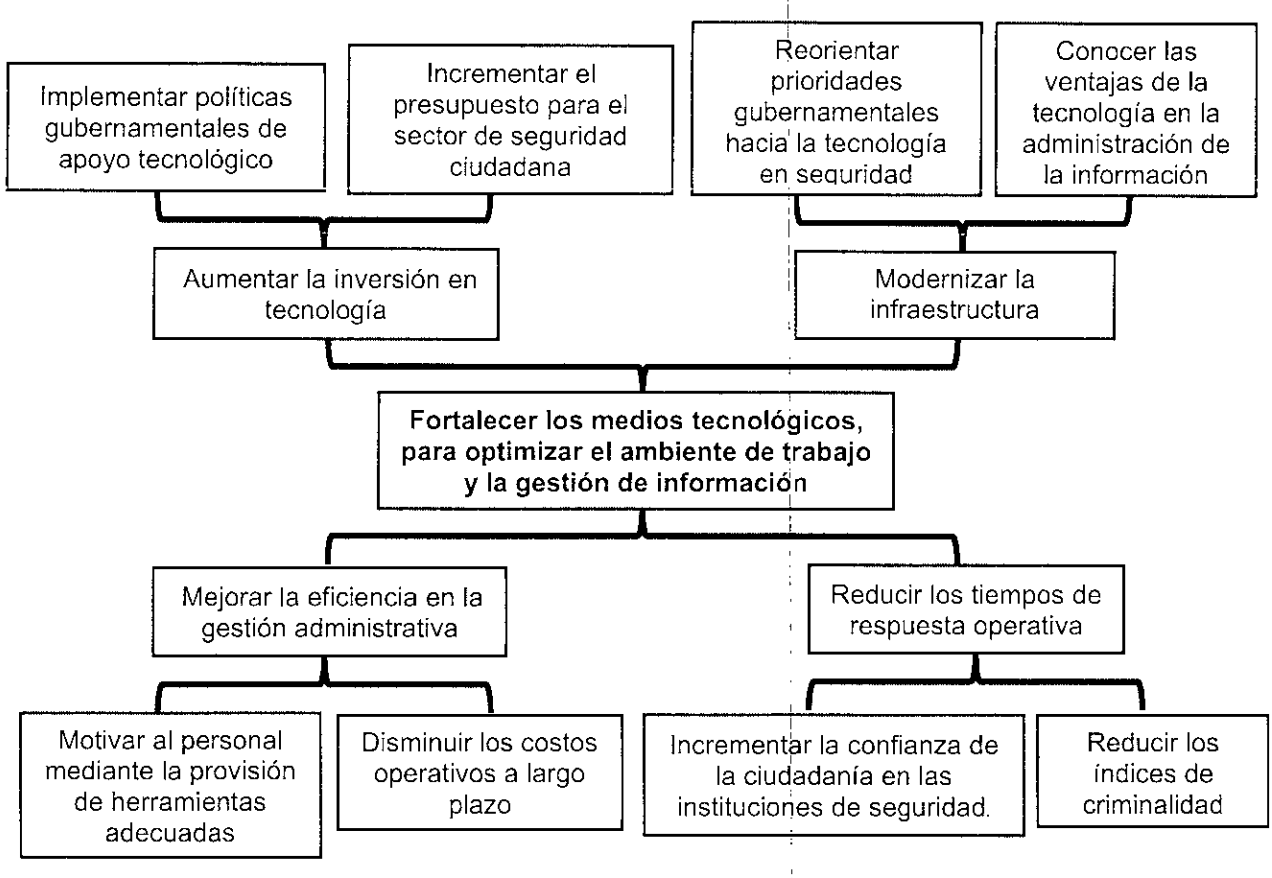
- Con 4 enfoques de intervención, así:
  - ✓ Control al multicrimen y sus finanzas
  - ✓ Adquisición de capacidades por la seguridad
  - ✓ Liderazgo corresponsable
  - ✓ Institucionalidad por la convivencia

- 5 delitos priorizados

  - ✓ Homicidio
  - ✓ Terrorismo
  - ✓ hurto en todas sus modalidades
  - ✓ Extorsión
  - ✓ Tráfico de estupefacientes

Alineado a la política pública de seguridad y convivencia ciudadana de Cali 2024 – 2033, buscando que toda la institucionalidad trabaje por la convivencia, existiendo sinergia con entidades corresponsables con la convivencia pacífica, robustecimiento el liderazgo del Modelo del Servicio de Policía Orientado a las personas y los Territorios MSOPT.

5. ÁRBOL DE OBJETIVOS



6. JUSTIFICACIÓN

La adquisición de elementos tecnológicos para la Policía Metropolitana Santiago de Cali es crucial para mejorar la seguridad y la eficiencia operativa en la ciudad. Esta necesidad se alinea directamente con la misión constitucional de la Policía Nacional de Colombia, que es contribuir al mantenimiento de la convivencia como condición necesaria para el ejercicio de los derechos y libertades públicas, y aportar a la construcción de paz.

La adquisición de elementos tecnológicos específicos, como dispositivos móviles PDA modernos, es crucial para mejorar la eficiencia y efectividad de la Policía Metropolitana Santiago de Cali. Estos elementos optimizan el servicio de policía, potenciando las capacidades operativas y preventivas de la policía.

Adquirir dispositivos PDA puede mejorar significativamente la atención de motivos de Policía que son reportados por la ciudadanía así:

1. **Respuesta rápida y eficiente**: Las patrullas en calle pueden recibir y responder llamadas de emergencia de manera inmediata, lo que reduce el tiempo de respuesta y permite una intervención más rápida en situaciones críticas.

2. **Mejor comunicación**: Los dispositivos celulares facilitan la comunicación directa y constante entre los policías y el centro de control, permitiendo una mejor coordinación y manejo de recursos.

3. **Acceso a información en tiempo real**: Los policías pueden acceder a bases de datos, aplicaciones y otra información relevante en tiempo real, lo que mejora la toma de decisiones y la efectividad en el cumplimiento de sus funciones.

4. **Registro de incidentes**: Los dispositivos pueden ser utilizados para registrar y documentar incidentes, tomar fotografías y videos, para generar reportes de manera inmediata, lo que mejora la transparencia y la rendición de cuentas.

5. **Seguridad del personal**: La capacidad de comunicación constante mejora la seguridad de los policías, ya que pueden solicitar apoyo o asistencia en caso de encontrarse en situaciones peligrosas.

Funcionamiento de un servicio de telefonía con plan de datos:

Un servicio de telefonía con plan de datos funciona de la siguiente manera:

1. **Tecnología 4G**: La tecnología 4G (cuarta generación) es un estándar de telecomunicaciones que ofrece velocidades de transmisión de datos mucho más rápidas que las generaciones anteriores (3G). Utiliza tecnologías como LTE (Long Term Evolution) para proporcionar una conexión más rápida y estable

2. **Protocolo IP**: La red 4G se basa en el protocolo IP (Internet Protocol), lo que permite una mayor eficiencia en la transmisión de datos y una mejor calidad de servicio.

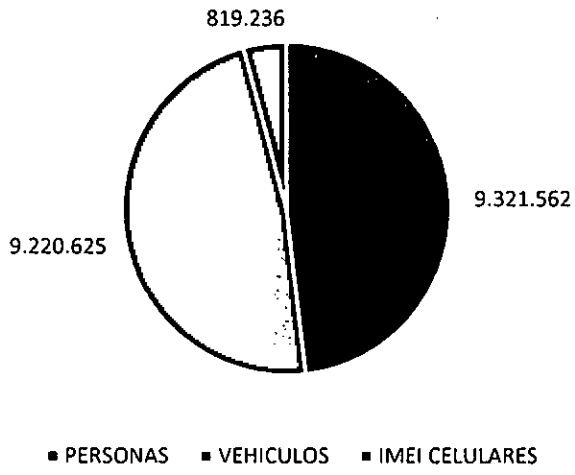
3. **Velocidades de transmisión**: La tecnología 4G permite velocidades de descarga de hasta 1 Gbps en condiciones óptimas y velocidades de subida de hasta 100 Mbps, lo que facilita la transmisión de datos pesados, como videos en alta definición y aplicaciones en tiempo real.

4. **Cobertura y conectividad**: La red 4G ofrece una cobertura amplia y robusta, permitiendo la conexión de múltiples dispositivos sin afectar la calidad del servicio. Esto es especialmente útil en áreas urbanas densamente pobladas.

5. **Planes de datos**: Los planes de datos son ofrecidos por las operadoras de telecomunicaciones y permiten a los usuarios acceder a internet móvil a altas velocidades. Estos planes suelen incluir una cantidad determinada de datos que se pueden utilizar para navegar, ver videos, usar aplicaciones, etc.

Estadísticas de uso y efectividad:

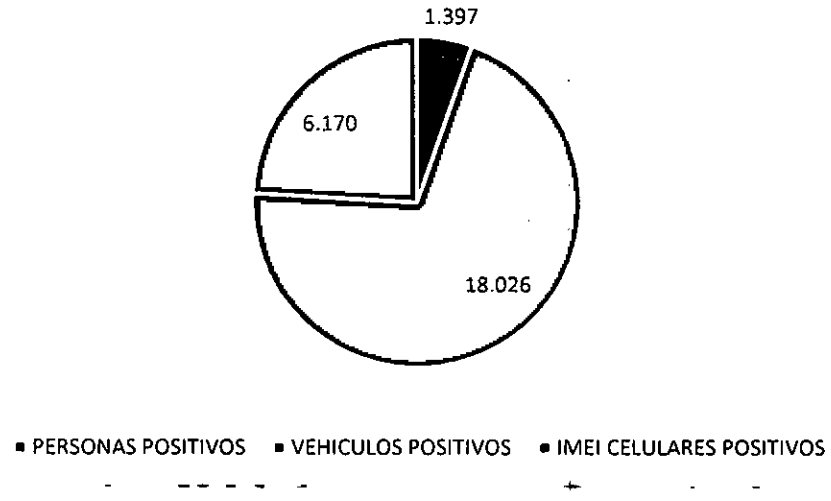
A continuación, se presente la gráfica de la cantidad de antecedentes que fueron solicitados por las patrullas de vigilancia a través de los dispositivos PDA, así:



Fuente: Sistema de información GESPO. 2025.

Como se puede evidenciar durante la vigencia 2025 se realizaron un total de diecinueve millones trescientos sesenta y un mil cuatrocientos veintitrés (9.321.562) de consultas entre personas, vehículos e IMEI de celulares, lo que demuestra el impacto positivo en la búsqueda de resultados operativos para capturar personas por orden judicial o recuperar vehículos y celulares, delitos que afectan en gran porcentaje a los ciudadanos.

Como resultado de la consulta de antecedentes, la Policía Metropolitana Santiago de Cali logro los siguientes resultados, así:



Fuente: Sistema de información GESPO. 2025.

Se puede observar que, en las consultas realizadas, se lograron 1.397 antecedes positivos por requerimientos judiciales, 18.026 vehículos con algún requerimiento judicial pendiente y 6.170 celulares recuperados reportados por hurto.

Teniendo en cuenta los anteriores argumentos la Policía Metropolitana Santiago de Cali requiere la adquisición de los siguientes servicios y dispositivos, así:

PLAN DE VOZ Y DATOS PARA DISPOSITIVOS PDA:

Estado actual del servicio:

No.	Descripción	En almacén	Asignados	En servicio	Fuera de servicio
1	Planes de voz y datos para PDA (incluye el dispositivo)	20 stock	762	762	0

Motivo por el cual se requiere renovar el servicio:

- Se requiere la continuidad del servicio de voz y datos para los dispositivos PDA para las zonas de atención del área urbana y rural de la Ciudad de Santiago de Cali, toda vez que es un servicio primordial para garantizar la convivencia y seguridad ciudadana de los habitantes de la ciudad.

- El servicio debe garantizar el acceso a los aplicativos de la Policía Nacional, como lo son (GESPO), (APPOLO), (AppPol) y (RNMC2), ya que estas permiten el seguimiento de las patrullas en la prestación del servicio, así como la consulta de antecedentes a personas y vehículos para lograr los resultados operativos.

PLAN DE VOZ Y DATOS PARA DISPOSITIVOS DE TELEFONIA DE COMANDANTES:

Estado actual del servicio:

No.	Descripción	En almacén	Asignados	En servicio	Fuera de servicio
1	Planes de voz y datos para telefonía de comandantes (incluye el dispositivo)	0	100	100	0

Motivo por el cual se requiere renovar el servicio:

1. **Comunicación constante**: permite mantener una comunicación directa y continua con los Policías en el campo (zonas de atención), el centro de control y otras agencias de seguridad, lo que es crucial para la coordinación de operaciones y la toma de decisiones rápidas.

2. **Acceso a información en tiempo real**: los comandantes pueden recibir actualizaciones en tiempo real sobre incidentes, mapas y otra información relevante que les permita tomar decisiones informadas y estratégicas.

3. **Gestión de emergencias**: en situaciones de emergencia, un teléfono celular permite al comandante coordinar la respuesta, movilizar recursos y comunicarse con otras autoridades y servicios de emergencia de manera eficiente.

4. **Supervisión y control**: facilita la supervisión y el control de las operaciones policiales, permitiendo al comandante monitorear el progreso de las misiones y ajustar las estrategias según sea necesario.

5. **Coordinación de operativos**: durante un operativo, el comandante puede dar instrucciones precisas y recibir informes de progreso en tiempo real.

6. **Resolución de conflictos**: en caso de disturbios o situaciones de alto riesgo, el comandante puede coordinar la respuesta y tomar decisiones críticas rápidamente.

7. **Gestión de recursos**: permite al comandante reasignar recursos y personal de manera eficiente según las necesidades del momento.

7. OBJETIVO GENERAL

Garantizar la implementación y operatividad eficiente de servicios de voz y datos para dispositivos PDA, con el fin de mejorar la capacidad de respuesta, la seguridad y la eficiencia operativa en la ciudad de Santiago de Cali.

8. OBJETIVOS ESPECÍFICOS, PRODUCTOS Y ACTIVIDADES

1. Garantizar la continuidad y disponibilidad del servicio de voz y datos móviles para los dispositivos PDA asignados a las patrullas de vigilancia y a los dispositivos de telefonía móvil de los comandantes de la Policía Metropolitana Santiago de Cali, durante la vigencia del proyecto.

2. Optimizar los tiempos de respuesta operativa y la atención de los requerimientos ciudadanos, mediante la provisión de conectividad móvil continua y acceso en tiempo real a los aplicativos institucionales de la Policía Nacional.

3. Fortalecer las capacidades operativas, de supervisión y control de los comandantes de la Policía Metropolitana Santiago de Cali, a través del suministro de servicios de voz y datos confiables que faciliten la coordinación de operativos y la toma de decisiones estratégicas.

4. Mejorar la gestión de la información y el registro de los procedimientos policiales, permitiendo la consulta de antecedentes, el reporte inmediato de incidentes y la generación de evidencias digitales desde los dispositivos móviles asignados.

5. Incrementar la eficiencia administrativa y la trazabilidad del servicio de policía, mediante el uso de dispositivos móviles integrados a los sistemas de información institucionales, garantizando un manejo seguro y oportuno de los datos.

6. Contribuir al fortalecimiento de la seguridad y la convivencia ciudadana en el Distrito Especial Santiago de Cali, mediante el apoyo tecnológico a las actividades de prevención, control y reacción frente a los delitos de mayor impacto.

9. POBLACIÓN BENEFICIARIA

Impacto nacional	Impacto local		Total, población	Focalización
	Departamento	Municipio y/o distrito		
No aplica	Valle del Cauca	Distrito Especial Santiago de Cali	2.234.millones	Administrativamente el Municipio está conformado por la cabecera municipal, 249 barrios, 22 comunas y 15 corregimientos, según POT.

10. ALCANCE

Con el fin de satisfacer la necesidad en materia de servicios de voz y datos, y dar continuidad a la prestación del servicio para garantizar las condiciones de convivencia y seguridad en la ciudad de Santiago de Cali, la Policía Metropolitana Santiago de Cali requiere la contratación del servicio de voz y datos, así como la entrega de equipos móviles celular.

Una vez la entidad territorial vaya a realizar la entrega formal a la Policía Nacional- Policía Metropolitana Santiago de Cali, mediante comodato, convenio o transferencia, de los bienes y servicios adquiridos para facilitar a la institución realizar el registro o reconocimiento contable; deberá anexar los documentos idóneos que correspondan de acuerdo a la procedencia y origen del hecho económico.

Los documentos soporte para las entradas de almacén entre otros son:

- Factura con requisitos de Ley (impresa o electrónica)
- Copia del contrato y sus modificaciones si las hay (electrónica)
- Acta de entrega
- Acta de recibo a satisfacción firmada por el supervisor.
- Certificado de pruebas de laboratorio. (cuando aplique)
- Especificaciones técnicas de los bienes de acuerdo al contrato.
- Concepto técnico

11. PRESUPUESTO DETALLADO

Fase 1						
ÍTEM	BIEN Y/O SERVICIO	UNIDAD DE MEDIDA	CANTIDAD	VALOR MENSUAL POR UN DISPOSITIVO	VALOR MENSUAL TOTAL DISPOSITIVOS	VALOR TOTAL VIGENCIA 2026
1	Servicio de voz y datos para dispositivos PDA (incluye el dispositivo móvil).	UN	762	$ 243.964,43	$ 185.900.900,00	$ 2.230.810.800,00
2	Servicio de voz y datos para dispositivos de telefonía de comandantes. (incluye el dispositivo móvil).	UN	100	$ 110.991,00	$ 11.099.100,00	$ 133.189.200,00

Nota 1: Los valores estimados del proyecto corresponden a un análisis de la demanda, mercado y oferta, así como a un análisis de precios de referencia, históricos, catalogo o portales web y mercado.

PRESUPUESTO TOTAL

RECURSO ASIGNADO PARA EL PROYECTO	**$ 2.364.000.000**

PRESUPUESTO DE ESTUDIOS Y DISEÑOS			
DESCRIPCIÓN	**ÁREA A INTERVENIR M2**	**VALOR M2**	**TOTAL**
No aplica	No aplica	No aplica	No aplica
INTERVENTORÍA A ESTUDIOS Y DISEÑOS			No aplica
VALOR TOTAL PRESUPUESTO ESTUDIOS Y DISEÑOS			No aplica

PRESUPUESTO DE OBRA			
☐ Construcción ☐ Ampliación ☐ Adecuación ☐ Mantenimientos mayores	No aplica	No aplica	No aplica
INTERVENTORÍA DE OBRA			No aplica
VALOR TOTAL PRESUPUESTO DE OBRA			No aplica
VALOR TOTAL DEL PROYECTO			No aplica

Observaciones: No aplica

12. COFINANCIACIÓN

Nombre del financiador	% financiación	Valor
No aplica	No aplica	No aplica

13. RIESGOS

☐	Riesgo Alto	X	Riesgo Medio	☐	Riesgo Bajo

14. ESPECIFICACIONES TÉCNICAS DEL BIEN Y/O SERVICIO

Ficha técnica dispositivo Móvil celular PDA

ÍTEM	ESPECIFICACIÓN MÍNIMA REQUERIDA
1	PLAN DE DATOS
1.1	El proveedor de servicio debe garantizar la disponibilidad y velocidad total eficiente de datos para uso de las aplicaciones definidas por la Policía Nacional.
1.2	El proveedor de servicio deberá ofertar en la propuesta y proveer un plan de datos ilimitado-consumibles en los tres tipos de red (3G - 4G - 5G) para cada una de las líneas a adquirir.

	1.3	El servicio de telefonía celular no deberá generar cargos adicionales (plan cerrado o controlado), por fuera de los que solicita la Policia Nacional, para uso de las aplicaciones móviles institucionales definidas, o aquellas otras que defina la Oficina de Tecnologías de la Información y las Comunicaciones, para ello el proveedor de servicio deberá restringir todos aquellos servicios que generen consumos adicionales.
	1.4	El proveedor de servicio deberá entregar un servicio de datos con la máxima tecnología existente en la zona (3G ,4G LTE o 5G), en caso de ser inferior a este, deberá garantizar la conexión con otro operador que se ajuste al requerimiento sin costo adicional para la Policía Nacional y en cumplimiento a la presente ficha técnica para el plan de datos.
	1.5	Garantizar el 100% de la cobertura del servicio de telefonía celular de voz y datos. Cubrir con las tecnologías 3G , 4G/LTE o 5G para la totalidad de las líneas a contratar, en los sitios donde se va prestar el servicio público de telefonía celular para la conectividad de las líneas celulares, el proveedor de servicio deberá implementar el operador con mejor cobertura en cada uno de los sitios donde se cuente con dispositivos móviles para la prestación del servicio de policía, para lo cual la empresa que se le asigne la suscripción del servicio, deberá subcontratarlo con el operador indicado, garantizando de esta manera la cobertura del servicio sin la utilización de Roaming Nacional.
	1.6	El proveedor de servicio deberá realizar todos los trámites necesarios para entregar las líneas a la Policía Nacional (los costos de los trámites serán asumidos por el operador).
	1.7	La Policía Nacional cuenta con números de abonados telefónicos asignados a las patrullas de policía, para lo cual el prestador del servicio realizará la portabilidad de las líneas, en un término no superior a cinco (05) días hábiles, de acuerdo con el cronograma establecido con la Policía Nacional.
	1.8	En caso de cambio del proveedor del servicio, el operador móvil saliente, deberá prestar el servicio de la solución móvil por el tiempo requerido para la implementación del servicio público por el operador entrante, de igual forma, se seguirá pagando la factura mensual sin afectar la transición. El periodo de facturación del servicio se iniciará, a partir de la activación de la totalidad del servicio contratado, así como la implementación y recepción a satisfacción de los entregables de la suscripción de servicios por el supervisor (debidamente aprobado diseños, prototipo y demás accesorios requeridos en la presente ficha técnica). El operador deberá enviar dentro de los cinco (05) primeros días de cada mes, la factura correspondiente al periodo del mes anterior, adjuntando en medio magnético (formato Excel), el reporte del consumo de datos correspondiente a cada una de las líneas adquiridas en el presente proceso con la siguiente información: • Periodo corte. • Departamento o Metropolitana de policía donde esta asignada la línea. • Unidad policial donde se encuentra asignada la línea. • Código de cuadrante. • Número de línea virtual del cuadrante. • Número de línea abonado del cuadrante. • Cantidad de consumo (Bytes) por línea. • Cantidad de líneas con consumo de 0 Bytes Así mismo deberá adjuntar en formato Excel la relación de quipos asociados al servicio de policia y atención al ciudadano del presente proceso vinculados al APN de la Policía Nacional con la siguiente información: • IMEI • Serial • SIM CARD • IP • Fecha de vinculación a la APN De Policía • Versión del sistema operativo • Porcentaje de almacenamiento en uso del dispositivo

	• Versiones de aplicaciones de policía por dispositivo. También deberá entregar de manera mensual el reporte de los equipos con novedades como son: reposiciones, garantías, daños, hurtos y perdidas, entre otras novedades que se lleguen a evidenciar durante la suscripción del servicio.
1.9	El operador del servicio deberá realizar la cantidad de dashboard en la herramienta de inteligencia de negocios que disponga el operador, necesarios para el análisis de los reportes indicados en el ítem 1.8 sin generar costo adicional; los cuales deberán ser coordinados y aprobados previamente con el supervisor del servicio. Para ello hará entrega de los usuarios para el despliegue y control del mismo.
1.10	Como parte integral del servicio, el operador deberá suministrar el envío y recepción de mensajes de texto SMS a cualquier operador de manera masiva disponible 7X24 para el servicio a suscribir.
1.11	El proveedor del servicio deberá suministrar minutos ilimitados para llamadas de voz de todas las líneas de la suscripción del servicio público, igualmente incluir la administración de dichas líneas con el fin de activar y desactivar el servicio de voz por demanda y necesidad.
1.12	El proveedor del servicio deberá garantizar el funcionamiento y cobertura de las líneas de telefonía celular para el servicio de policía y atención al ciudadano en los sitios donde se cuente con servicio de policía a nivel país.
2	**DISPOSITIVO MÓVIL**
2.1	El dispositivo móvil requerido para la prestación del servicio público de telefonía celular en la Policía Nacional debe cumplir con las siguientes características técnicas:

ÍTEM		**ESPECIFICACIONES TECNICAS EQUIPO**
Procesador	Ref/marca	Exynos 1580
	Cant núcleos	8 núcleos
	Velocidad CPU	2,9 GHz
Pantalla	Dimensiones	6,7 Pulgadas
	Resolución	2340 * 1080 (FHD+)
	Tasa de Refresco	120 Hz
	Tecnología	Super AMOLED
	brillo	1200 nits
Marca y Modelo	Samsung	A 56 SM-A566EZKMLTC
Cámara principal	Cámaras Traseras	Principal de 50 MP, f/1.8, PDAF, OIS - Ultra gran angular de 12 MP, f/2.2, 123° - Macro de 5 MP, f/2.4
	Resolución Foto	50 Mp/12 Mp/5 Mp
	Resolución de video	FHD (1920 x 1080) @30fps
	Flash	Si - LED
	Auto Foco	Si - PDAF
Cámara frontal	Resolución Foto	32 MP, f/2.2
	Resolución de video	1080p@30/60fps
Formato de foto y video		Reproductor de video MP4/H.265
Memoria	RAM	Mínimo 8GB de RAM
	ROM	Mínimo 256GB
Bandas	2G	GSM850, GSM900, DCS1800, PCS1900
	3G	B1(2100), B2(1900), B5(850), B8(900)
	4G/LTE	B1(2100), B2(1900), B3(1800), B5(850), B7(2600), B8(900), B20(800), B28(700)

			5G	SA/NSA/Sub6
		Conectividad	GPS	GPS con soporte A-GPS, GLONASS, GALILEO, BDS, QZSS
			WiFi	Wi-Fi 802.11 a/b/g/n/ac/ax; Wi-Fi Direct; banda dual
			Bluetooth	v5.3
			USB Interface	USB TIPO C
			USB Versión	2.0
		Cargador		CARGA RÁPIDA Type-C 45 W
		Sistema operativo		Android 15
		Sensores	Acelerómetro	SI
			Giróscopo	SI
			Proximidad	SI
			Brújula digital	SI
			hall	SI
			Sensor de luz RGB	SI
			Luz Ambiente	SI
			Geomagnético	SI
			Lector de huella bajo pantalla	SI
		Dimensiones		162.2*77.5*7.4 mm
		Peso		198 gr
		Batería	Capacidad mA	5000 mAh
			Uso internet LTE	10 HORAS
			Removible	NO
		Resistencia	IP67	SI
			Gorilla Glass	Gorilla Glass Victus+
		Colores		Negro
		SIM CARD		DOBLE SIM - eSIM

2.2	Se debe entregar por cada uno de los equipos una carcasa protectora que cumpla con los estándares mínimos de protección, marcada de forma imborrable con las palabras POLICIA NACIONAL, debidamente adaptada al equipo establecido en el presente proceso; el diseño será definido por la Policía Nacional, a través de la Oficina de Tecnologías de la Información y las Comunicaciones. Se deberá entregar un stock del 5% por cada año hasta el cumplimiento de la suscripción del servicio.
2.3	Se debe entregar por cada uno de los equipos un cargador compatible con el equipo móvil especificado en el item 2.1 con clavija o enchufe tipo A y cable de carga original del dispositivo móvil.
2.4	Un estuche elaborado en material lona impermeable de color negro doble bolsillo adaptable al cinturón multipropósito; el diseño será definido por la Policía Nacional, a través de la Oficina de Tecnologías de la Información y las Comunicaciones. Se deberá entregar un stock del 5% cada año hasta el cumplimiento de la suscripción del servicio.
2.5	Un protector para la pantalla que absorba los golpes y caídas del dispositivo móvil, diseñado y adaptado al equipo definido en la presente ficha técnica. Se deberá entregar un stock del 5% durante de cada año hasta el cumplimiento de la suscripción del servicio.
2.6	Para el funcionamiento de la solución móvil, el proveedor de servicio deberá suministrar un equipo (1) por cada línea celular a un valor de $0, por cuanto el servicio se suscribe por el rubro de servicios públicos – Telefonía celular, sin generar costo adicional a la Policía Nacional.
2.7	Los equipos se activarán de acuerdo con la programación o cronograma establecido por el supervisor de la prestación de servicio de telefonía celular para el servicio de policía y atención al ciudadano.
2.8	El proveedor de servicios deberá marcar e imprimir en la parte trasera de cada dispositivo, el

	número IMEI y serie de cada uno de los equipos, de manera que no permita ser retirado o borrado por el usuario.
2.9	El proveedor de servicio deberá contar con la venta de todos los accesorios por unidad a demanda durante toda la vigencia de la suscripción de la prestación del servicio público de telefonía celular.
3	**TRANSFERENCIA DE LLAMADAS**
3.1	La Policía Nacional suministrará al operador un servicio web privado, que permite identificar a través de un sistema de información el usuario y la línea celular activa o en servicio, con el fin de que el proveedor realice la transferencia de la llamada generada por parte del ciudadano al número virtual del cuadrante en tiempo real.
3.2	En aquellos casos que la llamada no sea contestada, o la línea activa para el turno de servicio se encuentre apagada, las llamadas entrantes deberán ser direccionadas a la línea de emergencia de cada jurisdicción.
3.3	El levantamiento de requerimientos técnicos para la transferencia de llamadas se llevará a cabo una vez se firme y adjudique la suscripción del servicio al operador, si por algún motivo la Policía Nacional solicita el retiro de este servicio y la configuración de otro para el funcionamiento y transferencia de las llamadas, el operador del servicio deberá realizarlo sin costo adicional.
3.4	Los servidores para la solución de transferencia de llamadas deben ser instalados por el proveedor del servicio, los cuales serán ubicados en el centro de procesamiento de datos de la Policía Nacional, esta instalación y mantenimiento debe estar a cargo del operador y no debe generar costos adicionales para la Policía Nacional.
3.5	La infraestructura en la que se instalará la solución móvil de la suscripción para la transferencia de llamadas en el centro de datos de la Policía Nacional por parte del operador, deberá ser monomarca de última generación y su fabricación no deberá ser anterior al año 2024, con soporte y mantenimiento durante la duración de la suscripción del servicio por parte del fabricante; además, deberá instalar los certificados de seguridad SSL Secure Sockets Layer (Capa de sockets seguros) por cada servidor con vigencia y soporte durante la duración de la suscripción.
4	**CONECTIVIDAD MÓVIL – APN POLICÍA**
4.1	El proveedor de servicio suministrará como parte integral un canal de datos con alta disponibilidad que deberá soportar la totalidad del ancho de banda requerido por los dispositivos móviles para la transmisión y recepción de información de la Policía Nacional. En caso de que se necesite ampliación del canal dedicado, el proveedor de servicio deberá aumentar la capacidad del canal hasta satisfacer el tiempo de respuesta requerido para que la información se trasmita correctamente sin costo adicional para la Policía Nacional, por cuanto será parte integral del valor del servicio.
4.2	El proveedor de servicio deberá configurar un servicio de APN, conforme a los parámetros de conexión que defina la Policía Nacional, para el acceso a la información privada, que dará acceso a las aplicaciones móviles. Para la vinculación de dispositivos móviles al APN de Policía Nacional se deberá realizar previa autorización del supervisor de la suscripción del servicio. Dicha APN deberá tener un usuario diferente para cada una de las líneas y contraseña a configurarse en cada dispositivo.
4.3	En caso de encontrarse irregularidades en las asignaciones de las APN atribuibles al proveedor, la Policía Nacional aplicará un descuento del 10% al valor de la factura.
4.4	A través de este canal centralizado, la solución móvil accederá a todos los servicios que requieran las aplicaciones definidas por la Policía Nacional o para aquellas que con posterioridad defina la Oficina de Tecnologías de la Información y las Comunicaciones, dicho canal debe contar con una protección suministrada por la empresa, para garantizar el filtrado de contenido en los dispositivos.
4.5	La Policía Nacional entregará al proveedor de servicio el rango de IP'S que deberán ser configuradas en los dispositivos móviles, las cuales deben de ir fijas en cada una de las líneas a suscribir.
4.6	El proveedor de servicio deberá entregar la relación de los seriales e IMEI de los equipos móviles, número de abonado, número de abonado virtual del cuadrante, número de la Sim Card, IP asignada al equipo, una vez se inicie la ejecución de la suscripción del servicio de telefonía celular para el servicio de policía y atención al ciudadano.
4.7	El proveedor de servicio deberá entregar al grupo de seguridad de la información de la Oficina de

		Tecnologías de la Información y las Comunicaciones una herramienta tecnológica que permita monitorear los equipos en tiempo real que se encuentran vinculados a la APN de acceso a la red de la Policía Nacional asignada al operador.
	5	**SOFTWARE INSTALADO EN LOS DISPOSITIVOS**
	5.1	La Policía Nacional cuenta con aplicaciones móviles para el servicio de policía desarrolladas en lenguaje de programación MAUI para dispositivos Android, las cuales deben ser instaladas en los equipos móviles por el operador, previa coordinación por el supervisor del servicio público.
	5.2	En los casos donde la Policía Nacional desarrolle e implemente nuevas aplicaciones móviles, es necesario que el proveedor de servicio realice la instalación y configuración de acuerdo con los requerimientos de la Oficina de Tecnologías de la Información y las comunicaciones en los dispositivos, sin costo adicional, esta actividad debe de ser realizada por un ingeniero en sitio de forma inmediata.
	5.3	El proveedor del servicio deberá suministrar el licenciamiento necesario del software MDM (SOTI MobiControl), con el que actualmente la Policía Nacional realiza el monitoreo, administración y control de la totalidad de los dispositivos móviles por el término de tiempo que dure la suscripción del servicio público, de igual forma deberá mantener actualizado todo el componente de MDM en la última versión para un correcto funcionamiento sin ningún costo adicional. El operador del servicio deberá disponer de un funcionario certificado en la administración de dispositivos móviles, con el fin de dar soluciones de soporte, configuraciones y actualizaciones. Adicionalmente debe contar con personal con Certificación vigente en "Android Certified Expert".
	5.4	El proveedor de servicios deberá agregar las licencias del software MDM soti mobicontrol en los servidores propios del operador los cuales deben estar en alta disponibilidad e instalados en el centro de procesamiento de datos de la Policía Nacional.
	5.5	En caso de ser estrictamente necesario, la Oficina de Tecnologías de la Información y las Comunicaciones entregará un usuario de VPN para el acceso al proveedor del servicio, firmando previamente los certificados de confidencialidad y acceso a la información, con los permisos y parámetros que defina la Policía Nacional, para que brinde soporte técnico durante la vigencia de la suscripción del servicio de telefonía celular. Este usuario solo puede ser utilizado en horario no hábil.
	5.6	El MDM SOTI Mobicontrol debe ser compatible con las aplicaciones de la Policía Nacional, adaptándolo a los cambios que se tiene de versiones en el sistema operativo de los equipos móviles.
	5.7	La infraestructura en la que se instalará la solución móvil de la suscripción para| MDM SOTI MOBILCONTROL en el centro de datos de la Policía Nacional deberá ser monomarca de última generación y su fabricación no deberá ser anterior al año 2024, con soporte y mantenimiento durante la duración de la suscripción del servicio por parte del fabricante; además, deberá instalar los certificados de seguridad SSL Secure Sockets Layer (Capa de sockets seguros) por cada servidor con vigencia y soporte durante la duración de la suscripción.
	6	**GRABACIÓN DE LLAMADAS**
	6.1	El prestador del servicio debe disponer de todos los componentes de hardware, software y licenciamiento que sean necesarios para que se realice la grabación de las llamadas entrantes a los dispositivos móviles.
	6.2	El proceso de transferencia y grabación de llamadas deberá realizarse en el Centro de Datos de la Oficina de Tecnologías de la Información y las Comunicaciones de la Policía Nacional con infraestructura tecnológica instalada y actualizada conforme al estándar de servidores definido por la institución, sin ningún tipo de costos adicionales. El soporte deberá ser asumido por el proveedor de servicio, disponiendo a su vez de la infraestructura tecnológica que garantice la alta disponibilidad, confidencialidad e integridad de la información, así mismo se debe garantizar que una vez la grabación de la llamada en formato MP3 es alojada en el Centro de Datos de la Policía Nacional ésta deberá ser eliminada de la infraestructura del operador que la generó.
	6.3	El almacenamiento donde se guardará la grabación de la llamada será suministrado por la Policía Nacional.
	6.4	La grabación de la llamada debe ser en formato MP3 a mínimo 128Kbps.
	6.5	La Policía Nacional, entregará un servicio web con el fin de almacenar en base de datos estructurada, el registro básico de la llamada, el cual debe contener:

	• Fecha de la llamada. Número de origen. Número de destino. • Tipo de llamada (llamadas completadas, llamadas caídas). • Tipo de desconexión (origen, destino, red). El levantamiento de requerimientos técnicos lo deberá realizar el proveedor de servicio una vez se le adjudique la suscripción para la prestación del servicio, si por algún motivo la Policía Nacional solicita el retiro de este servicio y la configuración de otro para el funcionamiento de la grabación de la llamada, el operador del servicio deberá realizarlo sin costo adicional.
6.6	El proveedor deberá entregar la grabación de las llamadas en formato MP3, a través de un procedimiento o método de comunicación entre la NAS de la Policía Nacional y el sitio de grabación del operador del servicio.
6.7	Se debe contar al inicio de la llamada con un mensaje de información donde se indique que la llamada será grabada y monitoreada.
6.8	Todas las llamadas realizadas a las patrullas de policía deben ser grabadas desde el replique al celular y hasta la finalización de esta, sin importar las trasferencias que sucedan en el proceso.
6.9	La infraestructura en la que se instalará la solución móvil de la suscripción para la grabación de llamadas en el centro de datos de la Policía Nacional deberá ser monomarca de última generación y su fabricación no deberá ser anterior al año 2024, con soporte y mantenimiento durante la duración de la suscripción del servicio por parte del fabricante; además, deberá instalar los certificados de seguridad SSL Secure Sockets Layer (Capa de sockets seguros) por cada servidor con vigencia y soporte durante la duración de la suscripción.
7	**CONDICIONES GENERALES**
7.1	El proveedor del servicio que se le adjudique el servicio deberá entregar una póliza de cumplimiento del 10% del valor de la suscripción de servicio durante la vigencia establecida, de acuerdo con los tiempos legales contractuales.
7.2	El presupuesto proyectado de manera mensual para el pago del servicio público de las 762 líneas telefónicas con datos será de $ 185.900.900,00 mensuales incluidos todos los impuestos, por un periodo de 12 meses.
7.3	La eSim o sim card utilizada debe estar aprovisionada con un número celular de la red móvil nacional, no se podrán utilizar servicios con numeración internacional o Sim Card que no se puedan utilizar en cualquier equipo comercial, o servicios con tecnologías administradas M2M.
7.4	Una vez finalice la suscripción de servicio público de telefonía celular para el servicio de policía y atención al ciudadano, la Policía Nacional podrá disponer de la totalidad de los dispositivos móviles del presente proceso para los diferentes servicios de policía que se requieran de acuerdo con las necesidades propias teniendo en cuenta el estado técnico y físico de los dispositivos, será la Policía Nacional quién definirá su disposición final a través del operador móvil según lo establecido en la normatividad vigente y la reglamentación expedida por el Ministerio del Medio Ambiente.
7.5	El proveedor de servicio deberá ofertar el valor del servicio de manera unitaria por línea celular de acuerdo con los planes y configuraciones solicitados según el servicio de policía indicado.
7.6	El proveedor del servicio deberá describir en la oferta el valor de reposición de los equipos por hurto, pérdida o daño, el cual no deberá superar el cincuenta por ciento (50%) del valor comercial en línea prepago-incluido impuestos, esta reposición se aplicará al trece por ciento (13%) de los equipos móviles entregados en el proceso o que se encuentren homologados para la fecha. El proveedor de servicio deberá realizar un ajuste mensual al valor del equipo incluido impuestos, teniendo en cuenta la depreciación y obsolescencia tecnológica del mismo y el cual será aplicado a las reposiciones restantes.
7.7	El proveedor de servicio deberá entregar los equipos, para el funcionamiento del servicio a un valor de cero pesos ($0) incluidos impuestos, sin cláusulas de permanencia activas, por cuanto el servicio se suscribe por el rubro de servicios públicos – Telefonía celular.
7.8	El proveedor de servicio deberá entregar cada 12 meses durante la vigencia de la suscripción un STOCK adicional del 5% de la cantidad de equipos entregados, una vez se inicie la implementación del proyecto, debidamente configurados, con todas las aplicaciones requeridas para el servicio de policía y atención al ciudadano como se describe en el item 5.1.
7.9	El proveedor de servicio deberá entregar al Grupo de Tecnologías de la Información y las Comunicaciones de cada unidad policial a nivel nacional un STOCK de tarjetas SIM electrónicas

		(eSim) del 10% adicional sobre la cantidad de equipos entregados, con el fin de que el cambio del chip se realice en un tiempo no mayor a veinticuatro horas cuando se presente alguna novedad. El sitio y la fecha de entrega será suministrado por el supervisor de la suscripción del servicio de la Policía Nacional. El botiquín de tarjetas SIM electrónica (eSim) debe estar disponibles y activas sin vencimientos durante la vigencia del servicio.
	7.10	El proveedor de servicio deberá enviar a la unidad policial de manera presencial, personal idóneo de la Oficina de Tecnologías de la Información y las Comunicaciones y del operador del servicio que apoye y capacite a los funcionarios que sean definidos por el supervisor de la prestación de servicio, con el fin de que se garantice el correcto funcionamiento de la solución móvil en cada unidad.
	7.11	El proveedor de servicio deberá cumplir con lo establecido en el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional.
	7.12	El proveedor de servicio debe restringir en los equipos para que no se pueda realizar instalaciones de aplicaciones o configuraciones diferentes a las estipuladas por la Policía Nacional, en caso de requerirse, deberán ser aprobadas por la Oficina de Tecnologías de la Información y las Comunicaciones.
	7.13	Si dentro del desarrollo de la suscripción del servicio de telefonía celular se presenta una falla, suspensión o desconexión del servicio por causas atribuibles al operador o por caso fortuito o fuerza mayor; el operador realizará las compensaciones a que haya lugar de acuerdo con la normatividad vigente de la Comisión de Regulación de Comunicaciones CRC.
	8	**GARANTÍA DE EQUIPOS Y ACCESORIOS**
	8.1	Los dispositivos móviles deberán tener una garantía certificada y extendida de 12 meses que incluya el buen funcionamiento del sistema operativo instalado, software de fábrica, hardware ensamblado y accesorios durante la vigencia de la suscripción para prestación del servicio.
	8.2	Las revisiones de los equipos por garantía deben ser realizadas porel proveedor de servicio, sin costo adicional; igualmente, si se renueva o extiende la vigencia de la suscripción para prestación del servicio, deberá realizar los diagnósticos para los equipos sin costo para la entidad, siempre y cuando por presupuesto no se actualicen los existentes.
	8.3	En caso de fallas técnicas presentadas en los equipos móviles con una concurrencia de más de tres (3) veces por el mismo motivo, el equipo deberá ser reemplazado sin costo para la unidad contratante.
	8.4	La reparación de los equipos por garantía no deberá superar nueve (9) días hábiles a partir de la recepción los equipos por parte del operador (bien sea por transportadora o centro de servicio sin costo adicional), si se llega a superar los nueve (9) días de reparación, el operador deberá entregar un equipo nuevo de acuerdo a la ficha técnica vigente.
	9	**SOPORTE TÉCNICO DE EQUIPOS Y ACCESORIOS**
	9.1	La Policía Nacional cuenta con un sistema de información para la atención de requerimientos en TIC, en el cual le será suministrado usuario y contraseña al proveedor de servicio, con el fin de recepcionar y atender los casos que se generen a causa de fallas técnicas en hardware y software de los equipos suministrados, esta atención deberá ser 7X24.
	9.2	El proveedor de servicio deberá proveer una línea de soporte para software y hardware, donde la Policía Nacional pueda reportar los inconvenientes presentados en la solución móvil.
	9.3	El proveedor deberá disponer de una mesa de ayuda dedicada y exclusiva que atienda las veinticuatro (24) horas del día, siete (7) días a la semana, quien recibirá y atenderá las novedades sin retraso y con el personal necesario para que no se presente encolamiento de los tickets durante el tiempo de ejecución de la suscripción para prestación del servicio, con el fin de atender las fallas que se puedan presentar en las integraciones (Web Service publicados por Policía Nacional para transferencia y grabación de la llamada, MDM Soti MobiControl, APN con Policía Nacional, Servidores para SIVICC 2 (Sistema de Información de Vigilancia Comunitaria por Cuadrantes) o el que haga sus veces, método para grabación de llamada a la NAS de Policía Nacional), entre otras, que se efectúen con la plataforma de la Policía Nacional. El funcionario disponible las veinticuatro (24) horas del día deberá dar solución a las fallas que se presenten en sitio, en las instalaciones de la Oficina de Tecnologías de la Información y las Comunicaciones de la Policía Nacional, el cual deberá hacer presentación con tiempo máximo de dos horas contados a partir del reporte de la novedad.

	9.4	El proveedor de servicio deberá disponer de un gerente de proyectos dedicado y exclusivo durante la vigencia de la suscripción de servicios contratado de manera directa por el operador del servicio.
	9.5	Para el soporte y atención de los diferentes requerimientos técnicos, el operador deberá contar con personal en sitio (Oficina de Tecnologías de la Información y las Comunicaciones), que atienda el soporte del que trata el ítem 9.3, debidamente certificado, administre y de solución oportuna a la infraestructura, arquitectura y tecnología instalada para la solución móvil, las asignaciones de recursos de las líneas, suspensión y activación de servicios, administración de APN, configuración de la trasferencia de llamadas, garantía de los equipos móviles, recolección y logística de equipos para soporte técnico, activaciones de Sim Card o eSim con las unidades, atención de requerimientos reportados por la herramienta de mesa de ayuda de la Policía Nacional, conocimientos en desarrollo de aplicaciones móviles para mantenimiento y soporte de SIVICC móvil, en el horario de lunes a viernes de 08:00 horas a 18:00 horas en las instalaciones de la Oficina de Tecnologías de la Información y las Comunicaciones de la Dirección General – Ciudad de Bogotá. En caso de inasistencia del funcionario en sitio por razones de fuerza mayor o por disposición del proveedor de servicios, se obliga a presentar el respectivo reemplazo en el horario indicado.
	9.6	El proveedor del servicio deberá de disponer del personal necesario para dar soporte a los usuarios de la solución móvil, a través de línea telefónica, servicio presencial o vía e-mail, para lo cual el proveedor del servicio debe enviar al supervisor de la suscripción el listado del personal que atenderá los incidentes. Cada funcionario debe firmar un acuerdo de confidencialidad y no revelación de la información. El proveedor de servicio se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución de la suscripción para prestación del servicio público de telefonía celular y la conectividad en el servicio de policía y atención al ciudadano; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo. El proveedor de servicio deberá firmar un acuerdo de confidencialidad y no revelación de la información.
	9.7	El proveedor de servicio debe garantizar que el ticket generado desde el sistema de requerimientos de la Policía Nacional "tenga un seguimiento adecuado, se maneje de forma rápida y eficiente y se lleve a los niveles de servicio hasta su cierre y solución; además, se debe informar por escrito al supervisor de la prestación de servicio al inicio de cada semana, las novedades presentadas respecto a los tickets atendidos.
	9.8	Cuando el funcionario policial, marque a la mesa de ayuda del Proveedor de servicio, deberá existir una sola opción de comunicación del usuario y operador, ya que debe ser un servicio exclusivo para el servicio de policía y atención al ciudadano de la Policía Nacional. Al realizarse la llamada no deberá tener propagandas, desde el momento que el usuario marque a la línea de soporte hasta la finalización y solución del requerimiento.
	9.9	Los funcionarios que se asignen, por parte del proveedor de servicio para realizar soportes de hardware y software, integración tecnológica a la Policía Nacional y gerencia del proyecto, deberán portar el uniforme y carnet que identifique a la empresa contratista para el ingreso a las instalaciones de la Policía Nacional – Oficina de Tecnologías de la Información y las Comunicaciones en la ciudad Bogotá.
	9.10	INEXISTENCIA DE RELACIÓN LABORAL. - Las partes manifiestan expresamente que ninguno de los empleados, agentes o dependientes adquiere, por la celebración de la presente suscripción del servicio relación laboral alguna con la otra parte, extendiéndose esta salvedad a las personas que en desarrollo de la suscripción del servicio llegue a contratarse por cualquier causa por parte del operador.
	9.11	El proveedor de servicio mantendrá indemne a la Policía Nacional, por cualquier daño o perjuicio originado en reclamaciones de terceros y que se deriven o tengan como causa las actuaciones, omisiones, ocasionadas por su parte o cualquiera de sus subcontratistas o dependientes durante la ejecución de la presente suscripción del servicio. Por lo tanto, el operador asumirá la responsabilidad por el manejo de la información suministrada en desarrollo de la presente suscripción del servicio y responderá civil y penalmente tanto por el incumplimiento de las obligaciones derivadas del mismo, como por los hechos u omisiones que le fueran imputables.
	9.12	Cumplir con la implementación del Sistema de Gestión de Seguridad y Salud en el Trabajo, de acuerdo a lo establecido en el Decreto 1072 de 2015, Decreto Único Reglamentario del sector Trabajo, Resolución No. 01956 del 25 abril 2018 Salud y Seguridad en el Trabajo y demás normas

	que lo complementen, para lo cual deberá diligenciar el Formulario "*Sistema de Gestión de la Seguridad y Salud en el Trabajo*" y presentar la "*certificación no superior a tres meses emitido por la Administradora de Riesgos Laborales (ARL) donde conste una calificación que se encuentre en una escala de valoración aceptable (puntaje mayor a 85%)*" y mantener la calificación y evidencia a disposición, para el caso de los consorcios, uniones temporales u otras formas de asociación, se deberá presentar el certificado por cada empresa que conforme la unión temporal o consorcio.
9.13	El Proveedor de servicio deberá contar, con un protocolo de soporte para solucionar las novedades que se puedan presentar de software, hardware, servicio de voz y datos, previa aprobación por el supervisor de la suscripción del servicio.
9.14	La Policia Nacional, entregará al funcionario de soporte en sitio, un usuario del Sistema de Información para la Gestión de Incidentes en TIC, con el fin de que se brinde soporte de software, hardware y se logre evidenciar la trazabilidad de cada uno de los incidentes atendidos y solucionados por parte del operador.
9.15	El proveedor de servicio deberá suministrar dos lectores de código de barras de los equipos a contratar con lectura en la pantalla principal de cada equipo en su código de barras y serial, con el fin de realizar inventarios y asignaciones de manera rápida y oportuna.
10	**PROCEDIMIENTO PARA ENTREGA DE DISPOSITIVOS MÓVILES**
10.1	El Grupo de Tecnologías de la Información y las Comunicaciones MECAL, determinará el plan de distribución de los dispositivos móviles, para lo cual el proveedor de servicio entregará el cronograma una vez se adjudique la prestación del servicio, con el fin de ser aprobado por el supervisor de la suscripción del servicio.
10.2	El proveedor de servicio deberá entregar los equipos configurados y activados en la Oficina de Tecnologías de la información y las Comunicaciones, donde se revisarán para luego ser enviados por parte del operador del servicio a cada unidad de policía de acuerdo con el cronograma establecido.
10.3	El proveedor de servicio deberá anexar un documento con el recibido, indicando los datos de quién recibió a satisfacción los equipos, cantidad, líneas asignadas, Sim Card, IMEI y serie de los equipos entregados a los Grupos de Tecnologías de la Información y las Comunicaciones, dirigido al supervisor de la prestación del servicio.
10.4	El tiempo para la entrega de los equipos adquiridos en la presente suscripción de servicio, será con plazo máximo de cuarenta y cinco (45) días calendario después de la adjudicación de la prestación de servicio de telefonía celular para el servicio de policía y atención al ciudadano, a partir del día cuarenta y seis (46) se iniciará el periodo de los 12 meses para la prestación del servicio, pero el valor del consumo generado será asumido por el operador, hasta la entrega de la totalidad de los equipos.
11	**DISPONIBILIDAD DEL SERVICIO**
11.1	Teniendo en cuenta que el servicio a contratar es de misión crítica para la Policía Nacional, el proveedor de servicio deberá garantizar una disponibilidad mínimo de 99.5% y actuará de forma inmediata a las posibles interrupciones por novedades en la red, hardware y software. **NOTA:** En caso de que falle la solución móvil por las razones antes mencionadas y las unidades se queden sin servicio, el proveedor de servicio deberá realizar los ajustes y compensaciones en la factura del período correspondiente, de acuerdo con la normatividad vigente de la Comisión de Regulación de Comunicaciones CRC para estos casos.

Ficha técnica dispositivo Móvil celular para comandantes

ÍTEM	ESPECIFICACIÓN MÍNIMA REQUERIDA
1	**PLAN DE DATOS**
1.1	El proveedor de servicio deberá ofertar en la propuesta y proveer un plan de datos ilimitado-consumibles en los tres tipos de red (3G - 4G - 5G) para cada una de las líneas a adquirir.
1.2	El proveedor de servicio deberá entregar un servicio de datos con la máxima tecnología existente en la zona (3G ,4G LTE o 5G), en caso de ser inferior a este, deberá garantizar la conexión con otro operador que se ajuste al requerimiento sin costo adicional para la Policía Nacional y en cumplimiento a la presente ficha técnica para el plan de datos.

	1.3	El servicio de telefonía celular no deberá generar cargos adicionales (plan cerrado o controlado), por fuera de los que solicita la Policía Nacional.
	1.4	Garantizar el 100% de la cobertura del servicio de telefonía celular de voz y datos. Cubrir con las tecnologías 3G , 4G/LTE o 5G para la totalidad de las líneas a contratar, en los sitios donde se va prestar el servicio público de telefonía celular para la conectividad de las líneas celulares, el proveedor de servicio deberá implementar el operador con mejor cobertura en cada uno de los sitios donde se cuente con dispositivos móviles para la prestación del servicio de policía, para lo cual la empresa que se le asigne la suscripción del servicio, deberá subcontratarlo con el operador indicado, garantizando de esta manera la cobertura del servicio sin la utilización de Roaming Nacional.
	1.5	El proveedor de servicio deberá realizar todos los trámites necesarios para entregar las líneas a la Policía Nacional (los costos de los trámites serán asumidos por el operador).
	1.6	En caso de cambio del proveedor del servicio, el operador móvil saliente, deberá prestar el servicio de la solución móvil por el tiempo requerido para la implementación del servicio público por el operador entrante, de igual forma, se seguirá pagando la factura mensual sin afectar la transición. El periodo de facturación del servicio se iniciará, a partir de la activación de la totalidad del servicio contratado, así como la implementación y recepción a satisfacción de los entregables de la suscripción de servicios por el supervisor (debidamente aprobado diseños, prototipo y demás accesorios requeridos en la presente ficha técnica). El operador deberá enviar dentro de los cinco (05) primeros días de cada mes, la factura correspondiente al periodo del mes anterior, adjuntando en medio magnético (formato Excel), el reporte del consumo de datos correspondiente a cada una de las líneas adquiridas en el presente proceso con la siguiente información: • Periodo corte. • Departamento o Metropolitana de policía donde esta asignada la línea. • Unidad policial donde se encuentra asignada la línea. • Cantidad de consumo (Bytes) por línea. • Cantidad de líneas con consumo de 0 Bytes También deberá entregar de manera mensual el reporte de los equipos con novedades como son: reposiciones, garantías, daños, hurtos y perdidas, entre otras novedades que se lleguen a evidenciar durante la suscripción del servicio.
	1.7	El proveedor del servicio deberá suministrar minutos ilimitados para llamadas de voz de todas las líneas de la suscripción del servicio público, igualmente incluir la administración de dichas líneas con el fin de activar y desactivar el servicio de voz por demanda y necesidad.
	2	**DISPOSITIVO MÓVIL**
	2.1	El dispositivo móvil requerido para la prestación del servicio público de telefonía celular en la Policía Nacional debe cumplir con las siguientes características técnicas:

ITEM	DESCRIPCION	
1	**PANTALLA**	
1.1	Tamaño	6.7"
1.2	Resolución	720 * 1610 px
1.3	Tecnología	TFT o IPS
1.4	Intensidad de brillo	700 nits
1.5	Frecuencia de actualización	120hz
2.	**MEMORIA**	
2.1	Memoria RAM GB	8 GB
2.2	Almacenamiento	256 GB
3.	**Conectividad**	
3.1	bandas	5G, 4G LTE, 3g

	3.2	Inalámbrica	Wi-Fi
	3.3	Bluetooth	
	3.4	Gps	
	3.5	NFC	
	3.6	USB -C	
	3.7	SIM	Dual SIM
	4.	**Cámaras**	
	4.1	Trasera	- Dual - 50 Mpx - Secundario 2Mpx - Modo retrato, panorámica, cámara lenta - Video 1080p (Full HD)
	4.2	Frontal	5 MP
	5.	**Bateria**	
	5.1	Capacidad	5.000 mAh
	5.2	Carga rápida	30 W
	5.3	Puerto de carga	USB-C
	6.	**Procesador**	
	6.1	Referencia	Mediatek, Qualcomm o Exynos
	6.2	Velocidad	2.3 Ghz
	6.3	Tipo	Octa - core
	7.	**Sensores**	
	7.1	Lector de huellas	
	7.2	Acelerómetro	
	7.3	Giroscopio	

2.2	Se debe entregar por cada uno de los equipos una carcasa protectora que cumpla con los estándares mínimos de protección, marcada de forma imborrable con las palabras POLICIA NACIONAL, debidamente adaptada al equipo establecido en el presente proceso; el diseño será definido por la Policía Nacional, a través de la Oficina de Tecnologías de la Información y las Comunicaciones. Se deberá entregar un stock del 5% por cada año hasta el cumplimiento de la suscripción del servicio.
2.3	Se debe entregar por cada uno de los equipos un cargador compatible con el equipo móvil especificado en el ítem 2.1 con clavija o enchufe tipo A y cable de carga original del dispositivo móvil.
2.4	Un estuche elaborado en material lona impermeable de color negro doble bolsillo adaptable al cinturón multipropósito; el diseño será definido por la Policía Nacional, a través de la Oficina de Tecnologías de la Información y las Comunicaciones
2.5	Un protector para la pantalla que absorba los golpes y caídas del dispositivo móvil, diseñado y adaptado al equipo definido en la presente ficha técnica.
2.6	Para el funcionamiento de la solución móvil, el proveedor de servicio deberá suministrar un equipo (1) por cada línea celular a un valor de $0, por cuanto el servicio se suscribe por el rubro de servicios públicos – Telefonía celular, sin generar costo adicional a la Policía Nacional.
2.7	Los equipos se activarán de acuerdo con la programación o cronograma establecido por el supervisor de la prestación de servicio de telefonía celular para el servicio de policía y atención al ciudadano.
2.8	El proveedor de servicios deberá marcar e imprimir en la parte trasera de cada dispositivo, el número IMEI y serie de cada uno de los equipos, de manera que no permita ser retirado o borrado por el usuario.
2.9	El proveedor de servicio deberá contar con la venta de todos los accesorios por unidad a demanda durante toda la vigencia de la suscripción de la prestación del servicio público de telefonía celular.
3	**GARANTÍA DE EQUIPOS Y ACCESORIOS**
3.1	Los dispositivos móviles deberán tener una garantía certificada y extendida de 12 meses que incluya el buen funcionamiento del sistema operativo instalado, software de fábrica, hardware ensamblado y accesorios durante la vigencia de la suscripción para prestación del servicio.
3.2	Las revisiones de los equipos por garantía deben ser realizadas porel proveedor de servicio, sin costo adicional; igualmente, si se renueva o extiende la vigencia de la suscripción para prestación del servicio, deberá realizar los diagnósticos para los equipos sin costo para la entidad, siempre y cuando por presupuesto no se actualicen los existentes.
3.3	En caso de fallas técnicas presentadas en los equipos móviles con una concurrencia de más de tres (3) veces por el mismo motivo, el equipo deberá ser reemplazado sin costo para la unidad

	contratante.
3.4	La reparación de los equipos por garantía no deberá superar nueve (9) días hábiles a partir de la recepción los equipos por parte del operador (bien sea por transportadora o centro de servicio sin costo adicional), si se llega a superar los nueve (9) días de reparación, el operador deberá entregar un equipo nuevo de acuerdo a la ficha técnica vigente.

15. CONCEPTOS TÉCNICOS
Viabilidad planeación GS-2026-012538-MECAL, ACTA - 003338 - GUDES-GUTIC - 2.21
16. DATOS DE CONTACTO
Técnico de Tecnologías de la Información y las Comunicaciones MECAL Subintendente. **ANDRES DAVID DELGADO AMELINES** Correo electrónico: andres.delgado3661@correo.policia.gov.co Teléfono móvil: 3128814026

FORMULADOR DEL PROYECTO:

Firma
Capitán. **DUVAN ALBERTO CASAÑOVA VASCO** C.C.: 1.085.297.086
Cargo: Jefe grupo de Tecnologías de la Información y las Comunicaciones

RESPONSABLE UNIDAD QUE LO PRESENTA:

Firma
Coronel **ANDRES ARIAS BUITRAGO** C.C.: 79763101
Cargo: Comandante Policía Metropolitana Santiago de Cali (E)

Elaboró: SI. Andrés David Delgado Amelines
MECAL – GUTIC

Revisó: SC. Uriel Gutiérrez Rengifo
MECAL – GESTER

15
EV

Página: 1 de 19 Código: 1DE-FR-0051 Fecha: 02-07-2024 Versión: 1	DIRECCIONAMIENTO ESTRATÉGICO **FORMULACIÓN DE PROYECTOS Y PROGRAMAS EN LA POLICÍA NACIONAL**	POLICÍA NACIONAL

FECHA	29 ENE 2026
UNIDAD QUE LO PRESENTA	Policía Metropolitana Santiago de Cali – Grupo Tecnologías de la Información y las Comunicaciones – Alcaldía Santiago de Cali.
NOMBRE DEL PROYECTO	Modernización de Computadores para Fortalecer la Convivencia, la Seguridad y el Servicio Ciudadano en Santiago de Cali, con Enfoque en los CIEPS y la Planeación del Servicio de Policía, Integrando Analítica e IA Predictiva.
LÍNEA DE INVERSIÓN	☐ Infraestructura ☐ Adquisición de predios ☐ Estudios y diseños ☐ Construcción ☐ Ampliación ☐ Adecuación ☐ Mantenimientos ☐ Movilidad ☐ Terrestre ☐ Aérea ☐ Fluvial ☐ Mantenimiento aeronáutico ☐ Armamento ☐ Intendencia ☒ Tecnología y comunicaciones ☐ Política educativa ☐ Programas de prevención ☐ Bienestar social y familia ☐ Sanidad ☐ Otros ¿Cuál?
ENTIDAD A LA QUE VA DIRIGIDO	*Alcaldía Santiago de Cali* ☒ Nacional ☐ Internacional
PRESUPUESTO TOTAL	*$ 157.500.000,00*
COFINANCIACIÓN	☐ Sí ☒ NO
FASES DEL PROYECTO	☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Mas de 5

DURACIÓN DEL PROYECTO	*Tres meses*

1. ANÁLISIS DEL PROBLEMA

La Policía Metropolitana de Santiago de Cali enfrenta un riesgo crítico de continuidad operativa y de seguridad de la información debido a la obsolescencia y no conformidad del parque de equipos de cómputo con los requisitos mínimos del sistema operativo Windows, elementos necesarios hoy para garantizar integridad, soporte y controles de seguridad basados en hardware. Sin esta renovación, se compromete la prestación del servicio policial a la comunidad, la respuesta oportuna y el cumplimiento de la Política de Gobierno Digital que exige servicios públicos digitales seguros, confiables y de calidad.

Situación actual de la Policía Metropolitana Santiago de Cali

Inventario en riesgo: la Policía Metropolitana Santiago de Cali registra 456 computadores en la bodega del Grupo de Tecnologías de la Información y las Comunicaciones con resolución para baja (≥10 años de uso) con fallas recurrentes (discos, memoria, NIC, fuentes). Adicionalmente, la Policía Metropolitana opera 527 computadores con obsolescencia tecnológica que no cumplen requisitos mínimos de Windows 11 (TPM 2.0/UEFI/Secure Boot/CPU/RAM), adicional a ello los equipos institucionales que encuentran con delegación de control de dominio policia.gov.co, que con cuenten con sistemas operativos actualizados a Windows 11 Pro, serán eliminados por parte de la Oficina de Tecnologías de la Información y las Comunicaciones de consola, ya que el contar con Windows 11 Pro afecta lo descrito en la Norma ISO 27001;2022, NUMERAL 6.1.3 que establece la necesidad de gestionar riesgos de seguridad de la información, por lo cual se recalca que la falta de actualización representa una vulnerabilidad que compromete la triada de la información "integridad, disponibilidad y confidencialidad" de los activos tecnológicos de la institución policial.

Afectación misional: más del 50% del parque no garantiza operación eficiente en investigación, inteligencia, prevención y disuasión, atención a las necesidades en materia de seguridad y convivencia ciudadana, generando interrupciones, retrasos en decisiones y exposición a ciber-riesgos.

Fuentes: Microsoft – Requisitos Windows 11 · Análisis de obsolescencia y sus riesgos en organizaciones (bajas de soporte, más fallas, mayor indisponibilidad) B-Secure · Riesgos en infraestructuras por obsolescencia (impacto en continuidad y seguridad) MAPFRE Global Risks

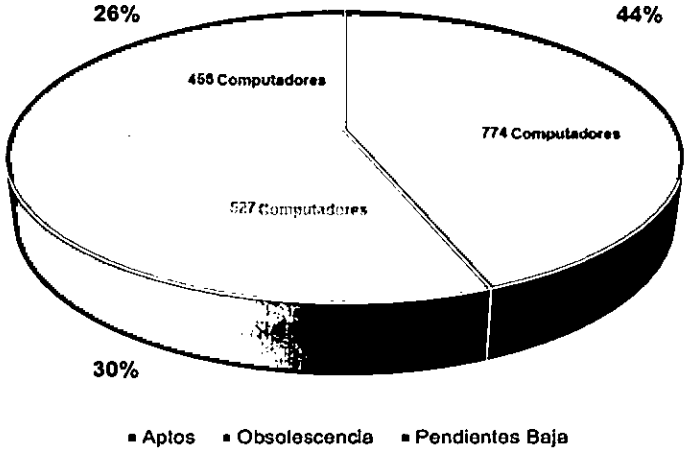
De manera complementaria al diagnóstico técnico, se evidencia una brecha funcional que afecta la planeación del servicio de policía desde los CIEPS y a las unidades de investigación criminal, inteligencia, la obsolescencia y heterogeneidad del parque de cómputo limita la operacionalización de los aplicativos institucionales de analítica e inteligencia artificial orientados a la predicción de delitos y comportamientos contrarios a la convivencia. Esta condición reduce la capacidad para procesar datos oportunamente, generar alertas tempranas y producir boletines estratégicos con la periodicidad y calidad requeridas, lo que se traduce en retrasos en la priorización territorial,

asignación preventiva de recursos y orientación de patrullajes proactivos, afectando la oportunidad de respuesta y la eficacia en el servicio a la ciudadanía.

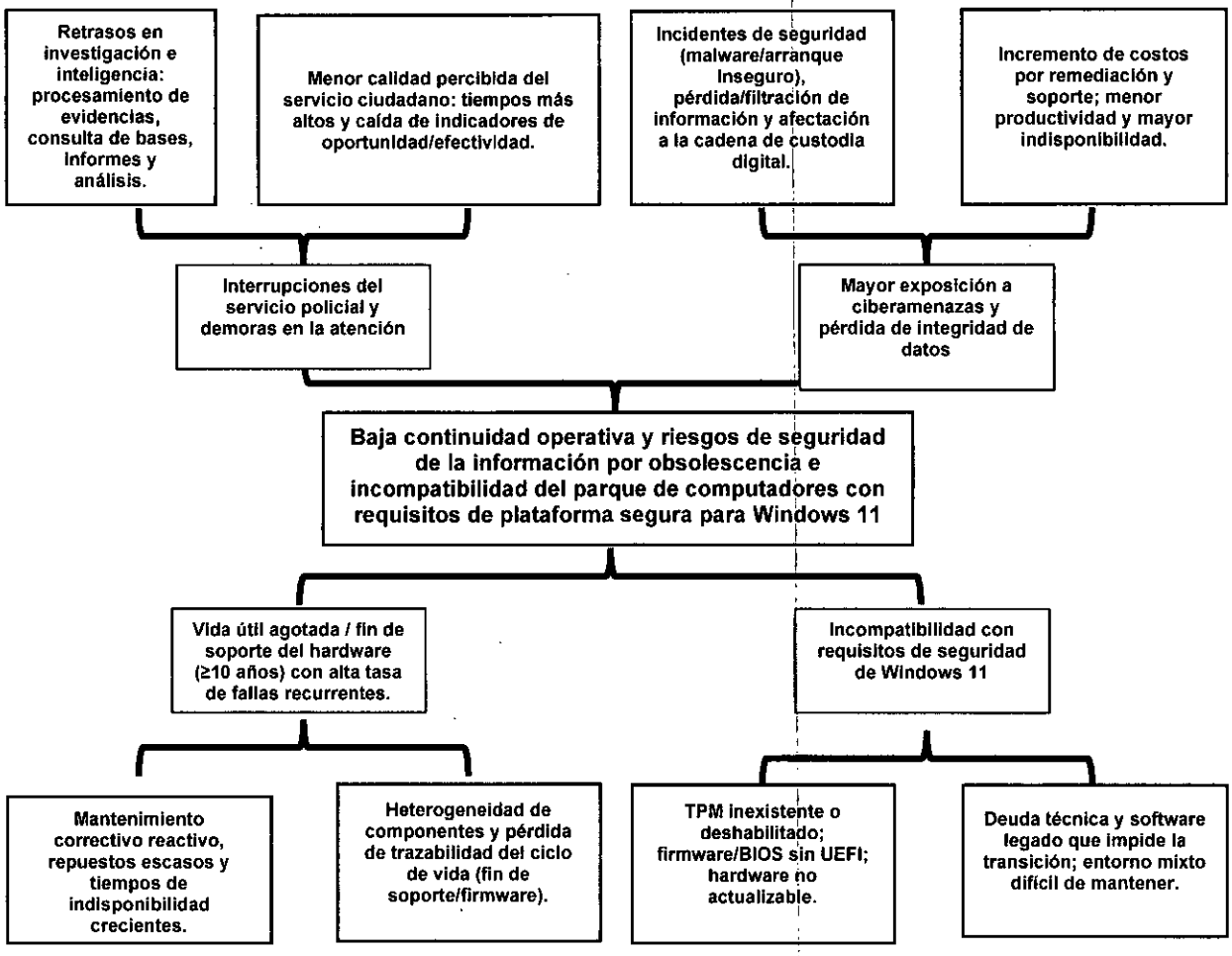
Asimismo, la falta de una plataforma homogénea, segura y confiable en los puestos de trabajo —especialmente en CIEPS y en las dependencias misionales— dificulta sostener ciclos de analítica e IA con estándares de gobernanza, auditoría y trazabilidad (registros de uso, control de accesos por rol, respaldo seguro de evidencias y llaves, validación periódica del desempeño y detección de deriva en los modelos). En el estado actual, la inconsistencia de configuraciones incrementa la probabilidad de falsos positivos/negativos, expone a riesgos de seguridad de la información (incluida la cadena de custodia digital) y perpetúa una dinámica reactiva que eleva la indisponibilidad y la baja calidad analítica. La no intervención mantiene esta brecha, contraviniendo los lineamientos de continuidad operativa y valor público exigidos para servicios soportados en TIC, y limita el aprovechamiento real de los aplicativos predictivos institucionales.

Actualmente, más del 50% de los equipos de cómputo no cumplen con las condiciones necesarias para garantizar el desarrollo eficiente de los procesos misionales en las labores investigativas, de inteligencia, prevención y disuasión desarrolladas diariamente por el personal policial en las distintas especialidades y zonas de atención de la ciudad.

GRAFICA COMPUTADORES POLICÍA METROPOLITANA DE CALI



ÁRBOL DE PROBLEMAS



2. DESCRIPCIÓN DEL PROBLEMA

La continuidad operativa y la seguridad de la información de la Policía Metropolitana de Santiago de Cali se encuentran comprometidas por la obsolescencia y la no conformidad del parque de equipos de cómputo frente a los requisitos de plataforma segura exigidos por Windows 11 (p. ej., TPM 2.0, UEFI/Secure Boot, CPU de 64 bits, RAM y almacenamiento mínimos, GPU compatible con DirectX 12). Esta brecha técnica impide el acceso a controles de seguridad basados en hardware (BitLocker, arranque seguro) y limita el soporte oficial del fabricante, afectando la confiabilidad del entorno y la integridad de los servicios apoyados en TIC (Microsoft, *Especificaciones y requisitos de Windows 11*; MinTIC, *Política de Gobierno Digital*).

El inventario institucional evidencia 456 computadores con resolución para baja (≥10 años, con fallas en discos, memoria, tarjetas de red y fuentes) y 527 equipos en operación con obsolescencia tecnológica que no cumplen los prerrequisitos mínimos del sistema operativo vigente. En consecuencia, más del 50 % del parque no garantiza el desempeño requerido por los procesos misionales (investigación, inteligencia, prevención y disuasión), contraviniendo la orientación de

la PGD de prestar servicios públicos seguros, confiables y de calidad mediante infraestructura adecuada (Microsoft; MinTIC).

El impacto operativo es transversal: se presentan interrupciones y demoras en recepción de denuncias, consulta de bases, elaboración de informes y análisis operativo, lo que deteriora la oportunidad de respuesta y la experiencia del ciudadano. Esto contraría los principios de valor público de la Política de Gobierno Digital PGD, que demandan capacidades digitales disponibles y resilientes para la interacción Estado-ciudadanía y la prestación de servicios con estándares de eficiencia y confianza (MinTIC; DNP – MGA, sobre la necesidad de diagnósticos que evidencien la afectación a resultados y productos).

La exposición a ciberamenazas aumenta cuando los equipos carecen de TPM 2.0 y Arranque Seguro, o cuando no pueden recibir actualizaciones y parches en tiempo debido a restricciones de hardware. Esta situación amplia la superficie de ataque (malware, bootkits), compromete confidencialidad, integridad y disponibilidad de datos y puede afectar la cadena de custodia digital en actuaciones misionales, con implicaciones probatorias y reputacionales (Microsoft; B-Secure).

Las causas técnicas identificadas incluyen: (i) vida útil agotada y fin de soporte del hardware (≥10 años), con incremento de fallas y escasez de repuestos; (ii) incompatibilidad con los requisitos de seguridad y desempeño de Windows 11 (TPM 2.0 ausente o deshabilitado, BIOS heredada sin UEFI/Secure Boot, CPU/RAM/GPU insuficientes); y (iii) deuda técnica y heterogeneidad del parque, que elevan la complejidad del soporte y los tiempos de atención, deteriorando la continuidad del servicio (MAPFRE Global Risks; B-Secure).

Adicionalmente, se evidencia una brecha en la gestión integral de activos TIC (inventario, clasificación por criticidad, ciclo de vida, políticas de seguridad y actualización), lo que dificulta la priorización de la reposición y la sostenibilidad del servicio. La PGD y sus lineamientos específicos para inventario y clasificación de activos de información recomiendan modelos de gobierno de TI que aseguren trazabilidad, propiedad y criticidad, como insumo para decisiones de inversión y continuidad (MinTIC – Lineamientos de activos; MinTIC – PGD).

El riesgo de no intervención proyecta un aumento de la indisponibilidad, la frecuencia de incidentes de seguridad y los sobrecostos derivados del mantenimiento correctivo y de la pérdida de productividad, perpetuando ineficiencias operativas y debilitando la respuesta institucional ante la ciudadanía. La literatura en gestión de obsolescencia y continuidad operativa respalda que mantener activos sin soporte eleva costos, vulnerabilidades y tiempos de recuperación (B-Secure; MAPFRE Global Risks).

En este contexto, el proyecto requiere la renovación y estandarización del parque de equipos de cómputo Windows 11-ready (TPM 2.0, UEFI/Secure Boot, CPU 64-bit con ≥2–4 núcleos, RAM y almacenamiento adecuados al perfil, GPU compatible con DirectX 12), junto con la gestión integral de activos TIC (inventario, clasificación, hardening y actualización).

La situación descrita se agrava en la medida en que los CIEPS y las dependencias misionales requieren procesar información en tiempo oportuno para la planeación operativa, incluyendo el uso de aplicativos institucionales con analítica e inteligencia artificial orientados a la predicción de delitos y comportamientos contrarios a la convivencia. La obsolescencia y heterogeneidad del parque actual impiden ejecutar con confiabilidad los flujos de gestión, procesamiento y

visualización necesarios para generar alertas tempranas, priorizar zonas y franjas horarias críticas, orientar patrullajes preventivos y emitir boletines estratégicos con la periodicidad requerida. Este rezago tecnológico se traduce en demoras, brechas de información y pérdida de oportunidad en la toma de decisiones tácticas y operativas, afectando la experiencia del ciudadano y el cumplimiento de metas misionales.

Asimismo, la ausencia de una plataforma homogénea, segura y trazable en los puestos de trabajo limita la gobernanza y auditoría de los procesos analíticos y predictivos (control de accesos por rol, registros de uso, respaldo seguro de evidencias y llaves), y dificulta la validación periódica del desempeño de los modelos (precisión, falsos positivos/negativos y deriva frente a la dinámica delictiva). Esta condición incrementa la exposición a riesgos de seguridad de la información —incluida la cadena de custodia digital— y perpetúa una operación reactiva, con mayor indisponibilidad y costos de soporte. En consecuencia, mientras no se modernice y estandarice la dotación de cómputo, la institución seguirá limitada para aprovechar plenamente sus aplicativos de analítica e IA predictiva y para garantizar continuidad operativa y valor público en la prestación del servicio.

3. ANÁLISIS DE INVOLUCRADOS

Mapa de Actores

	Posición frente al proyecto			
Actores	**Beneficiarios**	**Oponentes**	**Afectados**	**Financiadores**
Alcaldía Santiago de Cali				*X*
Comunidad zona urbana	*X*			
Comunidad zona rural	*X*			
Policía Metropolitana Santiago de Cali	*X*			

4. ALINEACIÓN ESTRATÉGICA

Plan Estratégico Institucional 2023 – 2026:

- Contribuir a la afectación de las organizaciones multi crimen, economías ilícitas, finanzas criminales y lucha contra el cibercrimen.
- Implementar el nuevo modelo servicio de Policía orientado a las personas.
- Fortalecer el servicio de Policía para atender población de especial protección constitucional.
- Contribuir a la protección del ambiente y el desarrollo sostenible.
- Potencializar el desarrollo humano y calidad de vida para el Policía y su familia.

Política de Defensa, Seguridad y Convivencia Ciudadana:

Objetivo
Proveer condiciones de seguridad y protección para la vida y patrimonio

- Abordar el problema mundial de las drogas.
- Avanzar en la seguridad urbana

- Fortalecer la seguridad de los grupos poblacionales en situación de vulnerabilidad

Objetivo
Fortalecer la Fuerza Pública

- Fortalecer el Talento Humano
- Legitimidad de la Fuerza Pública (Transparencia – DDHH, Género)
- Policía y Transformación Policial más humana

Objetivo
Proteger el medio ambiente

- Contribuir a la Gestión del Cambio Climático y Protección al Medio Ambiente

Plan Nacional de Desarrollo:

Seguridad humana y justicia social

- Transformación de la Policía Nacional para responder a los propósitos de la vida y generar las condiciones para la paz total
- Estrategia de articulación nación territorio para la convivencia y seguridad ciudadana

Plan Distrital de Desarrollo Municipal:

Metas de Producto Sector de Seguridad y Convivencia Ciudadana
Estrategia: Implementar el Plan Integral de Seguridad y Convivencia Ciudadana

Plan Integral de Seguridad y Convivencia Ciudadana:

Eje 3: Cali con autoridad para la disrupción del crimen
Componente: Fortalecimiento al control institucional del territorio
Subcomponente: Fortalecimiento de la fuerza pública y agencias de seguridad y justicia

MACRO ESTRATEGIA DISTRITAL DE SEGURIDAD

- CALI UNIDAD POR LA SEGURIDAD

De igual manera se encuentra alineado, con el Macroplan Metropolitano de Seguridad, diseñado para continuar con la consolidación de la Policía Nacional en la Metropolitana Santiago de Cali, con el fin de garantizar la seguridad y convivencia ciudadana a los habitantes de Santiago de Cali, poniendo las capacidades de todos los horizontes institucionales, enfocados en el talento humano, tecnología, medios logísticos, entre otros, así:

- Soportada en 3 actores estratégicos, comunidad, autoridades y policía

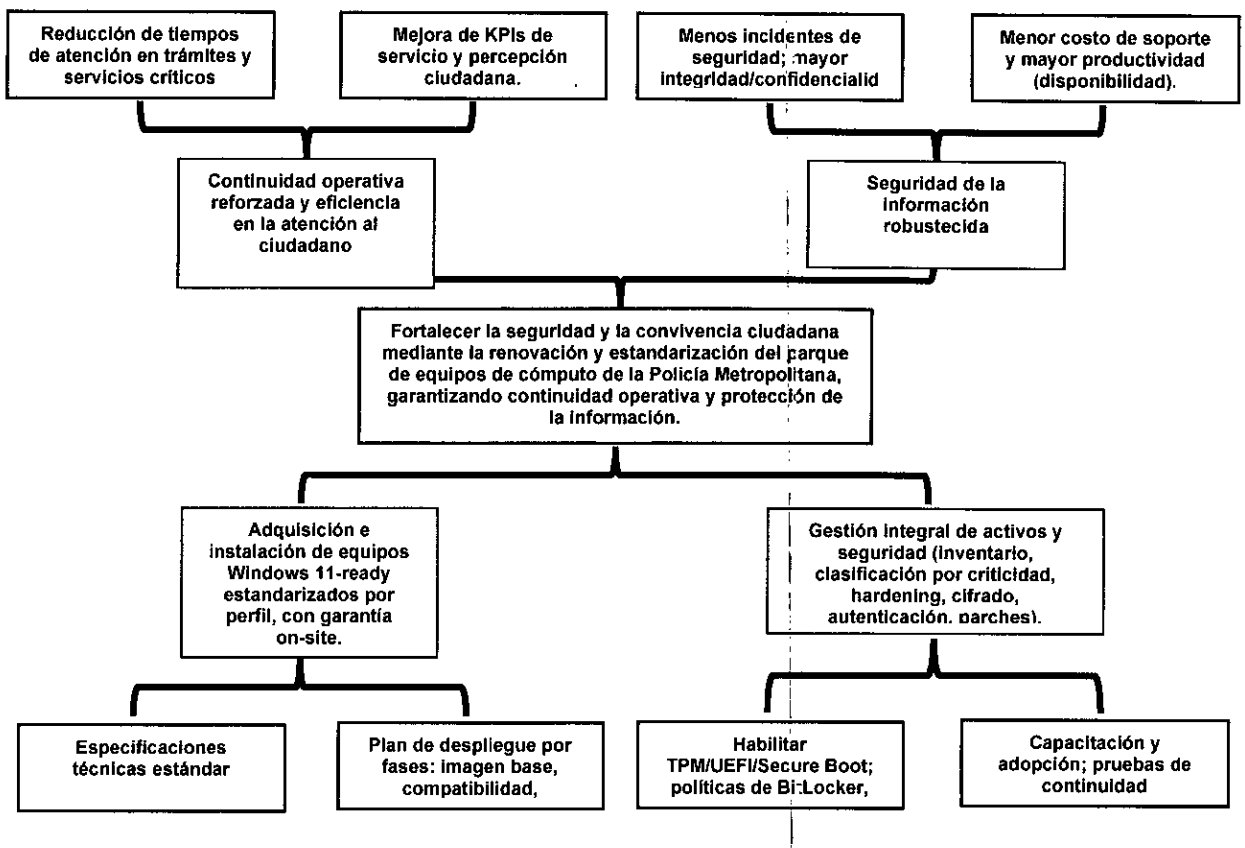
- Con 4 enfoques de intervención, así:
  - ✓ Control al multicrimen y sus finanzas
  - ✓ Adquisición de capacidades por la seguridad
  - ✓ Liderazgo corresponsable
  - ✓ Institucionalidad por la convivencia

- 5 delitos priorizados

- ✓ Homicidio
- ✓ Terrorismo
- ✓ hurto en todas sus modalidades
- ✓ Extorsión
- ✓ Tráfico de estupefacientes

Alineado a la política pública de seguridad y convivencia ciudadana de Cali 2024 – 2033, buscando que toda la institucionalidad trabaje por la convivencia, existiendo sinergia con entidades corresponsables con la convivencia pacífica, robustecimiento el liderazgo del Modelo del Servicio de Policía Orientado a las personas y los Territorios MSOPT.

5. ÁRBOL DE OBJETIVOS



6. JUSTIFICACIÓN

Necesidad pública y propósito.

El presente proyecto se justifica por la afectación directa a la continuidad operativa y a la seguridad de la información que soportan la seguridad y convivencia ciudadana en la Policía Metropolitana de Santiago de Cali y la MECAL. La obsolescencia y la no conformidad del parque de equipos de cómputo con los requisitos de plataforma segura exigidos por Windows 11 (TPM 2.0, UEFI/Secure Boot, CPU/RAM/GPU mínimas) impiden el acceso a controles críticos (BitLocker, arranque seguro) y limitan el soporte del fabricante, debilitando la prestación de servicios misionales al

ciudadano. Este proyecto, por tanto, busca restablecer capacidades tecnológicas esenciales para garantizar servicios públicos confiables y seguros, en coherencia con la Política de Gobierno Digital (PGD) del MinTIC.

Magnitud del problema y evidencia.

La MECAL registra 456 computadores con resolución para baja (≥10 años, fallas en disco/memoria/red/energía) y la Policía Metropolitana opera 527 equipos con obsolescencia tecnológica que no cumplen los mínimos de Windows 11. En conjunto, más del 50 % del parque no garantiza la operación eficiente en investigación, inteligencia, prevención y disuasión. La literatura técnica evidencia que mantener infraestructura sin soporte incrementa indisponibilidad, vulnerabilidades y costos por remediación y pérdida de productividad.

Pertinencia misional y valor público.

Renovar y estandarizar equipos Windows 11-ready se traduce en continuidad operativa, reducción de tiempos de atención y mejor protección de datos para la ciudadanía. La PGD exige que las entidades dispongan de TIC confiables y seguras; por ello, la modernización del parque tecnológico impacta directamente la calidad del servicio policial en los territorios y contribuye a fortalecer la confianza Estado-ciudadano.

Pertinencia técnica y estándar mínimo.

El proyecto implementará especificaciones estandarizadas por perfil (operativo/analítico/administrativo): TPM 2.0, UEFI/Secure Boot, CPU 64-bit (≥2–4 núcleos), RAM adecuada por rol (≥8–16 GB), SSD (≥256–512 GB) y GPU compatible DirectX 12. Estas condiciones aseguran la compatibilidad plena con Windows 11 y habilitan controles basados en hardware para fortalecer la seguridad (cifrado, arranque seguro, autenticación).

Eficiencia económica y costo-efectividad.

La renovación reduce la tasa de fallas y el soporte correctivo, disminuye tiempos de indisponibilidad y mejora la productividad del personal, lo que conlleva ahorros en costos ocultos (retrabajos, demoras, alternativas transitorias). La evidencia indica que la obsolescencia tecnológica eleva el riesgo operativo y el costo total de propiedad (TCO); actualizar el parque de equipos es una inversión costo-efectiva al aumentar disponibilidad y mitigar incidentes.

Coherencia normativa y ruta de contratación.

La formulación y registro se realizarán con la Metodología General Ajustada (MGA–DNP), asegurando diagnóstico, evaluación ex-ante y programación de metas/recursos en MGA Web/BPIN. Dada la naturaleza de bienes de características técnicas uniformes, la adquisición se enmarca en Selección Abreviada y/o Acuerdos Marco de Precios, garantizando eficiencia y transparencia conforme a la Ley 1150 de 2007 y el Decreto 1082 de 2015 (Sistema de compras públicas y PAA).

Riesgos de no intervención y mitigación.
Mantener equipos no conformes implica mayor exposición a ciberamenazas (sin TPM/UEFI/Secure Boot), posibles pérdidas/filtraciones de información, y deterioro de indicadores de servicio al ciudadano. La modernización tecnológica y la gestión integral de activos TIC (inventario, clasificación por criticidad, ciclo de vida) son medidas de mitigación que reducen incidentes y aseguran continuidad.

Sostenibilidad y seguimiento (MGA/PGD).

El proyecto establecerá indicadores de línea base y metas: % de equipos conformes a Windows 11, variación % de incidentes de hardware, tiempo promedio de atención al ciudadano, con fuentes de verificación (inventario TIC, auditorías técnicas, mesa de ayuda). Se implementarán prácticas de hardening, cifrado, gestión de parches y capacitación, consolidando la sostenibilidad operativa y la generación de valor público.

La modernización propuesta permite operacionalizar la planeación basada en evidencia desde los CIEPS, integrando los aplicativos institucionales de analítica e IA predictiva como insumo directo para la priorización territorial, la programación de patrullajes preventivos y la gestión oportuna de alertas. Con una dotación estandarizada y segura, los productos analíticos (boletines, tableros y reportes de riesgo) podrán generarse con mayor periodicidad y calidad, habilitando decisiones tácticas y operativas más oportunas y coherentes con los objetivos de convivencia y seguridad ciudadana. Este enfoque fortalece la articulación con el Plan Integral de Seguridad y Convivencia Ciudadana y con los instrumentos de planeación locales, incrementando el valor público al reducir tiempos de respuesta y mejorar la focalización de recursos en los puntos de mayor impacto.

En paralelo, el proyecto consolida gobernanza y trazabilidad sobre los procesos analíticos: controles de acceso por rol, registros de uso de los aplicativos, respaldo seguro de insumos y productos, y validación periódica del desempeño de los modelos (seguimiento a precisión, falsos positivos/negativos y deriva frente a la dinámica delictiva). Estas capacidades, sumadas a la capacitación operativa y a la estandarización de procedimientos, favorecen la sostenibilidad de la inversión y la mejora continua, al tiempo que protegen la cadena de custodia digital y refuerzan la confianza en los resultados que soportan la planeación del servicio de policía. En consecuencia, la intervención no solo renueva equipos: institucionaliza prácticas analíticas confiables y auditables que elevan la efectividad del servicio y la percepción de seguridad en el territorio.

7. OBJETIVO GENERAL

Fortalecer la seguridad, la convivencia ciudadana y las capacidades de inteligencia e investigación criminal de la Policía Metropolitana de Santiago de Cali, mediante la modernización y estandarización de la dotación de cómputo institucional, garantizando la continuidad operativa y la protección de la información con prácticas de gestión integral de activos TIC, y habilitando la planeación del servicio desde los CIEPS y el aprovechamiento de aplicativos institucionales de analítica e IA predictiva para la toma de decisiones oportuna y basada en evidencia.

8. OBJETIVOS ESPECÍFICOS, PRODUCTOS Y ACTIVIDADES

Objetivo específico No 1.

Estandarizar, contratar y adquirir equipos de cómputo Windows 11-ready (TPM 2.0, UEFI/Secure Boot, CPU/RAM/GPU conforme a perfiles) con Sistema Operativo Windows 11 Pro licenciado, garantizando calidad, oportunidad y trazabilidad.

Productos	Actividades	Duración de la actividad	Ruta Crítica
Especificaciones técnicas estandarizadas por perfil (operativo, analítico, administrativo) con Windows 11 Pro como edición mínima	Elaborar estudios y documentos previos (mercado/TCO) y definir requisitos: hardware Windows 11 Pro como edición obligatoria para unión a dominio, políticas y cifrado (BitLocker).	1 mes	Sí
Contrato adjudicado y equipos recibidos con actas y pruebas de aceptación (QA).	Estructurar y publicar el proceso; evaluar y adjudicar; recepcionar lotes; verificar en QA: presencia de marca digital OA3/activación y estado "Windows está activado con una licencia digital"; registrar inventario/seriales.	3 meses	Sí

Objetivo específico No 2.

Desplegar, asegurar y poner en producción los equipos adquiridos, con imagen corporativa, controles de seguridad basados en hardware y trazabilidad.

Productos	Actividades	Duración de la actividad	Ruta Crítica
Imagen base certificada y dispositivos configurados en Windows 11 Pro (SO, apps	Diseñar y probar la imagen en Windows 11 Pro; habilitar TPM/UEFI/Secure Boot; cifrar discos con BitLocker; migrar datos/perfiles; validar compatibilidad.	2 meses	Si
Inventario y clasificación de activos (CMDB) con trazabilidad de licencia (Windows 11 Pro OEM OA3: equipo-licencia asociada), actas de instalación y RAEE de equipos retirados.	Etiquetar e inventariar; capturar evidencia de activación (captura de Configuración > Sistema > Activación y lectura de MSDM/OA3); clasificar por criticidad/ciclo de vida; emitir actas; gestionar RAEE.	1 mes	Sí

9. POBLACIÓN BENEFICIARIA

Impacto nacional	Impacto local		Total población	Focalización
	Departamento	Municipio y/o distrito		
No aplica	Valle del Cauca	Distrito Especial Santiago de Cali	2.234.millones	Administrativamente el Municipio está conformado por la cabecera municipal, 249 barrios, 22 comunas y 15 corregimientos, según POT.

10. ALCANCE

El proyecto comprende la adquisición, puesta en operación y aseguramiento de equipos de cómputo estandarizados para la Policía Metropolitana de Santiago de Cali, orientados a fortalecer la planeación del servicio desde los CIEPS y a robustecer las capacidades de investigación criminal, inteligencia, convivencia y seguridad ciudadana. Los equipos a dotar cumplirán el estándar Windows 11 Pro con TPM 2.0 y UEFI/Secure Boot habilitados, contarán con licenciamiento digital (OA3) y especificaciones de CPU, memoria RAM, almacenamiento SSD y capacidades de gráficos acordes a los perfiles operativo, analítico y administrativo, garantizando continuidad operativa, desempeño adecuado para tareas analíticas y protección de la información institucional.

El alcance incluye la definición y aplicación de especificaciones técnicas por perfil, la contratación y recepción por lotes con pruebas de aceptación (QA) y evidencias de activación de licencias, así como la gestión de garantía onsite y soporte posventa de acuerdo con las condiciones contractuales. En la fase de puesta a punto se realizará la configuración estandarizada de software mediante imagen base certificada o, alternativamente, a través de provisión moderna (Autopilot/Intune), incorporando aplicaciones base institucionales (ofimática, navegador, agentes de seguridad/EDR, VPN, lectores y utilitarios), y los controladores (drivers) validados para los modelos adquiridos. Como parte del endurecimiento de la plataforma, se activarán TPM y Arranque Seguro, se implementará BitLocker con respaldo institucional de llaves de recuperación, y se aplicarán políticas y baselines de seguridad (firewall, control de puertos, actualización y cumplimiento).

Adicionalmente, el alcance contempla la trazabilidad integral de activos TIC: etiquetado y registro en CMDB, captura de seriales, números de activo, evidencia de activación OA3 y asociación equipo-licencia, así como la clasificación por criticidad y ciclo de vida. Se emitirán las actas de instalación y se ejecutará la gestión de RAEE para los equipos retirados, asegurando la disposición ambientalmente responsable y la debida documentación. Se desarrollará un plan de pruebas funcionales y de seguridad, con piloto y despliegue por anillos antes de pasar a producción general, y se impartirá capacitación breve a usuarios finales y a la mesa de ayuda, junto con guías prácticas para la operación segura y la recuperación de claves.

En coherencia con la misión, el proyecto habilita en los CIEPS seccionales estaciones con capacidad de análisis y visualización de información para la planeación operativa y la elaboración de boletines estratégicos; en investigación criminal, puestos de trabajo aptos para la gestión de cadena de custodia digital, consulta de bases y redacción de informes; en inteligencia, equipos con controles reforzados para el tratamiento de fuentes y generación de productos analíticos; y en convivencia y seguridad ciudadana, estaciones de atención y coordinación que contribuyan a reducir tiempos de respuesta y mejorar la oportunidad de la información que soporta el servicio policial en el territorio.

Para la aceptación del proyecto, se considerará la entrega del 100% de los equipos conforme a especificaciones y con licencia Windows 11 Pro activada; la habilitación efectiva de controles de seguridad (con al menos el 95% de estaciones cifradas con BitLocker y políticas aplicadas); la validación misional por parte de los responsables de CIEPS, investigación criminal, inteligencia y convivencia de que las estaciones cumplen los casos de uso definidos; la CMDB actualizada con trazabilidad equipo-licencia y documentación completa de RAEE.

Este alcance se ejecutará dentro del plazo de tres meses, sujeto a la disponibilidad de licencias y conectividad institucional, y se enmarca en la MGA-DNP y en la modalidad de contratación aplicable a bienes de características técnicas uniformes, asegurando transparencia y costo-efectividad. Como parte del seguimiento, se medirán indicadores tales como el porcentaje de equipos conformes a Windows 11 (TPM/Secure Boot), el porcentaje de estaciones con BitLocker y baseline aplicada, la reducción de tiempos de atención en los procesos misionales y la disminución de incidentes de hardware, así como la tasa de éxito del despliegue y el tiempo de provisión desde OOBE hasta escritorio operativo. Estos resultados se orientan a mejorar la continuidad operativa, robustecer la seguridad de la información y elevar la calidad del servicio al ciudadano.

En concordancia con los avances institucionales en analítica e inteligencia artificial, el proyecto asegurará que la dotación tecnológica soporte los flujos predictivos orientados a anticipar la comisión de delitos y comportamientos contrarios a la convivencia, en especial los que alimentan la planeación del servicio desde los CIEPS. Para ello, los perfiles analíticos incluirán capacidad de preprocesamiento local de datos y compatibilidad con los agentes y librerías requeridas por las aplicaciones existentes, garantizando la protección criptográfica del entorno (TPM 2.0, Secure Boot y cifrado con BitLocker) y la trazabilidad de los insumos consultados. Los resultados generados por los modelos de IA se integrarán como insumo de decisión dentro de procesos con supervisión humana (human-in-the-loop), priorizando la respuesta operativa, la asignación de recursos, la gestión de alertas y la orientación de patrullajes preventivos, sin reemplazar el criterio profesional ni los protocolos vigentes.

Adicionalmente, el alcance contempla lineamientos de gobernanza y uso responsable de IA: registros de auditoría sobre consultas y salidas de los modelos, validación periódica de desempeño (precisión y falsos positivos) y mecanismos de detección de deriva para mantener la pertinencia de los algoritmos frente a la dinámica delictiva. Se implementarán controles de acceso por rol, segmentación de redes y gestión de credenciales bajo buenas prácticas, junto con capacitación específica a analistas y personal operativo en interpretación de salidas y mitigación de sesgos. Como parte del seguimiento, se medirán indicadores como reducción del tiempo de generación de alertas y boletines, porcentaje de alertas útiles validadas por analistas y mejoras en la priorización de casos atribuibles al componente predictivo, asegurando que la inversión tecnológica se traduzca en resultados verificables para la convivencia y la seguridad ciudadana.

11. PRESUPUESTO DETALLADO

Fase 1					
ÍTEM	**BIEN Y/O SERVICIO**	**UNIDAD DE MEDIDA**	**CANTIDAD**	**VALOR UNITARIO ÍTEM**	**TOTAL ÍTEM**
1	*Equipos de cómputo con licenciamiento de Windows 11 Pro*	*Unidad.*	*20*	*$ 5.500.000*	*$110.000.000*
2	*Paquete de ofimática*	*Unidad.*	*20*	*$ 2.375.000*	*$ 47.500.000*
				VALOR TOTAL	*$157.500.000*

Nota 1: en los valores de este presupuesto se contemplan todos los costos directos e indirectos, licencias, equipos y periféricos entre otros.), que se requieren para la ejecución del proyecto. Las especificaciones no deben incluir marcas.

Nota 2: los valores estimados del proyecto deben corresponder a un análisis de la demanda, mercado y oferta, así como a un análisis de precios de referencia, históricos, catalogo o portales web y mercado del cual se anexan las evidencias de este estudio.

Nota 3: para todos los efectos, los valores de cada componente aquí presentados deberán ser actualizados por la entidad contratante mediante el respectivo estudio de mercado que debe adelantarse en el respectivo proceso contractual de acuerdo a lo establecido en la ley 80 de 1993 y demás leyes, decretos resoluciones entre otros que lo regulen.

Nota 4: en los valores unitarios de los componentes de tecnología **no se tendrá en cuenta el IVA** de conformidad con la Ley 1819 del 29 de diciembre de 2016, en su artículo 188 se modifica el artículo 477 del Estatuto Tributario, quedando así; Artículo 477. Bienes que se encuentran exentos del impuesto. Están exentos del impuesto sobre las ventas, con derecho a compensación y devolución, los siguientes bienes: numeral 3 literal N "Equipos, software y demás implementos de sistemas y comunicaciones para uso de las Fuerzas Militares y la Policía Nacional".

12. COFINANCIACIÓN

Nombre del financiador	% financiación	Valor
No aplica	*No aplica*	*No aplica*

13. RIESGOS

	Riesgo Alto		Riesgo Medio		Riesgo Bajo	x

14. ESPECIFICACIONES TÉCNICAS DEL BIEN

Especificaciones técnicas equipos de computo

1. COMPUTADOR DE ESCRITORIO ALL IN ONE			
	DESCRIPCIÓN	**CUMPLE**	**NO CUMPLE**
1.1	***Cantidad***: Especificar		
1.2	***Marca***: Especificar.		
1.3	***Modelo***: Especificar.		
1.4	***Factor de Forma:*** AIO (ALL IN ONE)		
1.5	***Año de fabricación:*** última versión con respecto a la vigencia de suscripción del contrato		
1.6	***Pantalla***: Tecnología de panel IPS o equivalente (WVA, PLS, etc.) mínimo 23".8, máximo 27".		
1.7	***Bezel Laterales:*** Borderless.		
1.8	***La pantalla:*** debe ser antirreflejo y no táctil.		
1.9	***La base de la pantalla:*** debe permitir Inclinación y altura ajustable.		
1.10	***Resolución mínima de la pantalla***: 1920*1080 (Full HD)		
1.11	***Color del equipo de cómputo***: Negro o Gris		
PROCESADOR			
1.12	***Marca***: Especificar		
1.13	***Modelo***: Especificar		
1.14	***Fecha de lanzamiento:*** Debe estar dentro de los ***18 meses anteriores*** a la fecha de lanzamiento por parte del fabricante del procesador. La fecha de lanzamiento del procesador deberá estar publicada en la página WEB oficial del fabricante		
1.15	***Potencia de diseño térmico (TDP):*** Mínimo 65W		
1.16	***Número de cores:*** Mínimo 14		
1.17	***Número de Subprocesos:*** Mínimo 14		
1.18	***Frecuenta Máxima Turbo:*** Mínimo 5.1 GHZ		

1.19	***Memoria Caché:*** Mínimo 26 MB		
1.20	***Tipo***: Procesador para ambiente corporativo, y modelo para ambiente empresarial. El BIOS debe estar bloqueado para la opción de OVERCLOCKING. Debe ser verificable en la página web del fabricante del equipo.		
1.21	***Anexar certificación***: Del fabricante del procesador ofertado, donde sea posible verificar que el procesador es para ambiente corporativo y que cumple con todas las especificaciones técnicas solicitadas.		
1.22	***Anexar Link:*** Donde se evidencien todas las especificaciones mínimas relacionadas con el procesador a través de la página WEB del fabricante del procesador.		
1.23	***Chipset Corporativo:*** especificar.		
ADMINISTRACIÓN FUERA DE BANDA			
1.24	Mínimo debe tener habilitada la administración fuera de banda.		
DISCO DURO			
1.25	***Capacidad:*** Mínimo una (01) unidad de estado sólido SSD, 512 GB, Gen 4x4 PCIe NVMe M.2		
MEMORIA RAM			
1.26	***Mínimo***: DDR5 16 GB		
1.27	***Configuración***: debe ser DDR5 6400 MT/s, en configuración dual channel (2×8 GB o superior)		
TARJETA DE VIDEO			
1.28	Gráficos integrados del mismo fabricante del procesador, con soporte mínimo para resolución Full HD (1920×1080) y salida simultánea a dos monitores		
CÁMARA WEB			
1.29	***Integrada***: mínimo 1080p FHD con capacidad IR y micrófono integrado Debe incluir un **mecanismo físico de seguridad de privacidad**, integrado al equipo, que permita la desactivación de la cámara de manera manual.		
FUENTE DE PODER INTERNA O EXTERNA			
1.30	***Marca***: Especificar ***(De la misma marca del fabricante del computador)*** ***Modelo***: Especificar ***En caso de ser fuente interna:*** debe dar cumplimiento a la certificación 80 PLUS: Interna Platinum o superior. La fuente propuesta se debe poder verificar en la página http://80plus.org/ o verificable en la página del fabricante (anexar URL). La fuente de poder debe ser compatible con el factor de forma del equipo de cómputo solicitado. ***En caso de ser fuente externa***: se debe suministrar un accesorio de seguridad a fin de evitar el hurto de la misma.		
PUERTOS			
1.31	**ENTRADA:** Mínimo 4 puertos USB (tipo A o C), de los cuales al menos 2 deben ser USB 3.2 Gen 1 (5 Gbps) o superior. **SALIDA:** Salida de video mediante DisplayPort y HDMI, ya sea nativa o mediante adaptador incluido.		
MULTIMEDIA			
1.32	Conectores auriculares y micrófono de 3,5 mm independiente o en combo y parlante o altavoz interno mono o estero		
PERIFÉRICOS			
1.33	***Mouse:*** Debe contar con cable de conexión USB, con sensor óptico, debe tener 2 botones y scroll, ***(De la misma marca del fabricante del computador).***		
1.34	***Teclado:*** En español debe contar con cable con conexión USB, en español distribución latinoamericana, ***(De la misma marca del fabricante del computador).***		
DISPOSITIVO DE RED			
1.35	Ethernet (RJ-45) 10/100/1000 integrada con compatibilidad nativa de IPv6 en coexistencia con IPv4.		
PATCH CORD			
1.36	Suministro Patch Cord categoría 6A de fábrica de mínimo 3 mts.		
TARJETA GRAFICA			
1.37	Integrada de la misma marca del procesador, mínimo HD.		
ADMINISTRACIÓN DE SEGURIDAD			
1.38	Seguridad con chip TPM (Trusted Platform Module), Versión 2.0 o superior, Discreto o Embebido		
CERTIFICACIONES			
1.39	El oferente debe garantizar que, los equipos de cómputo cuentan con las siguientes certificaciones: • Certificación que indique que los equipos ofrecidos son de un fabricante con representación en Colombia, ***(Anexar certificación).*** • Certificación EPEAT Gold, ***(Anexar certificación).*** • Certificación en el Estándar Militar MIL-STD 810H o MIL-STD 810G, ***(Anexar certificación).***		

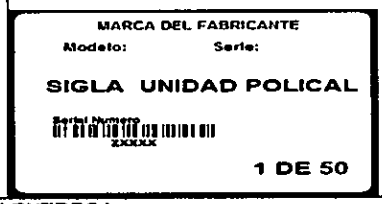
	• Certificación TCO CERTIFIED, ***(Anexar certificación).*** • Certificación Energy Star Versión 8.X o superior ***(Anexar certificación).*** • Certificación que indique que los equipos ofrecidos cuentan con sistema operativo instalado por el fabricante. ***(Anexar certificación).***		
SISTEMA OPERATIVO			
1.40	Licenciamiento del sistema operativo Los equipos de cómputo deberán entregarse con Windows 11 Pro OEM, versión de 64 bits en español, preinstalado desde fábrica, debidamente activado y completamente funcional. La versión del sistema operativo debe corresponder a la más reciente disponible al momento de la entrega, adecuada para entornos corporativos.		
OFIMÁTICA			
1.41	Microsoft Office Home & Business última versión liberada en el mercado ESD (Electronic Software Distribution) edición de 64 bits. El contratista deberá entregar la licencia de ofimática instalada en cada equipo de cómputo en coordinación con el supervisor del contrato, quien dará los lineamientos previos respectivos para la activación de las mismas. El contratista debe entregar al supervisor del contrato; documento en Excel que incluya toda la información requerida para la administración de las licencias, el cual, a través del supervisor del contrato, deberá ser integrado en una herramienta tecnológica de análisis de datos, que permita la gestión y visualización de toda la información que más adelante se relaciona, así:		

No.	SERIAL DE LA MÁQUINA	TOKEN	CUENTA DE CORREO ASOCIADA	CONTRASEÑA	NUMERO TELEFÓNICO ASOCIADO A LA CUENTA DE CORREO	CUENTA DE CORREO DE RECUPERACIÓN	CONTRASEÑA	FECHA DE CANJE TOKEN
1	------	------	As***@hotmail.com	-------	-------	As***@hotmail.com	********	20/12/2023
2	------	------	As***@hotmail.com	-------	-------	As***@hotmail.com	********	20/12/2023

	** Para el proceso de alistamiento e instalación de la ofimática, en cada uno de los equipos de cómputo para la Policía Nacional, es importante tener presente que, en coordinación con el supervisor del contrato, se darán los lineamientos previos respectivos para establecer los parámetros en la elaboración de la nemotecnia del total de las cuentas de correo, para la respectiva activación y administración.* El Contratista se obliga a NO suministrar, revelar o dar a conocer, los usuarios, contraseñas, cuentas de correo, números de celular, lugares de distribución y demás información que sea registrada en el documento Excel a personas ajenas a la Institución o pertenecientes a la misma (La información solamente deberá ser entregada al supervisor del contrato). Así mismo, se obliga al contratista entregar el documento Excel en versión editable (con roles de lectura y escritura), sin restricciones de ningún tipo y sin limitaciones de edición, con el propósito de lograr adicionar información considerando las necesidades de la Institución, sin que esto genere costos adicionales a la Policía Nacional.

	GENERALIDADES	CUMPLE	NO CUMPLE
1.	***Garantía***: dos (02) años contra defectos de fabricación, a partir del acta de recibido a satisfacción por parte del supervisor del contrato, sin que esto genere costo para la Policía Nacional. Durante el tiempo de la garantía el contratista debe prestar todo el acompañamiento necesario para realizar las actualizaciones en el sistema operativo de los equipos al momento de que sean instaladas nuevas versiones.		
2.	El contratista deberá entregar dos usuarios que permitan acceder a un sistema de información que soporte la mesa de ayuda o autoservicio (acceso vía web) del proveedor, con el objetivo de realizar seguimiento a los casos o tickets generados. Los funcionarios administradores funcionales del sistema de información serán designados por el supervisor del contrato. El sistema de información debe permitir exportar reportes, para mayor control por parte del supervisor.		

	La garantía ofrecida por el contratista deberá tener un control y seguimiento de los tickets o casos generados para los soportes técnicos, donde se escale a los niveles adecuados para su solución y cierre.		
3.	La Gestión de la garantía se realiza por parte del contratista mediante los casos creados por parte de Policía Nacional. El contratista deberá disponer los recursos necesarios para la atención de los casos, dentro de los tiempos definidos en el apartado de soporte técnico.		
CALIDAD DE LOS EQUIPOS DE CÓMPUTO ENTREGADOS (APLICAN DURANTE EL TIEMPO DE GARANTÍA)			
4.	Si el equipo de cómputo presenta dos (2) veces la misma falla en el hardware, el contratista debe cambiar el equipo por un equipo nuevo de características iguales o superiores, en un tiempo máximo de (5) días hábiles contados a partir del momento en el que se registra la segunda (2ª) falla.		
5.	Si el equipo de cómputo presenta tres (03) fallas en distintas partes en el Hardware, el contratista debe cambiar el equipo de cómputo por un equipo nuevo de características iguales o superiores, en un tiempo máximo de cinco (5) días hábiles contados a partir del momento en el que se registra la tercera (3ª) falla.		
6.	Si del total de los equipos de cómputo por lote o lotes ofertados adquiridos falla el cinco por ciento (5%) por diferentes causas, el contratista debe cambiar el porcentaje de los equipos de cómputo que presenta falla por equipos nuevos de características iguales o superiores y debe entregarlos en un tiempo menor o igual a treinta (30) días hábiles contados a partir del momento en el que se registra el incidente.		
7.	Si del total de los equipos de cómputo por lote o lotes ofertados adquiridos falla el diez por ciento (10%) en la misma pieza de Hardware, el contratista debe cambiar el porcentaje de los equipos que presenta falla por equipos nuevos de características iguales o superiores y debe entregarlos en un tiempo máximo de treinta (30) días hábiles contados a partir del momento en el que se registra el incidente.		
ASPECTOS INCLUIDOS EN LA GARANTÍA			
8.	En caso de presentarse fallas en los equipos adquiridos, el contratista es responsable de realizar la reparación por defectos del bien, suministro e instalación de los repuestos necesarios sin que esto genere costo alguno para la Policía Nacional.		
9.	Es responsabilidad del contratista, asumir toda la logística necesaria para atender las fallas y reparaciones necesarias en los equipos de cómputo en los lugares donde los equipos se encuentren asignados, sin que esto genere costo alguno para la Policía Nacional.		
PRESENTACIÓN DE LA OFERTA			
10.	Las propuestas se harán en forma clara y en idioma español. Deberán presentar la carta de representación del fabricante o de distribuidor autorizado donde se indique su nombramiento tanto por el tiempo de ejecución del contrato, como también en los tiempos de garantía.		
11.	La propuesta presentada, deberá ser firmada y avalada por un ingeniero electrónico o ingeniero de sistemas o Ingeniero en telecomunicaciones anexando la respectiva tarjeta profesional. Esto de acuerdo a lo indicado en el ARTÍCULO 20 de la LEY 842 DE 2003 "PROPUESTAS Y CONTRATOS.: "Las propuestas que se formulen en las licitaciones y concursos abiertos por entidades públicas del orden nacional, seccional o local, para la adjudicación de contratos cuyo objeto implique el desarrollo de las actividades catalogadas como ejercicio de la ingeniería, deberán estar avalados, en todo caso, cuando menos, por un ingeniero inscrito y con tarjeta de matrícula profesional en la respectiva rama de la ingeniería".		
SOPORTE TÉCNICO			
12.	Al inicio del contrato se establecerá el procedimiento de solicitud de la garantía y soporte técnico tanto para el hardware y ofimática ofertados.		
13.	El horario de atención para las actividades de soporte técnico deberá ser los días hábiles de 08:00 a 18:00 horas.		
14.	El contratista deberá poner a disposición de la Policía Nacional, de manera permanente, los siguientes medios para el reporte de casos: • Mesa de servicio o autoservicio con acceso vía web. • Número telefónico. • Correo electrónico.		
15.	El contratista deberá garantizar soporte técnico vía telefónica e Internet, como primer nivel de atención, en idioma español y por personal técnico certificado		
16.	**MARCACIÓN DE LAS CAJAS** Cada uno de los equipos será entregado con sus respectivas cajas individuales las cuales deberán estar debidamente marcadas e identificadas así: Marca del equipo Modelo del equipo Referencia del equipo		

	Serial del equipo Unidad policial Número del equipo; es decir 1 de 50, 2 de 50, 3 de 50. 		
LUGAR DE ENTREGA			
17.	La entrega de los computadores de acuerdo con las especificaciones técnicas mínimas requeridas establecidas en el presente estudio previo; será establecida de acuerdo al plan de distribución de equipos establecido por la Policía Nacional.		
AMBIENTAL			
18.	El fabricante y el representante del fabricante en Colombia para los computadores y todos sus componentes, certificará que cumple con lo estipulado en la Resolución 15/12/2010 expedida por el Ministerio de Ambiente, Vivienda y Desarrollo Territorial "Por la cual se establecen los Sistemas de Recolección Selectiva y Gestión Ambiental de Residuos de Computadores y/o Periféricos y se adoptan otras disposiciones", (Anexar documento).		
CONFIDENCIALIDAD DE LA INFORMACIÓN			
19.	Si la Policía Nacional, considera pertinente someter a estudio de seguridad al personal que prestará los servicios, el contratista permitirá y facilitará todos los medios que la Entidad le solicite para tal fin.		
20.	El Contratista se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del futuro contrato y que se encuentra marcada como confidencial; así como de los lugares a los cuales tenga acceso con ocasión de su servicio y sea revelada información marcada como confidencial, para lo cual el contratista deberá diligenciar y firmar un acuerdo de confidencialidad y no revelación de la información, (Anexar documento).		
SEGURIDAD DE INSTALACIONES			
21.	Durante el tiempo de garantía el contratista deberá cumplir con el protocolo de seguridad de instalaciones y normas internas de seguridad física en cada una de las unidades policiales en todo el territorio colombiano y Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional (resolución 04408 del 26/12/2024).		
SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO			
22.	El contratista deberá cumplir con la implementación del sistema de Gestión de la Seguridad y Salud en el Trabajo, para lo cual deberán diligenciar el Formulario Sistema de Gestión de la Seguridad y Salud en el Trabajo. (Anexar documento).		
COMPROMISO ANTICORRUPCIÓN			
23.	Cumplir con el compromiso de anticorrupción dentro del proceso manifestando que se encuentra dispuesto a suministrar la información propia que resulte necesaria para aportar transparencia al mismo y si se comprueba el incumplimiento del proponente, sus empleados, representantes, asesores o de cualquier otra persona que en el proceso de contratación actúe en su nombre, es causal suficiente para el rechazo de la oferta o para la terminación anticipada del contrato, si el incumplimiento ocurre con posterioridad a la adjudicación del mismo, para lo cual deberá diligenciar en su totalidad el Formulario Compromiso Anticorrupción. (Anexar documento).		

15. CONCEPTOS TÉCNICOS

Concepto de viabilidad emitido por planeación MECAL mediante comunicación oficial No GS-2026-012538-MECAL.

16. DATOS DE CONTACTO

Jefe Grupo Tecnologías de la Información y las Comunicaciones
Capitán, DUVAN ALBERTO CASANOVA VASCO.
Correo electrónico. duvan.casanova1182@correo.policia.gov.co
Teléfono móvil. 3188382288

FORMULADOR DEL PROYECTO:

Firma
Capitán **DUVAN ALBERTO CASANOVA VASCO**
C.C.: 1.085.297.086
Cargo: Jefe Grupo de Tecnologías de la Información y Las Comunicaciones

RESPONSABLE UNIDAD QUE LO PRESENTA:

Firma
Coronel **ANDRÉS ARIAS BUITRAGO**
C.C.: 79763101
Cargo: Comandante Policía Metropolitana Santiago de Cali (E)

Elaboró: IJ. Yamit Arvey Narváez Ramírez
MECAL – GUTIC

Revisó: IJ. Rafael Ignacio Cárdenas Mera
MECAL – GUTIC

Revisó: SO. Uriel Gutiérrez Rengifo
MECAL – GESTER