Unidad Administrativa: secretaria general
No. Radicado del proyecto en POAI: 26-9-19-001-02687
Nombre del Proyecto: "Fortalecimiento de la Seguridad Digital Institucional de la Alcaldía de Popayán"

1. INTRODUCCIÓN

En Popayán, la mayoría de interacciones entre la comunidad y su administración ya ocurre por canales digitales: pagos y acuerdos de **impuestos**, **PQRSD**, **SISBÉN**, **catastro**, **cupos educativos**, **Comisarías de Familia**, entre otros. Cuando estos servicios **se interrumpen** o **no son seguros**, la afectación es directa para las personas: filas y traslados innecesarios, pérdida de tiempo y dinero, exposición de **datos personales** y, en consecuencia, **desconfianza** en lo público. Por eso, la seguridad digital no es un fin interno ni un "sostenimiento tecnológico"; es el **medio** para que la ciudadanía **acceda de forma continua, segura y confiable** a sus trámites y derechos.

El proyecto **"Fortalecimiento de la Seguridad Digital Institucional de la Alcaldía de Popayán"** se formula precisamente para **proteger a la población usuaria y asegurar la continuidad** de los servicios críticos que sostienen la vida cotidiana del municipio. Lo hará mediante dos frentes que se traducen en beneficios concretos para la gente:

Seguridad y continuidad del servicio: adopción operativa de la Política de Seguridad Digital, protocolos y roles claros, operación de un **SOC integrado al monitoreo**, modernización de **servidores, firewalls, respaldos y enlaces redundantes**, e **interoperabilidad** entre plataformas; todo orientado a **evitar caídas**, **prevenir fraudes** y **proteger datos personales**.

Así, las acciones técnicas se justifican por su **valor público**: **menos interrupciones**, **más trámites resueltos a la primera**, **menores costos por contingencias** y **mayor confianza** en los canales digitales. Las metas de desempeño (como la **disponibilidad ≥ 90 %** y la mejora en los componentes de Gobierno y Seguridad Digital) se usarán como **evidencia medible** de que los servicios que la ciudadanía utiliza funcionan, están protegidos y permanecen disponibles cuando más se necesitan. En síntesis, esta es una intervención **para la gente**, que garantiza derechos y facilita la vida diaria mediante una atención digital **simple,** segura y oportuna.

2. CONTRIBUCIÓN A LA POLÍTICA PÚBLICA

2. CONTRIBUCION ALA POLITICA PUBLICA

Plan Nacional de Desarrollo 2022 - 2026	**"Colombia, potencia mundial de la vida"**
Transformación: Seguridad humana y justicia social	
Pilar: Superación de privaciones como fundamento de la dignidad humana y condiciones básicas para el bienestar	
Catalizador: Conectividad digital para cambiar vidas	
Componente: Alfabetización y apropiación digital como motor de oportunidades para la igualdad	
Programa: Fomento del desarrollo de aplicaciones, software y contenidos para impulsar la apropiación de las Tecnologías de la Información y las Comunicaciones (TIC)	

Plan de Desarrollo Departamental: La Fuerza Del Pueblo 2024 - 2027
Estrategia: Buen gobierno y gestión institucional
Programa: Fomento del desarrollo de aplicaciones, software y contenidos para impulsa comunicaciones TIC
Plan de Desarrollo Municipio de Popayán Alianza con Popayán 2024 –2027:
Estrategia: Gobernanza Y Gobernabilidad
Programa: Alianza con el fortalecimiento institucional
Meta (s) Producto: Desarrollar la Política de Seguridad digital,

INFORMACIÓN PDM			**INFORMACIÓN MGA**	
N° Producto propuesto PDM	**Nombre Producto PDM**	**Meta – indicador PDM**	**Código producto MGA**	**Nombre producto MGA**
2302101	Servicios Tecnológicos.	Desarrollar la Política de Seguridad digital	230210101	Servicios tecnológicos implementados para la protección de la seguridad de la información

3. ANTECEDENTES

Desde 2017 la Alcaldía de Popayán ha consolidado una senda permanente de modernización tecnológica orientada a mejorar la gestión pública, ampliar la conectividad y proteger la información institucional, en concordancia con las políticas nacionales de Gobierno Digital. El recorrido se inició con el proyecto "Gobierno en Línea" (BPIN 2017190010045), que digitalizó trámites prioritarios y habilitó ventanillas únicas virtuales, complementado por la instalación de zonas Wi-Fi públicas (BPIN 2017190010044) que democratizó el acceso a internet en parques y plazas. Entre 2018 y 2019 se ejecutaron los programas generales de Gobierno en Línea (BPIN 2018190010074 y 2019190010075), profundizando la digitalización de procesos internos.

El avance continuó en 2020 con el "Plan de Tecnologías 2020" (BPIN 2020190010061), que modernizó la infraestructura de red y servidores centrales, y con el proyecto de "Modernización e Innovación Digital" (BPIN 2020190010092), que introdujo herramientas de colaboración en la nube. En 2021, el proyecto "Mejoramiento de las Tecnologías de la Información" (BPIN 2021190010038) incorporó los primeros controles de ciberseguridad. Para 2024 se ejecutó el proyecto "Fortalecimiento de los Procesos y Procedimientos de la Gestión Documental" (BPIN 2024190010057), que impulsó la digitalización de archivos y reforzó la protección de datos institucionales mediante componentes TIC. Finalmente, en 2025 se desarrolló el proyecto "Fortalecimiento de la Estrategia de Gobierno Digital en la Alcaldía del Municipio de Popayán" (BPIN 202500000003376), con el que se adoptó la Política de Seguridad Digital, se desplegó infraestructura perimetral de nueva generación (firewall NG, IDS/IPS y SIEM) y se aumentó el Índice de Madurez de Seguridad Digital del 27 % al 54 %, alcanzando una disponibilidad de servicios en línea del 98,9 %.

La experiencia acumulada deja lecciones clave: la interoperabilidad debe planearse desde el inicio para evitar silos de información; la ciberseguridad constituye un eje transversal que exige un SGSI alineado con ISO 27001; la capacitación continua reduce la resistencia al cambio y las malas prácticas de los usuarios finales; y la sostenibilidad de las inversiones requiere contemplar gastos operativos (OPEX) para licenciamiento, soporte y garantías.
Aun con estos logros persisten brechas relevantes: la infraestructura instalada en 2025 necesita renovación de licencias y garantías para sostener un SLA de disponibilidad igual o superior al 99,5 %; el monitoreo SIEM requiere un Centro de Operaciones de Seguridad (SOC) con análisis 24/7; y el Índice de Madurez de Seguridad Digital debe superar el 70 % recomendado por el CONPES 3995 de 2020.

Ante este panorama, el proyecto "Fortalecimiento a la Transformación Digital Segura del Municipio de Popayán" se concibe como la evolución natural de los esfuerzos previos. Su objetivo es mantener, optimizar y escalar los avances alcanzados, consolidando la confidencialidad, integridad y disponibilidad de los datos municipales, elevando la madurez de seguridad digital por encima del 70 % y garantizando una disponibilidad de servicios TIC superior al 99,5 %. Con ello, la Administración Municipal ratifica su compromiso con una transformación digital segura y sostenible, coherente con el Plan de Desarrollo Municipal 2024-2027 Alianza con Popayán y las expectativas de la ciudadanía en la era de la información.

4. JUSTIFICACIÓN

Las brechas evidenciadas en FURAG 2024 Gobierno Digital **60,8 %** y Seguridad Digital (POL 8) **53,0 %**, ambas por debajo del **≥ 70 %** no son un asunto interno de operación: afectan directamente a la comunidad**.** Cuando la seguridad digital no está plenamente adoptada (protocolos, roles, SOC 24/7, licencias vigentes) y la infraestructura carece de alta disponibilidad e interoperabilidad, se producen: **interrupciones de servicios** (trámites que se detienen), **exposición de** datos personales**,** demoras en la atención **y** desconfianza en los canales digitales. En términos de derechos, estas fallas comprometen el **hábeas data**, el **acceso oportuno a la información pública**, el debido proceso administrativo en entorno digital **y la** regularización de trámites**.**

La inversión **propuesta** busca resolver un problema **público** y generar **beneficios** medibles para la ciudadanía**,** al financiar exclusivamente acciones de seguridad digital institucional**:**

- **Adopción operativa de la Política de Seguridad Digital**: definición y socialización de protocolos y roles, operación de **SOC 24/7** integrado al SIEM, gestión de incidentes y vulnerabilidades, auditorías y pruebas de penetración periódicas.
- **Infraestructura resiliente y continua**: servidores de alta disponibilidad, **firewalls NG**, esquemas de **backups** y **enlaces redundantes**, renovación de **licencias críticas** y **mejoras de interoperabilidad** para reducir tiempos de respuesta y errores de tramitación.

Beneficios y resultados esperados (verificables):

- **Disponibilidad de servicios en línea ≥ 90 %**, disminuyendo caídas que hoy obligan a filas y desplazamientos.
- **FURAG – Seguridad Digital ≥ 70 %** y **FURAG – Gobierno Digital ≥ 75 %**, como evidencia del cierre de brechas.
- **Reducción del riesgo**: menos incidentes y **mejores tiempos MTTD/MTTR** del SOC, con impacto directo en la **oportunidad de la atención** y en la **confianza ciudadana**.

El proyecto adopta un enfoque de **ciclo de vida (CAPEX + OPEX)** para asegurar continuidad y sostenibilidad (licencias, soporte, operación SOC), alineado con los mandatos de **protección de datos** y **Gobierno Digital** vigentes y con el Plan de Desarrollo Municipal 2024–2027. En síntesis, la justificación radica en proteger derechos ciudadanos y mejorar la calidad del servicio público, cerrando causas estructurales que hoy generan interrupciones, sobrecostos y desconfianza, y sustituyéndolas por **servicios seguros, disponibles y confiables** para toda la población.

5. MARCO LEGAL

La formulación y ejecución del proyecto “Fortalecimiento de la Seguridad Digital Institucional de la Alcaldía de Popayán” se soporta en un marco jurídico que integra normas constitucionales, leyes estatutarias, decretos y resoluciones técnicas que responden a los retos de ciberseguridad y transformación digital del Estado. En concordancia con la Política de seguridad Digital, se adopta un enfoque de servicios digitales centrados en el ciudadano: la seguridad digital es un habilitador para garantizar el acceso continuo, seguro y equitativo a los servicios públicos en línea y para la protección efectiva de derechos como el hábeas data, el acceso a la información y el debido proceso administrativo en entornos digitales.

Constitución Política de Colombia

- Art. 15 (hábeas data y protección de la intimidad).
- Art. 20 (libertad de informar y recibir información veraz).
- Art. 74 (derecho de acceso a documentos públicos).
- Art. 209 (principios de publicidad y transparencia en la función administrativa).

Protección de datos, transparencia y control social

- Ley 1581 de 2012 — régimen general de protección de datos personales (art. 17 impone a las entidades el deber de adoptar políticas de tratamiento de datos).
- Ley 1712 de 2014 — Ley de Transparencia y Derecho de Acceso a la Información Pública.
- Ley 2195 de 2022 — refuerza la trazabilidad y la obligación de reportar información para prevenir la corrupción.
- Ley 1757 de 2015 — desarrolla los mecanismos de participación y control ciudadano, obligando a habilitar canales multicanal de interacción.

Sector TIC y conectividad

- Ley 1341 de 2009 (art. 2 y 4) — principios de universalidad y seguridad de las redes.
- Ley 1978 de 2019 — moderniza el sector TIC y prioriza la inversión para cerrar la brecha digital.
- Ley 2108 de 2021 — declara el acceso a Internet como servicio público esencial.

Gobierno Digital y seguridad de la información

- Decreto 1078 de 2015 (DUR TIC), Cap. 2.2.9, habilitador de Seguridad y Privacidad de la Información.
- Decreto 767 de 2022 — actualiza los lineamientos generales de la Política de Gobierno Digital y ratifica la obligación de todas las entidades de incorporar componentes de confianza y seguridad digital en sus planes de acción.

Función Pública

- Resolución 500 de 2021 (MinTIC) — adopta el Modelo de Seguridad y Privacidad de la Información – MSPI como habilitador transversal de la Política de Gobierno Digital.
- Resolución 02239 de 2024 (MinTIC) — actualiza la Política General de Seguridad y Privacidad de la Información del sector TIC, alineando sus lineamientos con la Ley 1581 y el Decreto 1078.
- Resolución 02277 de 2025 (MinTIC) — incorpora la versión ISO/IEC 27001:2022 en el MSPI y deroga disposiciones previas, obligando a las entidades a adoptar controles de seguridad digital acordes con estándares internacionales.

- Resolución 1978 de 2023 (MinTIC) — adopta la versión 3 del Marco de Referencia de Arquitectura Empresarial para el Estado, exigiendo que todo proyecto TIC garantice interoperabilidad y gobernanza de datos.
- Resolución 1519 de 2020 (MinTIC) — define los criterios de accesibilidad, datos abiertos y seguridad para los portales web públicos.
- Decreto 088 de 2022 — reglamenta la digitalización y automatización de trámites.

Políticas públicas nacionales

- CONPES 3995 de 2020 — Política Nacional de Confianza y Seguridad Digital, fija la meta de elevar la madurez de seguridad digital de las entidades por encima del 70 %.

Departamento Nacional de Planeación

- CONPES 3975 de 2022 — impulsa la transformación digital y la inteligencia artificial en el Estado.

Calidad y gestión institucional

- NTCGP 1000:2009 (adoptada mediante Decreto 4485 de 2009) — obliga a documentar y evaluar los procesos de prestación de servicios, incluidos los digitales.
- Decreto 1499 de 2017 — incorpora la dimensión de seguridad digital en el Modelo Integrado de Planeación y Gestión (MIPG).

Seguridad digital y delitos informáticos

- Ley 1273 de 2009 — tipifica los delitos informáticos y protege la integridad de los sistemas de información del Estado.
- CONPES 3701 de 2011 — lineamientos de política para ciberseguridad y ciberdefensa.
-

6. IDENTIFICACIÓN Y ANÁLISIS DE PARTICIPANTES

El proyecto “Fortalecimiento a la Transformación Digital Segura del municipio de Popayán” articula actores institucionales, técnicos y sociales que intervienen directa o indirectamente en la sostenibilidad del Sistema de Gestión de Seguridad de la Información (SGSI). A continuación, se describen sus roles, expectativas y aportes.

N°	ENTIDAD	POSICIÓN	EXPECTATIVA	CONTRIBUCIÓN
1	Municipio de Popayán	Cooperante	Asegurar recursos OPEX/CAPEX y demostrar eficiencia del gasto TIC ante ciudadanía y entes de control.	Asignación y administración presupuestal, articulación interdependencias, expedición de actos administrativos necesarios.
2	Oficina de TIC	Cooperante	Cumplir la meta del PDM “Servicios tecnológicos mantenidos” y elevar la madurez de seguridad digital ≥ 70 %.	Dirección técnica, operación, supervisión contractual y reporte de indicadores.

3	Comunidad del municipio de Popayán	Beneficiarios	Acceder a servicios digitales confiables y protegidos; salvaguardar sus datos personales.	Uso de los portales y aplicaciones, retroalimentación sobre la calidad del servicio, veeduría ciudadana.

7. POBLACIÓN AFECTADA

Personal de la 355.347 habitantes del municipio de Popayán. Resultados del censo nacional de población y la información que nos brinda el DANE
Todo el municipio de Popayán. Usuarios internos los cuales son:

TIPO DE POBLACIÓN	NÚMERO	FUENTE DE INFORMACIÓN	LOCALIZACIÓN GENERAL	LOCALIZACIÓN ESPECÍFICA
Personas	355.347	DANE	Sur Occidente – departamento del Cauca	Municipio de Popayán

8. POBLACIÓN OBJETIVO

Personal de 355.347 habitantes del municipio de Popayán. Resultados del censo nacional de población y la información que nos brinda el DANE, Todo el municipio de Popayán. Usuarios internos los cuales son:

TIPO DE POBLACIÓN	NÚMERO	FUENTE DE INFORMACIÓN	LOCALIZACIÓN GENERAL	LOCALIZACIÓN ESPECÍFICA
Personas	355.347	DANE	Sur Occidente – departamento del Cauca	Municipio de Popayán

7.3 CARACTERIZACIÓN DE LA POBLACIÓN OBJETIVO			
CLASIFICACIÓN	**DETALLE**	**NÚMERO**	**Políticas transversales**
Género	Masculino	171.976	Equidad de la mujer
	Femenino	183.371	
Etapa del ciclo de vida	Primera infancia 0 – 5 años		Primera infancia, infancia y adolescencia
	Infancia 6 – 11 años		
	Adolescencia 12 – 18 años		
	Juventud 14 – 26 años		
	Adultez 27- 26 años		
	Vejez 60 años y más		
Etaria	O – 14 Años	60.075	

	15 – 19 Años	23.394	
	20 – 59 Años	206.522	
	Mayores de 60 Años	56.412	
Grupos étnicos	Indígenas	12.440	Grupos étnicos comunidades indígenas
	Afrocolombianos	0	Grupos étnicos comunidades afrocolombianas
	Raizal	28	Grupos étnicos comunidades raizales
	ROM	11	Grupos étnicos comunidades pueblos ROM
	Mestizos	331.895	
	Comunidades negras	0	Grupos étnicos comunidades negras
	Palanqueros	20	Grupos étnicos comunidades palanqueras
Población vulnerable	Personas en reincorporación (acuerdos de paz)		
	Personas en reintegración exintegrantes de grupos armados organizados y otros en tránsito a la vida civil		
	Desplazados	0	
	Discapacitados	0	Discapacidad e inclusión social
	Víctimas	0	Víctimas

9. PLANTEAMIENTO DEL PROBLEMA

El FURAG 2024 muestra avances, pero también brechas críticas de madurez: Gobierno Digital alcanzó 60,8 % (frente a 49,0 % en 2023) y Seguridad Digital – POL 8 llegó a 53,0 % (frente a 21,7 %), aún por debajo del umbral recomendado de 70 %. Esta situación se traduce en un acceso limitado, inseguro e inequitativo a los servicios digitales de la Alcaldía de Popayán. En la práctica, significa trámites que se caen, demoras inesperadas, reprocesos y dudas sobre la protección de los datos personales; todo ello deteriora la confianza de la ciudadanía y dificulta el ejercicio de sus derechos en línea.

El impacto no es igual para todos. Las personas que menos pueden acudir a ventanillas habitantes de zonas rurales, adultos mayores, personas con discapacidad, cuidadores o quienes trabajan en horarios extensos dependen con mayor intensidad de los canales digitales. Cuando estos fallan o se perciben como inseguros, se crean barreras adicionales que obligan a viajes, filas y costos de oportunidad que muchas familias no pueden asumir. También se desalienta el uso de trámites en línea entre quienes tienen menor alfabetización digital, lo que profundiza desigualdades y congestiona los puntos de atención presenciales.

Estas brechas afectan directamente la calidad del servicio público: interrumpen la continuidad de los trámites, alargan los tiempos de respuesta y elevan los costos operativos de la administración. Al mismo tiempo, exponen a la población a riesgos sobre sus datos personales (hábeas data) y generan desconfianza en los canales institucionales, debilitando la participación y la transparencia.

Por ello, se requiere una intervención inmediata que cierre las brechas de madurez y garantice un ecosistema digital confiable. El proyecto se orienta a elevar los resultados de Seguridad Digital por encima del 70 % y de Gobierno Digital por encima del 75 %, y a asegurar una disponibilidad de servicios en línea igual o superior al 99,5 %. Con ello se busca proteger la información de la comunidad, mejorar la calidad del servicio y, sobre todo, asegurar que todas las personas especialmente quienes menos alternativas presenciales cuenten con trámites digitales continuos, seguros y fáciles de usar.
En síntesis, el problema público es claro: hoy el acceso digital municipal no es suficientemente seguro ni equitativo. Atenderlo no solo es una exigencia técnica o normativa; es una prioridad social para proteger derechos, reducir brechas y fortalecer la confianza de la ciudadanía en la gestión pública.

9.1. Descripción de la situación existente con respecto al problema

En el diagnóstico institucional más reciente, los resultados del FURAG 2024 confirman avances, pero también brechas de madurez que siguen afectando la experiencia ciudadana en los servicios digitales: Gobierno Digital alcanzó 60,8 % y Seguridad Digital (POL 8) 53,0 %, aún por debajo del umbral recomendado (≥ 70 %). En la práctica, esto se traduce en canales en línea que no siempre son confiables, procesos con trazabilidad incompleta y percepciones de riesgo sobre el manejo de datos personales.

1) Estado de los servicios y experiencia del usuario.
Se registran intermitencias y lentitud en picos de demanda (p. ej., periodos de pago de obligaciones, inscripción a programas o radicación masiva de solicitudes), que obligan a reintentos, reprocesos y uso de vías presenciales. Estas fallas impactan especialmente a poblaciones con menor acceso a ventanillas (zonas rurales, personas con discapacidad, adultos mayores, cuidadores y quienes trabajan en horarios extendidos), para quienes los servicios digitales son la opción principal. La desconfianza frente a la seguridad de la información desalienta el uso sostenido de trámites en línea y limita la adopción de canales electrónicos.

2) Gestión institucional y articulación de procesos.
Existen desalineaciones entre plataformas y procesos (trámites, gestión documental, recaudo, catastro, datos abiertos) que dificultan el intercambio seguro y oportuno de información. Esto se refleja en tiempos de atención mayores a los previstos, pasos manuales de validación y falta de interoperabilidad plena para cerrar casos de punta a punta. La adopción de lineamientos de Gobierno Digital y de Seguridad Digital avanza, pero no alcanza el nivel de madurez requerido para asegurar continuidad y trazabilidad homogéneas en todo el ciclo de atención.

3) Cumplimiento normativo y gestión de riesgo.
La administración ha incorporado políticas y controles, pero persisten vulnerabilidades operativas asociadas a la gestión del riesgo de información y al aseguramiento de la confidencialidad, integridad y disponibilidad de los datos. Esto expone a la entidad a contingencias (interrupciones, reprocesos, pérdida de productividad) y a posibles requerimientos de autoridad cuando se presentan incidentes de seguridad o fallas en la atención digital.

4) Efectos en equidad y calidad del servicio.
Las brechas actuales profundizan desigualdades: quienes tienen menos alternativas presenciales enfrentan mayores costos de tiempo y desplazamiento cuando los canales digitales fallan. Además, la alfabetización digital desigual dificulta que ciertos grupos naveguen trámites con cambios frecuentes o mensajes de error poco claros, lo que debilita la confianza y reduce la participación en mecanismos de gobierno abierto.

5) Consecuencias operativas y reputacionales.
Las intermitencias, la fragmentación de procesos y la baja madurez de seguridad se traducen en sobrecostos por contingencias, sobrecarga de puntos presenciales y percepción de baja calidad en la atención digital. La suma de estos factores erosiona la confianza ciudadana y limita el cumplimiento de metas institucionales de transformación digital.

9.2. ÁRBOL DE PROBLEMA.

Efectos indirectos	**Aumento del riesgo de incidentes de seguridad informática.**	**Incremento de trámites presenciales, congestión en los puntos de atención y mayores tiempos de respuesta a la ciudadanía.**	**Pérdida de eficiencia administrativa y afectación a la continuidad de los servicios digitales esenciales.**	**Desconfianza ciudadana en los servicios digitales municipales y disminución del uso de los canales electrónicos.**
Efectos directos	**Servicios digitales vulnerables, con interrupciones recurrentes y bajo nivel de confiabilidad.**		**Limitada disponibilidad y calidad de los servicios digitales ofrecidos a la ciudadanía y a las dependencias municipales.**	
Problema central	**Acceso limitado e inseguro a los servicios digitales de la Alcaldía de Popayán.**			
Causas directas	Política de Seguridad Digital no implementada ni operativa de manera integral.			
Causas indirectas	**Capacidad insuficiente en talento humano en seguridad digital y gestión de la información.**		**Infraestructura tecnológica y herramientas de seguridad desactualizadas o incompletas.**	

9.3. ÁRBOL DE FINES Y MEDIOS (OBJETIVOS)

Fines indirectos	**Reducción del riesgo de incidentes de seguridad informática.**	**Mayor uso de trámites digitales y menor congestión presencia**	**Impulso a la innovación y competitividad tecnológica de Popayán**	**Confianza ciudadana fortalecida en los servicios municipales**
Fines directos	**Servicios digitales eficientes, seguros y confiables**		**Soluciones TIC propias, seguras y de alto impacto**	
Objetivo General	**Garantizar un acceso seguro, eficiente e innovador a los servicios digitales de la Alcaldía de Popayán**			
Medios directos	**Implementar y operar integralmente la Política de Seguridad Digital**			
Medios indirectos	**Fortalecer la capacidad institucional en seguridad digital**		**Adquirir infraestructuras tecnológicas**	

9.4. INDICADORES PARA MEDIR EL OBJETIVO GENERAL.

Tabla 1. Indicadores para medir el objetivo general

Indicador objetivo General	Descripción		Fuente de verificación
Disponibilidad de los servicios TIC institucionales	Medido a través de	Numero	Reportes mensuales NOC/SOC, bitácoras SIEM, tableros de monitoreo, PIIP
	Meta	3	

10. ALTERNATIVAS DE SOLUCIÓN

La Administración Municipal de Popayán, a través de la Secretaría General y la Oficina TIC, adoptará una alternativa integral orientada a revertir el problema identificado —acceso limitado, inseguro e innovación restringida en los servicios digitales y cumplir las metas del Plan de Desarrollo alianza con Popayán 2024-2027. Esta alternativa articula seguridad digital, infraestructura, e innovación, en consonancia con la Política de Gobierno Digital, la Ley 1581/2012 (protección de datos), la Resolución 1519/2020 (estándares web), la Resolución 1978/2023 (Arquitectura Empresarial v3) y el CONPES 3995/2020 (confianza y seguridad digital).

Enfoque propuesto. Se implementará de manera coordinada la Política de Seguridad Digital como sistema de gestión, se modernizará la infraestructura crítica y se impulsará la innovación local mediante un servicio de apoyo financiero a proyectos de I+D+i en TIC, reduciendo la dependencia de terceros y elevando la calidad y disponibilidad de los servicios digitales para la ciudadanía.

Líneas de intervención:

Seguridad digital y SGSI operativo.

Contratar talento especializado para formular, adoptar y operar la Política de Seguridad Digital; poner en marcha un SOC integrado; establecer protocolos de gestión de incidentes, respaldos y continuidad; renovar licencias (EDR/XDR, cifrado, SIEM) y ejecutar auditorías y pruebas.

Infraestructura resiliente y de alto desempeño.

Adquirir, configurar e integrar servidores de alta disponibilidad, firewalls de nueva generación, protección de endpoints, copias de seguridad automatizadas y enlaces redundantes; monitorear desempeño y asegurar una disponibilidad ≥ 99,5 % de los servicios TIC.

G**obierno Digital articulado e interoperable.**

Implementar la Arquitectura Empresarial v3 para interoperar plataformas (trámites, gestión documental, recaudo, datos abiertos), optimizar el flujo de información y elevar el uso de trámites digitales, con analítica para la toma de decisiones.

Innovación e I+D+i en TIC

Operar el Servicio de apoyo financiero para financiar proyectos de IA, ciberseguridad, big data e IoT; crear un Centro de Experiencia en IA y Ciberseguridad para pilotos y transferencia tecnológica; articular cofinanciación y mentoría con MinTIC, academia y sector productivo.

Gestión del cambio y visibilización.

Estandarizar guías de uso seguro para dependencias y ciudadanía; publicar tableros de avance y visibilizar las iniciativas de la Oficina TIC para fortalecer la confianza y la cultura digital.

Resultados esperados y valor público.

Con esta alternativa, la Alcaldía mitigará riesgos y mejorará la experiencia ciudadana, logrando: servicios digitales eficientes, seguros y confiables, soluciones TIC propias de alto impacto, menores costos por incidentes, mayor uso de trámites digitales y confianza ciudadana fortalecida. En términos

de desempeño, se proyecta FURAG Seguridad Digital ≥ 70 %, FURAG Gobierno Digital ≥ 75 %, disponibilidad ≥ 99,5 % y al menos 5 proyectos de I+D+i financiados en la vigencia.
Riesgos y mitigación.
Riesgos: ciberataques de alta severidad, escasez/rotación de talento y retrasos de proveedores. Mitigación: SOC 24/7 con ANS, contratación por hitos y retención de conocimiento, cronograma faseado con pruebas de continuidad y monitoreo mensual de indicadores en PIIP/FURAG.
Sostenibilidad.
La alternativa asegura OPEX y CAPEX planificados, gobernanza mediante Comité de Seguridad Digital, mantenimiento programado de plataformas y un ciclo anual de innovación que reinvierte aprendizajes de los proyectos financiados. Así, Popayán consolida un ecosistema digital resiliente, eficiente e innovador, coherente con la normativa vigente y las expectativas de la ciudadanía.

ALTERNATIVAS	**SELECCIONADA**	
	SI	**NO**
“Fortalecimiento de la Seguridad Digital Institucional de la Alcaldía de Popayán”	**X**	
Estrategia Escalonada de Modernización Comunicativa”		**X**

10.1. ESTUDIO DE NECESIDADES

El propósito de este apartado es medir la brecha entre la demanda ciudadana de información pública y la oferta efectiva de servicios comunicativos que actualmente presta la Administración Municipal, sin considerar todavía la ejecución del proyecto. Para ello se identifican los bienes y servicios críticos que el proyecto aportará, se describe su evolución reciente (2022-2025) y se cuantifica el déficit resultante.

BIEN O SERVICIO	MEDIDO A TRAVÉS DE	DESCRIPCIÓN	AÑO INICIO HISTORIA	AÑO FIN HISTORIA	ÚLTIMO AÑO
Infraestructura tecnológica de seguridad y continuidad (servidores HA, firewalls NG, enlaces redundantes, backups)	Número	Adquisición, configuración e integración de servidores de alta disponibilidad, firewalls de nueva generación, enlaces de datos redundantes, almacenamiento y sistemas de respaldo automatizado, con telemetría para gestión proactiva.	2018	2025	2025
		Servicios de asistencia técnica especializada para seguridad digital			

AÑO	OFERTA	DEMANDA	DÉFICIT
2018	100	100	0
2019	112	112	0
2020	129	129	0

2021	131	152	-21
2022	152	182	-30
2023	222	222	0
2024	274	274	0
2025	274	274	0

BIEN O SERVICIO	MEDIDO A TRAVÉS DE	DESCRIPCIÓN	AÑO INICIO HISTORIA	AÑO FIN HISTORIA	ÚLTIMO AÑO
servicios profesionales y no profesionales en seguridad digital y gestión tic	Número	Vinculación de profesionales y no profesionales en (ingenierías de sistemas/informática/electrónica y afines) para operación del sistema de seguridad digital, administración de servidores y red, gestión de incidentes, gobierno de datos, continuidad y mejora de servicios digitales.	2022	2025	2025

AÑO	OFERTA	DEMANDA	DÉFICIT
2022	6	8	-2
2023	7	10	-3
2024	8	12	-4
2025	9	14	-5
2026	10	22	-12

11. METODOLOGÍA

11.1. OBJETIVO ESPECÍFICO / MEDIO DIRECTO 1: Desarrollar e implementar la política de seguridad digital	
PRODUCTO	**MGA: Servicios tecnológicos**
	PDM: Desarrollar la Política de seguridad digital

ACTIVIDAD 1 Fortalecer la capacidad institucional en seguridad digital
ENTREGABLE: (Según EDT) N/A

INSUMO.	CANTIDAD.	METODOLOGÍA.	PLAZO EJECUCIÓN.
Profesional en Ingeniería de Sistemas o Física o afines, con Experiencia profesional o laboral mínima de 1 año	**2**	Desarrollará una puesta en marcha estructurada del esquema de seguridad digital con énfasis en estabilización y documentación, dejando capacidades instaladas en la Entidad. Para ello, iniciará con el levantamiento e inventario de activos y el diagnóstico de brechas frente al MSPI/ISO 27001, a partir del cual definirá un plan de implementación con responsables, hitos y criterios de aceptación. Ejecutará el Harding inicial de servidores y servicios críticos, la parametrización base de las herramientas de seguridad (protección de endpoints, copias de seguridad y monitoreo esencial), y realizará pruebas de restauración y continuidad para validar la confiabilidad de la configuración. En paralelo, diseñará y dejará formalizados los procedimientos de gestión de incidentes, vulnerabilidades, accesos, copias y cambios; las matrices de roles y responsabilidades (RACI); y los formatos	Hasta el 31 de diciembre del 2027

		y listas de verificación necesarios para su operación rutinaria, junto con una línea base de indicadores alineada a FURAG/MSPI. Todo el proceso quedará soportado en un expediente técnico con manuales, guías y actas de prueba que faciliten auditoría y trazabilidad. Finalmente, efectuará la transferencia de conocimiento al equipo TIC mediante sesiones teórico-prácticas y un plan de transición que precise pendientes de mejora y condiciones de cierre.	
Técnico en redes de datos	**1**	El Técnico apoyará la puesta a punto, estabilización y documentación inicial de la infraestructura de red que soporta los servicios digitales de la Alcaldía de Popayán, en el marco de la Política de Seguridad Digital. Para ello, realizará diagnóstico e inventario de puntos de red, switches, routers, racks, patch panel, UPS, cableado estructurado y enlaces de conectividad; apoyará actividades de mantenimiento preventivo y correctivo, organización de racks, etiquetado, canalización y pruebas de continuidad; y verificará la conectividad de estaciones, plataformas y sistemas asociados a trámites digitales. Cada intervención deberá registrarse en bitácoras o tickets, con evidencia de la actividad realizada y resultado obtenido. Esta metodología busca dejar la red organizada, estable, segura y documentada, como condición para mejorar la continuidad de los servicios tecnológicos, sin constituir operación recurrente permanente.	Hasta el 31 de diciembre del 2027
Técnico en redes eléctricas	**1**	El Técnico apoyará la puesta a punto, estabilización y documentación inicial de la infraestructura eléctrica que soporta los servicios tecnológicos de la Alcaldía de Popayán, en el marco de la Política de Seguridad Digital. Para ello, realizará diagnóstico básico de puntos eléctricos, tomas reguladas, UPS, tableros, canalizaciones, cableado eléctrico y condiciones de carga de los equipos tecnológicos; apoyará actividades de mantenimiento preventivo y correctivo, organización de conexiones, verificación de continuidad, revisión de protecciones eléctricas y adecuaciones menores necesarias para garantizar el funcionamiento seguro de servidores,	Hasta el 31 de diciembre del 2027

		estaciones de trabajo, equipos de red y sistemas de respaldo. Cada intervención deberá registrarse en bitácoras o tickets, con evidencia de la actividad realizada y resultado obtenido. Esta metodología busca dejar la infraestructura eléctrica ordenada, segura, estable y documentada, como condición para mejorar la continuidad de los servicios tecnológicos y reducir riesgos de fallas por energía, sin constituir operación recurrente permanente.	
Bachiller con conocimiento en mesas de servicio con (1) un año mínimo de experiencia laboral.	**1**	El perfil de Mesa de Ayuda opera bajo un esquema de atención continúa orientado a la estabilización y trazabilidad de los servicios tecnológicos. Sus funciones se ejecutan conforme a ANS/SLA y buenas prácticas ITSM (GLPI/ITIL) e incluyen: (i) recepción, registro y categorización de tickets; (ii) priorización por criticidad e asignación a N2/N3; (iii) resolución de primer nivel (credenciales, ofimática, impresión, conectividad básica, restablecimientos y verificación de accesos); (iv) seguimiento hasta el cierre con validación del usuario; (v) actualización de la base de conocimiento y del inventario/CMDB; y (vi) reporte periódico de indicadores (volumen, tiempos de respuesta/solución, reincidencias, satisfacción). Deberá garantizar disponibilidad permanente (24/7), garantizar disponibilidad permanente para soporte y atender oportunamente los requerimientos e incidentes que puedan afectar la continuidad de los servicios tecnológicos. En caso de presentarse incidentes críticos o de alta prioridad —P1/P2—, deberá realizar el escalamiento inmediato al soporte especializado correspondiente, asegurando una respuesta rápida y coordinada.	Hasta el 31 de diciembre del 2027
Profesional en ingeniería de sistemas o informática, con Experiencia profesional o	**1**	Elaborará fichas técnicas tecnológicas para la actualización de equipos conectados a la red de datos. Su metodología comprende: levantamiento e inventario (CMDB) y diagnóstico de estado/criticidad; definición de requisitos funcionales y no funcionales (desempeño, seguridad, energía, soporte); especificación técnica por categoría (PC, switches, AP, impresoras, UPS, etc.) con compatibilidad verificada (SO/drivers, PoE,	Hasta el 31 de diciembre del 2027

laboral mínima de 1 año		VLAN, Wi-Fi, puertos, cifrado); alineación a estándares TIA/EIA-568, IEEE, Energy Star y lineamientos de seguridad digital (ISO 27001/MSPI); criterios de homologación (garantía, ANS/soporte, repuestos, ciclo de vida/TCO); prueba piloto de interoperabilidad y validación con la Oficina TIC; y documentación en catálogo institucional y mesa de ayuda para su trazabilidad. Con ello se garantiza que las adquisiciones sean compatibles, seguras y sostenibles, soportando la continuidad de los servicios ofrecidos a la comunidad.	
Profesional en Ingeniería de Sistemas o Electrónica o afines, con Experiencia profesional o laboral mínima de 1 año	**1**	El Profesional realizará la administración integral de servidores de acceso, procesamiento, almacenamiento y comunicaciones de la Entidad. Su metodología comprende: monitoreo de salud y capacidad; gestión de sistemas operativos y virtualización (instalación, hardening y parches); administración de servicios (directorios, aplicaciones, bases de datos y archivos); gestión de almacenamiento y copias de seguridad con pruebas periódicas de restauración; alta disponibilidad/replicación cuando aplique; gestión de cambios con ventanas controladas y plan de reversa; coordinación con SOC/SIEM para respuesta a incidentes; y documentación en mesa de ayuda/CMDB (procedimientos, configuraciones y actas). Reportará indicadores de disponibilidad, tiempos de atención y respaldo exitoso, garantizando el funcionamiento continuo y seguro de los sistemas que soportan el registro, consulta y trámite de funcionarios y ciudadanía.	Hasta el 31 de diciembre del 2027
Profesional en Ingeniería de Sistemas o Electrónica o afines, con Experiencia profesional o laboral mínima de 1	**1**	El Profesional actualizará e implementará operativamente la Política de Seguridad de la Información y protección de datos conforme a Ley 1581, DUR 1078/2015 y MSPI/ISO 27001. Su metodología incluye: diagnóstico de brechas y riesgos sobre activos/ tratamientos de datos; actualización de políticas y procedimientos (control de accesos, clasificación y cifrado de la información, copias de seguridad, retención y disposición); ajuste de controles técnicos en infraestructura (MFA, hardening, cifrado en tránsito y reposo, registros y trazabilidad); verificación de cumplimiento mediante	Hasta el 31 de diciembre del 2027

año		listas de chequeo y evidencias para FURAG/Comité de Seguridad; coordinación con el SOC/SIEM para respuesta a incidentes; y documentación en mesa de ayuda/CMDB. Con ello se garantiza que los servicios digitales a la comunidad cumplan estándares legales y técnicos de protección de datos.	
Profesional en Ingeniería de Sistemas o Electrónica o afines, con Experiencia profesional o laboral mínima de 1 año	**2**	El Profesional ejecutará la migración de IPv4 a IPv6 bajo un enfoque por fases: levantamiento e inventario de activos y mapa de dependencias; diseño del plan de direccionamiento IPv6 y estrategia dual-stack (priorizando servicios críticos); configuración de routers/switches/firewalls (RA/SLAAC, DHCPv6, DNS AAAA, políticas/ACL, RA-Guard, IPS/IDS); mecanismos de compatibilidad (NAT64/DNS64, proxies) para sistemas legados; pruebas piloto y UAT, seguida de despliegue con ventanas de cambio y plan de reversa; monitoreo postcorte de desempeño y seguridad; actualización documental/CMDB y transferencia de conocimiento a NOC/mesa de ayuda. Con ello se modernizan los sistemas, se cumplen lineamientos de Gobierno Digital y se habilita la integración con plataformas nacionales de información sin afectar la continuidad del servicio.	Hasta el 31 de diciembre del 2027
Profesional en ingeniería de sistemas o electrónica o afines con especialización con Experiencia profesional o laboral mínima de 1 año	**1**	El Profesional aplicará una metodología orientada a la gestión técnica de proyectos TIC: planificar y estructurar iniciativas (caso de negocio, alcance, cronograma, costos y riesgos); definir especificaciones y criterios de interoperabilidad/seguridad; hacer seguimiento a hitos, calidad y ANS; gestionar cambios y lecciones aprendidas; documentar avances (actas, informes, matrices de riesgos/beneficios) y reportar indicadores a PIIP/FURAG. Participará en los Comités de Proceso de Gestión TIC, aportando insumos para la planificación y priorización, y promoverá la innovación y actualización tecnológica (transferencia de herramientas de gestión y uso eficiente de las TIC) para la modernización de los servicios ofrecidos a la comunidad.	Hasta el 31 de diciembre del 2027

Tecnólogo en gestión empresarial, o afines o, Homologación Ocho (8) semestres aprobados en programas afines con Experiencia laboral mínima de 1 año	**1**	El Tecnólogo realizará el seguimiento y control del archivo físico y digital de la Unidad TIC mediante: organización y depuración de expedientes según Tablas de Retención Documental (TRD); digitalización, indexación y control de versiones en el Sistema de Gestión Documental (SGD); inventario, foliación y trazabilidad de préstamos/transferencias; respaldo y verificación de integridad de los repositorios digitales; y custodia conforme a Ley 594 de 2000 y Ley 1581 de 2012. Todas las actuaciones se documentan en bitácoras/tiques, con reportes periódicos de indicadores (n.º de expedientes organizados y transferidos, tiempos de respuesta y disponibilidad del archivo), asegurando oportunidad y evidencia para la validación del funcionamiento de los servicios tecnológicos de la Entidad.	Hasta el 31 de diciembre del 2027
Profesional en Administración de Empresas o afines, con experiencia Laboral mínima de un (1) año.	**1**	El Profesional realizará la estructuración financiera y la planificación estratégica de inversión de los contratos y proyectos de la Unidad TIC. Su metodología comprende: levantamiento de requerimientos con la Oficina TIC; presupuestación detallada CAPEX/OPEX (análisis costo–beneficio y TCO), definición de fuentes de financiación y flujo de caja; programación de hitos y cronograma de pagos; matriz de riesgos financieros y plan anual de adquisiciones alineado con PDM, POAI y PAC. Brindará soporte a la contratación (estudios previos, anexos y criterios de evaluación económica, cargue en SECOP), verificación de CDP/RP, y seguimiento a la ejecución (desembolsos, variaciones, alertas). Todas las actuaciones se documentan y reportan con indicadores de avance y ejecución financiera en MGA/PIIP, asegurando trazabilidad y el impacto oportuno sobre los servicios tecnológicos de la Entidad.	Hasta el 31 de diciembre del 2027
Profesional en derecho o afines, con experiencia Laboral mínima de un (1) año.	**1**	Se apoya la integración y coordinación de las actividades contempladas en el desarrollo del proyecto de inteligencia artificial liderado por la Unidad TIC, incluyendo el seguimiento a cronogramas, la articulación con equipos técnicos y administrativos, y la consolidación de resultados e informes. Así mismo, se realiza acompañamiento en la planeación y ejecución de las jornadas de capacitación relacionadas, asegurando su organización,	Hasta el 31 de diciembre del 2027

		registro, evaluación y coherencia con los objetivos del proyecto. Esta labor contribuye a una implementación estructurada y efectiva de las acciones del proyecto, fortaleciendo el impacto institucional y el aprovechamiento de las nuevas tecnologías.	
Talleres de inteligencia artificial en seguridad digital	**5**	Se realiza la contratación de talleres especializados en inteligencia artificial, en seguridad digital orientados al fortalecimiento de capacidades institucionales y al desarrollo de competencias técnicas en servidores públicos y personal vinculado a la estrategia de transformación digital. Esta adquisición incluye el diseño, desarrollo y ejecución de sesiones teórico-prácticas, con contenidos enfocados en fundamentos de IA, herramientas y plataformas aplicadas, casos de uso en el sector público y metodologías para la implementación de soluciones basadas en datos. Los talleres deberán ser impartidos por profesionales con experiencia demostrada, incluir material pedagógico, evaluaciones de aprendizaje, y un componente práctico que permita 5aplicar los conocimientos adquiridos a contextos reales de la Entidad. Así mismo, deberá entregarse un informe consolidado con los resultados obtenidos, niveles de participación, evidencias de desarrollo y recomendaciones para la continuidad del proceso formativo.	Hasta el 31 de diciembre del 2027
Programa de difusión de Centro PotencIA	**1**	Se realiza la contratación para la adquisición de productos comunicacionales orientados a la difusión del Centro PotencIA, que incluyan la elaboración de piezas gráficas, artículos informativos y contenidos digitales destinados a visibilizar ante la comunidad los servicios, beneficios y espacios disponibles en este centro. Esta adquisición contempla el diseño creativo, la producción de materiales en formatos físicos y virtuales, y la definición de una estrategia de divulgación que permita su circulación a través de medios institucionales y comunitarios. Así mismo, se exige la entrega de reportes que evidencien el desarrollo, cobertura y resultados de la estrategia implementada, asegurando alineación con los objetivos de posicionamiento del Centro PotencIA como un referente de innovación tecnológica en el municipio.	Hasta el 31 de diciembre del 2027

ACTIVIDAD 2 Adquirir infraestructura tecnológica en seguridad
ENTREGABLE: (Según EDT) N/A

INSUMO	CANTIDAD	METODOLOGÍA	PLAZO EJECUCIÓN
Licenciamientos perimetrales	**1**	Se contrata el paquete de licencias iniciales asociado a los equipos y plataformas de seguridad perimetral de la Entidad con el propósito de habilitar, poner en operación y estabilizar la infraestructura de seguridad digital (fase de arranque). Esta adquisición cubre, por única vez en la vigencia del proyecto, las licencias necesarias para activar funcionalidades de firewall de nueva generación, prevención de intrusos (IPS), control de acceso, filtrado de contenido y monitoreo de tráfico, así como su gestión centralizada para el alistamiento del ecosistema de seguridad. El alcance incluye: (i) activación y configuración inicial conforme a los requerimientos técnicos definidos por la Unidad TIC y al MSPI/Arquitectura Empresarial; (ii) pruebas de funcionamiento y endurecimiento (políticas base, reglas mínimas, perfiles de inspección); (iii) documentación técnica y transferencia de conocimiento al equipo institucional; y (iv) acta de aceptación de la fase de estabilización. Este licenciamiento no financia operación recurrente ni renovaciones periódicas posteriores; su finalidad es dejar operativa y estable la capa perimetral como condición habilitante del esquema de seguridad	Hasta el 31 de diciembre del 2027
Compra espacio en la nube (Correos y Storage)		Se realiza la adquisición para la migración, puesta en operación y estabilización inicial de servicios en la nube para correo institucional y almacenamiento (storage), como acción de modernización tecnológica orientada a la seguridad, disponibilidad y continuidad del servicio. El alcance contempla: diseño y alistamiento (verificación de dominios, dimensionamiento de capacidad y definición de políticas de seguridad y retención), migración técnica de buzones y repositorios priorizados con verificación de integridad, configuración endurecida (autenticación	Hasta el 31 de diciembre del 2027

		multifactorial, cifrado en tránsito y en reposo, anti phishing/antimalware, DLP básico, auditoría y trazabilidad), definición de RPO/RTO y habilitación de respaldo y recuperación; gestión centralizada de accesos y roles; e interoperabilidad con directorio institucional/SSO cuando aplique, en alineación con MSPI y Arquitectura Empresarial. Se ejecutan pruebas de servicio, validación del SLA del proveedor y se suscribe acta de estabilización. Se entrega documentación técnica (matrices de configuración, manuales, procedimientos de respaldo/contingencia) y transferencia de conocimiento al equipo TIC. Esta intervención deja la plataforma cloud operativa y estabilizada como capacidad habilitante de seguridad y continuidad; las operaciones recurrentes posteriores (administración diaria y renovaciones) no hacen parte del alcance de la fase de inversión.	
Sistema de Interoperabilidad		Se realiza la contratación para la compra de un sistema de interoperabilidad entre servidores, con el objetivo de integrar y facilitar el intercambio seguro, eficiente y automatizado de información entre las diferentes plataformas tecnológicas de la Entidad. Esta adquisición contempla herramientas y componentes que permitan la comunicación entre servidores heterogéneos, asegurando la compatibilidad entre sistemas, el uso de protocolos estandarizados y la trazabilidad de los datos compartidos. El sistema deberá permitir la orquestación de servicios, la transformación de datos, el control de acceso y la gestión centralizada de flujos de información, cumpliendo con los lineamientos técnicos establecidos por la Unidad TIC y las normas vigentes sobre protección de datos e interoperabilidad. Así mismo, deberá incluir soporte técnico, capacitación, documentación detallada y mecanismos de seguimiento que garanticen su integración efectiva en la infraestructura existente.	Hasta el 31 de diciembre del 2027
Plan de Gestión de Riesgos de Ciberseguridad		se realiza la contratación para la elaboración e implementación de un Plan de Gestión de Riesgos de Ciberseguridad que permita identificar, analizar, evaluar y tratar los riesgos asociados a los activos de información y la	Hasta el 31 de diciembre del 2027

		infraestructura tecnológica de la Entidad. Esta adquisición incluye el desarrollo de una metodología adaptada al contexto institucional, el levantamiento de información sobre amenazas y vulnerabilidades, la clasificación y priorización de riesgos, así como la definición de controles y estrategias de mitigación alineadas con estándares internacionales y la normatividad vigente en materia de seguridad digital. El plan deberá contemplar escenarios de impacto, niveles de exposición, mecanismos de monitoreo continuo, indicadores de riesgo y un esquema de mejora continua. Adicionalmente, se deberá entregar documentación técnica, cronograma de ejecución, herramientas de seguimiento y sesiones de socialización con los equipos responsables de su aplicación y mantenimiento, asegurando su apropiación y sostenibilidad dentro de la gestión institucional.	
Licenciamiento de estaciones de trabajo		Se realiza la contratación para la normalización y estandarización del parque tecnológico de la Entidad mediante la puesta a punto inicial de licencias de software en estaciones de trabajo. El objetivo es cerrar brechas de seguridad y cumplimiento normativo (legalidad del software, gestión de parches y protección endpoints) y dejar un ecosistema digital seguro y homogéneo que soporte los procesos misionales. El alcance incluye: provisión e instalación de licencias originales y vigentes para sistema operativo, suite ofimática, antimalware/EDR y herramientas corporativas definidas por la Unidad TIC; inventario y trazabilidad en CMDB; gestión centralizada de activación y políticas; endurecimiento básico (cifrado de disco, control de dispositivos, firewall local, actualizaciones automáticas); verificación de compatibilidad con la infraestructura existente y lineamientos de Arquitectura Empresarial/MSPI; y pruebas de funcionamiento por perfiles de usuario. Se entrega documentación técnica (listado licencias por equipo, claves/contratos, políticas aplicadas y procedimiento de reinstalación) y transferencia de conocimiento al equipo TIC. Esta inversión corresponde a la estabilización inicial y a la estandarización del parque de estaciones, necesaria para asegurar confiabilidad,	Hasta el 31 de diciembre del 2027

		disponibilidad y cumplimiento. Las renovaciones periódicas u operación recurrente posteriores no hacen parte del alcance de esta fase de inversión.	
Equipos de RED		Se realizará la puesta a punto inicial (no operación recurrente) de la infraestructura de red institucional, orientada a modernizar, ampliar y asegurar la conectividad como habilitador directo de la seguridad digital y la continuidad del servicio. El alcance comprende: actualización y ampliación de capacidad de switching y distribución (puertos G/10G, PoE/PoE+ para puntos de acceso y dispositivos de seguridad), incorporación de enlaces y rutas de respaldo para alta disponibilidad, y segmentación lógica por VLAN con listas de control de acceso y políticas de NAC/802.1X en acceso cableado e inalámbrico. Se optimizará la capa Wi-Fi (migración a Wi-Fi 6/6E cuando aplique, perfiles por rol y control de radiofrecuencia), y se estandarizará el cableado y pasivos (patch paneles, organizadores, etiquetado, canalización y puesta a tierra) para garantizar confiabilidad y trazabilidad. La red quedará observabile y monitoreada mediante telemetría (SNMP/syslog), tableros de desempeño y registro en CMDB con mapas de topología. La metodología incluye configuración inicial, pruebas de redundancia y conmutación, verificación de hardening básico (control de puertos, QoS para servicios críticos, restricciones de administración), documentación técnica completa (planos lógicos/físicos, matrices de VLAN/ACL, respaldos de configuración) y transferencia de conocimiento al equipo TIC para su operación. Con ello se entrega una red robusta, segmentada y monitoreable, alineada con MSPI y Arquitectura Empresarial, que mejora disponibilidad y continuidad de los servicios digitales, reduce la superficie de ataque e integra de forma efectiva los controles perimetrales y de acceso.	Hasta el 31 de diciembre del 2027

1. LOCALIZACIÓN DE LA ALTERNATIVA

El proyecto se llevará a cabo en el Municipio de Popayán

2. CADENA DE VALOR

OBJETIVO GENERAL	**Garantizar un acceso seguro, eficiente e innovador a los servicios digitales de la Alcaldía de Popayán**

OBJETIVOS ESPECÍFICOS / MEDIOS DIRECTOS	NOMBRES Y CÓDIGO PRODUCTOS PDM Y MGA	Indicador de producto PDM	Unidad de medida	Meta Vigencia	Población beneficiaria por producto	NOMBRE ENTREGABLE NIVEL 1	ACTIVIDADES	VALOR POR ACTIVIDAD
Desarrollar e implementar la Política de Seguridad Digital	Servicios tecnológicos MGA PDM: Desarrollar la Política de seguridad digital	Servicios tecnológicos implementados	Numero	3	355.347	N/A	Fortalecer la capacidad institucional en seguridad digital	$ 1.374.500.000
						N/A	Adquirir herramientas tecnológicas	$ 2.397.200.000
TOTAL								$ 3.771.700.000

3. FOCALIZACIÓN.

Nombre Producto MGA/PDM	Actividad	Política transversal	Categoría	Subcategoría	Población beneficiaria	Valor

4. ANÁLISIS DE RIESGOS

Nivel de clasificación	Descripción	Tipo de riesgo	Descripción del riesgo	Probabilidad e impacto	Efectos	Medidas de mitigación
Garantizar un acceso seguro, eficiente e innovador a los servicios digitales de la Alcaldía de Popayán.	Ciberataque de alta severidad durante la transición	Operacional	incidentes (ransomware/DoS) mientras se estabiliza el nuevo esquema de seguridad	Probabilidad: 4. Probable 5. Casi seguro Impacto: 4. Probable	Indisponibilidad de servicios, pérdida/filtración de datos, afectación a la confianza ciudadana	Puesta a punto escalonada con ventanas controladas; SOC/NOC con monitoreo continuo; endurecimiento (hardening), segmentación y copias de seguridad verificadas; simulacros y plan de respuesta a incidentes (PRI) actualizado
Servicios tecnológicos	Dificultad para conformar el equipo mínimo de trabajo	Administrativo	Demora/renuncia de perfiles clave	Probabilidad: 4. Probable 5. Casi seguro Impacto: 4. Probable	Retraso en estabilización y documentación	Plan de atracción y retención; perfiles alternos homologables; transferencia de conocimiento obligatoria; solapes de entrega
Fortalecer la capacidad institucional en seguridad digital	Análisis de mercado; 3 cotizaciones; referencias equivalentes	Administrativo	Dependencias de personas y de procesos	Probabilidad: 4. Probable 5. Casi seguro	Cuellos de botella	Procedimientos normalizados matriz RACI capacitación cruzada

(perfiles temporales para puesta a punto	preaprobadas; reservas para imprevistos (≤10%).			Impacto: 4. Probable:		
Adquirir herramientas tecnológicas	Sobrecostos	Costos	Sobrecostos por cambios de referencia o importaciones urgentes	Probabilidad: 4. Probable 5. Casi seguro Impacto: 4. Probable	Presión presupuestal y reducción de alcance	Análisis de mercado cotizaciones referencias equivalentes

5. PRESUPUESTO

PRESUPUESTO DETALLADO DEL PROYECTO

PROYECTO RADICADO No.	**26-9-19-001-02687**
BPIN No.	
NOMBRE DEL PROYECTO:	**Fortalecimiento de la Seguridad Digital Institucional de la Alcaldía de Popayán"**
NUMERO DE UNIDADES DE PRODUCTO A GENERAR:	**1**

OBJETIVO GENERAL	OBJETIVOS ESPECIFICOS	PRODUCTOS	UNIDAD DE MEDIDA	META	ACTIVIDAD	ENTREGABLE	INSUMOS	CANTIDAD	UNIDAD DE MEDIDA	VR. UNITARIO	COSTO TOTAL				
											2026		2027		COSTO TOTAL
											PROPIOS	SGP	PROPIOS	SGP	
Garantizar un acceso seguro, eficiente e	Desarrollar e implementar la Política de	Servicios tecnológicos implementados	Número	3	Fortalecer la capacidad institucional en	N/A	Profesional en Ingeniería de Sistemas o Física o afines, con Experiencia profesional o	**2**	**Numero**	**$ 4.000.000**	**$ 40.000.000**		**$ 96.000.000**	**$ -**	**$ 144.000.000**

innovador a los servicios digitales de la Alcaldía de Popayán	Seguridad Digital				seguridad digital		laboral mínima de 1 año							
							Técnico en redes de datos	**1**	**Numero**	**$ 2.700.000**	**$ 13.500.000**		**$ 32.400.000**		
							Técnico en redes eléctricas	**1**	**Numero**	**$ 2.700.000**	**13.500.000**		**$ 32.400.000**		**$ 48.600.000**
							Bachiller con conocimiento en mesas de servicio con (1) un año mínimo de experiencia laboral	**1**	**Numero**	**$ 3.100.000**	**$ 15.500.000**		**$ 37.200.000**		**$ 55.800.000**
							Profesional en ingeniería de sistemas o informática, con Experiencia profesional o laboral mínima de 1 año	**1**	**Numero**	**$ 4.000.000**	**$ 20.000.000**		**$ 48.000.000**		**$ 72.000.000**
							Profesional en Ingeniería Electrónica o afines, con Experiencia profesional o laboral mínima de 1 año	**1**	**Numero**	**$ 4.000.000**	**$ 20.000.000**		**$ 48.000.000**		**$ 72.000.000**

						Profesional en Ingeniería de Sistemas o Electrónica o afines, con Experiencia profesional o laboral mínima de 1 año	3	Numero	$ 4.000.000	$ 60.000.000		$ 144.000.000		$ 216.000.000
						Profesional en ingeniería de sistemas o electrónica o afines con especialización con Experiencia profesional o laboral mínima de 1 año	1	Numero	$ 4.500.000	$ 22.500.000		$ 54.000.000		$ 81.000.000
						Tecnólogo en gestión empresarial, o afines o, Homologación Ocho (8) semestres aprobados en programas afines con Experiencia laboral mínima de 1 año	1	Numero	$ 3.100.000	$ 15.500.000		$ 37.200.000		$ 55.800.000
						Profesional en Administración de Empresas o afines, con experiencia Laboral mínima de un (1) año.	1	Numero	$ 4.000.000	$ 20.000.000		$ 48.000.000		$ 72.000.000

					Profesional en derecho o afines, con experiencia Laboral mínima de un (1) año.	1	Numero	$ 4.000.000	$ 20.000.000		$ 24.000.000		$ 48.000.000
					Talleres de inteligencia artificial en seguridad digital	2	Numero	$ 50.000.000	$ 100.000.000		$ 50.000.000		$ 150.000.000
					Programa de difusión de Centro PotencIA	5	Numero	$ 10.000.000	$ 50.000.000		$ 50.000.000		$ 100.000.000
			Subtotal 1						$ 410.500.000	0	$ 697.200.000		$ 1.107.700.000
			Adquirir infraestructura tecnológica en seguridad digital		Licenciamientos perimetrales	1	Numero	$ 300.000.000,00	$ 300.000.000		$ 350.000.000		$ 650.000.000,00
					Compra espacio en la nube (Correos y Storage)	1	Numero	$ 280.000.000,00	$ -		$ 300.000.000		$ 300.000.000,00
					Sistema de Interoperabilidad	1	Numero	$ 200.000.000,00	$ -		$ 200.000.000		$ 200.000.000,00

						Plan de Gestión de Riesgos de Ciberseguridad	1	Numero	$ 300.000.000,00	$ -		$ 300.000.000	$ 300.000.000,00
						Licenciamiento de estaciones de trabajo	1	Numero	$ 400.000.000,00	$ 400.000.000		$ 400.000.000	$ 800.000.000,00
						Equipos de RED	1	Numero	$ 264.000.000,00	$ 264.000.000		$ 150.000.000	$ 414.000.000,00
		Subtotal 2								**$ 964.000.000**		**$ 1.700.000.000,00**	**$ -**
TOTAL, PROYECTO										**$ 1.374.500.000**		**$ 2.397.200.000**	**$ 3.771.700.000**

EDWIN HEIVER MUÑOZ VASQUEZ
SECRETARIO GENERAL

Proyectó: *Oscar Toro Medina – Formulador de proyectos*
Aprobó: *Yerison Parra – Asesor jurídico secretaria general*

6. CRONOGRAMA

CRONOGRAMA DE ACTIVIDADES – PLANEACIÓN DE PRESUPUESTO.
VIGENCIA:2026

OBJETIVOS ESPECÍFICOS.	MES - VALOR / ACTIVIDADES	VR. MES 1	VR. MES 2	VR. MES 3	VR. MES 4	VR. MES 5	VR. MES 6	VR. MES 7	VR. MES 8	VR. MES 9	VR. MES 10	VR. MES 11	VR. MES 12	TOTAL
Desarrollar e implementar la Política de Seguridad Digital	Fortalecer la capacidad institucional en seguridad digital	0					$ 52.100.000	$ 52.100.000	$ 52.100.000	$ 52.100.000	$ 52.100.000	$ 52.100.000	$ 202.100,000	$ 462.600.000
	Adquirir infraestructura tecnológica en seguridad digital												$ 964.000.000	**$ 964.000.000**

CRONOGRAMA DE ACTIVIDADES – PLANEACIÓN DE PRESUPUESTO.
VIGENCIA:2027

OBJETIVOS ESPECÍFICOS.	MES - VALOR / ACTIVIDADES	VR. MES 1	VR. MES 2	VR. MES 3	VR. MES 4	VR. MES 5	VR. MES 6	VR. MES 7	VR. MES 8	VR. MES 9	VR. MES 10	VR. MES 11	VR. MES 12	TOTAL
Desarrollar e implementar la Política de Seguridad Digital	Fortalecer la capacidad institucional en seguridad digital	$58.433.333,33	$58.433.333,33	$58.433.333,33	$58.433.333,33	$58.433.333,33	$58.433.333,33	$58.433.333,33	$58.433.333,33	$58.433.333,33	$58.433.333,33	$58.433.333,33	$58.433.333,33	**$ 701.200.000**
	Adquirir infraestructura tecnológica en seguridad digital				$ 300.000.000							$1.400.000.000		**$1.700.000.000**

EDWIN HEIVER MUÑOZ VASQUEZ
SECRETARIO GENERAL

Proyectó: *Oscar Toro Medina – Formulador de proyectos*

Aprobó: *Yerison Parra – Asesor jurídico secretaria general*