

PERSONERIA DISTRITAL DE MEDELLIN	PROCESO DE GESTION			CODIGO	NDITC001		
	INNOVACIÓN Y TIC			VERSION	3		
	NORMA PLAN ESTRATEGICO TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI			VIGENCIA	DIA	MES	AÑO
					03	03	2026
			Página	1	de	3	

NORMA INTERNA

1. DEFINICIÓN Y ALCANCE

El Plan Estratégico de Tecnologías de la Información (PETI) es un documento que refleja la composición de elementos tecnológicos de la Personería Distrital de Medellín, y define la ruta de ejecución de proyectos para la modernización y mejoramiento de los servicios institucionales.

Las entidades tienen la responsabilidad de planear sus acciones de fortalecimiento y desarrollo, no solo en los asuntos misionales de servicios a la ciudadanía, sino en la modernización institucional que demanda la Política de Gobierno Digital, soportada por la implementación de las Tecnologías de la Información y las comunicaciones (TIC).


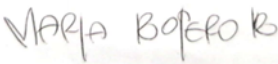

El PETI hace parte integral de la estrategia de la institución y es el resultado de un adecuado ejercicio de planeación estratégica de TI. Cada vez que se ejecuta un proyecto de Arquitectura Empresarial, su resultado debe ser integrado al PETI.

2. ACTUALIZACIÓN

El PETI debe ser actualizado en cada vigencia conforme a las necesidades o requerimientos de los procesos institucionales y del presupuesto aprobado para la realización de los proyectos establecidos.

3. COMPONENTES

En la construcción del PETI se deben considerar todos los elementos relacionados que reflejan el estado de la plataforma tecnológica de la Entidad, normatividad y las nuevas tendencias informáticas y tecnológicas, tales como: servicios tecnológicos, sistemas de información, infraestructura tecnológica y telecomunicaciones, sistemas de seguridad informática, recursos de Gestión Informática, presupuesto financiero, diagramas de arquitectura tecnológica, proyectos de innovación, políticas de gobierno digital, políticas de transformación digital, políticas de seguridad de la información, entre otros.

ELABORÓ			REVISÓ Y SUBIO AL SIG:			APROBÓ:			
DIEGO HERNANDO ZULUAGA SERNA			MARIA ALEJANDRA BOTERO BOTERO			FERNANDO ANDRÉS VALENCIA VALLEJO			
 PERSONERIA DE MEDELLIN VALLEJO S.G.C. FIRMA			 FIRMA			 FIRMA			
DIA	MES	AÑO	DIA	MES	AÑO	NRO. RESOLUCION	DIA	MES	AÑO
03	03	2026	03	03	2026	120	03	03	2026

PERSONERIA DISTRITAL DE MEDELLIN	PROCESO DE GESTION		CODIGO	NDITC001		
	INNOVACIÓN Y TIC		VERSION	3		
	NORMA PLAN ESTRATEGICO TECNOLOGÍAS DE LA INFORMACIÓN - PETI		VIGENCIA	DIA	MES	AÑO
			Página	03	03	2026
			2	de	3	

4. **RESPONSABLES**

Responsable de orientar la implementación del PETI.

El Comité de Informática en función delegada por el representante legal aprueba y hace seguimiento y verificación de la implementación del PETI.

Responsable de liderar la implementación del PETI.

El Director, Jefe de Oficina o Coordinador de Gestión Informática, tiene la responsabilidad de liderar la implementación y actualización del PETI. Algunas de las funciones relacionadas con el PETI son:

- Recopilar los requisitos tecnológicos de cada proceso institucional para analizar, estructurar, diseñar, y definir las estrategias, planes y proyectos de innovación que forman el PETI.
- Consultar los recursos financieros destinados a Gestión Informática en cada vigencia.
- En su rol de Secretario Técnico del Comité de informática debe presentar y buscar la aprobación del PETI en cada vigencia.

Es de anotar, que todos los integrantes del equipo de trabajo de Gestión Informática apoyan al líder del proceso en la construcción del documento.

5. **MEDICIÓN**

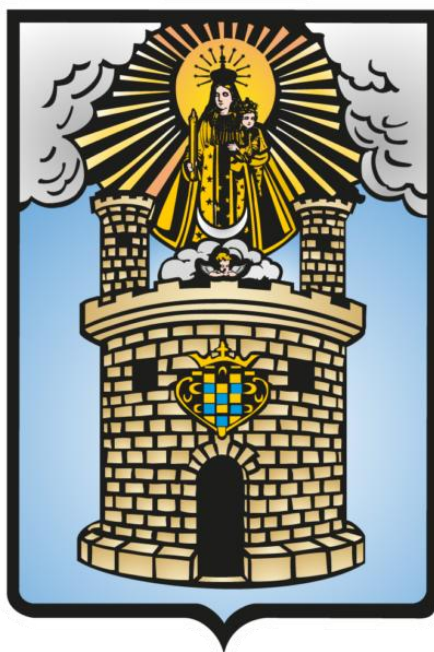
Gestión Informática rinde informes de avance al Comité de informática, buscando el cumplimiento total de las metas planeadas en el PETI. En caso de incumplir alguna de las actividades propuestas, debe sustentarse ante este Comité.

2. **RESPONSABLES DE LAS COPIAS CONTROLADAS**

Nº COPIA	CARGO	COPIA EN	
		PAPEL	ELECTRÓNICA EN INTRANET
1	Intranet		X

PERSONERIA DISTRITAL DE MEDELLIN	PROCESO DE GESTION		CODIGO	NDITC001		
	INNOVACIÓN Y TIC		VERSION	3		
	NORMA PLAN ESTRATEGICO TECNOLOGÍAS DE LA INFORMACIÓN - PETI		VIGENCIA	DIA	MES	AÑO
			Página	3	de	3

3. HISTORIAL						
VERSIÓN	RESOLUCIÓN	FECHA				NATURALEZA CAMBIO
		DÍA	MES	AÑO		
1	500	24	8	2023		Actualización Plan Estratégico Tecnologías de la Información y la Comunicaciones – PETI, para la vigencia 2020-2024, cuyas modificaciones se aprueban en Comité de Informática y Seguridad de la Información de la Personería Distrital de Medellín, mediante Acta número 003 de agosto 11 de 2023. Así mismo, se crea el documento como norma del proceso Gestión Informática en el SGC.
2	605	30	8	2024		“Por medio del cual se determinan nuevos códigos a los procesos modificados en el nuevo Mapa, con el fin de actualizar los documentos del Sistema de Gestión de la Calidad de la Personería Distrital de Medellín, y se realiza la distribución de los porcentajes y ponderación de cada uno de los procesos”.
3	120	03	03	2026		Actualización Plan Estratégico Tecnologías de la Información y la Comunicaciones – PETI, para la vigencia 2024 - 2028, cuyas modificaciones se aprueban en Comité de Informática y Seguridad de la Información de la Personería Distrital de Medellín, mediante Acta número 003 de diciembre 9 de 2026.



Personería

Distrital de Medellín

**Plan Estratégico de la Información y las Comunicaciones
(PETI)**

2024 - 2028

ACTUALIZACIÓN VIGENCIA 2024 - 2028

El Plan Estratégico de la Información y las Comunicaciones (PETI) es un marco normativo que le permitirá a la Personería Distrital de Medellín establecer los lineamientos y directrices para mantener y estandarizar todos sus procesos con el uso de las Tecnológicas de la Información y las Comunicaciones (TIC).

Tabla de Contenido

1. OBJETIVOS	4
2. ALCANCE DEL DOCUMENTO	6
3. GLOSARIO DE TÉRMINOS	9
4. MARCO NORMATIVO	13
5. RUPTURAS ESTRATÉGICAS	19
6. ANALISIS DE LA SITUACION ACTUAL	22
6.1. ESTRATEGIA DE TI.....	22
6.1.1. <i>Plan de las TIC y Desarrollos Tecnológicos</i>	25
6.1.2. <i>Infraestructura de TI</i>	28
6.1.3. <i>Planificación y Gestión Tecnológica</i>	37
6.2. USO Y APROPIACIÓN DE LA TECNOLOGÍA	39
6.3. SISTEMAS DE INFORMACIÓN	42
6.3.1. <i>Sistemas de información</i>	45
6.4. SERVICIOS TECNOLÓGICOS.....	51
6.5. GESTIÓN DE LA INFORMACIÓN	53
6.5.1. <i>Análisis de Demanda de información</i>	55
6.6. GOBIERNO DE TI.....	56
6.7. ANÁLISIS FINANCIERO	59
7. ENTENDIMIENTO ESTRATÉGICO.....	60
7.1. MODELO OPERATIVO	62
7.1.1. <i>Sistema de Gestión de Seguridad de la Información y el Manual de Seguridad</i> 65	
7.2. NECESIDADES DE INFORMACIÓN.....	68



N° SC735-1



7.3.	ALINEACIÓN DE TI CON LOS PROCESOS	71
8.	MODELO DE GESTIÓN DE TI	51
8.1.	ESTRATEGIA DE TI	51
8.1.1.	<i>Definición de los objetivos estratégicos de TI</i>	53
8.2.	GOBIERNO DE TI	56
8.2.1.	<i>Cadena de valor de TI</i>	56
8.2.2.	<i>Indicadores y Riesgos</i>	57
8.2.3.	<i>Estructura organizacional de TI</i>	59
8.3.	GESTIÓN DE INFORMACIÓN	59
8.3.1.	<i>Herramientas de Análisis</i>	59
8.3.2.	<i>Arquitectura de Información</i>	61
8.4.	SISTEMAS DE INFORMACIÓN	62
8.4.1.	<i>Arquitectura de Sistemas Información.</i>	64
8.4.2.	<i>Implementación de sistemas de información</i>	66
8.4.3.	<i>Evolución hacia un Sistema de Gestión de Documentos Electrónicos de Archivo – SGDEA</i>	68
8.4.4.	<i>Servicios de soporte técnico</i>	71
8.5.	MODELO DE GESTIÓN DE SERVICIOS TECNOLÓGICOS	73
8.5.1.	<i>Criterios de calidad y procesos de gestión de servicios de TIC</i>	73
8.5.2.	<i>Infraestructura</i>	75
8.5.3.	<i>Conectividad</i>	77
8.5.4.	<i>Servicios de operación</i>	79
8.5.5.	<i>Mesa de servicios</i>	83
8.5.6.	<i>Procedimientos de gestión</i>	86
8.5.7.	<i>Plan de Contingencia, Recuperación ante Desastres y Continuidad Operativa (DRP/BCP)</i>	89
8.6.	USO Y APROPIACIÓN	89
9.	MODELO DE PLANEACIÓN	92
10.	PLAN DE COMUNICACIONES DEL PETI	99



N° SC735-1



1. OBJETIVOS

Establecer los lineamientos estratégicos, técnicos y operativos para el desarrollo, gestión y fortalecimiento de las Tecnologías de la Información y las Comunicaciones (TIC) de la Personería Distrital de Medellín, garantizando la adecuada administración de los recursos tecnológicos, la infraestructura en la nube, la arquitectura de datos, la seguridad digital, los servicios institucionales y las comunicaciones, con el fin de soportar eficazmente la misión institucional orientada a la defensa y protección de los derechos humanos, la vigilancia de la conducta oficial y la atención oportuna a la ciudadanía.

Este objetivo general se desglosa en propósitos específicos:

1.1. Asegurar la disponibilidad, continuidad y escalabilidad de los servicios tecnológicos

- Mantener todos los servicios misionales operando en la nube con esquemas de alta disponibilidad.
- Garantizar operación continua bajo arquitecturas redundantes y resilientes.

1.2. Fortalecer la seguridad digital institucional

- Implementar controles avanzados mediante FortiGate, FortiWeb y FortiEDR.
- Consolidar un modelo Zero Trust para accesos seguros basados en identidad.
- Cumplir con ISO 27001, lineamientos de Seguridad y Privacidad del MinTIC y protección de datos personales.

1.3. Actualización y publicación del directorio telefónico institucional.

Con el fin de garantizar la continuidad, accesibilidad y eficiencia en las comunicaciones internas y externas, la Personería Distrital de Medellín mantendrá como actividad permanente la actualización, verificación y publicación del directorio telefónico institucional, asegurando que cada proceso cuente con sus números de contacto vigentes y que la información sea revisada durante todo el año, independiente de la rotación del personal.



N° SC735-1



1.4. Optimizar la gestión de redes y comunicaciones

- Mantener la red institucional bajo IPv6.
- Mantener y actualizar las VLAN para minimizar la superficie de ataque.
- Garantizar redes WiFi diferenciadas para invitados, funcionarios y servicios misionales.

1.5. Integrar y modernizar los sistemas de información institucionales

- Modernizar SIP 2.0, Personería en Línea, PQRS, Gestión Documental y otros sistemas clave.
- Consolidar API institucional para interoperabilidad entre módulos misionales.

1.6. Promover la analítica de datos para la toma de decisiones

- Integrar las principales fuentes de datos misionales y administrativas en modelos estructurados de analítica, permitiendo consolidar información del SIP, Personería en Línea, PQRS y otros sistemas institucionales.
- Desarrollar tableros estratégicos, operativos y de seguimiento utilizando herramientas como Power BI, soportadas en procesos de extracción, transformación y carga (ETL) adecuados a la infraestructura actual.
- Fortalecer las capacidades internas para el análisis de datos, interpretación de indicadores y toma de decisiones basada en evidencia, alineado con el propósito institucional de mejorar la atención ciudadana y la eficiencia operativa.
- Implementar estándares de calidad, trazabilidad y seguridad para el tratamiento de datos, asegurando consistencia y confiabilidad de la información analítica.

1.7. Garantizar buenas prácticas en la administración de recursos tecnológicos

- Optimizar licenciamientos, infraestructura, soporte técnico y operaciones TI.



N° SC735-1



- Fortalecer la gestión del ciclo de vida de activos tecnológicos.

1.8. Impulsar la transformación digital para mejorar la atención a la ciudadanía

- Implementar automatización, chatbot, servicios transaccionales y canales digitales accesibles.
- Reducir trámites y mejorar la experiencia de usuario.

1.9. Garantizar la conectividad y operación segura del trabajo de campo

- **Dotar a los funcionarios con tablets, cámaras, impresoras portátiles y dispositivos móviles** que permitan registrar información, evidencias y actuaciones misionales directamente en territorio.
- **Asegurar conectividad móvil segura** mediante planes corporativos, VPN y cifrado para acceder a los sistemas institucionales desde campo.
- **Permitir la generación inmediata de documentos en sitio** (actas, constancias, compromisos) para mejorar la atención al ciudadano.
- **Integrar los registros de campo al SIP en tiempo real**, fortaleciendo la trazabilidad, transparencia y seguridad de la información.
- **Estandarizar protocolos de captura, almacenamiento y custodia de evidencias**, en cumplimiento con el SGSI e ISO 27001.

2. ALCANCE DEL DOCUMENTO

El Plan Estratégico de Tecnologías de la Información (PETI) define el marco estratégico, operativo y técnico para la gestión, modernización y transformación de las Tecnologías de la Información y las Comunicaciones (TIC) de la Personería Distrital de Medellín. Su alcance comprende la alineación de las iniciativas de Innovación y Conocimiento con las metas institucionales establecidas en el Plan Estratégico, así como con la Misión y Visión de la Entidad, garantizando que la tecnología contribuya directamente a la defensa, protección y promoción de los Derechos Humanos, la vigilancia de la conducta oficial y la atención efectiva a la ciudadanía.

Este documento también orienta la consolidación de servicios digitales modernos, accesibles y seguros, fortaleciendo la relación entre la Personería y la ciudadanía



N° SC735-1



mediante la ampliación de los servicios en línea, la automatización de procesos misionales, la adopción de arquitecturas en la nube, el uso de IPv6, la segmentación de red mediante VLAN, y la implementación de modelos de seguridad Zero Trust.

El PETI se desarrolla en cuatro fases, que permiten una comprensión integral del estado de la Entidad y la definición de la estrategia de TI:

Fase 1. Análisis de la situación actual

Incluye la evaluación:

- De la estrategia institucional.
- De los procesos misionales y de apoyo.
- Del grado de madurez en la gestión de las TIC.
- De la infraestructura tecnológica actual (nube, seguridad, redes, sistemas).
- Del nivel de adopción tecnológica por parte de funcionarios y colaboradores.

Esta fase permite identificar brechas, oportunidades y capacidades reales para soportar la transformación digital de la Entidad.

Fase 2. Análisis del modelo operativo y organizacional

En esta fase se estudia:

- La estructura organizacional y roles asociados a TI.
- Las necesidades de información de los procesos misionales.
- La alineación entre TI, Gestión Documental y Sistemas de Información.
- La arquitectura tecnológica vigente (servicios en la nube, Fortinet, IPv6, VLAN, GPO).
- El grado de interoperabilidad entre los sistemas institucionales (SIP, Personería en Línea, PQRS, Intranet, Gestión Documental Digital).



N° SC735-1



El propósito es entender cómo la tecnología soporta la operación actual y qué ajustes se requieren para fortalecerla.

Fase 3. Formulación de la Estrategia de TI

A partir de la información consolidada en las dos fases anteriores se diseña la estrategia de TI, que incluye:

- Modelo de gestión de TI alineado a la estrategia institucional y al Programa de Transformación Digital del Plan Estratégico 2024–2028.
- Modelo de información y **arquitectura de datos basada en analítica institucional**, integrando fuentes misionales y administrativas mediante procesos de extracción, transformación y modelamiento que permitan análisis oportuno para la toma de decisiones.
- Modelo de sistemas de información que incluye la **modernización del SIP**, el fortalecimiento de la integración entre sistemas a través de servicios API, y la automatización de procesos de soporte y atención al ciudadano.
- Arquitectura tecnológica soportada en la nube, redes seguras, segmentación por VLAN, servicios de Microsoft 365 y Azure, y un enfoque de **seguridad Zero Trust**.
- Gobierno de TI y Gobierno Digital articulado a los lineamientos de MinTIC, MIPG y el Sistema de Gestión de Seguridad de la Información (SGSI).
- Estrategias de uso y apropiación tecnológica dirigidas a funcionarios, colaboradores y ciudadanía, apoyadas en capacitación, adopción de herramientas digitales y fortalecimiento de competencias.

Esta estrategia establece las prioridades, inversiones y capacidades necesarias para consolidar un ecosistema tecnológico moderno, seguro y orientado al mejoramiento del servicio al ciudadano.

Fase 4. Planeación e implementación

En esta fase se definen:

- Los lineamientos de implementación de la estrategia.
- El portafolio de proyectos estratégicos.



N° SC735-1



- Planes de acción y operativo a corto, mediano y largo plazo.
- Mecanismos de seguimiento, control y actualización anual.
- Ajustes basados en avances tecnológicos, cambios normativos o necesidades misionales.

Este modelo garantiza que la implementación del PETI sea flexible, medible, actualizable y orientada al impacto.

3. GLOSARIO DE TÉRMINOS

• Acuerdo de Nivel de Servicio (ANS / SLA)

Documento formal acordado entre Innovación y Conocimiento y las áreas usuarias que establece los niveles mínimos de calidad, tiempos de respuesta, disponibilidad, soporte, capacidad y desempeño que deben cumplir los servicios de TI. Incluye métricas, penalidades, responsabilidades y mecanismos de seguimiento.

• Arquitectura Empresarial

Disciplina estratégica que traduce la visión institucional en modelos claros de negocio, datos, aplicaciones y tecnología. Permite planear el estado futuro de la Entidad y su transición ordenada, alineada al Marco de Referencia de Arquitectura del MinTIC.

• Arquitectura de Servicios Tecnológicos

Describe el catálogo de productos, plataformas, infraestructura y herramientas tecnológicas que soportan los sistemas de información. Incluye servicios en la nube, redes (IPv6/VLAN), seguridad Fortinet, almacenamiento, virtualización y servicios de conectividad.

• Arquitectura de Software

Define la estructura de los sistemas de información, su modularidad, interfaces, APIs, integración, protocolos de comunicación y lineamientos de desarrollo. Permite asegurar interoperabilidad, escalabilidad y mantenibilidad.



N° SC735-1



- **Arquitectura de TI**

Conjunto de elementos tecnológicos que incluyen infraestructura en la nube, redes, seguridad, sistemas, bases de datos y servicios necesarios para soportar los procesos de la Entidad. Debe cumplir los requisitos de seguridad, continuidad y alineación con Gobierno Digital.

- **API Institucional**

Conjunto de interfaces y servicios interoperables que permiten integrar SIP, PQRS, Gestión Documental y otros sistemas. Habilita intercambios seguros de información y facilita la automatización y analítica.

- **Catálogo de Componentes de Información**

Inventario detallado que clasifica los datos institucionales, sus metadatos, propietarios, niveles de criticidad y relaciones. Es la base para el modelo de datos y la analítica institucional.

- **Capacidades de TI**

Conjunto de recursos humanos, tecnológicos, financieros y procedimentales que permiten a la Entidad operar, mantener y evolucionar su infraestructura tecnológica. Incluye personal, nube, seguridad, conectividad y sistemas.

- **Catálogo de Servicios de TI**

Inventario formal de los servicios que Innovación y Conocimiento presta a los procesos: soporte técnico, mesa de ayuda, administración de sistemas, redes, seguridad, hosting en la nube, bases de datos, automatización, desarrollos internos y analítica.

- **Catálogo de Servicios Tecnológicos**

Lista detallada de la infraestructura y recursos disponibles: equipos, servidores virtuales, redes WiFi y LAN, dispositivos Fortinet, almacenamiento y servicios cloud.

- **Catálogo de Sistemas de Información**



N° SC735-1



Relación de sistemas misionales y administrativos disponibles: SIP, Personería en Línea, PQRS, Gestión Documental Digital, Intranet, Moodle, tableros analíticos, entre otros.

- **Ciclo de Vida de los Sistemas o Componentes de Información**

Secuencia completa desde diseño, desarrollo, pruebas, implementación, operación, mantenimiento y retiro. Puede ser manual o automatizado, basado en mejores prácticas como DevSecOps, ITIL 4 y normas de calidad.

- **Esquema de Gobierno TI**

Modelo de decisiones, roles, políticas y controles que garantizan que TI soporte la estrategia institucional. Incluye comités, lineamientos, gestión de riesgos, controles financieros, SGSI y Gobierno Digital.

- **Estrategia TI**

Conjunto de directrices y acciones para garantizar que la tecnología contribuya al cumplimiento de la misión institucional. Incluye modernización, seguridad, nube, automatización, analítica y experiencia digital.

- **Gestión TI**

Conjunto de actividades para administrar recursos tecnológicos, servicios, infraestructura, personal, proyectos y presupuestos. Se basa en modelos como ITIL 4, COBIT 2019 y MIPG.

- **Gobierno de TI**

Conjunto de políticas, lineamientos, comités y responsabilidades que aseguran que los servicios y proyectos de TI estén alineados con los objetivos institucionales y normativas del sector público.

- **Gobierno Digital**

Modelo del MinTIC que articula la transformación digital, seguridad, interoperabilidad, analítica, gestión documental y servicios ciudadanos digitales en las entidades públicas.



N° SC735-1



- **Información**

Datos organizados y procesados que tienen valor para los procesos misionales, la toma de decisiones, la defensa de derechos y la vigilancia administrativa.

- **Lineamiento**

Norma o directriz establecida por la Entidad para orientar decisiones y acciones operativas o estratégicas en TIC.

- **Macroproceso de Gestión TI**

Nivel superior que agrupa procesos como: soporte, infraestructura, seguridad, desarrollo, datos, nube, innovación, analítica y proyectos. Asegura continuidad y sostenibilidad tecnológica.

- **Mapa de Ruta (Roadmap)**

Herramienta de planeación que define la evolución de la tecnología, prioridades estratégicas, cronogramas y proyectos de modernización.

- **Política de TI**

Regla autorizada que orienta el uso de recursos tecnológicos, acceso, seguridad, desarrollo, datos, automatización, nube y continuidad.

- **Seguridad Zero Trust**

Modelo donde ningún usuario, dispositivo o red es considerada confiable por defecto. Requiere autenticación continua, verificación, segmentación y controles por identidad.

- **Servicio Tecnológico**

Componente de infraestructura que soporta un sistema o proceso, como redes, almacenamiento, nube, seguridad y conectividad.

- **Servicio de TI**



N° SC735-1



Actividad o conjunto de actividades orientadas a satisfacer una necesidad tecnológica de un usuario interno o externo.

- **PETI**

Documento estratégico que define el estado actual y futuro de TI y orienta la transformación tecnológica de la Entidad.

- **Plan de Comunicación de la Estrategia TI**

Documento que define cómo se divulgará la estrategia de TI a funcionarios, directivos y ciudadanía.

- **SGSI – Sistema de Gestión de Seguridad de la Información**

Modelo basado en ISO 27001 que establece políticas, normas, controles y procedimientos para garantizar confidencialidad, integridad y disponibilidad de la información.

- **TI**

Tecnologías de la Información, infraestructura, sistemas, plataformas, comunicaciones y seguridad utilizadas para soportar los procesos institucionales.

4. MARCO NORMATIVO

La estructuración del PETI se fundamenta en el Decreto 2573 de 2014¹ en su TÍTULO. II - COMPONENTES, INSTRUMENTOS Y RESPONSABLES, que enfatiza sobre los fundamentos principales para desarrollar de manera correcta la implementación de la Estrategia de Gobierno en Línea. Se puede resaltar:

“(…). Artículo 5°. Componentes. Los fundamentos de la Estrategia serán desarrollados a través de 4 componentes que facilitarán la masificación de la oferta y la demanda del Gobierno en Línea.

¹ https://www.mintic.gov.co/portal/604/articles-14673_documento.pdf



N° SC735-1



- 1) TIC para Servicios. Comprende la provisión de trámites y servicios a través de medios electrónicos, enfocados a dar solución a las principales necesidades y demandas de los ciudadanos y empresas, en condiciones de calidad, facilidad de uso y mejoramiento continuo.
- 2) TIC para el Gobierno Abierto. Comprende las actividades encaminadas a fomentar la construcción de un Estado más transparente, participativo y colaborativo involucrando a los diferentes actores en los asuntos públicos mediante el uso de las Tecnologías de la Información y las Comunicaciones.
- 3) TIC para la Gestión. Comprende la planeación y gestión tecnológica, la mejora de procesos internos y el intercambio de información. Igualmente, la gestión y aprovechamiento de la información para el análisis, toma de decisiones y el mejoramiento permanente, con un enfoque integral para una respuesta articulada de gobierno y para hacer más eficaz la gestión administrativa entre instituciones de Gobierno.
- 4) Seguridad y Privacidad de la Información. Comprende las acciones transversales a los demás componentes enunciados, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada.

Parágrafo 1°. TIC para el gobierno abierto comprende algunos de los aspectos que hacen parte de Alianza para el Gobierno Abierto, pero no los cubre en su totalidad.

Artículo 6°. Instrumentos. Los instrumentos para la implementación de la estrategia de Gobierno en Línea serán los siguientes:

Manual de Gobierno en Línea. Define las acciones que corresponde ejecutar a las entidades del orden nacional y territorial respectivamente.

Marco de referencia de arquitectura empresarial para la gestión de Tecnologías de la Información. Establece los aspectos que los sujetos obligados deberán adoptar para dar cumplimiento a las acciones definidas en el Manual de Gobierno en Línea (...)

Desarrollando correctamente estos componentes el Ministerio de las Tecnologías de la Información y las Comunicaciones con la expedición del presente decreto específicamente lo enunciado en su Título III – Medición, Monitoreo y Plazos,



N° SC735-1



conforma un modelo de evaluación para los sujetos del orden territorial basado en un porcentaje de avance de los componentes del Manual de Gobierno en línea vigente, midiendo así el cumplimiento de la entidad evaluada, y lo relaciona de la siguiente manera:

“Artículo 9°. Medición y monitoreo. El Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Dirección de Gobierno en Línea y de la Dirección de Estándares y Arquitectura de Tecnologías de la Información, diseñará el modelo de monitoreo que permita medir el avance en las acciones definidas en el Manual de Gobierno en Línea que corresponda cumplir a los sujetos obligados, los cuales deberán suministrar la información que les sea requerida.”

En conclusión, es de vital importancia el cumplimiento del presente decreto por ser el mapa de ruta que las entidades territoriales deben promover en sus administraciones para así aplicar de manera correcta la estrategia nacional de Gobierno en Línea, apoyando a la creación de un Estado más eficiente, más transparente y más participativo gracias a las TIC, prestando los mejores servicios en línea al ciudadano, logrando la excelencia en la gestión, empoderando y generando confianza en los ciudadanos e impulsando y facilitando las acciones requeridas para avanzar en los Objetivos de Desarrollo Sostenible -ODS, facilitando el goce efectivo de derechos a través del uso de TIC.

Como complemento del Decreto Nacional 2573 de 2014, encontramos el dominio Estrategia TI que tiene como fin apoyar el proceso de diseño, implementación y evolución de la Arquitectura TI en las instituciones, para lograr que esté alineada con las estrategias organizacionales y sectoriales, su implementación cuenta con 4 ámbitos de aplicación que servirán como insumo para la correcta formulación, seguimiento y evaluación del PETI adoptado por la entidad.

Decreto 415 del 2016² "Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones." En su Artículo 2.2.35.3. Numeral 1 se establece los objetivos del fortalecimiento institucional. Para el

² <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=68717>



N° SC735-1



fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones las entidades y organismos a que se refiere el presente decreto deberán: (...)

Nombre	Descripción
Ley 23 de 1982	Ley 23 de 1982 "Sobre derechos de autor"
Decreto 235 de 2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas
Decreto 4147 de 2011	Por el cual se crea la Unidad Nacional para la Gestión del Riesgo de Desastres, se establece su objeto y estructura
Conpes 3701 de 2011	Lineamientos de política para la Ciberseguridad y Ciberdefensa
Ley 1523 de 2012	Por la cual se adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Decreto 2672 de 2013	Por el cual se modifica parcialmente la estructura de la Unidad Nacional para la Gestión del Riesgo de Desastres.", se ratifica la función de la Oficina Asesora de planeación e Información de la UNGRD como la oficina que debe "Administrar y mantener en funcionamiento el Sistema Integrado de Información de que tratan los artículos número 45 y 46 de la Ley 1523 de 2012 o los que hagan sus veces para avanzar y facilitar la Gestión del Riesgo de Desastres, articularlo con otros sistemas de información y monitorear su uso en los diferentes niveles territoriales".
Decreto 1377 de 2013	Decreto 1377 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012 protección de datos personales.
ISO 27001:2013	Sistema de Gestión de Seguridad de la Información

Nombre	Descripción
Ley 1712 DE 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector de TIC
Decreto 2434 de 2015	Por el cual se adiciona el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones; 1078 de 2015, para crearse el Sistema de Telecomunicaciones de Emergencias como parte del Sistema Nacional de Gestión de Riesgo de Desastres
Ley 1753 de 2015	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "TODOS POR UN NUEVO PAIS"
Resolución 3564 de 2015	Lineamientos respecto de los estándares de publicación y divulgación de la información, accesibilidad en medios electrónicos para población en situación de discapacidad, formulario electrónico para la recepción de solicitudes de acceso a la información pública, datos abierto y condiciones de seguridad en medios electrónicos
Decreto 415 de 2016	Definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las telecomunicaciones
Conpes 3854 de 2016	Política Nacional de Seguridad Digital
Resolución No. 445 de 2018	Por la cual se actualiza el Sistema Integrado de Planeación y Gestión SIPLAG de la Unidad Nacional para la Gestión del Riesgo de Desastres
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

Nombre	Descripción
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
CONPES 3920 de 2018	Política nacional de explotación de datos (Big Data) Bases del Plan Nacional de Desarrollo 2018-2022 Pacto por Colombia pacto por la Equidad
Resolución 1117 de 5 de abril de 2022 Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC	Resolución que define los lineamientos y condiciones para que las entidades territoriales adopten e implementen estrategias de Ciudades y Territorios Inteligentes, en el marco de lo previsto en el artículo 147 de la Ley 1955 de 2019.
Decreto 767 de 16 de mayo de 2022: Política de Gobierno Digital Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC	La Política de Gobierno Digital es la política del Gobierno Nacional que propende por la transformación digital pública. Con esta política pública se busca fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública y el Estado en general, a través del uso y aprovechamiento de las TIC. Hace parte del Modelo Integrado de Planeación y Gestión - MIPG y se integra con las políticas de Gestión y Desempeño Institucional.
Resolución 1951 de 9 de junio de 2022 - Anexo 1 Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC	Por el cual se establecen los requisitos, las condiciones y el trámite de la habilitación de los prestadores de servicios ciudadanos digitales especiales; se dan lineamientos y estándares para la integración de estos servicios y la coordinación de los prestadores con la Agencia Nacional Digital.
Decreto 088 de 24 de enero de 2022 Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC	Establece los conceptos, lineamientos, plazos, condiciones técnicas transversales para la digitalización y automatización de los trámites en línea, que deberán ser acogidos por las autoridades públicas y por los particulares que cumplan funciones públicas y/o administrativas.

Nombre	Descripción
Resolución 460 de Febrero 15 de 2022 Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)	Plan Nacional de Infraestructura de Datos (PNID) y su Hoja de Ruta, con el fin de impulsar la transformación digital del Estado y el desarrollo de una economía basada en los datos.
Directiva Presidencial 03 de 15 de marzo de 2021 Presidencia de la República	Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

5. RUPTURAS ESTRATÉGICAS

Las rupturas estratégicas representan los paradigmas, limitaciones y barreras que deben superarse para lograr la modernización tecnológica, operativa y misional de la Personería Distrital de Medellín. Estas rupturas fueron identificadas durante el análisis estratégico del proceso de Innovación y Conocimiento y constituyen los elementos clave que deben transformarse para consolidar una gestión de TI moderna, segura, interoperable y alineada con la defensa de los derechos humanos.

- **La tecnología debe ser reconocida como un habilitador estratégico.**

TI debe pasar de un rol operativo a convertirse en un componente central para el cumplimiento misional, la defensa de derechos, la vigilancia administrativa y la atención ciudadana.

- **La gestión de TI requiere una dirección integral orientada a resultados.**

Se requiere liderazgo tecnológico, portafolio de proyectos, medición de impacto y toma de decisiones basada en evidencia y buenas prácticas.

- **La información debe ser oportuna, confiable, integrada y explotable.**

La institución necesita consolidar un modelo de datos único, interoperabilidad entre sistemas (SIP, PQRS, Gestión Documental, Intranet) y tableros de analítica que soporten decisiones directivas.



N° SC735-1



- **Es necesario fortalecer la capacidad analítica de toda la institución.**
Los procesos deben aprovechar herramientas de analítica, data lake, modelos de integración y dashboards en tiempo real para orientar decisiones estratégicas y misionales.
- **Se requiere liderazgo institucional en gestión de sistemas de información.**
La transformación digital demanda patrocinio activo desde la alta dirección y articulación entre todos los procesos y el equipo de Innovación y Conocimiento.
- **Necesidad de estándares de integración e interoperabilidad.**
Se debe definir un estándar institucional basado en APIs, arquitectura modular, modelos de datos comunes y protocolos seguros para el intercambio de información.
- **Las soluciones tecnológicas deben alinearse plenamente con los procesos misionales.**
Las inversiones tecnológicas deben estar basadas en costo-beneficio, eficiencia, automatización y mejora directa del servicio a la ciudadanía.
- **Los sistemas de información deben dejar de operar de manera aislada.**
La meta es consolidar una plataforma interoperable, integrada y con flujo unificado entre SIP, PQRS, Personería en Línea, Gestión Documental y analítica institucional.
- **Existen brechas entre directivos y el proceso de Innovación y Conocimiento.**
Estas brechas limitan la adopción de tecnologías. Se requiere comunicación estratégica, cultura digital y procesos de alineación institucional.
- **Resolver el dilema entre desarrollar soluciones internas o adquirir software.**
Debe existir una política definida basada en TCO, seguridad, mantenimiento, integración, soporte y valor para la Entidad.
- **Necesidad de fortalecer el talento humano en Innovación y Conocimiento.**



N° SC735-1



Se requieren roles especializados en nube, seguridad digital, arquitecturas, datos, desarrollo, automatización y soporte avanzado.

- **Necesidad de fortalecer el talento humano de la Entidad en uso y apropiación de TIC.**
La transformación digital exige capacitación continua, acompañamiento, formación para directivos y apropiación tecnológica institucional.
- **Falta de apropiación de tendencias tecnológicas modernas.**
La institución debe fortalecer el uso de tecnologías como modelo Zero Trust, nube, analítica avanzada, APIs, automatización e inteligencia artificial responsable.
- **Deben fortalecerse las capacidades institucionales para garantizar el uso adecuado de las TIC.**
Se requiere madurez en gobernanza, políticas, procesos, documentación, SGSI, arquitectura y buenas prácticas.
- **La seguridad debe evolucionar hacia un modelo Zero Trust y una arquitectura Fortinet integrada.**
Todo acceso debe ser verificado, autenticado y monitoreado, incluyendo controles de FortiGate, FortiWeb y FortiEDR.
- **Consolidar una red moderna basada en IPv6, segmentación mediante VLAN y WiFi segregada.**
Se requiere operar con redes modernas, seguras y controladas mediante políticas GPO y segmentación completa.
- **Falta consolidar un modelo de servicio basado en ITIL 4.**
Se requiere fortalecer la mesa de servicios, catálogo de servicios, gestión de incidentes, solicitudes, cambios y mejora continua.
- **Es necesario formalizar el Gobierno Digital institucional.**
Incluye interoperabilidad, seguridad, servicios ciudadanos digitales, gestión documental digital, datos abiertos y transformación digital.



N° SC735-1



6. ANALISIS DE LA SITUACION ACTUAL

En este apartado se realiza un diagnóstico en cada uno de los dominios del marco de referencia de arquitectura TI³, con el fin de determinar el nivel de madurez tecnológico de la Entidad en relación con las dimensiones del modelo del marco de referencia, calificando dicho estado de madurez en un rango de alto, medio o bajo.

Este análisis permite conocer el estado actual o línea base a partir de la cual se debe comenzar a proyectar la visión de lo que se espera en materia de gestión de TI de la Personería Distrital de Medellín, así mismo permite plantear los Planes de Acción Estratégicos que faciliten alcanzar un grado de madurez aceptable en el dominio de las TIC.

Fuente de información interna: Comités de Informática, Planes Operativos y Círculos de Calidad.

6.1. Estrategia de TI

El artículo 178 de la Ley 136 de 1994 se refiere:

“El Personero ejercerá en el municipio, bajo la dirección suprema del Procurador General de la Nación, las funciones del Ministerio Público, además de las que determine la Constitución, la Ley, los Acuerdos y las siguientes (...).”

La Personería Distrital de Medellín siguiendo los mandatos Superiores y legales cuenta con el Plan Estratégico Institucional 2024 – 2028 AGENDA ESTRATEGICA 2: IMPLEMENTAR UN MODELO INNOVADOR, Y DESCONCENTRADO DE ATENCIÓN, PROGRAMA: TRANSFORMACION DIGITAL PARA LA PERSONERIA, PROYECTO: ECOSISTEMA DE GESTION INFORMATICA MODERNIZADO.

Dentro del proceso de ejecución de plan de acción y plan estratégico 2025 – 2028 “ La Personería Distrital de Medellín” se plantea construir una cultura digital, eficiente y transparente al servicio de la ciudadanía y al interior de la personería,

³ Marco de Referencia de Arquitectura de TI: Es el principal instrumento para implementar la **Arquitectura** TI de Colombia y habilitar la Estrategia de Gobierno en línea.



Nº SC735-1



articulando las tecnologías de la información, las comunicaciones en el modelo de gestión organizacional y de los lineamientos definidos en la estrategia y política de Gobierno Digital, mejorar la calidad de servicio al cliente y atención al ciudadano a través de una Infraestructura tecnológica actualizada de Hardware y software, que permita mejorar los servicios actuales y futuros prestados a la ciudadanía y las herramientas tecnológicas con que cuentan sus funcionarios.

La Personería Distrital de Medellín cuenta con una plataforma tecnológica moderna, híbrida y altamente disponible, soportada en servicios de nube, seguridad avanzada y arquitectura empresarial alineada con las prácticas de Gobierno Digital. Esta infraestructura permite garantizar continuidad operativa, disponibilidad, escalabilidad, seguridad de la información y eficiencia en la prestación de servicios a la ciudadanía y a los procesos internos.

- **Microsoft 365 como plataforma central de productividad y colaboración**

La Entidad opera bajo el ecosistema de Microsoft 365, que integra herramientas como OneDrive, Word, Excel, Teams y servicios de colaboración para todos los funcionarios, con altos estándares de seguridad, control de acceso y cumplimiento normativo.

- **Exchange Online para la gestión del correo electrónico institucional**

El correo institucional se encuentra alojado en la nube (Exchange Online), bajo un esquema de seguridad reforzado con MFA, cifrado, políticas anti-phishing, filtrado avanzado y disponibilidad garantizada.

- **SharePoint Online como repositorio del Sistema Integrado de Gestión (SIG)**

El Sistema Integrado de Gestión de la Personería (documentos, normatividad, procedimientos, formatos y registros) se encuentra centralizado en SharePoint Online, garantizando control de versiones, trazabilidad, acceso seguro, cumplimiento y colaboración entre dependencias.

- **Servidores institucionales en Windows Server 2022 integrados con Azure**

La Entidad cuenta con un datacenter operativo basado en Windows Server 2022, integrado con Azure Active Directory para autenticación híbrida, sincronización de



N° SC735-1



identidades, políticas avanzadas, copias de seguridad cloud, administración centralizada y planes de contingencia.

• **Arquitectura híbrida conectada a Azure**

La infraestructura on-premise opera como nodo de contingencia y soporte, mientras que los servicios críticos se encuentran alojados completamente en la nube, aprovechando escalabilidad, redundancia y continuidad.

• **VLAN para la segmentación de la red institucional**

La red se encuentra segmentada mediante VLAN separadas para:

- Función administrativa
- Sistemas misionales
- Servicios cloud
- Telefonía IP
- Equipos internos
- Invitados

Esta segmentación minimiza la superficie de ataque, mejora el desempeño y permite aplicar controles diferenciados.

• **Cumplimiento pleno con IPv6**

Toda la infraestructura de red opera bajo IPv6, lo que garantiza compatibilidad con servicios modernos, direccionamiento optimizado, mayor seguridad y continuidad tecnológica.

• **Infraestructura de seguridad basada en Fortinet**

Se cuenta con una arquitectura de seguridad integrada por:

- **FortiGate:** Firewall NGFW, IPS, filtrado web, inspección SSL, antivirus perimetral.
- **FortiWeb:** WAF para protección de aplicaciones web, APIs, OWASP Top 10, anti-bot.



N° SC735-1



- **FortiEDR:** Protección avanzada de endpoint, anti-ransomware, monitoreo continuo y contención automática.

Esta infraestructura permite un esquema de seguridad unificado bajo principios Zero Trust.

- **Servicio de conectividad WiFi segmentado y seguro**

La Entidad opera redes WiFi independiente para funcionarios, equipos misionales y visitantes, protegidas bajo WPA3 y controles definidos por políticas de seguridad y segmentación por VLAN.

6.1.1. Plan de las TIC y Desarrollos Tecnológicos

En el contexto nacional, la Política de Gobierno Digital, la estrategia de Transformación Digital del Estado y el Plan Nacional de Desarrollo impulsan iniciativas orientadas a llevar conectividad y servicios digitales al 100% de los centros poblados y municipios del país, mediante soluciones rurales y urbanas que buscan cerrar las brechas tecnológicas, sociales y territoriales. Estas iniciativas están acompañadas por la integración progresiva de los trámites y servicios del Estado en plataformas interoperables, seguras y accesibles para toda la ciudadanía.

En este marco, el Ministerio de Tecnologías de la Información y las Comunicaciones ha presentado la ruta nacional de conectividad, resaltando que la Ley 1978 de 2019, conocida como la Ley de Modernización de las TIC, permite fortalecer el ecosistema digital del país, mejorar la competitividad, acelerar la digitalización del sector público y habilitar las capacidades necesarias para el avance hacia la Cuarta Revolución Industrial. Esta ley impulsó la ampliación de infraestructura, la eficiencia en la gestión del espectro, la masificación del acceso y la consolidación de servicios gubernamentales digitales.

La Personería Distrital de Medellín, en cumplimiento de los mandatos constitucionales y legales que orientan su función misional, adopta el **Plan Estratégico Institucional 2024–2028**, el cual establece en su **Agenda**



N° SC735-1



Estratégica 2: “Implementar un modelo innovador y desconcentrado de atención”, el Programa: Transformación Digital para la Personería, y dentro de este, el Proyecto: Ecosistema de Gestión Informática Modernizado.

Este enfoque reconoce la necesidad de modernizar integralmente los sistemas de información, la infraestructura tecnológica, los modelos de atención y los servicios digitales ofrecidos tanto a la ciudadanía como a los funcionarios, garantizando que las tecnologías de la información y las comunicaciones se integren plenamente al modelo de gestión organizacional.

En desarrollo del **Plan de Acción y del Plan Estratégico 2025–2028**, la Personería plantea la consolidación de una **cultura digital sólida, eficiente, transparente y orientada al servicio de la ciudadanía**, fortaleciendo simultáneamente las capacidades tecnológicas internas y los procesos institucionales. Este propósito implica la integración de las TIC como habilitadores fundamentales de la operación misional, permitiendo:

- Mejorar la calidad del servicio al ciudadano.
- Facilitar la atención oportuna y desconcentrada.
- Dar soporte a la defensa de los derechos humanos y la vigilancia administrativa.
- Modernizar los canales de comunicación y atención digital.
- Optimizar el uso de los recursos tecnológicos institucionales.

La Entidad avanza hacia una infraestructura tecnológica moderna basada en servicios en la nube, conectividad con IPv6, segmentación por VLAN, seguridad digital mediante arquitectura Fortinet, integración con Microsoft 365, Exchange Online y SharePoint, así como el fortalecimiento del datacenter institucional bajo Windows Server 2022 integrado con Azure.

Esta infraestructura actualizada de hardware, software y servicios digitales permite ampliar, mejorar y asegurar la prestación de servicios actuales y futuros, consolidando un ecosistema informático robusto que facilite el acceso a la información, incremente la transparencia, optimice los procesos internos y



N° SC735-1



contribuya al cumplimiento de los lineamientos definidos en la **Estrategia de Gobierno Digital del MinTIC**.

En este marco, la Personería Distrital de Medellín continúa posicionándose como una entidad moderna, innovadora y comprometida con la transformación digital, garantizando que la tecnología sea un eje articulador para el cumplimiento de su misión institucional y la atención efectiva a la ciudadanía.

Desde el año 2024, la Personería Distrital de Medellín implementó **Personería en Línea**, una plataforma digital que permite a los ciudadanos acceder de manera remota, rápida y segura a diferentes servicios institucionales. Este sistema ha fortalecido la atención ciudadana, ampliado los canales de acceso y consolidado un modelo de atención moderno, desconcentrado y alineado con los lineamientos de Gobierno Digital.

Dentro de esta transformación, se desarrollaron e incorporaron nuevos servicios digitales, entre ellos:

• **Servicio de Citas en Línea:**

Plataforma que permite a los ciudadanos agendar de manera virtual una cita para recibir orientación y acompañamiento jurídico por parte de los profesionales de la Personería. Este servicio ha reducido tiempos de espera, mejorado la distribución de la demanda y ampliado el acceso a la justicia preventiva.

• **Sistema de PQRSD en Línea:**

Implementado en 2025, este sistema permite a la ciudadanía radicar Peticiones, Quejas, Reclamos, Sugerencias y Denuncias de manera digital, garantizando trazabilidad completa, seguimiento en tiempo real y una atención oportuna y transparente. La plataforma está integrada con los sistemas institucionales misionales y soportada sobre infraestructura segura y basada en la nube.

Gracias a estos servicios digitales, la Personería de Medellín ha logrado una mejora significativa en la relación con la ciudadanía, alcanzando:

- **8.347 atenciones prestadas en línea a través de Personería en Línea.**



N° SC735-1



- **441 PQRSD radicadas digitalmente durante su primer año de operación (2025).**

Estos avances fortalecen el **Proyecto “Ecosistema de Gestión Informática Modernizado”** del Plan Estratégico Institucional 2024–2028 y consolidan a la Personería Distrital de Medellín como una entidad moderna, innovadora y orientada a facilitar el acceso a la información, la defensa de los derechos humanos y la atención efectiva a la ciudadanía mediante el uso estratégico de las TIC.

6.1.2. Infraestructura de TI

La Personería Distrital de Medellín cuenta con una arquitectura de Tecnologías de la Información orientada al servicio, basada en una infraestructura moderna, segura, escalable y alineada con el modelo de Gobierno Digital. Las TIC se encuentran integradas en los procesos internos, la atención ciudadana y la defensa y promoción de los derechos humanos, permitiendo una operación eficiente, desconcentrada y segura.

Infraestructura y arquitectura tecnológica

La infraestructura de TI opera bajo un esquema híbrido compuesto por servicios en la nube, servidores institucionales, redes segmentadas, plataformas de colaboración y un robusto sistema de seguridad digital. La Entidad dispone de tres sedes con conectividad asegurada:

- Sede principal, donde se encuentra el centro de datos institucional, los principales equipos de red y la mayor parte del personal administrativo y misional.
- UPDH en el barrio El Bosque.
- Centro de Conciliaciones en el Centro Administrativo La Alpujarra.

Las sedes satélite están conectadas mediante LAN to LAN y servicios conmutados bajo líneas dedicadas que garantizan la continuidad, estabilidad y seguridad de la comunicación.



N° SC735-1



Servicios institucionales de TI

Todos los funcionarios pueden acceder a los servicios institucionales desde la sede principal mediante conexión por cable o WiFi segmentada, y desde las sedes alternas o en modalidad de trabajo en casa a través de servicios en la nube y canales seguros mediante autenticación multifactor.

Los servicios institucionales actualmente disponibles incluyen:

- Microsoft 365 como plataforma central de productividad, con Exchange Online, OneDrive, Teams y SharePoint.
- Personería en Línea, plataforma que reúne servicios digitales para la ciudadanía.
- Moodle, plataforma de formación virtual donde se ofrecen cursos, talleres y capacitaciones dirigidas a la ciudadanía y a los funcionarios.
- Sistema de Información Misional – SIP (en la nube), integrado a procesos de atención, defensoría, asesoría jurídica y seguimiento.
- Sistema de Gestión de Correspondencia – SIP, con trazabilidad digital.
- Sistema de PQRSD en Línea, implementado en 2025.
- Citas en Línea para agendamiento de asesoría con abogados.
- Intranet institucional (en la nube).
- Página web institucional, con servicios ciudadanos digitales.
- Gestión de usuarios y autenticación integrada con Azure AD.
- Servicio de impresión corporativa.
- Servicio de telefonía IP institucional (sede principal y sedes alternas).
- Mesa de ayuda y soporte técnico.
- Seguridad digital con FortiGate, FortiWeb y FortiEDR.
- Conectividad WiFi segmentada para funcionarios, equipos misionales e invitados.

Evolución del centro de datos institucional (Windows Server 2022 + Azure)

El centro de datos institucional, con operación mediante Windows Server 2022, actúa como nodo de respaldo, contingencia y servicios complementarios. Se encuentra totalmente integrado con Azure Active Directory, lo que permite:



Nº SC735-1



- Sincronización de identidades.
- Autenticación híbrida y segura.
- Políticas avanzadas de acceso.
- Copias de seguridad en la nube.
- Gestión centralizada de dispositivos.

Equipamiento del datacenter

Actualmente el centro de datos dispone de servidores físicos y virtuales que soportan los siguientes servicios internos de la Entidad:

- Servidor de red de voz (Telefonía IP).
- Servidor de red de datos y administración de VLAN.
- Controlador de dominio y controlador de dominio alterno.
- Servidor de virtualización para aplicaciones internas: Centro de Pensamiento y otros servicios en Linux.
- Servidor de bases de datos PostgreSQL y SQL Server.
- Servidor de archivos institucional.
- Servidor de impresión.
- Servidor de Mesa de Ayuda.
- Sistema de backups automáticos y recuperación ante desastres (DRP).

Servicios críticos alojados en la nube

Bajo el esquema de modernización del “Ecosistema de Gestión Informática Modernizado”, los siguientes servicios operan actualmente 100% en la nube, garantizando alta disponibilidad, seguridad, replicación geográfica y escalabilidad:

- SIP – Sistema de Información Misional
- Personería en Línea
- Intranet Institucional
- Página Web Institucional
- Sistema de PQRSD en Línea
- Sistema de Citas en Línea



N° SC735-1



- Moodle – Plataforma de Formación Ciudadana
- Exchange Online (correo institucional)
- SharePoint (Sistema Integrado de Gestión)

Seguridad y Contingencia:

Para garantizar la seguridad de la red, los sistemas de información y el centro de datos de la Personería Distrital de Medellín, la Entidad cuenta con una arquitectura de seguridad robusta basada en dispositivos Fortinet, controles de acceso, políticas del SGSI y medidas de continuidad operativa.

• FortiGate (NGFW – Firewall de Nueva Generación):

El FortiGate es el componente central de seguridad perimetral y de red. Ofrece control de aplicaciones, prevención de intrusiones (IPS), antivirus, antimalware, antispam, filtrado web, inspección de tráfico cifrado, seguridad P2P y mitigación de ataques.

El FortiGate administra de manera centralizada el **DHCP institucional**, lo que permite controlar todos los dispositivos que se conectan a la red, aplicar políticas por segmentos (VLAN), implementar Zero Trust a nivel de acceso y garantizar trazabilidad completa.

Con este dispositivo, la Entidad está protegida contra ransomware, sitios maliciosos, fugas de información, ataques externos, navegación no autorizada y amenazas perimetrales.

• FortiWeb (WAF – Web Application Firewall):

Es el sistema encargado de proteger las aplicaciones web institucionales como la página web, Personería en Línea, SIP (cuando aplica vía web), intranet y sistemas expuestos a internet.

El enfoque multicapa de FortiWeb protege las aplicaciones contra las vulnerabilidades más comunes establecidas en el OWASP Top 10 y amenazas avanzadas como inyección SQL, cross-site scripting, bots maliciosos,



N° SC735-1



desbordamientos de búfer, manipulación de cookies, URL sospechosas y ataques DDoS.

FortiWeb utiliza inteligencia de amenazas actualizada proveniente de FortiGuard Labs, lo que asegura la detección temprana de vulnerabilidades y ataques sofisticados.

• **FortiEDR (Endpoint Detection and Response):**

El EDR monitorea de manera continua todos los equipos de escritorio, portátiles y dispositivos conectados a la red institucional para detectar comportamientos sospechosos, bloquear ataques y realizar contención automática en caso de incidentes.

Esta solución evita que los ciberdelincuentes utilicen equipos de los funcionarios como puerta de entrada a los sistemas internos.

FortiEDR proporciona visibilidad completa de los endpoints, análisis en tiempo real y respuesta automatizada frente a ransomware, ataques de día cero, ejecución de código malicioso y explotación de vulnerabilidades.

• **Protección del Servidor de Archivos Institucional:**

La Personería cuenta con un servidor de archivos con capacidad de 40 TB destinado a almacenar información crítica, incluyendo:

- ✓ Máquinas virtuales y discos duros virtuales.
- ✓ Bases de datos institucionales.
- ✓ Carpeta de “Digitales” utilizada por Gestión Documental.
- ✓ Archivo histórico de funcionarios.
- ✓ Instaladores de software, licencias y herramientas internas.
- ✓ Sistema Integrado de Gestión (SIG).
- ✓ Unidad lógica R asignada a cada funcionario.



N° SC735-1



- ✓ Registros multimedia y respaldos de sistemas.

Todas las carpetas están protegidas mediante **permisos de acceso por roles**, garantizando que solo el propietario o los administradores puedan acceder a la información. Esto asegura la confidencialidad, integridad y disponibilidad de los datos institucionales.

- **Backups Diario de Información Crítica:**

La información almacenada en el servidor de archivos tiene un tratamiento de respaldo diario.

Los backups se almacenan en medios seguros, cifrados y únicamente restaurables mediante claves autorizadas, asegurando continuidad operativa ante incidentes, desastres o pérdidas de información.

Estos respaldos garantizan la recuperación rápida y completa de datos críticos en caso de fallas o ataques cibernéticos.

- **Seguridad Física del Centro de Datos:**

La Personería cuenta con controles de seguridad física que incluyen:

- ✓ Sistemas de control de acceso en la puerta principal, acceso al parqueadero y acceso al centro de datos.
- ✓ Sistema de CCTV en la sede central.
- ✓ Sistema de alimentación ininterrumpida (UPS).
- ✓ Sistema de detección de incendios.
- ✓ Sistema eléctrico independiente.
- ✓ Aire de precisión para mantener condiciones ambientales óptimas.

Estas medidas aseguran la operación estable del centro de datos y evitan riesgos físicos que puedan comprometer los servicios institucionales.

Conectividad.



N° SC735-1



La Personería Distrital de Medellín cuenta con una infraestructura de conectividad moderna, estable y segura, diseñada para garantizar el funcionamiento continuo de los procesos misionales, administrativos y de atención ciudadana. Para ello, se dispone de enlaces dedicados de alta capacidad, redes segmentadas, conectividad LAN to LAN y servicios especializados según las necesidades de cada sede.

La Entidad cuenta con un canal principal de **500 Mb de navegación dedicada en fibra óptica**, lo que permite una operación eficiente de los servicios alojados en la nube, acceso a plataformas institucionales, comunicaciones internas, videoconferencias y sistemas misionales.

Las sedes alternas (UPDH y Centro Administrativo La Alpujarra) están conectadas mediante enlaces **LAN to LAN de 30 Mb**, garantizando un flujo seguro y estable de información. Adicionalmente, se dispone de un enlace LAN to LAN independiente con la Alcaldía de Medellín, lo que permite el acceso directo al sistema **SAP – Gestión Financiera y Gestión de Bienes Administrativos**, facilitando la gestión de recursos, ejecución presupuestal y procesos administrativos de manera rápida, oportuna y segura.

La red institucional se encuentra estructurada mediante cableado de cobre categoría 6 en todas las sedes, permitiendo una conexión estable para los funcionarios y equipos de trabajo. La Entidad cuenta con una red **WiFi totalmente separada de la red LAN**, con redes independientes para:

- Funcionarios
- Equipos misionales
- Ciudadanía y visitantes (portal cautivo)

El portal cautivo permite controlar el acceso a internet para usuarios externos, registrando actividad y aplicando políticas de seguridad.

El **Despacho del Personero** cuenta con una conexión **independiente y aislada** del resto de la red institucional, garantizando mayor seguridad, privacidad y control de la información sensible manejada por esta dependencia.

La navegación e ingreso a internet están protegidos por un **firewall Fortinet (FortiGate)**, desde donde se administran políticas de seguridad y navegación, incluyendo:

- ✓ Bloqueo de categorías de contenido no permitido (ej. contenido para adultos).



N° SC735-1



- ✓ Filtrado de URL y protección contra ataques web.
- ✓ Inspección profunda de tráfico cifrado mediante SSL Inspection.
- ✓ Control granular de aplicaciones web.
- ✓ Prevención de intrusiones (IPS).
- ✓ Protección antimalware y antiphishing.

Este conjunto de mecanismos permite garantizar una conectividad segura, confiable y alineada con las políticas del SGSI y los lineamientos de Gobierno Digital.

Hardware equipos de escritorio y portátiles:

Para garantizar el cumplimiento de su misión institucional y la ejecución de los objetivos estratégicos, la Personería Distrital de Medellín ha adelantado un proceso de modernización integral de su plataforma tecnológica, orientado a asegurar continuidad, eficiencia operativa, seguridad digital y calidad en la prestación de los servicios a la ciudadanía y a los funcionarios.

En el marco de esta modernización, durante los años 2024 y 2025 se realizó la **renovación de 295 equipos de escritorio**, los cuales cuentan con especificaciones técnicas avanzadas que permiten soportar las herramientas institucionales, sistemas misionales basados en la nube, plataformas de productividad y aplicaciones de seguridad digital. Cada uno de estos equipos cuenta con:

- ✓ Discos de estado sólido (SSD), lo que garantiza tiempos rápidos de arranque, mayor rendimiento y confiabilidad.
- ✓ 32 GB de memoria RAM, optimizando el desempeño en sistemas misionales, aplicaciones en la nube y multitarea avanzada.
- ✓ Fuente energética protegida mediante UPS para asegurar continuidad ante fluctuaciones eléctricas.

Además de la renovación de los equipos de escritorio, la Entidad dispone de un parque tecnológico compuesto por computadores HP y Lenovo, tanto de escritorio como portátiles, destinados a las diferentes áreas misionales, administrativas, disciplinarias y de atención al ciudadano. Esta infraestructura permite el funcionamiento estable de los sistemas institucionales, herramientas de colaboración y servicios digitales, asegurando que los funcionarios cuenten con los



N° SC735-1



recursos necesarios para cumplir con sus responsabilidades y brindar atención oportuna a la ciudadanía.

La modernización del hardware es un componente fundamental del “Ecosistema de Gestión Informática Modernizado”, dado que soporta la operación de servicios en la nube, mantiene la compatibilidad con plataformas como Microsoft 365, SIP, Personería en Línea, SAP (vía LAN to LAN) y garantiza un desempeño óptimo en entornos de seguridad reforzada bajo arquitectura Fortinet.

Mantenimiento

El proceso de mantenimiento de la infraestructura tecnológica de la Personería Distrital de Medellín es realizado por el personal del área de Innovación y Conocimiento, garantizando la continuidad operativa, el desempeño óptimo de los sistemas y la seguridad de la información. Las actividades de mantenimiento se llevan a cabo mediante dos modalidades principales:

✓ Mantenimiento directo en el centro de datos:

El equipo técnico puede realizar intervenciones físicas sobre los servidores, equipos de red y dispositivos críticos utilizando el sistema KVM instalado en el datacenter. Esto permite gestionar de manera centralizada la administración de los servidores Windows Server 2022, la infraestructura virtualizada, los controladores de dominio, el servidor de archivos y los equipos asociados a la operación interna.

✓ Mantenimiento remoto seguro:

A través de conexiones remotas autorizadas, protegidas por autenticación multifactor y controles del firewall FortiGate, el personal puede realizar mantenimiento en servidores, equipos de red, sistemas en la nube, plataformas Microsoft 365, Azure AD, FortiWeb, FortiEDR, y demás servicios institucionales. Esta modalidad permite una respuesta ágil ante incidentes, actualizaciones, despliegue de parches de seguridad, administración de VLAN, monitoreo y respaldo de los sistemas.

El modelo de mantenimiento se ejecuta bajo estándares de seguridad definidos por el SGSI, aplicando controles técnicos como registro de auditoría, administración por perfiles, segmentación por VLAN, y políticas de



N° SC735-1



acceso seguro. Estas prácticas permiten garantizar la integridad, disponibilidad y confiabilidad de los sistemas institucionales y la continuidad del servicio a funcionarios y ciudadanía.

6.1.3. Planificación y Gestión Tecnológica

La Personería Distrital de Medellín ha consolidado una estrategia de planificación y gestión tecnológica que permite asegurar la modernización continua de la infraestructura, el fortalecimiento de la seguridad digital, la gestión eficiente de los recursos y la operación estable de los servicios institucionales. Esta planificación se articula con el Plan Estratégico Institucional 2024–2028 y con el Proyecto “Ecosistema de Gestión Informática Modernizado”.

Desde el año 2016 y durante los planes operativos ejecutados hasta 2023, la Entidad desarrolló actividades orientadas a la renovación de equipos, adquisición de servidores, implementación de sistemas de información, fortalecimiento de la seguridad tecnológica, mantenimiento del centro de datos y renovación de licenciamientos. Sobre esta base, entre los años **2024 y 2025** la Personería ha avanzado de manera significativa en la actualización de su plataforma tecnológica, incluyendo:

- Modernización de 295 equipos de escritorio con discos SSD, 32 GB de RAM y UPS individual.
- Implementación de red de impresión propia de impresoras, mantenimiento eléctrico, climatización, red de datos y datacenter.
- Adopción de infraestructura híbrida basada en Windows Server 2022 y Azure Active Directory.
- Consolidación de servicios en la nube: SIP, Personería en Línea, PQRSD, Citas en Línea, Intranet, SharePoint y Exchange.
- Fortalecimiento del ecosistema de seguridad con FortiGate, FortiWeb y FortiEDR.
- Segmentación total de la red mediante VLAN e implementación operativa de IPv6.
- Capacitación a funcionarios en sistemas misionales, servicios digitales, Microsoft 365 y políticas del SGSI.



N° SC735-1



Planificación Tecnológica 2024–2028

En el marco de esta modernización, para el periodo **2024–2028** la Personería orienta su planificación tecnológica hacia líneas estratégicas que permiten ampliar capacidades, garantizar la continuidad operativa, fortalecer la seguridad, consolidar la conectividad y avanzar hacia el uso de tecnologías emergentes:

- Evolución del SIP hacia SIP 2.0 con arquitectura moderna en la nube.
- Consolidación del ecosistema digital: Personería en Línea, PQRSD, Biblioteca Digital y Moodle.
- Fortalecimiento de la infraestructura cloud y de la integración con Azure.
- Optimización de procesos internos mediante automatización y servicios digitales.
- Implementación de capacidades avanzadas de analítica e interoperabilidad mediante API institucional.
- Implementación progresiva del modelo Zero Trust.
- Renovación continua del parque tecnológico para garantizar rendimiento, compatibilidad y seguridad.
- Mantenimiento de redes, VLAN, conexiones LAN to LAN y fibra óptica con 500 Mb de navegación dedicada.

Pilotos de Inteligencia Artificial (2024–2028)

Como parte del fortalecimiento del ecosistema tecnológico, la Personería desarrollará entre los años **2024 y 2028** proyectos piloto de Inteligencia Artificial utilizando modelos existentes que pueden ser entrenados con información institucional para casos de uso específicos. Estos pilotos permitirán explorar aplicaciones como:

- Clasificación automática de documentos y comunicaciones.
- Análisis predictivo de cargas de atención y tipos de casos.
- Asistencia virtual para orientación ciudadana.
- Automatización de tareas repetitivas internas.
- Búsqueda inteligente en el SIG y repositorios institucionales.



N° SC735-1



- Soporte técnico automatizado para la mesa de ayuda.

Todos los pilotos de IA se desarrollarán bajo principios de seguridad, ética, protección de datos personales y cumplimiento del SGSI.

Consumo, análisis y seguridad de la información

La Entidad cuenta con procesos para el consumo, análisis y aprovechamiento de la información mediante herramientas de reporte, controles de seguridad, roles, cifrado, políticas de acceso, antivirus, firewall, filtrado de sitios web y auditoría permanente. Se utilizan mecanismos modernos para garantizar calidad, seguridad, privacidad, trazabilidad e integridad de la información almacenada en los sistemas institucionales.

Equipo humano para la gestión tecnológica

El proceso de Innovación y Conocimiento cuenta con un equipo especializado conformado por:

- Técnicos en sistemas
- Tecnólogo en sistemas
- Ingeniero desarrollador
- Dos ingenieros de sistemas
- Auxiliar administrativo

Este equipo es responsable de la administración, mantenimiento y actualización de la infraestructura tecnológica, hardware, software, servicios cloud, seguridad Fortinet, Microsoft 365, plataformas institucionales y sistemas misionales.

La gestión tecnológica se desarrolla mediante un enfoque de mejora continua, priorización estratégica, y alineación con los lineamientos de Gobierno Digital y del Sistema de Gestión de Seguridad de la Información.

6.2. Uso y Apropiación de la Tecnología



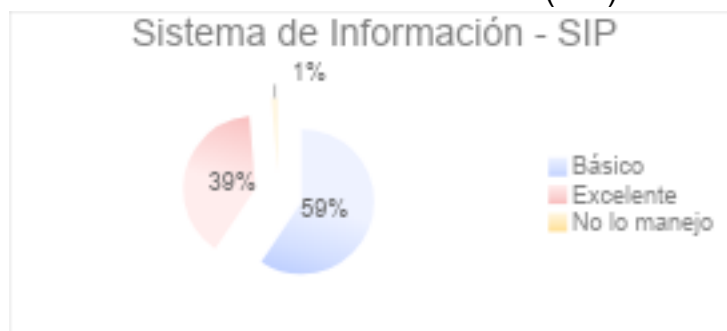
N° SC735-1



A continuación, se muestra el análisis producto del resultado de la encuesta, teniendo en cuenta que se envió la encuesta a los 100 funcionarios de planta, de libre nombramiento y remoción de los cuales se obtuvo respuesta del 74%, con los siguientes resultados:

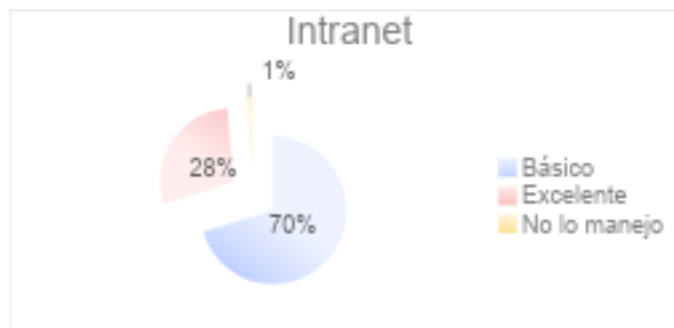
Qué nivel de dominio considera que posee en los siguientes sistemas e información o aplicativos:

- Aplicativo Web misional Sistemas de Información (SIP)



En el Aplicativo Web Sistemas de Información de la Personería (SIP), el 39% considera que posee un nivel de dominio excelente, el 60% considera que los domina en sus funciones básicas y solo un 1% indicó que no maneja o no usa esta aplicación en sus actividades. Estos resultados indican que se debe reforzar la capacitación para llegar a un mejor dominio en la herramienta misional.

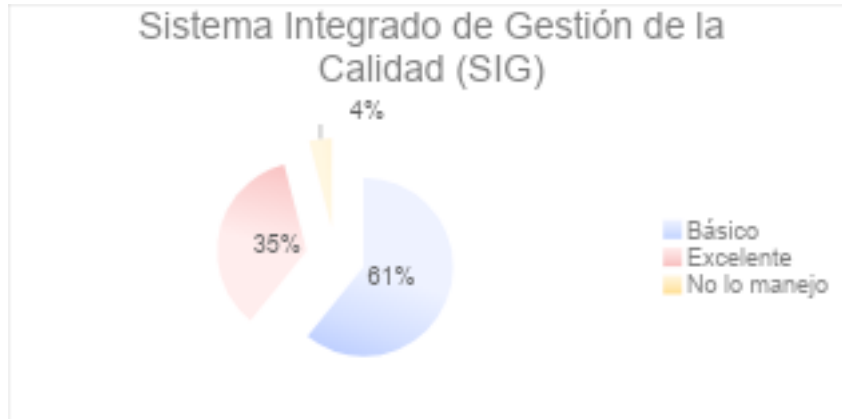
- Aplicativo Web Intranet



En el aplicativo web Intranet, se observa que solo un 1% de los encuestados no manejan esta aplicación, el 70% posee un dominio básico y el 29% excelente, es

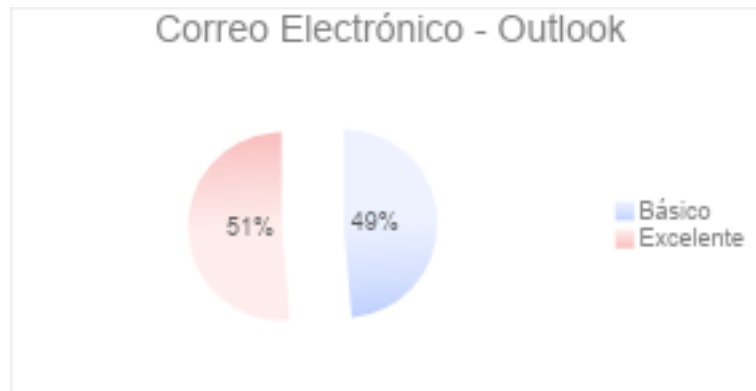
decir, la mayoría de los encuestados indicaron conocer y dominar esta herramienta web.

- **Aplicativo Web Sistema Integrado de Gestión (SIG)**



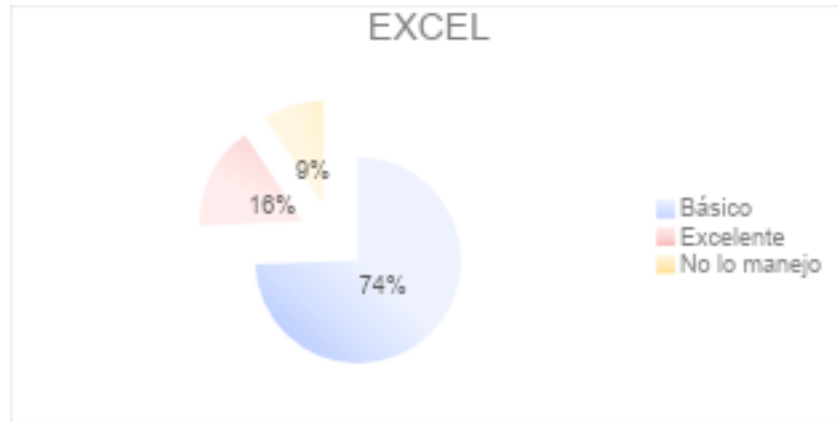
En el aplicativo **SIG**, se observa que la mayoría de los encuestados dominan esta herramienta con un 61% en nivel básico.

- **Aplicación correo electrónico Outlook**



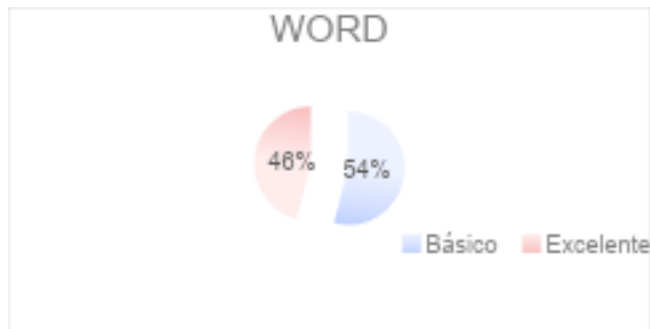
En cuanto a esta herramienta se observa que un gran porcentaje de los funcionarios dominan esta herramienta de correo electrónico, con un mayor porcentaje de excelente manejo de la herramienta.

- **Herramienta ofimática Excel**



En esta herramienta la encuesta indica que un 74% la dominan en un nivel básico, un 16% la dominan excelentemente y el 10% no la manejan, esto nos indica que se debe de crear campaña de capacitación en esta herramienta que ayuden a fortalecer la apropiación y un mejor dominio.

- Herramienta Ofimática Word



En esta herramienta indica que es una de las que más manejan los funcionarios, un 54% posee un dominio excelente y el otro 46% a un nivel básico.

En conclusión, se debe realizar mejoras para aumentar el porcentaje de dominio y usabilidad de las herramientas informáticas, así como procurar que sean más amigables para promover más el uso y manejo de la información.

6.3. Sistemas de Información

La Personería Distrital de Medellín cuenta con un conjunto de sistemas de información organizados según su función, los cuales soportan los procesos



N° SC735-1





misionales, administrativos, estratégicos y de seguridad de la Entidad. Estos sistemas permiten garantizar la atención ciudadana, la defensa de los derechos humanos, la vigilancia de la conducta oficial y la gestión interna institucional.

• Sistemas de Apoyo:

Incluyen las herramientas administrativas, de gestión documental, correo institucional, SharePoint (Sistema Integrado de Gestión), Microsoft 365, SAP (vía LAN to LAN), intranet, mantenimiento de activos, mesa de ayuda y demás aplicaciones de soporte interno.

• Sistemas de Seguridad:

Comprenden los sistemas que protegen la infraestructura tecnológica y los datos institucionales, tales como FortiGate, FortiWeb, FortiEDR, autenticación con Azure AD, sistemas de backup, administración de roles, auditoría y los controles definidos por el SGSI.

Arquitectura de Sistemas de Seguridad – Personería Distrital de Medellín

La siguiente arquitectura describe los componentes de seguridad implementados en la Personería Distrital de Medellín, incluyendo seguridad perimetral, seguridad de aplicaciones, protección de endpoints, autenticación, auditoría y respaldo de información.

Componente	Descripción
FortiGate (Firewall NGFW)	Control perimetral, IPS, filtrado web, DHCP centralizado, segmentación VLAN y políticas de acceso.
FortiWeb (WAF)	Protección de aplicaciones web y APIs contra OWASP Top 10, bots maliciosos y ataques DDoS.
FortiEDR	Protección avanzada de endpoints, análisis continuo,



Nº SC735-1



	detección y contención automática de amenazas.
Azure Active Directory	Autenticación, identidades, MFA, políticas Zero Trust y gestión de accesos.
Sistemas de Backup	Copias de seguridad cifradas, almacenamiento seguro, recuperación ante desastres.
Auditoría y Registros	Monitoreo de logs, seguimiento de eventos, trazabilidad y cumplimiento SGSI.
Administración de Roles	Gestión de permisos, reglas de acceso y segregación de funciones.
SGSI	Políticas y controles basados en ISO 27001 para la seguridad institucional.

• **Sistemas Misionales:**

Corresponden a los sistemas utilizados directamente para la atención a la ciudadanía y el ejercicio misional de la Entidad. Entre ellos se encuentran:

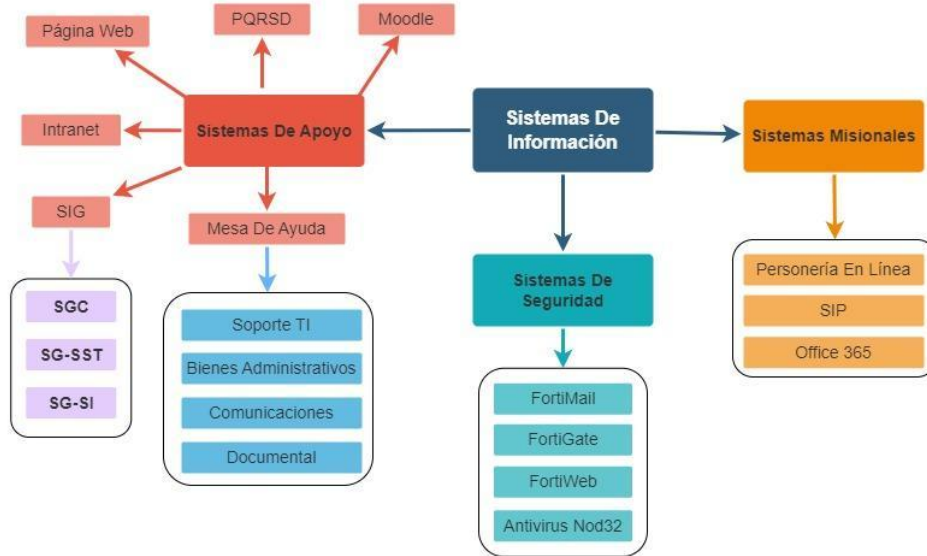
SIP – Sistema de Información Misional, Personería en Línea, Sistema de Citas en Línea, Sistema de PQRSD, Moodle para formación ciudadana, portal web institucional y otros servicios digitales orientados a facilitar el acceso a la justicia preventiva y la defensa de los derechos humanos.



N° SC735-1



Arquitectura Sistemas De Información



A continuación, se describen cada uno de los sistemas asociados a cada categoría:

6.3.1. Sistemas de información

Nombre	Sistema de Información SIP
Líder Funcional	Ingeniero de Sistemas
Descripción	Sistema misional en la nube para atención ciudadana, gestión documental, correspondencia, talento humano, proyectos y actividades.
Módulos	Atención y Reparto, Talento Humano, Gestión Documental, Correspondencia, Actividades, Proyectos, Activos.
Tipo de Sistema	Web en la nube
Motor de Bases de Datos	PostgreSQL
Sistema Operativo	Linux 64 bits



N° SC735-1



Grado de Aceptación	Muy buena
Fortalezas	Trazabilidad, integración, disponibilidad.
Debilidades	Requiere modernización de módulos heredados.
Recomendaciones	Migración completa a SIP 2.0 y depuración de datos.

Nombre	Personería en Línea
Líder Funcional	Ingeniero de Sistemas
Descripción	Plataforma digital para servicios ciudadanos: tutelas, peticiones, asesorías, consultas y atención virtual.
Módulos	Tutelas, Derechos de Petición, Desacatos, Conciliaciones, Reacción Inmediata, Asesoría.
Tipo de Sistema	Web en la nube
Motor de Bases de Datos	MySQL
Sistema Operativo	Linux 64 bits
Grado de Aceptación	Muy buena
Fortalezas	Acceso ciudadano 24/7, trazabilidad.
Debilidades	Debe ampliarse cobertura funcional.
Recomendaciones	Integración completa con SIP y analítica.

Nombre	Citas en Línea
Líder Funcional	Ingeniero de Sistemas
Descripción	Sistema para agendamiento de citas con abogados de la Personería.



N° SC735-1



Módulos	Agendamiento, Confirmación, Gestión de citas.
Tipo de Sistema	Web
Motor de Bases de Datos	Microsoft 365
Sistema Operativo	Microsoft 365
Grado de Aceptación	Excelente
Fortalezas	Agilidad, reducción de filas.
Debilidades	Faltan reportes avanzados.
Recomendaciones	Integración con SIP.

Nombre	Sistema PQRSD
Líder Funcional	Ingeniero de Sistemas
Descripción	Sistema para radicación, trazabilidad y gestión de peticiones, quejas, reclamos, denuncias y sugerencias.
Módulos	Registro, Gestión, Respuesta.
Tipo de Sistema	Web
Motor de Bases de Datos	MySQL
Sistema Operativo	Linux
Grado de Aceptación	Excelente
Fortalezas	Trazabilidad completa.
Debilidades	Apropiación de usuarios.
Recomendaciones	Capacitaciones continuas.

Nombre	Moodle – Capacitación Online
Líder Funcional	Ingeniero de Sistemas
Descripción	Plataforma virtual para cursos, talleres, capacitaciones y certificaciones.
Módulos	Foros, Cursos, Evaluaciones, Cuestionarios, Certificados.



N° SC735-1



Tipo de Sistema	Web
Motor de Bases de Datos	MySQL
Sistema Operativo	Linux
Grado de Aceptación	Muy buena
Fortalezas	Amplia capacidad formativa.
Debilidades	Falta personal dedicado.
Recomendaciones	Formación interna y nuevos cursos.

Nombre	Microsoft 365
Líder Funcional	Ingeniero de Sistemas
Descripción	Suite de productividad en la nube: correo, almacenamiento, reuniones y colaboración.
Módulos	Outlook, Teams, Word, Excel, OneDrive, SharePoint.
Tipo de Sistema	Cloud
Motor de Bases de Datos	N/A
Sistema Operativo	Cloud
Grado de Aceptación	Excelente
Fortalezas	Transformación digital.
Debilidades	Limitación de licencias.
Recomendaciones	Ampliación gradual de licencias.

Nombre	Sistema Integrado de Gestión (SIG)
Líder Funcional	Ingeniero de Sistemas
Descripción	Sistema para la gestión de calidad, SG-SST y SGSI soportado en SharePoint.
Módulos	Calidad, SST, Seguridad de la Información.
Tipo de Sistema	Apoyo



N° SC735-1



Motor de Bases de Datos	SharePoint Online
Sistema Operativo	Cloud
Grado de Aceptación	Excelente
Fortalezas	Control documental robusto.
Debilidades	Carga de formatos lenta.
Recomendaciones	Optimizar flujos y automatizaciones.

Nombre	Intranet Corporativa
Líder Funcional	Ingeniero de Sistemas
Descripción	Portal interno para documentos, trámites, comunicaciones y sistemas de apoyo.
Módulos	Archivo, Noticias, Biblioteca Jurídica, Manuales.
Tipo de Sistema	Apoyo
Motor de Bases de Datos	MySQL
Sistema Operativo	Linux
Grado de Aceptación	Excelente
Fortalezas	Confiabilidad.
Debilidades	Poca apropiación.
Recomendaciones	Mayor divulgación interna.

Nombre	Mesa de Ayuda
Líder Funcional	Ingeniero de Sistemas
Descripción	Sistema para solicitudes e incidentes internos.
Módulos	Registro, Gestión, Respuesta.
Tipo de Sistema	Apoyo
Motor de Bases de Datos	MySQL
Sistema Operativo	Linux
Grado de Aceptación	Excelente



N° SC735-1



Fortalezas	Eficiencia en requerimientos.
Debilidades	Apropiación parcial.
Recomendaciones	Capacitaciones periódicas.

Nombre	Firewall FortiGate
Líder Funcional	Ingeniero de Sistemas
Descripción	NGFW con IPS, filtrado web, antivirus, firewall, control de aplicaciones.
Módulos	IPS, Control Aplicaciones, Filtrado Web, Antivirus.
Tipo de Sistema	Seguridad UTM
Motor de Bases de Datos	N/A
Sistema Operativo	FortiOS
Grado de Aceptación	Excelente
Fortalezas	Seguridad y control.
Debilidades	Requiere HA.
Recomendaciones	Implementar alta disponibilidad.

Nombre	Firewall FortiWeb
Líder Funcional	Ingeniero de Sistemas
Descripción	Protección de aplicaciones web y APIs contra OWASP Top 10.
Módulos	WAF, Antibot, Anti-DDoS.
Tipo de Sistema	Seguridad Web
Motor de Bases de Datos	N/A
Sistema Operativo	FortiOS
Grado de Aceptación	Excelente
Fortalezas	Protección avanzada.
Debilidades	Sin HA.
Recomendaciones	Implementar redundancia.

Nombre	FortiEDR
Líder Funcional	Ingeniero de Sistemas
Descripción	Protección avanzada de endpoints con monitoreo continuo.
Módulos	Análisis, Detección, Respuesta.
Tipo de Sistema	Seguridad Endpoint
Motor de Bases de Datos	N/A
Sistema Operativo	Cloud
Grado de Aceptación	Excelente
Fortalezas	Prevención y contención.
Debilidades	Requiere capacitación.
Recomendaciones	Formación especializada.

6.4. Servicios Tecnológicos

La gestión de los servicios tecnológicos de la Personería Distrital de Medellín es administrada por el proceso de Innovación y Conocimiento, adscrito al proceso de Planificación Institucional. Su responsabilidad principal es garantizar la operación continua, estable y segura de la infraestructura tecnológica y de los sistemas de información institucionales, asegurando la prestación del servicio a la ciudadanía las veinticuatro (24) horas del día, los trescientos sesenta y cinco (365) días del año.

La administración y operación de la plataforma tecnológica está a cargo del equipo técnico compuesto por ingenieros de sistemas, desarrolladores, técnicos y tecnólogos en informática, y un auxiliar administrativo. Cada perfil cumple funciones especializadas en la gestión diaria de la infraestructura, aplicaciones, seguridad y soporte:

- **Ingeniero de Sistemas Especialista:** responsable de la administración del centro de datos, servidores físicos y virtuales, servicios en la nube, integración con Azure AD, arquitectura de red, seguridad Fortinet, continuidad del negocio y coordinación general del proceso.



N° SC735-1



- **Ingeniero de Sistemas:** encargado de la administración de aplicaciones institucionales (SIP, Personería en Línea, PQRSD, Citas en Línea, Moodle, Intranet), administración de la red de voz y datos, soporte a sedes satélite, manejo de bases de datos y acompañamiento a procesos misionales.
- **Desarrolladores en sitio:** responsables del análisis, desarrollo y mejora continua de sistemas internos, actualización de módulos del SIP, integración con servicios en la nube, automatizaciones, construcción de APIs, soporte de software, desarrollo de nuevas funcionalidades y atención de requerimientos técnicos de sistemas. Este rol es clave para la modernización SIP 2.0 y la evolución de los servicios digitales (Personería en Línea, Citas, PQRSD, Intranet y SIG).
- **Técnicos y Tecnólogos en Informática:** encargados del soporte a usuario final, instalación de software y hardware, configuración de equipos, mantenimiento básico, despliegues, soporte a sedes satélite, acompañamiento en capacitaciones y gestión operativa del parque tecnológico.
- **Auxiliar Administrativo:** apoya la gestión documental del proceso, manejo de inventarios tecnológicos, seguimiento de solicitudes, atención de proveedores y soporte administrativo a los proyectos de TI.

Como estrategia de **continuidad del negocio**, se realiza un mantenimiento semanal a los sistemas operativos de servidores, bases de datos, infraestructura de red, sistemas virtualizados y elementos de ciberseguridad (FortiGate, FortiWeb, FortiEDR), asegurando estabilidad y protección continua. El soporte a usuarios se gestiona mediante la Mesa de Ayuda institucional, donde se registran solicitudes, incidentes y requerimientos de manera ordenada y trazable.

El servicio de impresión institucional, garantiza el soporte permanente y los repuestos y consumibles requeridos para el correcto funcionamiento de la red de impresión.



N° SC735-1



La infraestructura tecnológica opera en un centro de datos aislado de la oficina principal, con aire de precisión, UPS, monitoreo ambiental, y un sistema de respaldo de climatización para asegurar condiciones óptimas de funcionamiento.

La Entidad cuenta con un **ambiente aislado de pruebas**, con servidores y bases de datos independientes, donde se realizan ajustes, desarrollos y validaciones antes de pasarlos a producción, garantizando estabilidad, calidad y disminución de riesgos técnicos.

6.5. Gestión de la Información

La gestión de la información en la Personería Distrital de Medellín es liderada por el proceso de Innovación y Conocimiento, el cual ha venido consolidando prácticas y controles que aseguran la calidad, integridad, disponibilidad, trazabilidad y seguridad de los datos institucionales. La información almacenada en los sistemas misionales y de apoyo es administrada bajo políticas del SGSI, controles de seguridad Fortinet, auditorías periódicas y mecanismos de validación en cada uno de los sistemas de información.

Los sistemas institucionales requieren la captura de datos precisos y estandarizados, lo que permite generar información confiable, consistente y de alto valor para la gestión misional, la atención a la ciudadanía, la vigilancia administrativa, la toma de decisiones y la elaboración de reportes estadísticos. La Personería ha avanzado en la consolidación de un modelo de gestión de datos basado en calidad, gobernanza y seguridad, que soporta el análisis de información en tiempo real y la construcción del Plan Estadístico Institucional.

La caracterización de la gestión de la información se realiza mediante el enfoque del **Proceso de Producción de Información Estadística (PPI)**, el cual agrupa las actividades relacionadas con la planeación, diseño, captura, almacenamiento, procesamiento, análisis, difusión y acceso a datos de tipo cuantitativo y cualitativo. De forma complementaria, se utiliza el concepto de **Operación Estadística (OE)**, definido como el conjunto de actividades que, a partir de la recolección sistemática de datos, conduce a la producción de información agregada útil para la gestión institucional.



N° SC735-1



Figura 1: Modelo de producción de información (MPI)



Fuente: DANE

La OE está compuesta por cinco procesos fundamentales:

- **Detección y análisis de requerimientos:** identificación de necesidades de información de las áreas misionales, administrativas, de control y atención al ciudadano.
- **Diseño:** definición de instrumentos, flujos de captura, validaciones y estructura de datos.
- **Producción:** recolección sistemática de información mediante SIP, Personería en Línea, PQRSD, Citas en Línea, SIG y demás plataformas institucionales.
- **Análisis:** procesamiento, depuración, consolidación y transformación de datos para generación de estadísticas, reportes y análisis misionales.
- **Difusión:** entrega de resultados a dependencias internas, entes de control, ciudadanía y publicación de datos en los mecanismos oficiales.

El análisis de estos cinco procesos permitió identificar la situación actual de la producción y uso de información en la Entidad, así como proponer acciones de mejora orientadas a fortalecer la calidad de los datos, la interoperabilidad entre sistemas y la analítica institucional. Estas acciones se incorporan en el Plan de Acción del PETI y se articulan con:

- La modernización del SIP hacia una versión orientada a datos (SIP 2.0).
- La operación en la nube de los sistemas misionales y de apoyo.
- La consolidación del SIG en SharePoint.
- La implementación del API institucional y el modelo de interoperabilidad.
- El uso de herramientas analíticas para la toma de decisiones.



N° SC735-1



- La depuración y estandarización de información histórica.
- La adopción de prácticas de Gobierno de Datos y Gobierno Digital.

La gestión de la información se convierte así en un habilitador fundamental para el cumplimiento de la misión institucional, la defensa de los derechos humanos, la vigilancia de la conducta oficial y la mejora continua de los servicios prestados a la ciudadanía.

6.5.1. Análisis de Demanda de información

Desde el año 2014 la Personería Distrital de Medellín adoptó PostgreSQL como base de datos principal para el almacenamiento de la información misional del Sistema de Información SIP. Esta base de datos, actualmente alojada en infraestructura en la nube, presenta un crecimiento estable y controlado, lo cual permite proyectar una alta disponibilidad de almacenamiento para los próximos años.

A pesar de la cantidad de información que se genera diariamente —en promedio 400 ciudadanos atendidos por día— el consumo real de almacenamiento es bajo en relación con la capacidad total disponible. Este comportamiento evidencia que la infraestructura es suficiente y está preparada para la expansión futura de los sistemas misionales, especialmente con la evolución hacia SIP 2.0.

Descripción: Tamaño BD SIP

Tamaño en GB: 40.000Gb

Capacidad disponible: 2Tb

Estos datos representan un consumo aproximado del **0,47 %** del total, lo que evidencia un amplio margen para crecimiento, integración de nuevos módulos y almacenamiento histórico.

En cuanto al consumo y análisis de la información, la Entidad utiliza herramientas como Excel, Power BI y consultas directas a la base de datos, las cuales permiten la construcción de tablas dinámicas, dashboards, reportes estadísticos y análisis de datos para la toma de decisiones. Sin embargo, se ha identificado que varios



N° SC735-1



funcionarios y contratistas presentan limitaciones en el manejo avanzado de estas herramientas, lo cual dificulta el aprovechamiento pleno de la información disponible. Este hallazgo se traduce en una acción del PETI orientada a fortalecer las capacidades analíticas mediante capacitación en el uso de MS Excel, Power BI y herramientas de consulta.

Respecto a las aplicaciones de apoyo institucional —Página Web, Intranet Corporativa, Sistema Integrado de Gestión (SIG), Plataforma Moodle, Personería en Línea, PQRSD, Citas en Línea y Mesa de Ayuda— estas utilizan MySQL como motor de base de datos. MySQL es una de las soluciones open source más robustas y ampliamente utilizadas a nivel mundial, lo que garantiza estabilidad, alta disponibilidad, compatibilidad con múltiples plataformas web y facilidad de integración con los sistemas institucionales.

El análisis de la demanda de información muestra que la Personería cuenta con capacidad técnica suficiente en almacenamiento, infraestructura de bases de datos y sistemas de apoyo; sin embargo, requiere fortalecer competencias de análisis de datos, consolidar modelos de interoperabilidad y avanzar hacia una analítica institucional más completa y oportuna.

6.6. Gobierno de TI

El Gobierno de Tecnologías de la Información en la Personería Distrital de Medellín es liderado por el proceso de Innovación y Conocimiento, el cual actualmente se encuentra ubicado en el nivel de apoyo. No obstante, conforme a la auditoría de calidad 2023 y a las necesidades actuales de la Entidad, se recomienda su traslado al **nivel estratégico**, dada su incidencia directa en la planificación institucional, la transformación digital, la gestión de riesgos tecnológicos, la seguridad de la información y la continuidad del negocio.

La Personería cuenta con un **Comité de Seguridad de la Información** activo, responsable de orientar y controlar proyectos, iniciativas y políticas asociadas al fortalecimiento de la infraestructura, la protección de datos, la seguridad digital, la gestión del riesgo y la operación tecnológica.



N° SC735-1



En el marco del Decreto 415 de 2016 y de las políticas de Gobierno Digital del MinTIC, se requiere formalizar la figura del **Líder de Tecnologías de la Información (LTI)**, encargado de dirigir los planes, programas y proyectos tecnológicos, definiendo estándares, priorizando iniciativas, gestionando riesgos, liderando la transformación digital y velando por el cumplimiento normativo.

Talento Humano y Roles Operativos

La operación tecnológica se realiza por un equipo compuesto por **Ingenieros de Sistemas, Desarrolladores, Técnicos, Tecnólogos y un Auxiliar Administrativo**, quienes llevan a cabo actividades alineadas con las necesidades actuales de la infraestructura híbrida (nube + datacenter), los sistemas de seguridad Fortinet, servicios Microsoft 365, SIP, Personería en Línea y demás plataformas institucionales.

Ingeniero de Sistemas – Administrador de la Plataforma Tecnológica

Responsable de la administración integral de la infraestructura:

- Administración del centro de datos (Windows Server 2022, almacenamiento, virtualización).
- Administración de sistemas en la nube (Azure AD, Exchange Online, SharePoint, SIP cloud).
- Administración de Moodle, Intranet, Personería en Línea, PQRSD y Citas en Línea.
- Gestión de la red de voz y datos, VLAN, IPv6 y WiFi segmentada.
- Coordinación de proyectos tecnológicos y actualización de servidores.
- Gestión de bases de datos PostgreSQL y MySQL (limpieza, reindexación, monitoreo).
- Gestión de sistemas Fortinet: FortiGate (DHCP, seguridad, IPS), FortiWeb (WAF), FortiEDR.
- Administración del sistema de backups, recuperación ante desastres y continuidad operativa.
- Actualización del SIP, creación de maestros, usuarios y roles según áreas.



N° SC735-1



- Revisión periódica de eventos de seguridad, auditorías internas y monitoreo de incidentes.
- Supervisión de contratos de infraestructura y soporte tecnológico.
- Acompañamiento técnico al SIG y proyectos como Cero Papel y Modernización SIP 2.0.

Ingeniero de Sistemas – Soporte y Administración de Aplicaciones

Encargado del soporte de tercer nivel en aplicaciones y equipos:

- Administración de sistemas institucionales y software corporativo.
- Instalación, configuración y despliegue de nuevos equipos de cómputo.
- Soporte en brigadas móviles, conciliaciones, UPDH y sedes externas.
- Diagnóstico y solución avanzada de incidentes.
- Administración de la red de impresión y proveedores externos de impresión.
- Soporte especializado en SIP, Personería en Línea, Office 365 y SIG.
- Inventario tecnológico, diagnósticos y revisión de fallas críticas.
- Acompañamiento técnico en audiencias, salas, equipos de audio y video.
- Hardening y actualización mensual de equipos institucionales.
- Capacitación a funcionarios en sistemas y automatización de oficina.

Desarrolladores en Sitio

Clave para la modernización 2024–2028:

- Desarrollo y actualización de módulos del SIP (camino hacia SIP 2.0).
- Integración de servicios mediante API institucional.
- Mejoras a Personería en Línea, PQRSD, Citas y sistemas de apoyo.
- Automatización de procesos internos.
- Integración con Azure AD y servicios cloud.
- Desarrollo de tableros y analítica avanzada.
- Participación en pilotos de Inteligencia Artificial desde 2024.
- Pruebas controladas en ambiente de desarrollo aislado.

Técnicos y Tecnólogos en Informática – Soporte de Primer y Segundo Nivel



N° SC735-1



Responsables del soporte operativo diario:

- Instalación, configuración y mantenimiento de equipos de escritorio y portátiles.
- Soporte en sedes internas, UPDH, conciliaciones y móviles.
- Administración de usuarios en Active Directory, SIP, Intranet, SIG y Moodle.
- Soporte en sistemas de impresión, escáneres, fotocopiadoras y salas de reunión.
- Seguimiento del cableado estructurado, cámaras y equipos audiovisuales.
- Gestión del EDR (detección, contención y acciones correctivas).
- Apoyo en instalación y migración de servidores.
- Capacitación a funcionarios en SIP, impresoras, scanners y herramientas ofimáticas.
- Realización de análisis básicos de datos para generación de reportes.

6.7. Análisis Financiero

El presente análisis financiero estima los costos necesarios para la ejecución del Plan Estratégico de Tecnologías de la Información 2024–2028 de la Personería Distrital de Medellín. Incluye licenciamiento, infraestructura, seguridad digital, desarrollos, servicios en la nube, modernización de equipos y talento humano especializado por prestación de

Categoría	Detalle	Costo Estimado (Anual)
Licenciamiento Microsoft 365	Licencias Exchange Online, SharePoint, OneDrive, Teams y Windows.	\$150.000.000
Fortinet (FortiGate, FortiWeb, FortiEDR)	Suscripciones UTM, WAF, EDR y filtrado de contenidos.	\$120.000.000



N° SC735-1



Servicios en la Nube	Hosting SIP, Personería en Línea, PQRSD, Intranet, Moodle y APIs.	\$180.000.000
Desarrollo de Software	Modernización SIP 2.0, integraciones, automatización, mejoras a sistemas.	\$200.000.000
Talento Humano Especializado	Ingenieros, desarrolladores, técnicos y administradores TI por prestación de servicios.	\$700.000.000
Infraestructura y Modernización	Switches, UPS, renovación de equipos, servidores y redes.	\$300.000.000
Capacitación y Formación	Excel, Power BI, SGSI, herramientas TIC, seguridad y nube.	\$30.000.000
Soporte y Mantenimiento	Garantías, mantenimientos preventivos, soporte técnico, reemplazos.	\$80.000.000

7. ENTENDIMIENTO ESTRATÉGICO

El entendimiento estratégico constituye la base sobre la cual se define la arquitectura tecnológica, los lineamientos de modernización y la planificación del ecosistema de TI de la Personería Distrital de Medellín. Esta fase permite analizar cómo las Tecnologías de la Información soportan, fortalecen y habilitan el



N° SC735-1



cumplimiento de la misión institucional, la prestación de servicios a la ciudadanía y la defensa y promoción de los derechos humanos.

En esta etapa se realiza un estudio integral de las políticas, lineamientos, capacidades tecnológicas, estructura organizacional y necesidades actuales y futuras de información de la Entidad. Este análisis permite identificar el grado de madurez digital, la articulación entre los procesos misionales y la tecnología, y los cambios necesarios para avanzar hacia un modelo moderno, seguro y eficiente.

El proceso de entendimiento estratégico incluye los siguientes aspectos clave:

• **Revisión del modelo operativo y organizacional:**

Se analiza la estructura actual de la Personería, las interacciones entre procesos y el rol transversal de Innovación y Conocimiento como habilitador estratégico. Se identifican ajustes necesarios para fortalecer el Gobierno de TI, posicionar el proceso en un nivel estratégico y consolidar la figura del Líder TI.

• **Alineación de TI con las necesidades institucionales:**

Las soluciones tecnológicas deben responder a los requerimientos misionales, administrativos, disciplinarios, de atención al ciudadano y de gestión documental. Se analizan las necesidades específicas de cada proceso y cómo los sistemas actuales (SIP, Personería en Línea, PQRSD, Citas, Intranet, SIG, Moodle) contribuyen a su operación.

• **Diagnóstico de infraestructura, seguridad y servicios tecnológicos:**

Se evalúa la situación actual de la infraestructura híbrida (nube + datacenter), la red LAN y VLAN, WiFi segmentada, IPv6, sistemas de seguridad Fortinet (FortiGate, FortiWeb, FortiEDR), Microsoft 365, Active Directory, servidores virtualizados, sistemas de backup y continuidad del negocio, identificando fortalezas y oportunidades de mejora.

• **Identificación de necesidades de información y capacidades analíticas:**

Se revisan los sistemas de captura, producción, almacenamiento y análisis de información, así como la demanda interna y externa de datos. Esto permite definir



N° SC735-1



acciones para mejorar la calidad de la información, la interoperabilidad, la analítica institucional y las competencias de los funcionarios en uso de datos.

• **Evaluación de sistemas de información y servicios digitales:**

Se establece la madurez actual de los principales sistemas institucionales: SIP, Personería en Línea, PQRSD, Moodle, SIG, Página Web, Intranet y Mesa de Ayuda. Se identifican ajustes para fortalecerlos, modernizarlos o integrarlos, orientados a mejorar la experiencia del ciudadano, la trazabilidad y la eficiencia operativa.

• **Análisis estratégico de recursos humanos especializados:**

Se revisa la capacidad actual del equipo TI (ingenieros, desarrolladores, técnicos y tecnólogos) frente a los nuevos retos: nube, automatización, IA, seguridad avanzada, interoperabilidad, virtualización y analítica de datos. Esto permite proyectar necesidades futuras de talento humano especializado.

• **Identificación de rupturas estratégicas y oportunidades tecnológicas:**

Se analizan los paradigmas que deben transformarse para avanzar hacia una Personería digital, moderna, segura y orientada al ciudadano. Entre ellos, la migración progresiva del SIP hacia la nube, el uso de IA para análisis de datos, la automatización de procesos, la consolidación de un ecosistema integral de servicios digitales, el fortalecimiento del SGSI y el uso pleno del Gobierno Digital.

Este entendimiento estratégico permite construir una visión clara y sustentada del estado actual de la tecnología en la Entidad, así como los lineamientos para orientar la formulación de la estrategia de TI y la definición del plan de implementación del PETI 2024–2028.

7.1. Modelo Operativo

La Personería Distrital de Medellín, en cumplimiento de los mandatos superiores y el marco normativo vigente, adopta el Plan Estratégico Institucional 2024–2028, dentro del cual se establece la **Agenda Estratégica 2: Implementar un modelo innovador y desconcentrado de atención**. En este contexto, el **Programa 2.1 “Transformación Digital para la Personería”** orienta la modernización de los



N° SC735-1



procesos institucionales a través del fortalecimiento de la infraestructura tecnológica, la incorporación de nuevas herramientas digitales, el desarrollo de competencias del talento humano y la protección integral de la información.

Este programa busca potenciar la eficiencia operativa mediante la adopción de tecnologías modernas, el uso estratégico del análisis de datos, la automatización de procesos, el fortalecimiento de la seguridad digital y la implementación de soluciones innovadoras que permitan avanzar hacia una Personería más ágil, accesible, eficiente y alineada con las exigencias del entorno digital contemporáneo.

La Entidad cuenta además con un Sistema de Gestión de la Calidad certificado bajo la Norma **ISO 9001**, el cual establece un **Mapa de Procesos Institucional** que define los procesos misionales, estratégicos y de apoyo. En este marco, **Innovación y Conocimiento** se encuentra adscrito al nivel de Personería Auxiliar, con un rol transversal y estratégico cuyo propósito es:

“Asesorar en la articulación, coordinación y supervisión de iniciativas que impulsen el fortalecimiento de la entidad mediante el uso y aplicación de las Tecnologías de la Información y las Comunicaciones (TIC), como un factor estratégico para el desarrollo del Gobierno Digital, la mejora en la prestación de servicios a la ciudadanía y la consolidación de una Personería digital. Gestionar todas las actividades informáticas necesarias para el buen desempeño de la organización y el logro de sus objetivos institucionales.”

Bajo este modelo operativo, Innovación y Conocimiento se constituye como el habilitador tecnológico de la Entidad, garantizando:

- La operación continua de los sistemas de información misionales y de apoyo (SIP, Personería en Línea, PQRSD, Citas en Línea, SIG, Intranet, Moodle, Mesa de Ayuda).
- La gestión integral del centro de datos, servicios en la nube y plataformas Microsoft 365.
- La implementación de soluciones de seguridad digital basadas en la suite Fortinet (FortiGate, FortiWeb, FortiEDR).



N° SC735-1



- La administración de la infraestructura de red (LAN, VLAN, WiFi segmentado, IPv6) y conectividad institucional.
- El soporte técnico, funcional y operativo a todas las dependencias.
- El liderazgo en proyectos de modernización, automatización e innovación tecnológica.
- La adopción de lineamientos del MinTIC, el SGSI, el Modelo de Gobierno Digital y el Plan Estratégico Institucional.

Este modelo operativo permite a la Personería avanzar hacia un ecosistema robusto de servicios digitales, orientado al ciudadano, con mayor capacidad analítica, mayor seguridad, mejor trazabilidad, y una institucionalidad preparada para los desafíos tecnológicos de los próximos años.



Con el fin de cumplir con el objetivo se tiene documentado 13 procedimientos operativos los cuales son:

- ✓ PGIN001 RESPALDO DE LA INFORMACION
- ✓ PGIN002 RESTAURACION DE LA INFORMACION
- ✓ PGIN003 INSTALACION DE SOFTWARE
- ✓ PGIN004 INVENTARIO DE HARDWARE Y SOFTWARE
- ✓ PGIN005 CREACION Y ACTUALIZACION DE USUARIOS
- ✓ PGIN007 REPORTE SOLUCIÓN Y ANÁLISIS DE REQUERIMIENTOS
- ✓ PGIN008 PERMISOS DE NAVEGACION EN INTERNET
- ✓ PGIN009 LISTA DE CHEQUEO DE ESTADO SERVIDORES Y CENTRO DE DATOS
- ✓ PGIN012 CONTROL DE LICENCIAS DE SOFTWARE
- ✓ PGIN013 ACTUALIZACION TECNOLOGICA
- ✓ PDIC014 MANTENIMIENTO DE EQUIPOS
- ✓ PDC015 IDENTIFICACIÓN DE ACTIVOS TI

7.1.1. Sistema de Gestión de Seguridad de la Información y el Manual de Seguridad

La Personería Distrital de Medellín cuenta con un **Sistema de Gestión de Seguridad de la Información (SGSI)** fundamentado en los lineamientos de la norma internacional **NTC-ISO/IEC 27001:2013**, las buenas prácticas de la norma ISO/IEC 27002:2022 y las directrices establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones en materia de Seguridad y Privacidad de la Información y Gobierno Digital.

El SGSI incorpora el **Manual de Seguridad de la Información**, documento rector aprobado institucionalmente y soportado por la **Resolución 054 del 13 de febrero de 2019**, mediante la cual se conforma el **Comité de Seguridad de la Información** y se definen funciones, roles y responsabilidades para la protección de los activos de información. Este Comité realiza seguimiento y define directrices estratégicas



N° SC735-1



para la protección de los datos, mitigación de riesgos tecnológicos, fortalecimiento de controles, cumplimiento normativo y la gestión de incidentes de seguridad.

La Personería ha adaptado el SGSI a su realidad tecnológica actual, integrando mecanismos modernos como la autenticación basada en Azure Active Directory, la protección perimetral con **FortiGate**, la protección de aplicaciones web con **FortiWeb**, y la protección de endpoints mediante **FortiEDR**, complementados con políticas internas, controles de red, segmentación VLAN e implementación de IPv6.

A continuación, se describen las políticas y procedimientos principales del Manual de Seguridad de la Información:

- **Capacitación y Sensibilización del Personal:**
Define la metodología institucional para capacitar a funcionarios y contratistas en temas de seguridad de la información, SGSI, phishing, protección de datos, gestión de contraseñas, acceso seguro a los sistemas, análisis de riesgos y uso adecuado de las TIC. Incluye periodicidad, roles y estrategias de formación continua.
- **Ingreso Seguro a los Sistemas de Información:**
Establece controles para el acceso seguro a aplicaciones y plataformas utilizando mecanismos de autenticación robusta, prevención de ataques de fuerza bruta, cifrado TLS, validaciones de acceso, uso de Azure AD, segmentación de roles, bloqueo automático por intentos fallidos y auditoría de accesos.
- **Gestión de Usuarios y Contraseñas:**
Define los lineamientos para creación, modificación y desactivación de usuarios en Active Directory, SIP, SIG, Intranet, Moodle y demás plataformas. Establece políticas de contraseñas seguras, tiempos de expiración, bloqueo por intentos fallidos y restricciones de reutilización. Todo acceso se otorga bajo el principio de **mínimo privilegio**.
- **Controles Criptográficos:**



N° SC735-1



Describe el uso de cifrado para datos en tránsito (TLS/SSL), datos en reposo, claves, certificados, autenticación en Microsoft 365, cifrado de backups y mecanismos de integridad. Define niveles de cifrado según criticidad de la información.

- **Control de Acceso Físico:**
Regula el ingreso a las instalaciones y especialmente al **Centro de Datos**, mediante control biométrico, registro de ingresos, cámaras CCTV, permisos especiales, supervisión y registro de eventos. Incluye áreas restringidas como racks de servidores, equipos de comunicaciones, UPS y sistemas de backup.
- **Gestión de Capacidad:**
Determina la planificación de capacidad para servidores, bases de datos, almacenamiento, red, servicios en la nube y sistemas de seguridad. Contempla eliminar datos obsoletos, cerrar servicios en desuso, optimizar recursos y proyectar necesidades futuras en función de la demanda tecnológica.
- **Separación de Ambientes:**
Indica la separación de ambientes **Desarrollo – Pruebas – Producción**, utilizando infraestructura aislada, bases de datos alternas y mecanismos de validación antes de despliegues en producción. Permite minimizar riesgos operativos y garantizar calidad en la implementación de mejoras o nuevas funcionalidades.
- **Protección contra Códigos Maliciosos:**
Describe el uso de FortiEDR, antivirus corporativo, actualizaciones automáticas, análisis heurístico, listas negras, detección de comportamientos anómalos, procedimientos ante infecciones, cuarentena y reporte de eventos de malware.
- **Aseguramiento de Servicios en la Red:**
Define los controles para proteger la red cableada, VLAN, WiFi segmentado (usuarios internos y ciudadanos), inspección profunda de paquetes en el FortiGate, cifrado de datos en tránsito, protección de tráfico SSL, monitoreo de logs y mecanismos de prevención de intrusiones (IPS).



N° SC735-1



- **Seguridad en los Acuerdos con Proveedores:**
Se establecen obligaciones contractuales en materia de seguridad, niveles de servicio, protección de datos, confidencialidad, auditoría, gestión de incidentes, reportes periódicos y cumplimiento de normas aplicables. Incluye proveedores de nube, internet, impresión, hosting, software y seguridad.
- **Control de Software:**
Regula la instalación y uso de software institucional. Define quiénes pueden instalar software, cómo se gestionan solicitudes, el inventario de licencias, prohibición de software no autorizado, validaciones de seguridad y procedimientos de eliminación segura.
- **Gestión de la Continuidad del Negocio:**
Define los mecanismos para garantizar la continuidad de los procesos misionales ante fallas, desastres o incidentes críticos. Incluye políticas de backup, redundancia, procedimientos de restauración, roles durante emergencias, priorización de sistemas críticos y activación del **Plan de Continuidad y Recuperación ante Desastres (DRP)**.

7.2. Necesidades de Información

El inciso segundo del artículo 178 de la Ley 136 de 1994 establece que el Personero ejercerá en el municipio, bajo la dirección suprema del Procurador General de la Nación, las funciones del Ministerio Público, además de las que determine la Constitución, la Ley y los Acuerdos. En cumplimiento de este mandato, la Personería Distrital de Medellín desarrolla funciones esenciales relacionadas con la **promoción, guarda y defensa de los derechos humanos**, la **vigilancia de la conducta oficial**, la **protección del interés público** y la **solución alternativa de conflictos**.

Estas funciones requieren un flujo permanente, confiable y seguro de información, lo cual convierte a los sistemas institucionales en una fuente crítica de datos para la toma de decisiones, la atención a la ciudadanía y la respuesta a los entes de control. Para garantizar este proceso, la Personería utiliza su sistema misional SIP



N° SC735-1



y sus servicios digitales complementarios —Personería en Línea, PQRSD, Citas en Línea, Moodle, SIG en SharePoint, Intranet corporativa y sistemas de apoyo— para registrar, categorizar y analizar todas las atenciones y actuaciones institucionales.

Los sistemas permiten capturar información relacionada con:

- Datos básicos de ciudadanos atendidos.
- Tipo de atención y servicio solicitado.
- Hechos y situaciones reportadas.
- Registros y caracterización de víctimas.
- Vigilancias de conducta oficial.
- Procesos disciplinarios.
- Conciliaciones y mecanismos alternativos de solución de conflictos.
- Revisiones penales.
- Atención a niños, niñas y adolescentes.
- Solicitudes virtuales recibidas a través de Personería en Línea.
- Peticiones, quejas, reclamos, denuncias y sugerencias (PQRSD).

De esta operación se derivan múltiples requerimientos de información por parte de organismos públicos, privados y de cooperación, lo que convierte a la Personería en una entidad clave de consulta y análisis. A continuación, se presentan las principales categorías de información solicitadas y reportadas:

- Total de tutelas en materia de salud.
- Registros de víctimas por tipo de hecho victimizante.
- Información relacionada con atención a adulto mayor.
- Quejas por presuntos abusos de autoridad.
- Georreferenciación de atenciones por comunas, corregimientos y sedes.
- Total de servicios prestados por tipo, modalidad y área.
- Informe anual y especial de Derechos Humanos.
- Informe sobre la situación actual de los derechos humanos en Medellín.
- Información del sistema carcelario y visitas a centros de reclusión.
- Vigilancias realizadas a secretarías municipales y entidades descentralizadas.
- Informes de Control Interno y entes de control externo.
- Planes estratégicos, operativos y de acción.



N° SC735-1



- Atención y seguimiento a requerimientos institucionales.
- Gestión documental y archivo.
- Gestión financiera, presupuestal y contractual.
- Gestión administrativa y de talento humano.
- Gestión de la información para organismos de control.
- Producción y análisis de contenido institucional.
- Definición y ajuste de políticas públicas o institucionales.

La Personería Distrital de Medellín es una entidad de consulta para organismos como la Fiscalía General de la Nación, Policía Nacional, Ejército Nacional, Unidad de Víctimas, Defensoría del Pueblo, ONG, Concejo de Medellín, Alcaldía de Medellín, personerías locales y entes de control.

El flujo de información institucional se gestiona bajo el **ciclo de vida del dato**, el cual permite garantizar calidad, integridad y trazabilidad, e incluye las fases de:

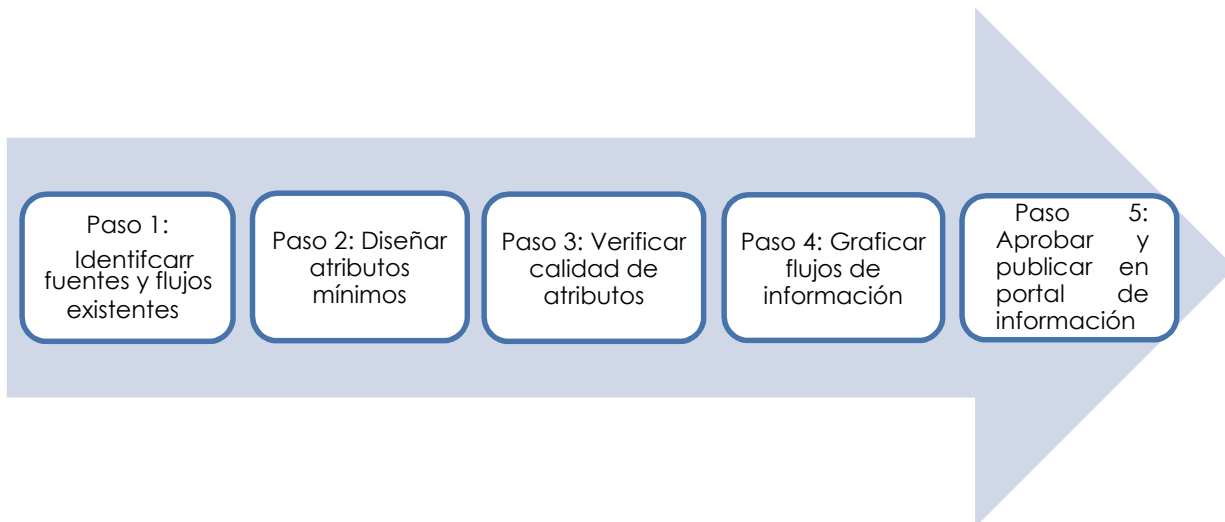
1. Captura y registro.
2. Validación y estandarización.
3. Almacenamiento seguro.
4. Procesamiento y análisis.
5. Distribución y difusión.
6. Archivo y disposición final.

Este ciclo es fundamental para asegurar que funcionarios, directivos, entes de control y ciudadanía cuenten con información confiable, oportuna y pertinente para la toma de decisiones y el cumplimiento de la misión constitucional de la Personería Distrital de Medellín.



N° SC735-1





Se recomienda realizar las siguientes actividades para favorecer el flujo de la información en cada consulta:

Módulos del Sistema de Información SIP actualizados

- Es necesario y dado los cambios normativos, mantener actualizado los módulos del Sistema Misional SIP, el cual es la herramienta que permite obtener y suministrar información a los interesados.
- Generar un módulo de reportes para los funcionarios sobre los temas más asiduos de consulta.

Gestión de expedientes digitales

- Adecuar el Sistema de Información SIP con el objetivo de permitir la gestión de expedientes digitales, además de implementar todo lo relacionado con el inventario documental, que permita de manera ágil consultar un expediente electrónico.

7.3. Alineación de TI con los procesos



N° SC735-1



Los sistemas de información de la Personería Distrital de Medellín están diseñados para soportar de forma directa los procesos misionales, estratégicos y de apoyo definidos en el Mapa de Procesos Institucional. En este sentido, la **alineación entre los procesos y la tecnología** es fundamental para garantizar eficiencia, trazabilidad, oportunidad en la información y cumplimiento de los objetivos institucionales.

La automatización de procesos debe estar soportada en prácticas de gestión estandarizadas y bajo criterios de calidad, con el fin de evitar la sistematización de actividades ineficientes o desarticuladas. Si un proceso no está adecuadamente definido o no cuenta con lineamientos claros, existe el riesgo de que el sistema de información refleje o amplifique dichas debilidades. Por ello, el éxito de la arquitectura tecnológica depende de la correcta integración entre los procesos institucionales, los flujos de información y los sistemas que los soportan.

En esta sección se realiza la articulación entre los procesos institucionales y el inventario de sistemas de información identificado en el numeral 6.3, con el propósito de determinar:

- Qué procesos requieren fortalecimiento tecnológico o automatización adicional.
- Cuáles sistemas deben ser actualizados, reagrupados o integrados para evitar duplicidad.
- Qué herramientas están en desuso o no aportan valor al proceso.
- Cuáles plataformas deben consolidarse para mejorar la eficiencia y la trazabilidad.
- Qué sistemas requieren evolucionar hacia una arquitectura más moderna basada en nube, APIs e interoperabilidad.

Del análisis realizado se destacan los siguientes hallazgos:

1. El Sistema SIP continúa siendo el eje central de la operación misional

El **Sistema de Información Misional SIP** es el ERP institucional más utilizado por todas las áreas misionales, disciplinarias, administrativas y operativas. Este sistema soporta:



N° SC735-1



- Atención al ciudadano
- Derechos Humanos
- Vigilancia de la conducta oficial
- Procesos disciplinarios
- Gestión documental
- Correspondencia
- Gestión de actividades y proyectos
- Activos fijos
- Gestión de talento humano

Dado su rol estratégico, es el sistema al que se debe dar prioridad en su modernización y evolución hacia un **SIP 2.0**, incorporando nuevas funcionalidades, interfaz mejorada, interoperabilidad con otras entidades, automatización de flujos y análisis avanzado de datos.

2. Los servicios digitales complementarios fortalecen la operación misional

Sistemas como:

- **Personería en Línea**
- **Citas en Línea**
- **PQRSD**
- **Moodle**
- **Intranet corporativa**
- **Sistema Integrado de Gestión (SIG en SharePoint)**

están alineados con los procesos de atención, participación ciudadana, formación, gestión documental, control interno y gobierno corporativo.

El incremento en el uso de estos servicios durante 2024–2025 demuestra su valor en la estrategia de transformación digital.

3. La Mesa de Ayuda se consolida como herramienta transversal

Las mesas de ayuda de Informática, Gestión Documental, Comunicaciones y Bienes Administrativos son plataformas utilizadas por toda la entidad, permitiendo:

- Registro de incidentes
- Trazabilidad
- Indicadores de servicio
- Identificación de necesidades



N° SC735-1



- Priorización de requerimientos

Lo que demuestra su alineación directa con los procesos de soporte y mejora continua.

4. Necesidad de integración y eliminación de duplicidad

El cruce entre procesos y sistemas evidencia oportunidades para:

- Integrar módulos duplicados entre SIP, SIG e Intranet.
- Consolidar funcionalidades en plataformas existentes.
- Estandarizar procesos antes de su automatización.
- Reducir herramientas paralelas que generan dispersión de información.

La integración mediante **APIs institucionales**, Azure AD y servicios en la nube permitirá alinear completamente los sistemas con los procesos.

5. TI como habilitador del modelo operativo

La infraestructura tecnológica —Microsoft 365, Azure AD, Fortinet, base de datos PostgreSQL, servicios en nube, redes VLAN, WiFi segmentada, IPv6— está alineada con:

- La gestión misional
- La seguridad institucional
- La eficiencia operativa
- La prestación de servicios a la ciudadanía
- La estrategia de Gobierno Digital

El fortalecimiento de esta plataforma permitirá avanzar hacia un modelo moderno de gestión digital, interoperable, seguro y orientado a datos.



N° SC735-1



Sistemas de Información / PROCESOS	ERP Sistema de información Misional de la Personería SIP	Sistema de Gestión Integrado	Personería en Línea	Intranet	Mesa de Ayuda Comunicaciones	Mesa de Ayuda Informática	Gestión del Conocimiento (Moodle)	Peticiones, Quejas, Reclamos y sugerencias	Correo Microsoft 365	Datos Abierto	Mesa de Ayuda Gestión Documental	SAP (Systems, Applications, Products in Data Processing)
Asesores del despacho	X	X		X	X	X	X		X		X	
Despacho del Personero	X	X		X	X	X	X		X		X	X
Dirección de control interno	X	X		X	X	X	X		X		X	
Gestión contractual		X		X	X	X	X		X		X	X
Gestión financiera		X		X	X	X	X		X		X	X
Gestión jurídica	X	X		X	X	X	X		X		X	
Gestión documental	X	X		X	X	X	X		X		X	
Gestión bienes administrativos	X	X		X	X	X	X		X		X	
Gestión informática	X	X		X	X	X	X		X		X	
Gestión talento humano	X	X		X	X	X	X		X		X	
Investigaciones en DDHH	X	X		X	X	X	X		X		X	
Observatorio medio ambiente	X	X		X	X	X	X		X		X	
Observatorio penal	X	X		X	X	X	X		X		X	
Obs. Presupuesto participativo	X	X		X	X	X	X		X		X	
Observatorio reasentamiento	X	X		X	X	X	X		X		X	
Observatorio salud	X	X		X	X	X	X		X		X	
Oficina de comunicaciones	X	X		X	X	X	X		X		X	
Oficina planeación	X	X		X	X	X	X	X	X	X	X	
Personería auxiliar	X	X		X	X	X	X		X		X	
Conciliaciones	X	X	X	X	X	X	X		X		X	
UPDH - Atención al público	X	X		X	X	X	X		X	X	X	
UPDH – Penal	X	X	X	X	X	X	X	X	X		X	

Plan Estratégico de la Información y las Comunicaciones (PETI)



UPDH - Unidad permanente	x	x	x	x	x	x	x	x	x	x	x	
Unidad para la protección del interés público	x	x		x	x	x	x		x		x	
Unidad para la vigilancia de la conducta oficial	x	x	x	x	x	x	x		x		x	
UVCO- Disciplinarios	x	x		x	x	x	x		x		x	





...

8. MODELO DE GESTIÓN DE TI

8.1. Estrategia de TI

La estrategia de Tecnologías de la Información de la Personería Distrital de Medellín se fundamenta en la alineación directa entre los objetivos institucionales definidos en el Plan Estratégico 2024–2028 y las capacidades tecnológicas actuales y futuras de la Entidad. Este direccionamiento permite garantizar que las iniciativas tecnológicas respondan a las necesidades misionales, administrativas y operativas, asegurando eficiencia, transparencia, continuidad del servicio, seguridad de la información y calidad en la atención a la ciudadanía.

Siguiendo el modelo de estrategia de TI, se establece un enfoque estructurado donde la arquitectura institucional —procesos, información, aplicaciones, infraestructura, seguridad y talento humano— se articula con los mecanismos de Gobierno de TI y con los lineamientos del Modelo de Gobierno Digital del MinTIC. Esta integración se materializa a través de políticas, procedimientos, servicios tecnológicos, controles de seguridad y un portafolio de proyectos que fortalecen la capacidad institucional.

La estrategia de TI contempla:

- La **sincronización de la estrategia tecnológica con las líneas estratégicas institucionales**, especialmente con el Programa 2.1 “Transformación Digital para la Personería”.
- La consolidación de una **arquitectura empresarial** basada en datos, interoperabilidad, servicios en la nube, automatización y seguridad avanzada.
- El fortalecimiento de los **mecanismos de Gobierno de TI**, que incluyen el Comité de Seguridad de la Información, el SGSI, las políticas tecnológicas, la priorización de proyectos y la gestión de riesgos.



- La definición de una **infraestructura tecnológica robusta**, moderna y segura que soporte la operación misional, el crecimiento institucional y las nuevas demandas de servicio
- El aseguramiento de procesos internos orientados a la **eficiencia operativa, la trazabilidad, la transparencia, el control y el mejor aprovechamiento de los recursos tecnológicos**.
- La incorporación de prácticas avanzadas de **seguridad de la información**, continuidad del negocio y gestión del riesgo tecnológico
- La consolidación de un **portafolio de proyectos estratégicos**, priorizados conforme a necesidades institucionales, impacto social, riesgos, recursos disponibles y madurez tecnológica.
- La orientación hacia un **ecosistema integral de servicios digitales**, interoperables, centrados en el ciudadano y basados en analítica de datos.
- La adopción de tecnologías innovadoras —inteligencia artificial, automatización, APIs institucionales, digitalización avanzada— que aporten valor y fortalezcan los servicios a la ciudadanía.
- El fortalecimiento del **talento humano digital**, mediante capacitación continua, apropiación tecnológica y especialización en seguridad, nube, análisis de datos y desarrollo.

Con este direccionamiento, la estrategia de TI se convierte en un habilitador fundamental para consolidar una Personería moderna, conectada, segura y preparada para los desafíos del entorno digital. Las decisiones tecnológicas se enmarcan en los seis dominios del marco de referencia adoptado, garantizando una cobertura integral entre:

1. **Estrategia**
2. **Gobierno de TI**
3. **Arquitectura**
4. **Servicios y Aplicaciones**
5. **Infraestructura y Seguridad**



N° SC735-1



6. Talento Humano y Capacidades Digitales

Esta estructura asegura que cada componente tecnológico aporte valor real al cumplimiento de la misión, la prestación de servicios a la ciudadanía y la transformación digital institucional.



8.1.1. Definición de los objetivos estratégicos de TI

Los objetivos estratégicos de Tecnologías de la Información se orientan a consolidar un ecosistema digital moderno, seguro, interoperable y centrado en el ciudadano, apoyando la operación misional de la Personería Distrital de Medellín y su proceso de transformación digital. Estos objetivos permiten alinear la estrategia tecnológica con el Plan Estratégico Institucional 2024–2028 y con los lineamientos del Modelo de Gobierno Digital del MinTIC.

Los objetivos estratégicos de TI son los siguientes:



N° SC735-1



- **Integrar y consolidar los sistemas de información institucionales**, garantizando interoperabilidad, calidad de datos y disponibilidad para la toma de decisiones sostenibles, la gestión misional y la formulación y seguimiento de políticas públicas.
- **Promover la innovación y la competitividad institucional**, fortaleciendo las competencias digitales, la apropiación tecnológica y la confianza del personal en los sistemas de información, las herramientas de analítica y los servicios en la nube.
- **Fomentar el uso de los servicios digitales por parte de la ciudadanía**, fortaleciendo la confianza en los canales virtuales y ampliando la oferta de trámites y servicios en línea de la Personería Distrital de Medellín.
- **Fortalecer la gestión de las Tecnologías de la Información y las Comunicaciones**, garantizando eficiencia operativa, continuidad del servicio, atención oportuna y protección integral de la información mediante un enfoque de seguridad y gestión del riesgo.
- **Habilitar capacidades tecnológicas avanzadas**, que impulsen las transformaciones institucionales, mediante infraestructura moderna, servicios en la nube, seguridad digital, analítica de datos, automatización, APIs institucionales e inteligencia artificial.
- **Implementar un Sistema de Gestión de Servicios de TI**, que permita gestionar, controlar y mejorar de manera formalizada los servicios prestados, alineándolos con las necesidades de los usuarios, los niveles de servicio y las demandas institucionales.
- **Fortalecer, mantener y modernizar los servicios en línea**, mediante tecnologías emergentes como cloud computing, herramientas de colaboración, plataformas móviles, seguridad avanzada y mecanismos de disponibilidad y resiliencia.

Iniciativas estratégicas contempladas en el Plan de Acción 2025



N° SC735-1



El Plan de Acción 2025 incluye una renovación tecnológica orientada a robustecer los servicios misionales, administrativos y digitales de la Entidad. Las principales iniciativas son:

- **Migración de servicios a la nube**, incluyendo:
 - Página web institucional
 - Sistema de Información Misional SIP
 - Personería en Línea
 - Servidor de bases de datos
 - Centro de Pensamiento
 - Intranet corporativa
- **Integración de todos los servicios institucionales con el SIP**, permitiendo interoperabilidad, eliminación de duplicidad de información y mayor eficiencia operativa.
- **Desarrollo de una aplicación móvil institucional**, que permita el acceso a servicios, consultas, agendamiento de citas, orientación y seguimiento de casos.
- **Ampliación de servicios virtuales**, orientados a mejorar la atención al ciudadano, el autoservicio y la trazabilidad.
- **Fortalecimiento del sistema PQRSD**, mediante un formulario moderno, trazable, seguro y conectado con el SIP.
- **Implementación de un módulo de reportes y analítica en el SIP**, que integre información institucional, genere indicadores y soporte la toma de decisiones basada en datos.
- **Desarrollo de una aplicación para la administración de la tiquetera de bienestar**, facilitando su control y uso.



N° SC735-1

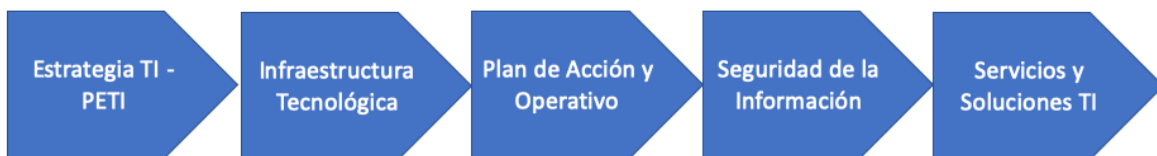


- **Habilitación del módulo de Bienes Administrativos en el SIP**, para fortalecer el control, inventario y trazabilidad de los activos institucionales.

8.2. Gobierno de TI

8.2.1. Cadena de valor de TI

La cadena de valor de TI está dada en función de 5 grupos de procedimientos



Los roles de TI en la Personería Distrital de Medellín, que se encuentran asociados en las actividades de los contratistas de TI y los roles y procedimientos del proceso conforme a lo definido en el numeral 5.6 Gobierno TI.

a) Gestionar la planeación estratégica de TI:

- ✓ Definir y mejorar el proceso Innovación y Conocimiento.
- ✓ Definir y gestionar el PETI aplicando lineamientos de MINTIC, y las mejores prácticas de administración de gobierno TI y servicios informáticos

b) Gestión de servicios y soluciones de TI:

- ✓ Administrar los servicios de TI
- ✓ Gestionar el ciclo de vida de las soluciones TI.

c) Gestionar la seguridad Informática y seguridad de la información:

- ✓ Gestionar la seguridad la información.
- ✓ Gestionar la continuidad del negocio

d) Gestionar la infraestructura de TI:

- ✓ Gestionar la disponibilidad de los servicios de TI.
- ✓ Gestionar la capacidad de la infraestructura TI



N° SC735-1





e) Gestionar los proyectos de TI:

- ✓ Gestionar los proyectos de TI.
- ✓ Gestionar los indicadores y seguimiento a los proyectos de TI

8.2.2. Indicadores y Riesgos

✓ Indicadores de calidad

Para esta vigencia se define desde el Sistema de Gestión de la Calidad mediante resolución 131 de 2022, que el proceso Innovación y Conocimiento se mide con la ejecución de las actividades del Plan de acción de cada vigencia que se encuentra alineado con el Plan Estratégico Institucional. Las actividades de este plan se encuentran descritas en el numeral 6.3 Análisis Financiero.

✓ Riesgos de TI

RIESGO	CLASIFICACION	CAUSAS	RIESGO INHERENTE			
			PROBABILIDAD	IMPACTO	ZONA RIESGO INHERENTE	CONTROL
Interceptación de datos confidenciales al momento de transmitir por las redes instaladas	Riesgo Tecnológico Seguridad Digital	Espionaje remoto, pirata informático	Muy alta	Menor	Alta	Actualizar licenciamiento a los sistemas de seguridad perimetral, establecer controles de acceso al centro de datos, encriptar información transmitida

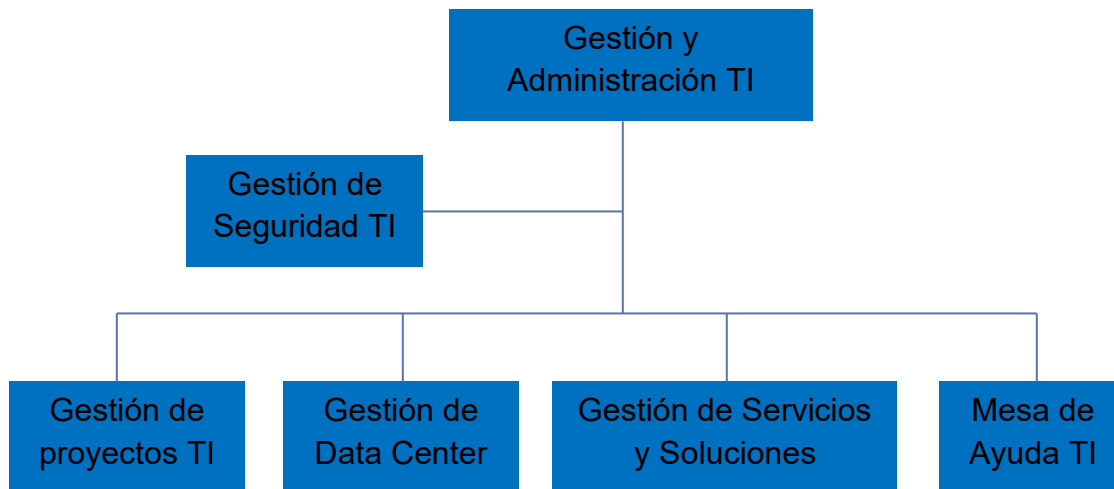


Alteración y/o eliminación de información sin autorización en las bases de datos institucionales, piratería, ingeniería social, intrusión, accesos forzados al sistema, acceso no autorizado al sistema	Riesgo Tecnológico Seguridad Digital	Modificación no autorizada, ataques de fuerza bruta, suplantación de identidad, virus informáticos o código malicioso	Muy alta	Menor	Alta	Establecer contraseñas seguras, mantener el sistema de <i>backup</i> en funcionamiento, encriptar la información
Uso no autorizado de los computadores y portátiles	Riesgo Tecnológico Seguridad Digital	Instalación de software pirata, uso inadecuado del computador y las contraseñas, no bloqueo de la sesión	Muy alta	Menor	Alta	Divulgar política de seguridad de la información
Modificación, alteración y/o ocultamiento en forma ilegal de la información que se encuentra en los sistemas de información para obtener un beneficio para si u otra persona	Riesgo de Corrupción	Interés en obtener beneficios o perjudicar a alguien	Rara vez	Catastrófico	zona de Riesgo Extrema	Sensibilización del grupo de trabajo, sobre conductas constitutivas de corrupción.
Manipulación de licenciamiento original de software en forma ilegal con la intención de obtener un beneficio para si o interpuesta persona	Riesgo de Corrupción	Intención de obtener beneficio económico, familiar, personal o de otra índole por falta de asignación de responsable	Rara vez	Catastrófico	zona de Riesgo Extrema	Procedimiento que establece responsabilidades y funciones para control de licenciamientos, PGIN012 CONTROL DE LICENCIAS DE SOFTWARE.
Posibilidad de pérdidas económicas y reputacionales ante una deficiente administración de la Plataforma Tecnológica	Riesgo Operativo	1. Falta definición de la Arquitectura de sistemas de información de la Plataforma Tecnológica 2. Falta definición de la Arquitectura de datos de la Plataforma Tecnológica 3.	Alta	Moderado	Alto	El líder del proceso verificará la ejecución del plan operativo implementado para la vigencia, en caso de evidenciar desviaciones tomará acciones de fondo para encausar dichas actividades (modificaciones PA, correcciones)

		Obsolencia de los sistemas de información 4. Obsolencia de los equipos 5. Falta de Plan de continuidad.				
--	--	--	--	--	--	--

8.2.3. Estructura organizacional de TI

Conforme al modelo de gestión y buscando que Innovación y Conocimiento se estructure conforme a los lineamientos del ministerio de la TIC, se propone la siguiente estructura operativa de TI para la Personería Distrital de Medellín:



8.3. Gestión de información

8.3.1. Herramientas de Análisis

La Personería Distrital de Medellín cuenta actualmente con herramientas básicas de apoyo al análisis de la información, tales como **Excel**, **Power BI** y conexiones directas a las bases de datos institucionales (PostgreSQL y MySQL). Estas herramientas permiten generar tableros, indicadores, reportes estadísticos y análisis descriptivos que apoyan la toma de decisiones. Sin embargo, la creciente



N° SC735-1



demanda de información, la necesidad de analítica avanzada y los nuevos servicios digitales requieren evolucionar hacia un ecosistema más robusto y estructurado.

En el marco del PETI 2024–2028 y del programa de Transformación Digital, se proyecta incorporar herramientas y capacidades tecnológicas que permitan:

- **Implementación de bodegas de datos (Data Warehouse) y modelos de datos unificados**, que integren información proveniente del SIP, Personería en Línea, PQRSD, Citas en Línea, SIG, Intranet y demás sistemas institucionales.
- **Desarrollo de capacidades en inteligencia de negocios (Business Intelligence)**, para generar reportes dinámicos, tableros analíticos, indicadores estratégicos y visualizaciones interactivas orientadas a la gestión misional, disciplinaria, administrativa y operativa.
- **Publicación de información analítica institucional**, incluyendo estadísticas sobre atención ciudadana, derechos humanos, vigilancia administrativa, procesos disciplinarios, conciliaciones, víctimas y otros indicadores sectoriales.
- **Integración con sistemas de información geográfica (SIG)**, para la georreferenciación de casos, denuncias, atenciones y problemáticas de territorio, permitiendo análisis espacial y toma de decisiones basada en patrones geográficos.
- **Estrategia institucional de datos abiertos y analítica**, en cumplimiento de las políticas de Gobierno Digital, respetando criterios de protección de datos personales.
- **Fortalecimiento de las capacidades del talento humano** en analítica, visualización de datos, estadística, manejo de Power BI, Excel avanzado, consultas SQL, manejo de APIs y herramientas de análisis institucional.



N° SC735-1



- **Incorporación progresiva de modelos de analítica avanzada e Inteligencia Artificial**, orientados a predicción de demanda, priorización de casos, análisis de textos de tutelas y PQRS, y clasificación automática de información.

Las necesidades específicas de gestión, integración y análisis de datos serán refinadas una vez finalice el ejercicio de **Arquitectura Empresarial**, el cual permitirá definir:

- Modelo de datos institucional
- Flujos de información
- Sistemas prioritarios de integración
- Esquema del Data Warehouse
- Mecanismos de interoperabilidad
- Lineamientos para analítica avanzada y servicios cognitivos

Este fortalecimiento permitirá a la Personería evolucionar hacia un modelo de gestión basado en datos, aumentando la calidad, eficiencia y oportunidad de la información que soporta la defensa de los derechos humanos, la vigilancia administrativa y la atención al ciudadano.

8.3.2. Arquitectura de Información

La Arquitectura de Información de la Personería Distrital de Medellín constituye el marco que define cómo se estructura, organiza, integra, almacena, protege y distribuye la información a lo largo de todos los procesos institucionales. Su propósito es garantizar que los datos sean accesibles, confiables, seguros, oportunos y consistentes, permitiendo soportar las funciones misionales, administrativas y de control, así como la prestación de servicios digitales a la ciudadanía.

En el marco del PETI 2024–2028 y del Programa de Transformación Digital, la Entidad avanza hacia la consolidación de una arquitectura basada en:

- **Integración y consolidación de fuentes de información institucional** (SIP, Personería en Línea, PQRS, Citas, Intranet, SIG, Moodle).



N° SC735-1



- **Estandarización de datos y metadatos**, para garantizar uniformidad, calidad y trazabilidad.
- **Uso de servicios en la nube**, como SharePoint, Azure AD y hosting institucional, que permiten disponibilidad, resiliencia y escalabilidad.
- **Seguridad de la información** mediante controles Fortinet (FortiGate, FortiWeb, FortiEDR) y políticas del SGSI.
- **Interoperabilidad**, mediante futuras APIs institucionales y alineación con lineamientos del Modelo de Gobierno Digital.
- **Gestión del ciclo de vida del dato**, desde la captura hasta la disposición final.
- **Preparación para analítica avanzada e inteligencia artificial**, en línea con la estrategia de datos institucional.

El ejercicio de **Arquitectura Empresarial** actualmente en ejecución permitirá definir de manera más detallada:

- El **modelo de datos institucional** y sus entidades principales.
- Los **flujos de información** entre sistemas misionales, de apoyo y servicios digitales.
- La **matriz de integración** entre aplicaciones y bases de datos.
- El **modelo de interoperabilidad** con entidades externas (Fiscalía, Policía, Unidad de Víctimas, Alcaldía, Concejo, Defensoría).
- La **estructura ideal del repositorio central de información** (Data Warehouse).
- La **clasificación de la información** según su confidencialidad, criticidad y uso.
- La **arquitectura objetivo** para el periodo 2024–2028.

Una vez finalizado este ejercicio, la Personería contará con una **arquitectura de información robusta, moderna y sostenible**, que permitirá mejorar la toma de decisiones, fortalecer la trazabilidad, optimizar la gestión misional y ampliar los servicios ciudadanos digitales con calidad y seguridad.

8.4. Sistemas de información



N° SC735-1



La Personería Distrital de Medellín cuenta con un conjunto de sistemas de información que soportan la operación misional, administrativa y de atención al ciudadano, según lo descrito en el numeral 6.3. Estas plataformas constituyen el núcleo tecnológico de la Entidad y permiten garantizar trazabilidad, eficiencia, disponibilidad y calidad en el servicio.

Actualmente, varias de las iniciativas de modernización y fortalecimiento de sistemas de información se encuentran en ejecución o en proceso de implementación, incluyendo:

- **Migración de servicios a la nube**, como la página web institucional, el sistema misional SIP, Personería en Línea, la base de datos institucional, el Centro de Pensamiento y la Intranet.
- **Ampliación y fortalecimiento de los servicios digitales**, tales como PQRSD, Citas en Línea y servicios ciudadanos virtuales.
- **Modernización gradual del ecosistema SIP**, incluyendo rediseño de módulos, mejoras de usabilidad, interoperabilidad, limpieza de datos, integración con nuevas herramientas y construcción de APIs institucionales.
- **Consolidación del SIG institucional en SharePoint**, con mayor integración documental y facilidad de consulta.
- **Desarrollo de nuevos servicios digitales**, como la APP institucional para dispositivos móviles.
- **Actualización del sistema Moodle para formación ciudadana y funcional.**

En este marco, se establece como proyecto estratégico la **actualización, fortalecimiento y mantenimiento del Sistema de Información Misional SIP** — detallado en el numeral 8.4.2—, dado que constituye el eje central de la operación misional y administrativa de la Personería Distrital de Medellín.



N° SC735-1



Este proyecto contempla:

- Mejoras funcionales.
- Actualización de módulos existentes.
- Integración con sistemas de apoyo y servicios ciudadanos en línea.
- Tecnologías modernas de desarrollo.
- Rediseño de la arquitectura en ambiente cloud.
- Limpieza y estandarización de datos.
- Mejoras en seguridad y control de accesos.
- Construcción de reportes y analítica integrada.
- Mayor usabilidad y experiencia de usuario.

Con estas iniciativas, la Personería avanza hacia un ecosistema digital robusto, integrado y centrado en la ciudadanía, que permita una gestión más eficiente, transparente y moderna de sus procesos misionales y de apoyo.

8.4.1. Arquitectura de Sistemas Información.

La Arquitectura de Sistemas de Información de la Personería Distrital de Medellín está definida y documentada en el ejercicio de Arquitectura Empresarial (AE) y se encuentra en proceso de actualización permanente conforme a la incorporación de nuevos sistemas, servicios digitales y componentes tecnológicos descritos en el numeral 6.3. Esta arquitectura permite organizar, integrar y gestionar de manera estructurada el ecosistema de aplicaciones que soportan los procesos misionales, disciplinarios, administrativos y de atención al ciudadano.

La arquitectura actual está compuesta por:

- **Sistema de Información Misional SIP**, como eje central de la operación institucional, soportando los módulos de atención al ciudadano, derechos humanos, vigilancia administrativa, procesos disciplinarios, gestión documental, correspondencia, proyectos, actividades, talento humano y activos administrativos.
- **Servicios ciudadanos digitales en la nube**, tales como:
 - Personería en Línea
 - PQRSD
 - Citas en Línea



N° SC735-1



- Portal Web Institucional
 - Moodle (formación ciudadana y capacitación funcional)
 - Intranet corporativa
 - SIG Documental en SharePoint
- **Sistemas complementarios de apoyo**, incluyendo mesa de ayuda, gestión de noticias, biblioteca jurídica, comunicaciones internas, gestión de bienes y administración de contenidos.
 - **Servicios tecnológicos basados en Microsoft 365**, como Exchange Online, OneDrive, Teams, SharePoint y Azure AD, que permiten colaboración institucional, continuidad del servicio y autenticación centralizada.
 - **Bases de datos institucionales**, principalmente PostgreSQL para el SIP, MySQL para sistemas de apoyo y bases en la nube para nuevos desarrollos.
 - **Servicios de seguridad integrados**, articulados con la arquitectura de aplicaciones mediante FortiGate (perímetro), FortiWeb (protección de aplicaciones web), FortiEDR (protección de endpoints) y el SGSI basado en ISO 27001.

La arquitectura de sistemas de información contempla además un proceso de **modernización y evolución hacia un modelo basado en interoperabilidad y servicios**, que permitirá:

- Integración de sistemas mediante **APIs institucionales**.
- Priorización de sistemas misionales y de apoyo según impacto.
- Eliminación de duplicidades funcionales.
- Simplificación de procesos.
- Migración progresiva a arquitectura cloud.
- Implementación de reportes y analítica integrada.
- Consolidación del ciclo de vida del dato.

Esta arquitectura constituye el fundamento para el proyecto estratégico de modernización del SIP y para el fortalecimiento de los servicios digitales que la Personería ofrece a la ciudadanía y a sus procesos internos.

8.4.1.1. Arquitectura en la Nube – Microsoft Azure (Vista Estratégica)



N° SC735-1



La Personería Distrital de Medellín adoptó un modelo de arquitectura **cloud-first**, en el cual los sistemas misionales, aplicativos de apoyo y servicios institucionales se encuentran alojados en la nube de Microsoft Azure. Actualmente, el SIP, la página web, la intranet, Personería en Línea, los sistemas de PQRSD, Moodle y demás servicios informáticos operan directamente desde Azure, lo que garantiza mayor disponibilidad, escalabilidad, continuidad operativa y seguridad.

Esta arquitectura se describe únicamente a nivel estratégico para proteger la seguridad institucional, sin divulgar configuraciones técnicas sensibles. Los componentes principales incluyen:

- **Azure Active Directory** como núcleo de identidad, autenticación y control de acceso.
- Servicios web institucionales desplegados en **App Services** o máquinas virtuales administradas.
- **Azure Storage** para repositorios documentales y copias de seguridad.
- **Azure Backup** y mecanismos de continuidad operativa.
- Integración con el ecosistema de seguridad Fortinet y herramientas nativas de seguridad en la nube.

Para el periodo 2024–2028, la estrategia contempla:

- Fortalecimiento del SIP y servicios misionales en la nube.
- Consolidación del SGDEA institucional sobre repositorios Azure.
- Adopción del modelo de seguridad Zero Trust.
- Expansión del análisis de datos y reportería avanzada.
- Optimización de la continuidad operativa mediante Azure Site Recovery y replicación en nube.

Esta arquitectura permite a la Entidad consolidar un entorno moderno, seguro y resiliente, alineado con la política de Gobierno Digital y las necesidades de atención a la ciudadanía.

8.4.2. Implementación de sistemas de información



N° SC735-1



Actualmente, la Personería Distrital de Medellín no tiene solicitudes para la adquisición o implementación de un nuevo sistema de información institucional. Sin embargo, se cuenta con un conjunto de requerimientos estratégicos orientados a la **actualización, mantenimiento y modernización del Sistema de Información Misional SIP**, el cual es el núcleo de la operación institucional. Estos requerimientos buscan fortalecer la trazabilidad, mejorar la experiencia de usuario, integrar servicios digitales y consolidar la arquitectura de información.

Los principales requerimientos identificados para el fortalecimiento del SIP son:

- **Actualización e implementación de Series, Subseries y Tipos Documentales** en el módulo de Gestión Documental, permitiendo la clasificación automática de documentos digitales una vez se aprueben las Tablas de Retención Documental (TRD).
- **Creación de una función de suspensión de procesos**, que permita registrar:
 - Fecha de inicio
 - Fecha de finalización
 - Motivo de la suspensión
 - Usuario que realiza la acción

Esta funcionalidad mejorará el control y seguimiento de procesos repartidos.

- **Integración completa entre Personería en Línea y el SIP**, para garantizar trazabilidad, evitar duplicidad y facilitar el seguimiento de las atenciones virtuales.
- **Integración del formulario de PQRSD del portal web con el SIP**, permitiendo que todas las solicitudes ingresen de forma automática al sistema misional, con número único, trazabilidad y asignación de responsables.
- **Creación de un módulo de reportes y analítica** dentro del SIP, que permita consolidar la información misional, generar métricas institucionales, indicadores de gestión y análisis en tiempo real.



N° SC735-1



Otras iniciativas tecnológicas en ejecución

Además del fortalecimiento del SIP, la Personería avanza en las siguientes iniciativas clave:

- **Renovación de la página web institucional**, cumpliendo con la Ley de Transparencia, Gobierno Digital y accesibilidad web, incorporando:
 - Formulario moderno de PQRSD
 - Servicios ciudadanos digitales
 - Acceso a Personería en Línea
 - Sección de datos e informes públicos
- **Migración a la nube de los servicios institucionales** alojados en servidores virtuales, siguiendo la estrategia de transformación digital.

Este proceso incluye servicios tales como:

- Página web
- SIP
- Personería en Línea
- Base de datos institucional
- Centro de Pensamiento
- Intranet corporativa
- Moodle
- PQRSD

La migración a la nube ya se inició con el servicio de correo corporativo (Microsoft 365) y continúa con los demás sistemas para garantizar **mayor disponibilidad, seguridad, escalabilidad, continuidad del negocio y reducción del riesgo tecnológico.**

8.4.3. Evolución hacia un Sistema de Gestión de Documentos Electrónicos de Archivo – SGDEA



N° SC735-1



En cumplimiento de la Ley 594 de 2000, el Acuerdo 004 de 2019 del Archivo General de la Nación (AGN), el Modelo Integrado de Planeación y Gestión – MIPG, y los lineamientos del componente de Gestión Documental del Gobierno Digital, la Personería Distrital de Medellín orientará su arquitectura de sistemas hacia la implementación progresiva de un **Sistema de Gestión de Documentos Electrónicos de Archivo – SGDEA**, que actúe como plataforma transversal y rector del ciclo de vida documental institucional.

Actualmente, el Sistema de Información Misional SIP integra funcionalidades avanzadas para la gestión documental operativa, tales como:

- Clasificación documental por **series, subseries y tipos documentales**, conforme a las Tablas de Retención Documental (TRD).
- Módulos para **inventarios documentales**, incluyendo soportes, cajas, carpetas, fechas iniciales/finales, asuntos y frecuencias de consulta.
- Gestión de **transferencias primarias** desde las oficinas productoras.
- Registro documental asociado a trámites misionales, permitiendo trazabilidad y control de actuaciones.

Estas capacidades fortalecen la operación institucional; sin embargo, el SIP no cumple de manera integral los **requisitos archivísticos normativos** para ser considerado un SGDEA, particularmente en aspectos como preservación digital a largo plazo, metadatos archivísticos normalizados, interoperabilidad archivística OAIS, controles de autenticidad e integridad, y cadena de custodia digital certificada.

Dirección estratégica y transformación propuesta

La estrategia de TI para el periodo 2024–2028 contempla evolucionar hacia un modelo híbrido de gestión documental donde:

1. **El SIP se mantenga como sistema misional y transaccional**, responsable de la producción, gestión y clasificación operativa de documentos asociados a los procesos de atención, disciplinarios, administrativos y misionales.



N° SC735-1



2. **El SGDEA se implemente como sistema archivístico institucional**, encargado de administrar el ciclo de vida de los documentos desde su producción hasta su disposición final, garantizando:
 - metadatos archivísticos estándar (METS, PREMIS, Dublin Core, NTC-ISO 15489, NTC-ISO 30301)
 - preservación digital
 - autenticidad e integridad
 - auditoría documental
 - transferencias primarias y secundarias
 - interoperabilidad con el Archivo Central e Histórico.
3. Se establezca un **modelo de interoperabilidad SIP ↔ SGDEA** que permita:
 - Transferencia automática o programada de documentos desde el SIP al SGDEA con metadatos completos.
 - Trazabilidad integral entre gestión misional y gestión documental.
 - Eliminación de reprocesos y duplicidades.
 - Sincronización de metadatos, TRD, tablas de valoración documental (TVD) y estados archivísticos.
 - Integración con repositorios electrónicos y servicios de preservación.
4. Se garantice que los documentos electrónicos generados desde aplicativos como SIP, Personería en Línea, SIG, PQRSD, Intranet o correo institucional sean **transferidos, preservados y gestionados** en el SGDEA conforme al AGN.

Impacto institucional esperado

La implementación del SGDEA interoperable permitirá:



N° SC735-1



- Cumplimiento pleno de la normativa archivística del AGN.
- Preservación del patrimonio documental institucional a largo plazo.
- Mejora de la trazabilidad, transparencia y auditoría del ciclo documental.
- Reducción de riesgos institucionales por pérdida, reproceso o incumplimiento normativo.
- Estandarización de la gestión documental en todos los procesos.
- Articulación con políticas de Seguridad de la Información (ISO 27001) y Gobierno Digital.
- Fortalecimiento del SIP como sistema transaccional y operativo, sin sobrecarga de funciones archivísticas.

La interoperabilidad entre SIP y el SGDEA consolidará una arquitectura documental moderna, sostenible y alineada con las necesidades misionales, técnicas y normativas de la Personería Distrital de Medellín, contribuyendo al fortalecimiento del ecosistema de información institucional.

8.4.4. Servicios de soporte técnico

Para mantener en óptimas condiciones los sistemas de información y servicios tecnológicos de la entidad, se definieron los tiempos de atención de incidentes y nivel de servicio (ANS) para la gestión de la plataforma, los cuales se pueden resolver de forma presencial y/o remota.

La meta es mantener todos los servicios de la Personería Distrital de Medellín, en alta disponibilidad y con un soporte presencial o remoto las 24 horas, el cual permita garantizar la continuidad de los servicios que se presta en la entidad.

Para el soporte remoto, Innovación y Conocimiento utiliza la herramienta Team Viewer, la cual se usa en las grandes compañías para realizar el soporte técnico a sedes satélites. Esta herramienta permite tomar control de los equipos y brindar la solución que se requiere interactuar con el usuario vía chat o llamada telefónica.



N° SC735-1



Para el soporte presencial se establece las siguientes premisas, las cuales permiten tener un soporte de solicitudes en la mesa de ayuda y la eficiencia en la solución de estas:

- ✓ Solicitar soporte técnico a través de la mesa de ayuda destinada para este, la cual se encuentra publicada en la intranet corporativa.
- ✓ Para efectos de brindar los primeros auxilios de soporte (cables de energía, red de datos y voz, asesoría en herramientas ofimáticas y Sistemas de información), se recomienda delegar una persona con características técnicas a quien se le brindará la capacitación técnica más enfocada a los servicios que se presta por cada Sede Satélite para proveer los primeros auxilios, y que interactúa con los ingenieros para brindar las soluciones.
- ✓ El servicio de soporte no contempla la capacitación en herramientas ofimáticas, ni tareas personales.
- ✓ El soporte de impresoras se realiza a través de outsourcing por la empresa que tenga el contrato, y solo se realiza soporte de primeros auxilios por parte de Innovación y Conocimiento.
- ✓ Los cambios y modificaciones en los sistemas de información deben realizarse a través de un levantamiento de requerimientos y ser evaluados desde planeación, ya que pueden ser cambios transversales que afecten otros procesos.
- ✓ Para la configuración de los puestos de trabajo sistemas recomienda que se tenga un máximo tres usuarios por equipo, para no afectar el rendimiento.

Tiempos de incidentes y tiempos de solución:

INCIDENTE	TIEMPO DE NOTIFICACIÓN	TIEMPOS DE RESPUESTA
Critico	Inmediato	30 min
Alto	15 min	1 hora



N° SC735-1



Medio	30 min	2 horas
Bajo	30 min	4horas
Crítico: Cuando el sistema está fuera de servicio.		
Alto: Situación que se presenta y genera impacto mayor para el negocio sobre el servicio por indisponibilidad de algunas componentes críticas del mismo.		
Medio: Cuando el sistema continúa funcionando con impedimentos menores y las tareas pueden continuar con una mínima disminución de performance.		
Bajo: Situación que se presenta pero que no genera afectación del servicio o cuando la entidad requiera una consulta técnica y/o de uso.		

	Cantidad	Tiempo de revisión y/o aprobación	Tiempo de ejecución
Cambio de políticas y/o configuración	Ilimitado	2 horas	4 horas
Cambios de políticas y/o configuración de Emergencia	2/mes	30 min	1 hora
Cambios de infraestructura	A convenir		

8.5. Modelo de gestión de servicios tecnológicos

8.5.1. Criterios de calidad y procesos de gestión de servicios de TIC

La calidad de los servicios de Tecnologías de la Información en la Personería Distrital de Medellín se garantiza mediante la aplicación de criterios técnicos, operativos y de seguridad definidos en los Acuerdos de Nivel de Servicio (ANS)



N° SC735-1



descritos en el numeral 8.4.3, y se articula con las políticas del Sistema de Gestión de Seguridad de la Información (SGSI) y el Modelo de Gobierno Digital del MinTIC.

Con la implementación de la estrategia de migración de sistemas a la nube, se espera un aumento significativo en la disponibilidad, estabilidad y eficiencia de los servicios tecnológicos, lo que permitirá ofrecer a los funcionarios, colaboradores y ciudadanía una experiencia más ágil, segura y confiable.

Los criterios de calidad y los procesos de gestión de servicios TIC se fundamentan en los siguientes aspectos:

1. Disponibilidad y rendimiento

- Infraestructura en la nube con alta disponibilidad.
- Mayor velocidad de procesamiento para consultas, cargas y descargas.
- Menor latencia en servicios que antes dependían del centro de datos físico.
- Reducción de interrupciones derivadas de fallos de hardware o recursos locales.

2. Seguridad de la información

- Controles avanzados mediante FortiGate, FortiWeb y FortiEDR.
- Autenticación centralizada con Azure AD y políticas Zero Trust.
- Cifrado en tránsito y en reposo.
- Monitoreo continuo y alertas ante incidentes.
- Cumplimiento de políticas del SGSI e ISO 27001.

3. Continuidad y contingencia

- Copias de seguridad automáticas y almacenamiento en infraestructura redundante.
- Menor riesgo de pérdida de información por desastres locales.
- Capacidad de recuperación más rápida ante fallos de sistemas o ataques cibernéticos.
- Acceso remoto seguro en caso de contingencias operativas.

4. Trazabilidad y gestión de incidentes

- Mesa de Ayuda institucional con registro de tickets de soporte.
- Indicadores de tiempos de respuesta, cierre y reincidencias.
- Priorización de incidentes por criticidad.



N° SC735-1



- Auditoría permanente a servicios tecnológicos, accesos y eventos de seguridad.

5. Calidad en la prestación del servicio

- Cumplimiento de ANS para soporte, disponibilidad y tiempos de recuperación.
- Evaluación periódica de satisfacción de usuarios internos.
- Actualización preventiva de servidores, sistemas y plataformas cloud.
- Revisión de indicadores de desempeño y mejora continua.

6. Mejora continua basada en demanda

- Evaluación permanente del uso de servicios misionales como SIP, Personería en Línea, PQRSD y Citas.
- Identificación de cuellos de botella y optimización de recursos.
- Incorporación progresiva de automatización e inteligencia artificial.
- Ajustes a los servicios tecnológicos conforme a los cambios institucionales.

Con estos criterios, la Personería Distrital de Medellín asegura que la gestión de servicios TIC se realice de forma eficiente, segura y alineada con los objetivos estratégicos institucionales y con las necesidades de atención a la ciudadanía, garantizando así un servicio de alta calidad y una operación tecnológica sostenida.

8.5.2. Infraestructura

La Personería Distrital de Medellín ha iniciado un proceso progresivo de transformación digital orientado a la modernización de su infraestructura tecnológica y a la migración de servicios estratégicos hacia la nube. Este proceso tiene como propósito mejorar la eficiencia operativa, aumentar la continuidad del servicio, fortalecer la seguridad de la información y optimizar los recursos físicos del centro de datos.

Durante las vigencias 2024–2025 se han ejecutado las siguientes acciones:

- **Migración a la nube de servicios institucionales**, tales como:
 - Correo corporativo (Exchange Online).
 - SIG institucional en SharePoint.



N° SC735-1



- Personería en Línea.
 - PQRSD.
 - Citas en Línea.
 - Portal Web institucional.
 - Ambientes de prueba para sistemas misionales.
 - Parte del almacenamiento documental.
- **Modernización del parque tecnológico**, con la adquisición e instalación de **295 equipos de escritorio de última generación**, equipados con:
 - **32 GB de memoria RAM**
 - **Unidades de estado sólido (SSD)**
 - **Sistemas operativos actualizados**
 - **UPS individuales para protección eléctrica**
 - **Actualización del Centro de Datos**, que opera con:
 - Servidores con **Windows Server 2022**
 - Controladores de dominio integrados con Azure AD
 - Sistemas de virtualización
 - Aire de precisión y UPS en operación estable
 - Segmentación de red bajo VLAN e implementación de **IPv6**
 - **Fortalecimiento de la seguridad perimetral y de aplicaciones**, con:
 - **FortiGate** como firewall de próxima generación (NGFW)
 - **FortiWeb** para protección de aplicaciones web (WAF)
 - **FortiEDR** como sistema de protección avanzada para endpoints
 - Inspección SSL, IPS, filtrado web y control de aplicaciones
 - **Optimización energética y operativa:**

La migración progresiva a la nube ha permitido apagar varios servidores que anteriormente estaban en operación continua, reduciendo:

- Consumo eléctrico
- Carga térmica del Centro de Datos
- Uso del aire de precisión
- Desgaste del sistema UPS

Proyecciones de Infraestructura 2025–2028



N° SC735-1



En línea con el PETI y el Plan Estratégico Institucional, se proyectan las siguientes acciones:

- **Migración total a la nube de los sistemas misionales**, incluyendo SIP, Centro de Pensamiento, base de datos institucional y la Intranet.
- **Implementación de un ambiente cloud híbrido**, combinando servicios de Azure y hosting especializado.
- **Integración completa de autenticación mediante Azure AD** para todos los sistemas institucionales.
- **Renovación tecnológica 2025–2026**, que contempla la adquisición de **290 computadores de escritorio All-in-One**, orientados a completar la modernización del parque tecnológico.
- **Reemplazo progresivo de servidores físicos** que queden obsoletos o en desuso tras la migración total a la nube.
- **Optimización de la red institucional**, reforzando:
 - Conectividad dedicada
 - VLAN por procesos
 - Red WiFi segmentada para funcionarios y ciudadanía
 - Integración con Fortinet y políticas de seguridad Zero Trust
- **Fortalecimiento de la infraestructura de seguridad**, incluyendo:
 - Alta disponibilidad para FortiGate
 - Nuevas capacidades avanzadas de EDR
 - Inteligencia artificial en la detección de amenazas

8.5.3. Conectividad

La Personería Distrital de Medellín continúa fortaleciendo su infraestructura de conectividad para garantizar disponibilidad, estabilidad, seguridad y velocidad en el acceso a los servicios tecnológicos institucionales. Para ello, se ha proyectado y



N° SC735-1



ejecutado una modernización progresiva de la red, tanto a nivel interno como en las conexiones externas entre sedes.

Como iniciativa prioritaria dentro del PETI 2024–2028, se está implementando un **backbone de fibra óptica** que conectará directamente la nueva sede central con el centro de datos institucional. Esta mejora permitirá:

- Mayor capacidad de transmisión de datos.
- Reducción significativa de la latencia.
- Mayor estabilidad en servicios misionales críticos (SIP, Personería en Línea, PQRSD).
- Conectividad óptima para servicios en nube y autenticación con Azure AD.
- Preparación para futuras actualizaciones de ancho de banda y servicios avanzados.

Las demás conexiones institucionales se mantienen con las capacidades actuales y con los siguientes componentes estructurales:

Conectividad entre sedes

- Enlaces **LAN to LAN** de **30 Mb** para la UPDH y la Alcaldía de Medellín.
- Conectividad principal con Internet dedicado de **500 Mb** para la sede central.
- Red preparada para servicios misionales, video, aplicaciones web y autenticación cloud.

Red interna y segmentación

- La red institucional opera bajo una arquitectura **LAN – VLAN – WiFi**.
- Segmentación por procesos, áreas y servicios para mejorar seguridad y desempeño.
- Implementación completa de **IPv6**, cumpliendo con lineamientos modernos de conectividad.

WiFi institucional

- Red WiFi interna para funcionarios, aislada de la red LAN.
- WiFi para ciudadanía mediante **portal cautivo**, con controles de seguridad y navegación administrados por FortiGate.



N° SC735-1



- Capacidad suficiente para salas de atención, conciliaciones y áreas comunes.

Seguridad y administración de red

- **FortiGate** administra:
 - Políticas de navegación
 - DHCP centralizado
 - Filtrado web
 - Inspección SSL
 - IDS/IPS
 - Control de aplicaciones
 - Segmentación segura de VLAN
- Monitoreo y control permanente del tráfico para prevenir ataques, garantizar disponibilidad y proteger datos.

Conexión con sistemas externos

- Conectividad directa con la Red SAP de la Alcaldía de Medellín para Gestión Financiera y Gestión de Bienes Administrativos.
- Integración estable y segura para garantizar operación continua en procesos administrativos.

Proyecciones 2025–2028

- Ampliación del backbone para soportar mayor tráfico y crecimiento digital.
- Optimización de VLAN y políticas de seguridad Zero Trust.
- Mayor capacidad para videoconferencias, servicios cloud y plataformas misionales.

8.5.4. Servicios de operación

Para garantizar la operación continua, segura y eficiente de la plataforma tecnológica institucional, la Personería Distrital de Medellín cuenta con un equipo especializado contratado bajo la modalidad de prestación de servicios, encargado de la administración de infraestructura, soporte técnico, mantenimiento de aplicaciones, modernización de sistemas de información y gestión operativa.

El equipo técnico está conformado por:



N° SC735-1



- **Dos ingenieros de sistemas**, responsables del centro de datos, servidores físicos y virtuales, servicios en la nube, seguridad Fortinet, Microsoft 365, bases de datos y coordinación operativa.
- **Un programador/desarrollador**, encargado del mantenimiento y evolución de sistemas como SIP, Personería en Línea, PQRSD, Citas e intranet, además del desarrollo de nuevas funcionalidades y automatizaciones.
- **Un diseñador web / webmaster**, encargado del mantenimiento y actualización de la página web institucional, contenidos digitales, accesibilidad y cumplimiento de la Ley de Transparencia.
- **Un tecnólogo en sistemas**, responsable de soporte de segundo nivel, instalación de equipos, actualizaciones, configuración de software y apoyo en sedes.
- **Un técnico en sistemas**, encargado de soporte de primer nivel, instalación de equipos, red de impresión, asistencia en salas de audiencias, mesas de ayuda y acompañamiento operativo.

Funciones clave dentro de los Servicios de Operación

1. Administración de infraestructura y centro de datos

Los ingenieros de sistemas realizan:

- Administración y monitoreo del dominio **PERSONERIA.COM**.
- Gestión de servidores Windows Server 2022, virtualización, almacenamiento y backup.
- Supervisión de energía, UPS, aire de precisión y ambiente del centro de datos.
- Evaluación de alertas, rendimiento y disponibilidad de la infraestructura.

2. Administración de servicios en la nube

Incluyendo:

- Exchange Online, Azure AD, SharePoint, OneDrive, Teams.



N° SC735-1



- Migración progresiva de sistemas institucionales (SIP, Intranet, Personería en Línea, SIG en SharePoint).
- Integración de autenticación mediante Azure AD.

3. Seguridad informática

En coordinación con el SGSI:

- Operación de **FortiGate** (DHCP, IPS, inspección SSL, control de acceso, filtrado web).
- Operación de **FortiWeb** (protección de aplicaciones web).
- Operación de **FortiEDR** en todos los equipos institucionales.
- Monitoreo diario de eventos y alertas de seguridad.
- Reporte de incidentes y recomendaciones de mitigación.

4. Mantenimiento y evolución de aplicaciones

El equipo de Innovación y Conocimiento asegura la operación de:

- SIP
- Personería en Línea
- Citas en Línea
- PQRSD
- Intranet
- SIG
- Moodle
- Mesa de ayuda
- Portal web institucional

Incluyendo:

- Actualización de módulos.
- Integraciones (SIP – PQRSD – Personería en Línea – Citas).
- Corrección de errores.
- Mejora de funcionalidades.
- Soporte funcional y técnico.



N° SC735-1



5. Soporte técnico a funcionarios

A través de la Mesa de Ayuda se brinda:

- Soporte de primer y segundo nivel.
- Configuración de equipos (Windows 10/11, Office 365, SIP, SIG, impresoras).
- Atención a sedes externas (UPDH, conciliaciones, palacio de justicia).
- Acompañamiento en salas de audiencias y brigadas móviles.
- Registro, trazabilidad y solución de incidentes.

6. Gestión de licencias y actualizaciones

Incluye:

- Renovación de licencias de software institucional.
- Gestión de M365, Fortinet y herramientas corporativas.
- Actualización de sistemas operativos, parches y antivirus.
- Validación de cumplimiento de software autorizado.

7. Modernización tecnológica permanente

El equipo propone y ejecuta proyectos de modernización como:

- Migración a la nube
- SIP 2.0
- Integraciones mediante API institucional
- Actualización del portal web
- Implementación de nuevas soluciones digitales
- Limpieza y depuración de datos
- Automatización e inteligencia artificial
- Renovación tecnológica del parque computacional

Con este modelo de servicios de operación, la Personería asegura:

- Continuidad del servicio 24/7
- Atención oportuna a incidentes



N° SC735-1



- Seguridad avanzada
- Confiabilidad de los sistemas
- Disponibilidad para funcionarios y ciudadanía
- Alineación con el PETI y con el Plan Estratégico 2024–2028

8.5.5. Mesa de servicios

La Mesa de Servicios de Innovación y Conocimiento es el punto único de contacto entre los usuarios de la Personería Distrital de Medellín y los servicios tecnológicos institucionales. Su propósito es garantizar una atención **eficiente, eficaz, efectiva, segura y oportuna** a todos los requerimientos relacionados con el uso, operación y disponibilidad de los sistemas de información, infraestructura tecnológica y servicios de TI.

La Mesa de Servicios opera bajo **Acuerdos de Nivel de Servicio (ANS)** definidos por Innovación y Conocimiento, los cuales establecen los tiempos máximos de respuesta, solución, priorización, escalamiento y retroalimentación para los usuarios internos. Estos ANS permiten asegurar estándares homogéneos de calidad, trazabilidad y satisfacción.

Funciones principales de la Mesa de Servicios

1. Recepción y registro de solicitudes

- Registro de incidentes, requerimientos y consultas a través del sistema web de Mesa de Ayuda.
- Clasificación automática y manual según tipo de servicio:
- Sistemas de información (SIP, Personería en Línea, PQRSD, Intranet, SIG, Citas, Moodle).
- Servicios tecnológicos (internet, red, WiFi, impresión, hardware, software).
- Seguridad informática (EDR, FortiGate, FortiWeb, Microsoft Defender, accesos).
- Servicios cloud (Office 365, Azure AD, SharePoint, Exchange Online).

2. Priorización basada en ANS

Las solicitudes se gestionan según criticidad:



N° SC735-1



- **Prioridad Crítica (P1):** Caída de servicios misionales (SIP, Personería en Línea, PQRSD), caída de red, afectación masiva.
- **Alta (P2):** Incidentes que afectan procesos misionales individuales o servicios estratégicos.
- **Media (P3):** Fallas en equipos de usuario, problemas de impresión, bloqueo de cuenta, lentitud.
- **Baja (P4):** Solicitudes de cambios, instalación de software, requerimientos de mejora.

Cada prioridad cuenta con tiempos de atención definidos en los ANS institucionales.

3. Seguimiento, actualización y trazabilidad

- Monitoreo permanente del estado de cada ticket.
- Registro de evidencias, acciones realizadas, tiempos de resolución y responsables.
- Notificación automática al usuario sobre avances y cierre.
- Históricos exportables para auditoría del SGSI y del Sistema Integrado de Gestión.

4. Escalamiento técnico

Cuando el incidente supera el nivel de atención inicial, se activa:

- **Escalamiento a segundo nivel** (tecnólogo o ingeniero).
- **Escalamiento funcional** al desarrollador del SIP o Personería en Línea.
- **Escalamiento especializado** a administradores de red, servidores, Fortinet o cloud.

Este proceso garantiza resolución dentro de los tiempos pactados en los ANS.

5. Soporte en sitio y remoto

- Soporte remoto para sedes satélite, conciliaciones y corregimientos.
- Soporte presencial cuando el tipo de incidente lo requiere (equipos, impresoras, red física).
- Acompañamiento técnico en salas de audiencia, brigadas móviles y eventos institucionales.

6. Cumplimiento de ANS



N° SC735-1



La Mesa de Servicios se mide con indicadores basados en ANS como:

- Tiempo promedio de atención
- Tiempo promedio de solución
- Porcentaje de incidentes atendidos dentro del tiempo objetivo
- Tasa de reincidencias
- Satisfacción del usuario final

Estos indicadores permiten optimizar la operación y garantizar la calidad del servicio.

7. Gestión del conocimiento

La Mesa de Servicios mantiene un repositorio actualizado con:

- Manuales de usuario
- Guías rápidas
- Buenas prácticas
- Preguntas frecuentes
- Procedimientos estandarizados

Este conocimiento fortalece el uso adecuado de los sistemas y reduce incidencias recurrentes.

8. Contribución a la transformación digital

La Mesa de Servicios se convierte en un mecanismo clave para:

- Medir la madurez digital de la Entidad.
- Identificar necesidades de mejora y oportunidades de automatización.
- Garantizar disponibilidad de los servicios 24/7 para la ciudadanía.
- Soportar la operación de la Personería en línea, PQRS, citas, buzón ciudadano y servicios digitales.

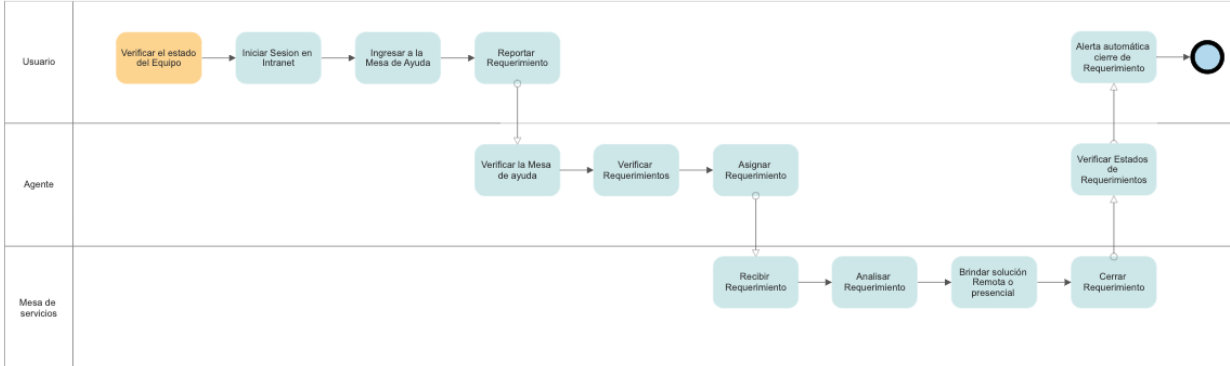
Con su operación robusta, la Mesa de Servicios asegura que funcionarios y ciudadanos cuenten con plataformas confiables, seguras y alineadas al Plan Estratégico Institucional 2024–2028.



N° SC735-1



Mesa de ayuda Online



8.5.6. Procedimientos de gestión

La gestión informática en la Personería Distrital de Medellín avanza hacia un modelo estratégico orientado a ofrecer servicios de Tecnologías de la Información y las Telecomunicaciones (TIC) altamente eficientes, seguros y alineados con los objetivos del Plan Estratégico Institucional 2024–2028 y el programa “Transformación Digital para la Personería”.

El propósito de Innovación y Conocimiento es consolidarse como un proceso clave para la modernización de la Entidad, aportando soluciones tecnológicas innovadoras, ágiles y sostenibles, que mejoren el funcionamiento institucional, fortalezcan la prestación de los servicios misionales y permitan responder a los retos actuales relacionados con la seguridad, la digitalización, la analítica de datos y la inteligencia artificial.

Enfoque estratégico de los procedimientos de gestión

Innovación y Conocimiento evoluciona hacia un modelo en el cual:

- Los procedimientos son **proactivos**, orientados al análisis, prevención y mejora continua.
- Se prioriza la **transformación digital**, la automatización y la calidad del servicio.



N° SC735-1



- Los servicios de TIC se integran con la infraestructura cloud, sistemas misionales, seguridad Fortinet, Microsoft 365 y el SGSI.
- El proceso se percibe como un **aliado estratégico**, no solo como un área de soporte.
- Se fomenta la investigación, innovación y adopción de nuevas tecnologías, incluyendo pilotos con IA y análisis avanzado de datos.

Este enfoque permite que la Personería sea una entidad más ágil, moderna, segura y centrada en el ciudadano.

Modernización de los procedimientos institucionales

Para la vigencia 2025-2028 se proyecta realizar una actualización completa de los procedimientos documentados en:

1. Sistema de Gestión de la Calidad (SIG) – ISO 9001

Se ajustarán procedimientos relacionados con:

- Soporte a usuarios
- Gestión de infraestructura
- Gestión de sistemas de información
- Actualización y mantenimiento del SIP
- Documentación de procesos asociados a servicios digitales (Personería en Línea, Citas, PQRSD)

2. Sistema de Gestión de Seguridad de la Información (SGSI) – ISO 27001

Se actualizarán procedimientos para incorporar:

- Controles relacionados con FortiGate, FortiWeb, FortiEDR
- Políticas Zero Trust
- Gestión de accesos con Azure AD
- Nuevas tecnologías en la nube
- Gestión de vulnerabilidades y respuesta a incidentes
- Procedimientos de auditoría interna de seguridad

3. Arquitectura tecnológica y operaciones

Se actualizarán los lineamientos relacionados con:

- Migración de servicios a la nube (SIP, Intranet, web, PQRSD, Personería en Línea)



N° SC735-1



- Integraciones mediante API institucional
- Gestión del centro de datos híbrido
- Virtualización, backup y recuperación ante desastres
- Segmentación de red y administración VLAN
- Gestión de parches y actualizaciones
- Monitoreo preventivo de la infraestructura Fortinet

Procedimientos orientados a las líneas estratégicas de las TIC

Los nuevos procedimientos estarán alineados con los ejes del PETI:

- Gobierno de TI
- Gestión de servicios
- Gestión de la información y analítica
- Seguridad de la información
- Arquitectura de sistemas
- Innovación y tecnología emergente

Esto incluye:

- Escalamiento estructurado por niveles de soporte (ANS).
- Procedimientos para pruebas en ambientes aislados.
- Controles de calidad para desarrollos y actualizaciones.
- Estándares de documentación técnica.
- Procedimientos para integraciones, interoperabilidad y limpieza de datos.
- Directrices para proyectos de automatización e IA.

Objetivo final del ajuste de procedimientos (2025–2028)

Crear un marco operativo que permita:

- Mantener servicios de TI estables, seguros y escalables.
- Garantizar la continuidad operativa de los sistemas misionales.
- Optimizar recursos y fortalecer la cultura digital.
- Alinear las TIC con los objetivos estratégicos institucionales.
- Incrementar la satisfacción del usuario interno y externo.
- Garantizar el cumplimiento normativo en materia de Gobierno Digital, SIG y SGSI.



N° SC735-1



8.5.7. Plan de Contingencia, Recuperación ante Desastres y Continuidad Operativa (DRP/BCP)

La Personería Distrital de Medellín requiere garantizar la continuidad de los servicios tecnológicos que soportan la operación misional y administrativa. Para ello, se implementará un **Plan de Contingencia y Recuperación ante Desastres (DRP)** articulado con un **Plan de Continuidad Operativa (BCP)**, aplicable al centro de datos local y a los servicios migrados a la nube.

El DRP/BCP definirá los procedimientos para restablecer los sistemas críticos ante fallas de infraestructura, incidentes de ciberseguridad, pérdida de servicios en la nube, fallos eléctricos o desastres físicos. Este plan establecerá responsables, recursos, tiempos de recuperación y mecanismos de comunicación interna.

Los sistemas considerados críticos incluyen: SIP, Personería en Línea, servicios de correo y colaboración (Microsoft 365), autenticación y directorio (Azure AD), red corporativa, sistemas de seguridad Fortinet (FortiGate, FortiWeb, FortiEDR), servidores de archivos y sistemas de gestión documental.

Las estrategias principales del DRP incluyen:

- Respaldos automáticos locales y en la nube
- Replicación de información crítica.
- Mecanismos de acceso remoto seguro;
- Uso de equipos portátiles para continuidad operativa en campo;
- Monitoreo permanente de seguridad;
- Procedimientos estandarizados de restauración.

El DRP/BCP será actualizado anualmente por Innovación y Conocimiento y revisado por el Comité de Seguridad de la Información, alineándose con el SGSI, Gobierno Digital, MIPG y los lineamientos del Archivo General de la Nación.

8.6. Uso y apropiación

La Personería Distrital de Medellín, como ente de control y garante de los Derechos Humanos, requiere que sus funcionarios, colaboradores y contratistas cuenten con



N° SC735-1



las competencias digitales necesarias para desempeñar sus funciones mediante el uso adecuado, eficiente y seguro de los sistemas de información y servicios tecnológicos institucionales.

Dado que gran parte de las actividades misionales dependen del acceso y uso de plataformas como SIP, Personería en Línea, PQRSD, Intranet, Citas en Línea, SIG, Microsoft 365 y las herramientas de analítica, el fortalecimiento del uso y apropiación de las TIC se convierte en un componente estratégico para garantizar una atención oportuna, transparente y efectiva a la ciudadanía.

Apropiación tecnológica desde el ingreso de los funcionarios

En los procesos de inducción y reinducción institucional se presenta el rol del proceso de Innovación y Conocimiento como un aliado estratégico que:

- Provee las herramientas tecnológicas necesarias (equipos, licencias, accesos).
- Explica los sistemas de información que soportan los procesos misionales.
- Orienta sobre el uso seguro de la tecnología bajo las políticas del SGSI.
- Sensibiliza sobre la importancia de la seguridad de la información, el uso adecuado de datos, la gestión documental digital y la trazabilidad institucional.

De acuerdo con el cargo y las funciones, cada funcionario recibe las herramientas tecnológicas necesarias para su labor: computador renovado, acceso a Office 365, licencias, SIP, Personería en Línea, Intranet y sistemas de apoyo.

Gestión del cambio y socialización tecnológica

Cada vez que se implementa un nuevo sistema, actualización o mejora en los servicios tecnológicos, Innovación y Conocimiento realiza:

- Socialización formal de las mejoras.



N° SC735-1



- Capacitación funcional sobre nuevas herramientas o módulos.
- Manuales de usuario y guías prácticas.
- Publicación de cambios en la Intranet.
- Acompañamiento inicial en la adopción.
- Soporte prioritario durante las primeras semanas.

Este proceso garantiza continuidad en el trabajo y minimiza traumatismos.

Formación tecnológica continua

En línea con la “Transformación Digital para la Personería” (Plan Estratégico 2024–2028), la entidad avanza en el fortalecimiento de capacidades digitales mediante:

- **Capacitación en Microsoft 365** enfocada en productividad, colaboración, Teams, SharePoint, OneDrive y herramientas cloud.
- Actualización en el uso de SIP, Personería en Línea, PQRSD y sistemas misionales.
- Uso de Moodle como plataforma de formación institucional.
- Sensibilización permanente en políticas de seguridad de la información del SGSI.
- Formación en analítica de datos utilizando Power BI, Excel avanzado y dashboards institucionales.
- Capacitaciones dirigidas a delegados, jefes de oficina y equipos misionales para fortalecer la toma de decisiones basada en datos.

Uso seguro y responsable de la tecnología

Dentro de las actividades de apropiación se incluyen:

- Publicación y socialización de las **Políticas de Seguridad de la Información**.
- Capacitación en protección de datos personales, contraseñas seguras, phishing, uso adecuado del correo institucional.
- Prácticas de trabajo remoto seguro y autenticación con Azure AD.
- Aplicación de las directrices del SGSI e ISO 27001.
- Estas acciones buscan crear una cultura institucional responsable y resiliente frente a riesgos tecnológicos.



N° SC735-1



Apropiación de los servicios digitales para la ciudadanía

El fortalecimiento del uso y apropiación de tecnologías no solo se realiza hacia los funcionarios, sino también hacia la ciudadanía mediante:

- Socialización del sistema de **Personería en Línea**.
- Uso de **Citas en Línea** para agendamiento con profesionales y abogados.
- Portal de **PQRSD** para la radicación y seguimiento de solicitudes.
- Acceso a la plataforma de **Moodle** para cursos y formación ciudadana.

Con esto se reduce la presencialidad, mejora la oportunidad del servicio y fortalece el enfoque de gobierno digital.

Objetivo final de la apropiación tecnológica

Impulsar una cultura digital sólida que permita:

- Un funcionamiento institucional más ágil y eficiente.
- Procesos misionales fortalecidos con tecnología.
- Alta calidad en los servicios prestados a la ciudadanía.
- Seguridad y protección de la información.
- Una Personería moderna, digital y adaptada a los desafíos actuales.

9. MODELO DE PLANEACIÓN

En esta fase se formula el Plan Estratégico de Tecnologías de la Información (PETI), en el cual se define el modelo de operación de TI, las estrategias por cada uno de los componentes del modelo de referencia, el portafolio de proyectos estratégicos y operativos, así como la proyección de los recursos financieros necesarios para garantizar la sostenibilidad tecnológica de la Personería Distrital de Medellín durante el periodo 2024–2028.

El modelo de planeación articula la estrategia institucional, el programa de Transformación Digital, las necesidades misionales y el avance tecnológico logrado durante las vigencias recientes, incluyendo la migración progresiva a la nube, el



N° SC735-1



fortalecimiento de la ciberseguridad, la modernización del parque computacional y la evolución del ecosistema de sistemas de información.

9.1. Lineamientos y Principios que Rigen el Plan Estratégico de TIC – Versión Actualizada

Los siguientes principios orientan la formulación, implementación y actualización del PETI, garantizando su coherencia con los lineamientos del gobierno digital, el SGSI, el SIG, la arquitectura institucional y la planificación estratégica de la Personería Distrital de Medellín:

1. El PETI como herramienta viva y en evolución permanente

El PETI es un instrumento flexible y dinámico que debe revisarse periódicamente para ajustarse a los cambios institucionales, tecnológicos y normativos. Refleja el estado actual de la tecnología y anticipa las necesidades futuras, especialmente en entornos donde prevalece la transformación digital, la nube, la seguridad y la analítica.

2. Participación activa de Innovación y Conocimiento en la toma de decisiones

La presencia del proceso en los Comités Estratégicos y de Dirección es fundamental para asegurar la correcta alineación entre la estrategia institucional y las decisiones tecnológicas. Su participación garantiza análisis oportunos, priorización de proyectos y definición coherente de la arquitectura tecnológica.

3. La tecnología como medio para la misión institucional

La tecnología no es un fin en sí misma; es un habilitador que soporta y fortalece el cumplimiento de la misión de la Personería: la defensa, promoción y garantía de los Derechos Humanos. Por ello, las decisiones de TI deben alinearse con las necesidades misionales, el servicio a la ciudadanía y la mejora de la gestión interna.

4. Apoyo tecnológico según nivel de madurez y disponibilidad



N° SC735-1



La implementación de soluciones tecnológicas debe considerar el nivel de desarrollo de cada proceso, su capacidad de adopción, la apropiación de herramientas digitales por parte de los funcionarios y la disponibilidad de plataformas tecnológicas seguras y confiables.

5. Seguridad de la información como principio transversal

Todas las decisiones del PETI se fundamentan en los lineamientos del SGSI basado en ISO 27001, la política de Gobierno Digital y los controles implementados con Fortinet, Azure AD y otros sistemas. La seguridad, privacidad, trazabilidad y disponibilidad de la información es un eje central del modelo de planeación.

6. Interoperabilidad e integración como prioridad institucional

La Planeación de TI prioriza la integración entre el SIP, Personería en Línea, PQRSD, Citas, SIG, Intranet y otros sistemas, promoviendo una arquitectura interoperable, eficiente y acorde con las exigencias del Estado colombiano.

7. Eficiencia y optimización del uso de recursos

Las acciones del PETI estarán orientadas a reducir costos mediante la migración a la nube, automatización, estandarización de procesos, modernización del hardware, y fortalecimiento del soporte técnico y operativo.

8. Digitalización como motor de la Transformación Institucional

Los lineamientos del PETI buscan impulsar la cultura digital en los funcionarios, fomentando el uso de servicios digitales, la capacitación continua y la adopción progresiva de tecnologías emergentes como analítica avanzada, automatización e inteligencia artificial.



N° SC735-1



Proyección de Proyectos TI 2025–2028

Servicios Tecnológicos

Año	Proyecto	Meta Estratégica	Inversión Proyectada
2025	Renovación tecnológica parcial (120 equipos AIO)	Modernizar áreas críticas.	\$ 420.000.000
2025	Backbone de fibra sede-datacenter	Conectividad estable.	\$ 120.000.000
2026	Renovación parcial de switches	Mejorar red interna.	\$ 150.000.000
2027	WiFi 6 institucional (fase 1)	Cobertura y seguridad.	\$ 120.000.000
2028	Migración gradual a nube híbrida	Reducción de carga local.	\$ 200.000.000

Sistemas de Información

Año	Proyecto	Meta Estratégica	Inversión Proyectada
2025	SIP 2.0 – Actualización parcial	Reportes + integraciones.	\$ 300.000.000
2026	Integración Personería en Línea – SIP	Unificar atención.	\$ 200.000.000

2027	Actualización página web y transparencia	Cumplimiento normativo.	\$ 80.000.000
2028	Modernización Intranet–SIG (fase 1)	Centralización documental.	\$ 120.000.000

Seguridad de la Información

Año	Proyecto	Meta Estratégica	Inversión Proyectada
2025	Expansión FortiEDR (200 equipos)	Protección endpoint.	\$ 150.000.000
2026	Actualización FortiWeb	Protección OWASP.	\$ 90.000.000
2027	Auditoría SGSI / ISO 27001	Cierre de brechas.	\$ 70.000.000
2028	DRP básico en nube	Continuidad del negocio.	\$ 130.000.000

Gobierno de TI

Año	Proyecto	Meta Estratégica	Inversión Proyectada
2025	Actualización SIG/SGSI	Alineación Gobierno Digital.	\$ 0
2026	Comité Arquitectura TI	Gobernanza.	\$ 0
2027	Implementación ITSM	Mesa con ANS.	\$ 280.000.000
2028	Integración PETI–PEI	Actualización estratégica.	\$ 0

Uso y Apropiación



N° SC735-1



Año	Proyecto	Meta Estratégica	Inversión Proyectada
2025	Capacitación Office 365	Productividad.	\$ 20.000.000
2026	Capacitación SIP + reportes	Apropiación.	\$ 15.000.000
2027	Capacitación en seguridad digital	Reducción incidentes.	\$ 10.000.000
2028	Capacitación Gobierno Digital	Cumplimiento.	\$ 10.000.000

Innovación y Tecnología Emergente (IA)

Año	Proyecto	Meta Estratégica	Inversión Proyectada
2025	Piloto IA SIP	Clasificación básica.	\$ 30.000.000
2026	Automatización PQRSD	Respuestas automáticas.	\$ 40.000.000
2027	IA para reportes SIP	Ahorro operativo.	\$ 50.000.000
2028	Chatbot jurídico	Atención 24/7.	\$ 80.000.000

Alineación de los proyectos de TI con las estrategias institucionales.

PROGRAMA ESTRATEGICO	DEFINICIÓN	PROYECTOS 2024-2028
Programa: "Transformación Digital para la Personería "	El programa está diseñado para potencializar los procesos a través de la infraestructura y las competencias tecnológicas del personal de la	Ecosistema de Gestión Informática Modernizado Competencias Digitales para el Futuro



N° SC735-1



PROGRAMA ESTRATEGICO	DEFINICIÓN	PROYECTOS 2024-2028
	<p>Personería, optimizando la eficiencia operativa y garantizando la seguridad de la información. Este programa busca capacitar al personal en competencias digitales, promover el uso estratégico del análisis de datos, e implementar tecnologías innovadoras. El objetivo es crear una institución más ágil, eficiente y adaptada a los desafíos del entorno digital contemporáneo.</p>	<p>Decisiones Estratégicas Basadas en Datos</p> <p>Vanguardia Tecnológica para la Gestión Documental</p> <p>Inteligencia Artificial para la Excelencia Operacional.</p>
<p>Programa: "Gestión Documental, del Conocimiento y la Innovación"</p>	<p>El programa se enfoca en fortalecer la gestión de la información, el conocimiento y la Innovación institucional, asegurando la accesibilidad, conservación, y disposición adecuada de los documentos y datos relevantes. Este programa busca promover la transparencia, la trazabilidad de los procesos, y la efectividad en la captura, transferencia, y aplicación del conocimiento en todas las áreas de acción. La tecnología y las herramientas digitales serán pilares fundamentales para alcanzar estos objetivos.</p>	<p>Vigilancia e Inteligencia Estratégica para la Toma de Decisiones</p>



PROGRAMA ESTRATEGICO	DEFINICIÓN	PROYECTOS 2024-2028
Programa: "Fortalecimiento del Ecosistema Multisectorial"	El programa tiene como objetivo principal consolidar y expandir las alianzas estratégicas de la Personería con diversas entidades, articulando la cooperación técnica, el intercambio de conocimiento y la integración de recursos para fortalecer la defensa de derechos y la efectividad institucional. Se centrará en buscar financiamiento externo, establecer colaboraciones con universidades y centros de investigación, y optimizar el uso de tecnologías digitales para maximizar el impacto de las acciones institucionales	Integración Digital y Gestión del Conocimiento

10. PLAN DE COMUNICACIONES DEL PETI

El Plan de Comunicaciones del PETI tiene como objetivo garantizar que los Directivos, funcionarios, colaboradores y ciudadanía conozcan, comprendan y adopten las acciones estratégicas definidas en el Plan Estratégico de Tecnologías de la Información 2024–2028, promoviendo la transparencia, la apropiación tecnológica y la articulación interdependencias para la transformación digital de la Personería Distrital de Medellín.

La comunicación del PETI se desarrolla mediante un enfoque bidireccional, permanente y multicanal, que facilita la comprensión del modelo de TI, sus proyectos, los beneficios esperados y su impacto en los servicios misionales y ciudadanos.



N° SC735-1



1. Comunicación estratégica dirigida a Directivos

Se realizarán espacios formales de presentación del PETI y su hoja de ruta, orientados a:

- Socializar avances, riesgos y necesidades del ecosistema tecnológico.
- Explicar la alineación del PETI con el Plan Estratégico Institucional 2024–2028.
- Facilitar la toma de decisiones basada en datos e información técnica.
- Presentar los proyectos priorizados, su impacto y cronogramas.

Estos espacios se desarrollarán en los Comités de Dirección, Comité de Seguridad de la Información y juntas técnicas internas, garantizando el acompañamiento estratégico de Innovación y Conocimiento.

2. Comunicación operativa dirigida a funcionarios y colaboradores

Se implementarán mecanismos internos para fortalecer la cultura digital y promover el uso adecuado de los servicios tecnológicos institucionales, tales como:

a. Mensajes institucionales en pantallas de inicio

Notificaciones automáticas en los equipos de los funcionarios con:

- Recomendaciones de seguridad digital (SGSI).
- Información sobre nuevos servicios y funcionalidades.
- Tips sobre buenas prácticas con Office 365, SIP, Personería en Línea, PQRSD y Citas.
- Recordatorios de actualizaciones o cambios relevantes.

b. Envío de correos institucionales temáticos

Comunicaciones breves, claras y periódicas con:

- Resúmenes del avance del PETI.
- Buenas prácticas de uso tecnológico.
- Alertas de ciberseguridad.
- Guías rápidas de los sistemas de información.



N° SC735-1



c. Capacitación y socialización presencial y virtual

- Charlas de apropiación digital.
- Capacitaciones Office 365, SIP, seguridad digital y nuevos servicios en nube.
- Socialización previa a la puesta en producción de mejoras o nuevos módulos.

3. Comunicación transversal y acceso público

El PETI se mantiene disponible para consulta en:

- **Página web institucional**, garantizando transparencia y acceso ciudadano.
- **Intranet corporativa**, para consulta de funcionarios y colaboradores.
- **SharePoint** del Sistema Integrado de Gestión, para mantener su versión vigente y control documental.

Esto permite que el documento esté accesible en todo momento y que los equipos de trabajo tengan claridad sobre los lineamientos estratégicos, avances y actualizaciones.

4. Objetivo del Plan de Comunicaciones

- Promover el entendimiento del PETI como hoja de ruta institucional.
- Generar cultura digital en funcionarios y colaboradores.
- Mantener informados a los Directivos para la toma de decisiones.
- Garantizar transparencia frente a la ciudadanía y entes de control.
- Fomentar el uso seguro, eficiente y estratégico de la tecnología en la Entidad.

11. CONCLUSIONES DEL PETI

El Plan Estratégico de Tecnologías de la Información (PETI) de la Personería Distrital de Medellín constituye la hoja de ruta que orienta la transformación digital institucional para el período 2024–2028, alineando los objetivos tecnológicos con el Plan Estratégico Institucional, el Sistema Integrado de Gestión y los lineamientos del MINTIC y del Gobierno Digital.



N° SC735-1



El PETI permite consolidar una visión clara y sostenible sobre el uso estratégico de la tecnología para mejorar la gestión interna, fortalecer la seguridad de la información, optimizar los recursos institucionales y garantizar un servicio moderno, eficiente y transparente a la ciudadanía, especialmente en los procesos misionales de defensa y promoción de los Derechos Humanos.

La ejecución del PETI representa un compromiso permanente de la alta dirección y de todos los procesos de la Entidad, que deberán articular su operación para avanzar de manera coordinada en la modernización tecnológica, la apropiación digital, la adopción de servicios en la nube, el fortalecimiento del SIP, la seguridad informática, la conectividad y la prestación de servicios digitales a la ciudadanía.

Este documento es un instrumento dinámico que será revisado y actualizado anualmente, teniendo en cuenta los avances de los proyectos, la disponibilidad presupuestal, los cambios tecnológicos, normativos y de contexto, garantizando así una evolución constante y pertinente del ecosistema tecnológico institucional.

La Personería Distrital de Medellín reafirma su compromiso con la innovación, la modernización tecnológica y la prestación de un servicio público oportuno, seguro y accesible para toda la ciudadanía.



N° SC735-1



PERSONERÍA DISTRITAL DE MEDELLIN
COMITÉ DE INFORMATICA Y SEGURIDAD DE LA INFORMACIÓN

SECRETARÍA DE GOBIERNO

ACTA 003 - 2025

FECHA	Medellín, 9 de diciembre de 2025		
HORA	De 11:00 am a las 12:30 m		
LUGAR	Despacho del Personero		
ASISTENTES	Mefi Boset Rave Gómez	Personero Distrital	
	Héctor Alfonso Gómez Trujillo	Personero Auxiliar	
	Fernando Valencia Vallejo	Jefe Oficina Asesora de Planeación	
	Juan Pablo Galvis Mejía	Personero Delegado 20D Atención al Público	
	Diego Alexander Hoyos Arroyave	Profesional Innovación y Conocimiento	
INVITADOS	Edison A. Oquendo M.	Representante ASOPERMED	
AUSENTES			

ORDEN DEL DÍA:
Orden del día:

1. Verificación del quórum
2. Lectura del acta anterior y revisión de compromisos anteriores
3. Intervención de los integrantes del comité

1. Verificación del quórum



Se verifica quórum y se cumple.

2. Lectura del acta anterior y compromisos

Se lee los compromisos que serán resueltos a través de la actual reunión.

3. Intervención de los integrantes del comité

Comienza el doctor Fernando dando la palabra a la ingeniera Olga para leer el acta y compromisos del acta anterior. Como primera pregunta será necesario cambiar este comité para Comité de Innovación y Conocimiento, y Seguridad de la Información. Y prosigue el ingeniero Diego con la presentación del cumplimiento de las tareas del acta anterior:

PROYECTÓ:			
	REVISÓ: 		
CODIGO	FGCT008	VERSION	11
RESOLUCION	804	VIGENCIA	10/11/2022
CENTRO CULTURAL PLAZA LA LIBERTAD			
Carrera 53A N° 42-101 / Conmutador +57(4)384 99 99 - Fax +57(4) 381 18 47			
Línea Gratuita: 018000941019			
Email: info@personeriamedellin.gov.co / Pág: www.personeriamedellin.gov.co			





- Implementar correos genéricos por proceso y por personas. R/ Para comenzar el 2026 con estos correos totalmente genéricos.
- Colocar una marca de agua para la identificación de las personas que imprimen. R/ Esto ha funcionado para controlar la impresiones.
- Volver a realizar la campaña de apagado automático de computadores a las 8 p.m. R/ Se realizó la campaña para sensibilizar a los usuarios con el objetivo de apagar los equipos. Se creó política de grupo GPO para apagado de forma automática a las 10:30 pm, excepto UPDH. Se ha observado que las personas por sí mismas apagan su computador antes de salir.
- Revisar ajustes al SIP en alertas de nuevos repartos y reclasificaciones, para luego hacerlo efectivo y divulgarlos. R/ Realizado.
- Poner en funcionamiento el módulo de PQRSD de Personería en Línea. R/ Se realizó la capacitación en el manejo del módulo a los jefes y sus auxiliares. A la fecha la trazabilidad de la información está integrada en la herramienta permitiendo generar informes.
- Controlar a través del SIP la actividad de los usuarios para desactivarlo cuando no entran en 1 mes y demás cambios acerca. R/ Se desactivan los usuarios que no ingresen en 30 días.
- Controlar a través del cuentas de correo la actividad de los usuarios para desactivarlo cuando no entran en 1 mes y demás cambios acerca.
- Investigar las firmas digitales para funcionarios. R/ Se realizó cotización con varias plataformas que proporcionan estos servicios, como se ve en la imagen adjuntan. Y seguir buscando la solución adecuada al implementar en el año 2026 el Programa de Gestión Documental.

Proveedor	Descripción	Valor
ANDES Servicio de Certificación Digital S.A. (ANDES SCD)	Certificado digital para Función Pública -- 1 año Reposición / renovación (mismo tipo) Por usuario/licencia	\$176.418 \$ 62.630
CERTICÁMARA S.A.	Certificado "Función Pública" (u otra categoría aplicable) -- vigencia 1 año Por usuario/licencia	\$ 256.000
Camerfirma Colombia S.A.S.	Certificado digital en token físico Función Pública - Por usuario/licencia	\$ 188.020

De acuerdo con la modernización de la infraestructura tecnológica en 2024 y 2025 se obtuvieron los siguientes hitos:

- 295 equipos modernizados (SSD + 32 GB RAM)
- Optimización de red LAN,
- Wifi institucional y portal cautivo. WiFi segmentado ciudadanía / funcionarios
- Backbone de fibra hacia nueva sede
- Optimización del Centro de Datos, con el peinado profesional de cableado estructurado,

PROYECTÓ: 		REVISÓ: 	
CODIGO	FGCT008	VERSION	11
RESOLUCION	804	VIGENCIA	10/11/2022
CENTRO CULTURAL PLAZA LA LIBERTAD Carrera 53A N° 42-101 / Conmutador +57(4)384 99 99 - Fax +57(4) 381 18 47 Línea Gratuita: 018000941019 Email: info@personeriamedellin.gov.co / Pág: www.personeriamedellin.gov.co			



- Re-organización de racks, patch panels y UPS.
- Monitoreo y mantenimiento de servidores Windows/Linux.
- Implementación completa de VLAN por procesos
- 30 Mb LAN-to-LAN con UPDH, Conciliaciones y Alcaldía para SAP
- Implementación de IPv6. Asignación de prefijos globales y DNS. Compatibilidad con Azure AD y servicios híbridos
- Fortalecimiento del SGSI, actualización de políticas y procedimientos ISO 27001
- Auditorías de seguridad y monitoreo
- Autenticación MFA y Zero Trust con Azure AD
- Cumplimientos clave en Gobierno Digital
- Transparencia activa y datos abiertos actualizados
- Servicios digitales a través de Personería en Línea, más de 8.347 atenciones digitales (2024-2025)
- 441 PQRSD con trazabilidad completa, implementado el 2025
- Implementación de programación de citas en la página web
- Evolución del sistema SIP 2024–2025, con la migración a la nube Azure, a los módulos reforzados y nuevas integraciones, trazabilidad y backup's de información crítica
- Plataforma Moodle a través del Centro de Pensamiento con cursos, talleres y diplomados para los ciudadanos, con certificación automática e integración con campañas de formación en DDHH

PERSONERIA-2024-01

Proyección Innovación 2026 –2028 usando IA. Realizar pruebas piloto con modelos IA internos:



- Chatbots para atención ciudadana
- Automatización de análisis y reportería
- Automatización (Gestión Documental, PQRSD, IA Jurídico)
- Modernización de sistemas de información
- Implementación de instrumentos archivísticos integrados con el SIP

El doctor Juan Pablo de Atención al Público interviene preocupado por la obtención de una cuenta de WhatsApp, no ha sido posible. A lo que el ingeniero Diego responde que es necesario crear una nueva cuenta de Facebook empresarial, es decir, es obligatorio tener una cuenta empresarial en Facebook Business Manager para poder usar la WhatsApp Business API. Esto se debe a que:

- Meta administra WhatsApp Business API a través de Business Manager, que centraliza la verificación de la empresa y la gestión de activos (páginas, cuentas publicitarias, WhatsApp Business Account- WABA).

Y durante el proceso, se debe:

- Crear o usar una cuenta de Facebook Business Manager.
- Completar la verificación del negocio (Meta Business Verification).

PROYECTO: 		REVISO: 	
CODIGO	FGCT008	VERSION	11
RESOLUCION	804	VIGENCIA	10/11/2022
CENTRO CULTURAL PLAZA LA LIBERTAD Carrera 53A N° 42-101 / Conmutador +57(4)384 99 99 - Fax +57(4) 381 18 47 Línea Gratuita: 018000941019 Email: info@personeriamedellin.gov.co / Pág: www.personeriamedellin.gov.co			



Nº 90735.1



- Asociar el número de WhatsApp a la cuenta empresarial.

Sin esta cuenta, no se puede configurar la API ni aprobar plantillas de mensajes.

Prosigue el ingeniero Diego hablando sobre el envío a los integrantes del comité del PETI para su lectura y posibles preguntas. Al respecto aduce el doctor Edison que ellos en ASOPERMED enviaron una serie de inquietudes para resolver. Y según esto, el doctor Mefi determina que es importante responder estos requerimientos antes de publicar el PETI, por lo que también ordena no cerrar el acta y esperar una nueva reunión de media hora en los días siguientes para oficializar la aprobación y publicación del PETI, junto a la resolución respectiva.



Al retomar la reunión del comité, se prosigue hablando a hablar sobre las respuestas que se le hicieron a la Asociación ASOPERMED sobre el PETI, se enviaron al correo. Y se pone a consideración la aprobación del PETI para su publicación y divulgación correspondiente y por unanimidad de los integrantes del comité es aceptado.

Luego se tocaron los siguientes temas que quedaran como compromisos y tareas

- Realizar un comité extraordinario para hablar lo de gestión documental.
- Evaluar la señal de Wifi en Conciliaciones y en UPDH.
- Ampliar la capacidad de megas a 300MB en la sede central y repetidores si es necesario.
- Revisar los teléfonos fijos para revisar y reintegrar los que están defectuosos.
- ASOPERMED, solicita evaluar cuáles son multipuertos adecuados para el buen desempeño de Atención al Público.

3. Compromisos y tareas.

No	TAREA	RESPONSABLE(S)	FECHA EJECUCIÓN
1	Cambiar el nombre del comité de Informática y Seguridad de la Información por Innovación y Seguridad de la Información. Preguntar si por Sistema de Gestión de la Calidad es necesario hacerlo	Innovación y Conocimiento con cada jefe	
2	Colocar una marca de agua para la identificación de las personas que imprimen	Innovación y Conocimiento	
3	Retirar a todos los permisos de YouTube desde enero 1 de 2026	Innovación y Conocimiento	
4	Precisar quiénes son los funcionarios que deben firmar digitalmente	Innovación y Conocimiento	
	Solicitar un concepto jurídico sobre la implementación de la firma digital	Innovación y Conocimiento	



PROYECTO:		REVISÓ:	
CODIGO	FGCT008	VERSION	11
RESOLUCION	804	VIGENCIA	10/11/2022
CENTRO CULTURAL PLAZA LA LIBERTAD Carrera 53A N° 42-101 / Conmutador +57(4)384 99 99 - Fax +57(4) 381 18 47 Línea Gratuita: 018000941019 Email: info@personeriamedellin.gov.co / Páq: www.personeriamedellin.gov.co			



No	TAREA	RESPONSABLE(S)	FECHA EJECUCIÓN
5	Indagar sobre el cambio el sistema de calidad para el procedimiento de firma y subir los documentos al SIP	Innovación y Conocimiento	
6	Investigar si se puede instalar Wifi en las Casas de Justicia y lugares en donde se tiene atención al público	Innovación y Satisfacción de Partes Interesadas	
7	Aire acondicionado de techo del centro de datos	Innovación y Conocimiento	
8	Solicitar a Control Interno una auditoría externa para Innovación	Innovación y Conocimiento	
9	Responder requerimientos de ASOPERMED respecto al PETI	Innovación y Conocimiento	
10	Evaluar la señal de Wifi en Conciliaciones y en UPDH.	Innovación y Conocimiento	
11	Evaluar la señal de Wifi en Conciliaciones y en UPDH.	Innovación y Conocimiento	
12	Ampliar la capacidad de megas a 300MB en la sede central y repetidores si es necesario.	Innovación y Conocimiento	
13	Revisar los teléfonos fijos para revisar y reintegrar los que están defectuosos.	Innovación y Conocimiento - Bienes	
14	Evaluar multipuertos adecuados para el buen desempeño de Atención al Público	Innovación y Conocimiento -	

CONVOCATORIA: Sin definir.

Meti Boset Rave Gómez
 Personero Distrital de Medellín

PROYECTO: 		REVISÓ: 	
CODIGO	FGCT008	VERSION	11
RESOLUCION	804	VIGENCIA	10/11/2022
CENTRO CULTURAL PLAZA LA LIBERTAD Carrera 53A N° 42-101 / Conmutador +57(4)384 99 99 - Fax +57(4) 381 18 47 Línea Gratuita: 018000941019 Email: info@personeriamedellin.gov.co / Pág: www.personeriamedellin.gov.co			



NP 80735-1

