

RENOBO

EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE BOGOTÁ



Integración de los Planes Institucionales y Estratégicos al Plan de Acción Institucional

Plan Estratégico de Tecnologías de la Información (PETI)

2026 – 2029

Dirección Administrativa y de TICs

Versión 1.0, enero de 2026

Tabla de contenido

Tabla de contenido.....	3
1. Introducción	10
2. Objetivo y alcance	11
2.1. Objetivo del documento	11
2.2. Alcance del documento	11
2.3. Exclusiones del alcance	12
2.3.1. Actividades operativas o de ejecución de proyectos	12
2.3.2. Definición de políticas institucionales o normativas internas	12
2.3.3. Procesos disciplinarios, administrativos o contractuales.....	13
2.3.4. Diseño detallado de arquitecturas técnicas o soluciones específicas.....	13
2.3.5. Actividades de operación, soporte o mantenimiento de TI	13
2.3.6. Desarrollo normativo en materia de seguridad y protección de datos	14
2.3.7. Procesos misionales o administrativos ajenos al ámbito de TI.....	14
2.4. Supuestos del PETI.....	15
2.4.1. Continuidad del direccionamiento estratégico institucional.....	15
2.4.2. Disponibilidad de recursos técnicos, financieros y humanos.	15
2.4.3. Adopción y cumplimiento del marco normativo vigente.....	16
2.4.4. Evolución tecnológica y disponibilidad de servicios digitales.....	16
2.4.5. Colaboración y participación de las áreas responsables	17
2.4.6. Gestión adecuada del riesgo tecnológico y de seguridad de la información.....	17
2.4.7. Actualización periódica del PETI	17
2.5. Relación con el MAE v3	18
3. Normatividad.....	19
4. Metodología de formulación del PETI	22
4.1. Mapa de anexos por fase.....	24
4.2. Enfoque AS-IS / TO-BE	25

4.2.1. Análisis AS-IS	25
4.2.2. Visión TO-BE.....	26
4.2.3. Identificación de brechas	26
4.3. Integración con el MAE v3 y el MSPI en cada fase	27
4.3.1. Fase 1 – Contexto.....	27
4.3.1.1. MAE v3:	27
4.3.1.2. MSPI:.....	27
4.3.2. Fase 2 – AS-IS	27
4.3.2.1. MAE v3:	27
4.3.2.2. MSPI:.....	28
4.3.3. Fase 3 – TO-BE	28
4.3.3.1. MAE v3:	28
4.3.3.2. MSPI:.....	28
4.3.4. Fase 4 – Hoja de Ruta	29
4.3.4.1. MAE v3:	29
4.3.4.2. MSPI:.....	29
4.3.5. Mapa visual de la relación PETI–MAE v3 y MSPI	29
5. Fase 1. Contexto de la Empresa.....	30
5.1. Prioridades estratégicas	30
5.1.1. Revitalización Urbana: Gestión de 3.000 hectáreas.....	30
5.1.2. Ejecución y Gestión de Proyectos Estratégicos: Calle 26 y San Victorino.....	30
5.1.3. Sostenibilidad Ambiental Urbana.....	31
5.1.4. Nuevos Negocios: Incremento de ingresos institucionales.....	31
5.1.5. Modernización: procesos y cultura	32
5.2. Estructura organizacional	32
5.3. Modelo operativo	33
5.3.1. Pilares.....	34
5.3.1.1. Retorno social y sostenibilidad.....	34
5.3.1.2. Crecimiento financiero	34
5.3.1.3. Gestión de suelo, gestión inmobiliaria, portafolio de servicios y excelencia operacional	34

5.3.2. Mapa de procesos institucional	35
5.3.2.2. Estratégicos:	36
5.3.2.3. Misionales:	36
5.3.2.4. De apoyo:	36
5.3.2.5. De evaluación:	36
5.3.3. Descripción de los procesos institucionales	37
6. Fase 2. Análisis de la situación actual y oportunidades de mejora	40
6.1. Alineación estratégica del PETI con el Plan Estratégico Institucional	40
6.1.1. Tabla 4: Objetivos Estratégicos de TI (OE-TI)	41
6.2. Alineación de TI con los procesos	41
6.2.1. Tabla 5: Nivel de cubrimiento tecnológico por proceso	42
6.2.2. Hallazgos clave	45
6.2.2.1. Procesos Estratégicos	45
6.2.2.2. Procesos Misionales	46
6.2.2.3. Procesos de <i>Evaluación y Control</i>	47
6.2.2.4. Procesos de apoyo	47
6.3. Interpretación estratégica del diagnóstico	48
6.3.1. Necesidad de un Ecosistema de datos institucional	50
6.3.2. Carencias estratégicas en la arquitectura actual	50
6.3.3. Justificación de un Sistema misional integral y una Plataforma de negocio digital	51
6.3.4. Nota importante	52
6.3.5. Ecosistema de datos	52
6.3.6. Carencias estratégicas	52
6.3.7. Plataforma de negocio digital	53
6.4. Estrategia y Gobierno de TI	53
6.4.1. Diagnóstico estratégico de TI (AS-IS)	55
6.4.2. Procesos de TI:	56
6.4.3. Principio de gobernanza de políticas (rol de TI):	56
6.5. Sistemas de información	57

6.5.1. Sistema misional.....	57
6.5.2. Sistema ERP	57
6.5.3. Integración.....	57
6.6. Infraestructura de TI	57
6.6.1. Infraestructura	57
6.6.2. Continuidad	58
6.7. Servicios de TI	59
6.8. Capacidades de TI.....	68
6.9. Indicadores de TI	70
6.10. Riesgos	73
6.11. Gestión financiera de TI.....	75
6.12. Políticas TI.....	77
6.13. Procedimientos documentados vigentes	79
6.14. Estructura y organización humana de TI	80
6.15. Sistemas de información.....	82
6.15.1. Catálogo de sistemas de información	82
7. Infraestructura	91
7.1. Arquitectura de infraestructura tecnológica	92
7.2. Administración de la operación	93
7.3. Seguridad	95
8. Fase 3. Situación deseada u objetivo	96
8.1. Estrategia de TI: Visión y Misión 2029.	96
8.2. Objetivos estratégicos de TI (OE-TI)	96
8.2.1. OE-TI 1. Habilitación de ingresos y gestión comercial	97
8.2.2. OE-TI 2. Transformación de datos y análisis estratégico	97
8.2.3. Fortalecimiento de la resiliencia y la seguridad digital.....	97
8.2.4. OE-TI 4. Excelencia y eficiencia operacional de TI	98
8.3. Sistemas de Información	98
8.3.1. Autogestión y comercial	99

8.4. Infraestructura TI: Arquitectura objetivo	100
9. Hoja de ruta y portafolio de proyectos 2026-2029	102
9.1. Macroproyectos estratégicos 2026-2029 con enfoque en generación de ingresos que puede apoyar TI.....	104
9.2. Detalle de los nuevos proyectos (2026-2029)	105
9.2.1. Macroproyecto: Plataforma de Negocio Digital y Comercialización.....	105
9.2.2. Macroproyecto: Inteligencia de Negocios y Analítica Predictiva	105
9.3. Matriz de alineación entre objetivos de TI y macroproyectos	106
10. Proyección financiera año 2026	109
11. Estrategia de Comunicación del PETI	110
11.1. Glosario	110
12. Anexos	112
12.1. Anexo 1: Fase 1 – Planear	112
12.2. Anexo 2: <i>Stakeholders</i> y comunicaciones.....	113
12.3. Anexo 3: Planes externos y obligaciones.....	115
12.4. Anexo 4: Mapa de integraciones.....	117
12.5. Anexo 5: Hojas de vida de indicadores	118
12.6. Anexo 6: Matriz RACI.....	120
12.7. Anexo 7: Acta modelo de aprobación.....	121
12.8. Anexo 8: Tabla brechas ISO 27001:2022	124
12.9. Anexo 9: Revisión y validación de la implementación IPv6.....	132
12.10. Anexo 10: Plan de socialización	134
12.11. Anexo 11: DOFA	135
12.11.1. Estrategia de TI	136
12.11.1.1. Acciones priorizadas	136
12.11.2. Gobierno de TI	137
12.11.2.1. Acciones priorizadas	137
12.11.3. Información	138
12.11.3.1. Acciones priorizadas	138

12.11.4. Sistemas de Información	139
12.11.4.1. Acciones priorizadas	139
12.11.5. Infraestructura de TI	140
12.11.5.1. Acciones priorizadas	140
12.11.6. Uso y Apropiación	141
12.11.6.1. Acciones priorizadas	141
12.11.7. Seguridad	142
12.11.7.1. Acciones priorizadas	142
12.12. Anexo 12: plan de implementación del PETI.....	143
12.12.1. Introducción	144
12.12.2. Objetivo	147
12.12.3. Fases del plan	147
12.12.4. Responsables (según Matriz RACI)	148
12.12.5. Evidencias esperadas	149
12.13. Anexo 13: Acta de no implementación del BCP	150
12.14. Anexo 14: Autodiagnósticos Gobierno Digital y Seguridad Digital	152
12.14.1. Introducción	153
12.14.2. Objetivos	153
12.14.3. Alcance	154
12.14.4. Metodología	154
12.14.5. Resultados de Gobierno Digital (2025).....	155
12.14.5.1. Arquitectura y planeación de TI.....	155
12.14.5.2. Interoperabilidad y datos (API-CDE)	155
12.14.5.3. Servicios digitales y accesibilidad.....	155
12.14.5.4. Datos abiertos y gobierno del dato	156
12.14.6. Resultados de seguridad digital (2025)	156
12.14.6.1. Gobernanza de seguridad digital y MSPI.....	156
12.14.6.2. Gestión de riesgos y continuidad (DRP)	156
12.14.6.3. Protección de datos personales y controles técnicos.....	157
12.14.6.4. Matriz de brechas y plan de acciones.....	157

12.14.6.5. Indicadores (KPIs) y metas	158
12.14.6.6. Trazabilidad normativa	159
12.14.6.7. Relación con el PETI (capítulos y anexos)	159
12.14.6.8. Conclusiones.....	160
12.15. Anexo 15: Brechas FURAG.....	160
12.15.1. Introducción	160
12.15.2. Alcance	160
12.15.3. Trazabilidad normativa.....	161
12.15.4. Metodología de autodiagnóstico y valoración	161
12.15.5. Matriz de brechas y plan de acciones	162
12.15.6. KPIs para el cierre de brechas FURAG	172
12.15.7. Evidencias verificables	175
12.15.8. Relación con el PETI (capítulos y anexos)	176
12.16. Anexo 16: Matriz de trazabilidad de hallazgos y planes de mejoramiento	177
13. Referencias	186
13.1. Referencias generales.....	186
13.2. Normatividad nacional aplicable	187
13.3. Marcos y estándares internacionales	187
13.4. Referentes técnicos del Ministerio TIC.....	189
13.5. Políticas internas vigentes de la Empresa.....	190
13.6. Procedimientos internos utilizados como referencia	190
13.7. Plataformas y herramientas tecnológicas citadas	190
Índice de ilustraciones	191
Índice de tablas	191

1. Introducción

El **PETI 2026–2029** consolida a la **Empresa** como un referente distrital en **transformación digital**, articulando tecnología, datos y seguridad para habilitar la revitalización urbana, la eficiencia operativa y la generación de valor público. Esta hoja de ruta no solo se alinea con la **Política de Gobierno Digital**, el **Plan Distrital de Desarrollo 2024–2027** y el **Plan Estratégico de Revitalización**, sino que también cumple con los lineamientos obligatorios de la **Circular 07 de 2024 emitida por la Consejería Distrital de TIC**, que establecen requisitos verificables para los **PETI** distritales en materia de **accesibilidad digital**: conforme a estándares como **WCAG 2.1 AA** y **seguridad de la información** bajo el marco del **SGSI** alineado con **ISO/IEC 27001:2022** y el **Modelo de Seguridad y Privacidad de la Información (MSPI)**. Estas disposiciones son auditables por entes de control internos y externos y se articulan con el **Programa de Transparencia y Ética Pública 2026**, en su componente de Accesibilidad, garantizando trazabilidad normativa, defendibilidad ante auditoría y generación de evidencias técnicas conforme a los hitos definidos en la hoja de ruta del **PETI**.

2. Objetivo y alcance

2.1. Objetivo del documento

Servir como la hoja de ruta estratégica y técnica que orienta las decisiones, inversiones y proyectos de **Tecnologías de la Información** necesarios para soportar el cumplimiento de los objetivos institucionales. Este documento guía la implementación de iniciativas de **Transformación Digital**, la gestión del riesgo tecnológico y el fortalecimiento de las capacidades organizacionales para el periodo **2026–2029**, asegurando la alineación con las políticas institucionales, el marco de gobierno de TI, la arquitectura empresarial, el Sistema de Gestión de Seguridad de la Información (SGSI) y la normativa vigente en materia de seguridad y protección de datos personales.

2.2. Alcance del documento

El presente documento abarca las fases de comprensión, análisis, construcción y presentación del Plan Estratégico de Tecnologías de la Información para el periodo 2026–2029. Su alcance integra el diagnóstico del estado actual, la definición de la visión objetivo, la identificación de brechas, la priorización de iniciativas y la formulación de la hoja de ruta tecnológica.

La construcción del PETI se encuentra alineada con los dominios del Marco de Arquitectura Empresarial – MAE v3 del MinTIC, incorporando los componentes de estrategia, gobierno, información, sistemas de información, infraestructura tecnológica, seguridad y privacidad, y uso y apropiación. En este sentido, el documento establece las orientaciones estratégicas de TI aplicables a toda la Entidad, abarcando procesos,

información, capacidades, plataformas tecnológicas y servicios digitales que soportan la operación institucional.

2.3. Exclusiones del alcance

El presente *Plan Estratégico de Tecnologías de la Información (PETI)* no incluye los siguientes elementos, los cuales se encuentran fuera del alcance de su formulación para el periodo 2026–2029:

1. Actividades operativas o de ejecución de proyectos.
2. Definición de políticas institucionales o normativas internas.
3. Procesos disciplinarios, administrativos o contractuales.
4. Diseño detallado de arquitecturas técnicas o soluciones específicas.
5. Actividades de operación, soporte o mantenimiento de TI.
6. Desarrollo normativo en materia de seguridad y protección de datos.
7. Procesos misionales o administrativos ajenos al ámbito de TI.

Cada uno de estos ítems se explica a continuación:

2.3.1. Actividades operativas o de ejecución de proyectos

El *PETI* establece lineamientos y definiciones de carácter estratégico, pero no detalla tareas operativas, cronogramas específicos de ejecución ni procedimientos técnicos de implementación.

2.3.2. Definición de políticas institucionales o normativas internas

La construcción de políticas y lineamientos corporativos corresponde a las instancias de dirección y gobierno institucional; el *PETI* únicamente orienta la planificación tecnológica que soporta su aplicación.

2.3.3. Procesos disciplinarios, administrativos o contractuales

Este documento no regula ni describe procedimientos sancionatorios, jurídicos o administrativos asociados con la gestión contractual o disciplinaria de la Entidad.

2.3.4. Diseño detallado de arquitecturas técnicas o soluciones específicas.

Se definen lineamientos, principios y capas de la arquitectura tecnológica. Sin embargo, la ingeniería detallada, diagramas técnicos, configuraciones o manuales de soluciones corresponden a documentos posteriores.

2.3.5. Actividades de operación, soporte o mantenimiento de TI

Las operaciones del día a día (soporte, mesa de ayuda, mantenimientos preventivos / correctivos, administración de plataformas, entre otros) se rigen por procedimientos internos y no forman parte del **PETI**.

2.3.6. Desarrollo normativo en materia de seguridad y protección de datos

Aunque el **PETI** se alinea con: la **Ley 1581 de 2012**, el **Decreto 1377 de 2013**, la **Resolución 448 de 2022 (MSPI)** y la norma **ISO 27001**, no sustituye ni redefine los instrumentos específicos del **Sistema de Gestión de Seguridad de la Información (SGSI)** ni el **Régimen de Protección de Datos Personales**.

2.3.7. Procesos misionales o administrativos ajenos al ámbito de TI

El documento no describe ni redefine procedimientos misionales de la Entidad; solo identifica y prioriza las capacidades tecnológicas que los soportan.

Estas exclusiones garantizan que el **PETI** mantenga su naturaleza estratégica, centrada en orientar decisiones, inversiones, capacidades y prioridades tecnológicas, sin sustituir instrumentos normativos, operativos o técnicos específicos.

2.4. Supuestos del PETI

La formulación y ejecución del **Plan Estratégico de Tecnologías de la Información (PETI)** para el periodo **2026 – 2029** se basa en los siguientes supuestos, necesarios para garantizar su coherencia, aplicabilidad y cumplimiento:

- Continuidad del direccionamiento estratégico.
- Disponibilidad de recursos técnicos, financieros y humanos.
- Cumplimiento normativo vigente.
- Evolución tecnológica y servicios digitales.
- Participación activa de áreas responsables.
- Gestión del riesgo tecnológico y de seguridad.
- Actualización periódica del PETI.

Cada uno de estos ítems se describe brevemente en los siguientes subcapítulos.

2.4.1. Continuidad del direccionamiento estratégico institucional

Se asume que los lineamientos estratégicos definidos por la Alta Dirección y las áreas misionales mantendrán su vigencia general durante el periodo del **PETI**, permitiendo la alineación continua entre la estrategia institucional y las inversiones en **TI**.

2.4.2. Disponibilidad de recursos técnicos, financieros y humanos.

La ejecución de las iniciativas contempladas en el **PETI** depende de: la asignación presupuestal periódica, la disponibilidad de talento competente y la capacidad operativa requerida para adelantar proyectos de modernización tecnológica.

2.4.3. Adopción y cumplimiento del marco normativo vigente

La formulación y ejecución del PETI 2026–2029 se fundamenta en la adopción integral del marco normativo aplicable a las entidades distritales, garantizando su cumplimiento verificable ante entes de control internos y externos. En este contexto, se destaca la **Circular 07 de 2024 emitida por la Consejería Distrital de TIC**, que establece lineamientos obligatorios para los PETI distritales en materia de **accesibilidad digital** (conforme a estándares como WCAG 2.1 AA), **interoperabilidad y seguridad de la información** bajo el marco del **SGSI** alineado con **ISO/IEC 27001:2022** y el **Modelo de Seguridad y Privacidad de la Información (MSPI)**. Estos lineamientos son requeridos por programas de ley como el **Programa de Transparencia y Ética Pública 2026**, en su componente de Accesibilidad, y se integran en la hoja de ruta del PETI mediante acciones medibles, trazabilidad normativa y generación de evidencias técnicas (actas de comité o mesa de trabajo, informes de accesibilidad, pruebas DRP, políticas de cifrado). De esta manera, el PETI asegura defendibilidad ante auditoría y coherencia con los principios de Gobierno Digital, la Ley 1581 de 2012, el Decreto 1377 de 2013, la Resolución MinTIC 448 de 2022 y los estándares internacionales aplicables.

2.4.4. Evolución tecnológica y disponibilidad de servicios digitales

Se presume la continuidad del ecosistema tecnológico necesario para la transformación digital, incluyendo infraestructuras, plataformas, servicios en la nube y herramientas de automatización que respalden la implementación de la hoja de ruta.

2.4.5. Colaboración y participación de las áreas responsables

El desarrollo del **PETI** exige el compromiso de las áreas misionales, de apoyo y de dirección para suministrar información, validar requerimientos, priorizar iniciativas y garantizar la articulación con los procesos institucionales.

2.4.6. Gestión adecuada del riesgo tecnológico y de seguridad de la información

El **PETI** se construye bajo el supuesto de que la Entidad mantendrá las prácticas necesarias para gestionar los riesgos asociados con TI, seguridad, privacidad, continuidad y protección de datos personales, conforme a los instrumentos del **SGSI** y al **MSPI**.

2.4.7. Actualización periódica del PETI

Se asume que el PETI podrá ajustarse durante su vigencia para atender cambios en el entorno normativo, tecnológico, estratégico o presupuestal, garantizando su vigencia y relevancia.

Estos supuestos proporcionan el marco de condiciones que habilita la correcta ejecución del PETI y permiten anticipar riesgos que podrían afectar su implementación durante el periodo 2026–2029.

2.5. Relación con el MAE v3

El *Plan Estratégico de Tecnologías de la Información (PETI)* se formula en coherencia con el *Marco de Arquitectura Empresarial – MAE v3* del *MinTIC*, el cual orienta la articulación entre la estrategia institucional, los procesos, la información, las capacidades tecnológicas y los servicios digitales.

En este sentido, el *PETI* se estructura considerando los siete dominios que componen el *MAE v3*: estrategia, gobierno, información, sistemas de información, infraestructura tecnológica, seguridad y privacidad, y uso y apropiación. Estos dominios sirven como referencia para: el análisis del estado actual, la identificación de brechas y la definición de la visión objetivo.

El *MAE v3* proporciona el marco conceptual y metodológico que permite al *PETI* asegurar que las inversiones tecnológicas, las iniciativas priorizadas y los proyectos estratégicos estén plenamente alineados con la arquitectura institucional. De este modo se garantiza la coherencia entre los objetivos misionales, la gestión de la información, los procesos organizacionales y los habilitadores tecnológicos.

Así mismo, el *PETI* adopta los lineamientos del *MAE v3* para fortalecer la toma de decisiones sobre tecnologías de la información, priorizar capacidades institucionales, asegurar la interoperabilidad, promover la transformación digital, y garantizar que la modernización tecnológica se realice bajo criterios de eficiencia, sostenibilidad, seguridad y valor público.

De esta manera, la relación entre el *PETI* y el *MAE v3* asegura que la planificación estratégica de *TI* esté alineada con las mejores prácticas del *Gobierno Digital*, el *Modelo de Seguridad y Privacidad de la Información (MSPI)* y las directrices de arquitectura empresarial definidas para el Estado colombiano.

3. Normatividad

Tipo de norma	No	Año	Emisor de la norma	Epígrafe	Temática	Enlace de verificación	Observaciones/Nota de vigencia
Decreto	767	2022	MinTIC	Mediante el cual se actualizó la política de Gobierno Digital del país.	Política de Gobierno Digital	https://www.mintic.gov.co/portal/715/articles-210461_recurso_1.pdf	subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015,
Decreto	88	2022	MinTIC	Por el cual se establecen los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea	Trámites en línea	https://mintic.gov.co/portal/715/articles-198550_decreto_88_24_enero_2022.pdf	se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020.
Resolución	460	2022	MinTIC	Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) expidió el 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.	Plan Nacional de Infraestructura	https://www.mintic.gov.co/portal/715/articles-198952_resolucion_004_60_2022.pdf	Nueva
Decreto	338	2022	MinTIC	Establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras	Seguridad Digital	https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%20338%20DEL%208%20DE%20MARZO%20DE%202022.pdf	Por el cual se adiciona el Título 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Tipo de norma	No	Año	Emisor de la norma	Epígrafe	Temática	Enlace de verificación	Observaciones/Nota de vigencia
				disposiciones			
Resolución	746	2022	MinTIC	Por la cual se fortalece el modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021.	Seguridad y privacidad de la información	https://www.mintic.gov.co/portal/715/articles-208143_recurso_1.pdf	Nueva
Resolución	1117	2022	MinTIC	Por la cual se establecen los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el marco de la Política de Gobierno Digital.	Política de Gobierno Digital	https://mintic.gov.co/portal/715/articles-208739_recurso_1.pdf	Nueva
Circular	07	2024	Consejería Distrital de TIC – Bogotá	a Circular 07 de 2024 emitida por la Consejería Distrital de TIC establece lineamientos obligatorios para los Planes Estratégicos de Tecnologías de la Información (PETI) en entidades distritales, orientados a garantizar la accesibilidad de los	Lineamientos para PETI distritales (accesibilidad, seguridad, interoperabilidad)	Circular 007 de 2024 Consejo Distrital de Política Económica y Fiscal - CONFIS	Obligatoria para entes de control internos y externos.

Tipo de norma	No	Año	Emisor de la norma	Epígrafe	Temática	Enlace de verificación	Observaciones/Nota de vigencia
				sistemas de información y portales web, así como la incorporación de medidas robustas de seguridad de la información. Estos lineamientos son requeridos por los entes de control y se articulan con programas de ley como el Programa de Transparencia y Ética Pública 2026, en su componente de accesibilidad.			

Tabla 1 – Normatividad

4. Metodología de formulación del PETI

La metodología aplicada para la formulación del Plan Estratégico de Tecnologías de la Información (**PETI**) de la **Empresa de Renovación y Desarrollo Urbano de Bogotá, D.C.** responde a lineamientos nacionales de planeación estratégica, al **Marco de Arquitectura Empresarial – MAE v3** del **MinTIC**, al **Modelo de Seguridad y Privacidad de la Información – MSPI (Resolución 448 de 2022)** y a buenas prácticas internacionales basadas en **ISO 27001**, **ISO 38500** y Gobierno Digital.

El propósito metodológico es asegurar que la planificación tecnológica de la **Empresa** sea coherente con sus prioridades estratégicas, responda a las necesidades del modelo operativo y permita identificar, priorizar y gestionar las capacidades TIC necesarias para el periodo 2026–2029.

La metodología se desarrolla en cuatro fases principales:

1. **Comprensión del contexto institucional**
2. **Análisis del estado actual (AS-IS)**
3. **Construcción de la visión y escenarios futuros (TO-BE)**
4. **Formulación de la hoja de ruta tecnológica.**

METODOLOGÍA DE FORMULACIÓN DE PETI

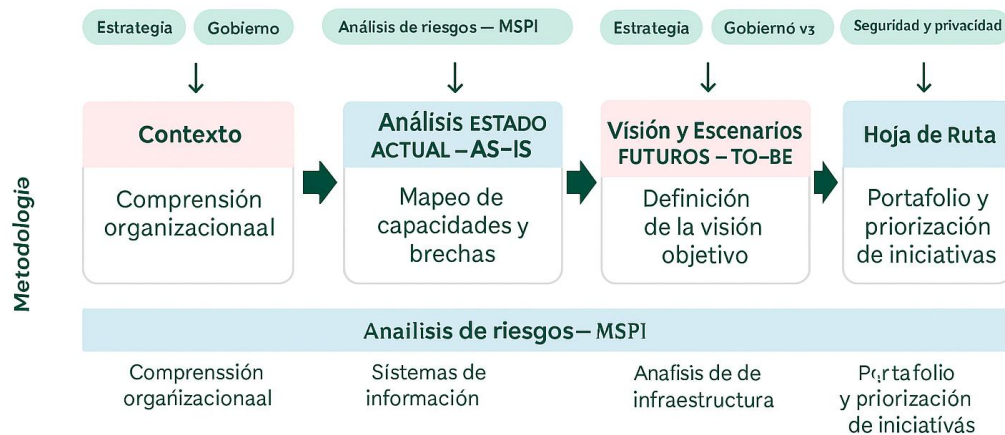


Ilustración 1: Metodología de formulación del PETI

Cada fase integra los dominios del **MAE v3** y los componentes del **MSPI** de acuerdo con su relevancia y contribución al análisis.

4.1. Mapa de anexos por fase

Este apartado establece la relación entre los **anexos del PETI** y las **fases metodológicas** definidas por la Guía **MGGTI.GE.ES.01 v3 del MinTIC** (Planear, Analizar, Construir y Socializar). Su propósito es garantizar la **trazabilidad** y la **defendibilidad** del documento ante auditorías y seguimientos, evidenciando cómo cada anexo refuerza los contenidos desarrollados en el documento base.

Fase PETI (MinTIC)	Anexos vinculados	Propósito
Planear	<ul style="list-style-type: none"> Anexo 1 (Equipo y stakeholders) Anexo 2 (Plan de comunicaciones) Anexo 7 (Acta modelo) Anexo 13 (Acta no BCP) 	Evidenciar conformación del equipo, planificación y decisiones iniciales
Analizar (AS-IS)	<ul style="list-style-type: none"> Anexo 8 (Brechas ISO 27001) Anexo 11 (DOFA) Anexo 14 (Autodiagnósticos Gobierno Digital) Anexo 15 (Brechas FURAG) 	Soportar diagnóstico, hallazgos y brechas
Construir (TO-BE y hoja de ruta)	<ul style="list-style-type: none"> Anexo 4 (Mapa de integraciones) Anexo 6 (Matriz RACI) Anexo 9 (IPv6) 	Detallar arquitectura objetivo, cronograma y responsabilidades

	<ul style="list-style-type: none"> Anexo 12 (Plan de implementación) 	
Socializar	<ul style="list-style-type: none"> Anexo 10 (Plan de socialización) Anexo 7 (Acta modelo) 	Evidenciar difusión y aprobación

Tabla 2 - Relación anexos - fase

4.2. Enfoque AS-IS / TO-BE

El **PETI** se fundamenta en un enfoque comparativo entre la situación actual (**AS-IS**) y la situación deseada (**TO-BE**). Este enfoque permite comprender las capacidades tecnológicas existentes, así:

- Identificar brechas y necesidades organizacionales.
- Proyectar los escenarios tecnológicos futuros que permitirán alcanzar los objetivos institucionales.
- Definir iniciativas estratégicas basadas en evidencia.

4.2.1. Análisis AS-IS

Incluye:

- Inventario de sistemas de información, datos, infraestructura y servicios.
- Evaluación de procesos, capacidades TIC, madurez digital y gobernanza.
- Valoración de riesgos asociada a activos de información (**MSPI – Resolución 448/2022**).
- Análisis de fortalezas, debilidades, oportunidades y amenazas tecnológicas.

El **AS-IS** proporciona una comprensión objetiva del estado actual de la tecnología y su alineación con el modelo operativo.

4.2.2. Visión TO-BE

Define el estado tecnológico deseado, considerando:

- Prioridades estratégicas de la **Empresa de Renovación y Desarrollo Urbano de Bogotá, D.C.**.
- Tendencias tecnológicas y lineamientos de **Gobierno Digital**.
- Principios de arquitectura del **MAE v3**.
- Requerimientos de seguridad, privacidad y gestión del riesgo derivados del **MSPI** e **ISO 27001**.
- Necesidades de interoperabilidad, experiencia digital y eficiencia operativa.

El resultado es un modelo objetivo de capacidades que orienta la modernización institucional.

4.2.3. Identificación de brechas

Comparar el **AS-IS** y el **TO-BE** permite identificar:

- Brechas tecnológicas
- Brechas de información y de datos
- Brechas de procesos y de automatización
- Brechas de seguridad y privacidad
- Brechas de talento y gobernanza

- Brechas de infraestructura

Estas brechas se convierten en la base para priorizar la hoja de ruta del **PETI**.

4.3. Integración con el **MAE v3** y el **MSPI** en cada fase

La metodología incorpora de manera estructural los dominios del **MAE v3**, garantizando coherencia entre los componentes estratégicos, misionales y tecnológicos de la Empresa. Asimismo, integra los lineamientos del **MSPI**, asegurando que los riesgos, controles y consideraciones de seguridad estén presentes en las decisiones de planificación tecnológica.

4.3.1. Fase 1 – Contexto

4.3.1.1. MAE v3:

- Estrategia
- Gobierno
- Información

4.3.1.2. MSPI:

- Identificación de activos
- Comprensión del entorno de seguridad
- Riesgos preliminares

4.3.2. Fase 2 – AS-IS

4.3.2.1. MAE v3:

- Información

- Sistemas de información
- Infraestructura tecnológica
- Seguridad y privacidad

4.3.2.2. MSPI:

- Valoración de riesgos
- Análisis de controles existentes
- Clasificación de la información

4.3.3. Fase 3 – TO-BE

4.3.3.1. MAE v3:

- Arquitectura objetivo
- Escenarios tecnológicos
- Capacidades digitales requeridas

4.3.3.2. MSPI:

- Requerimientos de seguridad por iniciativa
- Controles propuestos
- Privacidad desde el diseño

4.3.4. Fase 4 – Hoja de Ruta

4.3.4.1. MAE v3:

- Portafolio de iniciativas.
- Priorización con enfoque de valor.
- Dependencias entre dominios.

4.3.4.2. MSPI:

- Plan de tratamiento del riesgo
- Alineación con el SGSI institucional
- Aseguramiento y monitoreo de la implementación

4.3.5. Mapa visual de la relación *PETI–MAE v3 y MSPI*



Ilustración 2: Relación **PETI–MAE v3 y MSPI**

5. Fase 1. Contexto de la Empresa

La comprensión del contexto organizacional constituye el punto de partida para la formulación del **Plan Estratégico de Tecnologías de la Información (PETI)** de la **Empresa**. Este análisis permite identificar las prioridades institucionales, los retos del entorno y las capacidades requeridas para que las Tecnologías de la Información actúen como habilitadoras de los objetivos estratégicos de la empresa.

En este marco, las prioridades estratégicas definidas por la **Empresa de Renovación y Desarrollo Urbano de Bogotá, D.C.** orientan la planeación tecnológica y sirven como referencia para la identificación de brechas, necesidades y oportunidades de modernización institucional. Estas prioridades se presentan y describen de manera sucinta en los siguientes subcapítulos, con el fin de contextualizar los elementos que guían la formulación del **PETI**.

5.1. Prioridades estratégicas

5.1.1. Revitalización Urbana: Gestión de 3.000 hectáreas

La **Empresa de Renovación y Desarrollo Urbano de Bogotá, D.C.** tiene como mandato liderar procesos de transformación urbana a gran escala, lo que requiere: capacidades robustas de gestión de información territorial, analítica geoespacial, interoperabilidad con entidades del sector urbano y herramientas de seguimiento a intervenciones urbanísticas. La tecnología se convierte en un habilitador esencial para monitorear, planificar y gestionar el territorio de manera integral.

5.1.2. Ejecución y Gestión de Proyectos Estratégicos: Calle 26 y San Victorino

Los proyectos institucionales de alto impacto exigen sistemas que soporten la planificación, seguimiento, control y trazabilidad de obras e intervenciones. Esto incluye: herramientas de gestión de proyectos,

analítica para toma de decisiones, sistemas de monitoreo en tiempo real y plataformas de reporte alineadas con principios de transparencia y eficiencia.

5.1.3. Sostenibilidad Ambiental Urbana

La empresa mantiene un compromiso con la gestión del entorno ambiental en zonas urbanas. Para ello se requieren soluciones tecnológicas que permitan: capturar, integrar y analizar información ambiental, apoyar la toma de decisiones sostenibles y fortalecer la medición de indicadores asociados a calidad ambiental, espacio público y mitigación de impactos.

5.1.4. Nuevos Negocios: Incremento de ingresos institucionales

La estrategia de diversificación e incremento de ingresos demanda capacidades digitales orientadas a la innovación, la analítica de datos para identificar oportunidades de negocio, plataformas para prestación de servicios y herramientas que soporten modelos de generación de valor con sostenibilidad financiera.

5.1.5. Modernización: procesos y cultura

La transformación organizacional es un eje fundamental para la **Empresa de Renovación y Desarrollo Urbano de Bogotá, D.C.**. Esto implica avanzar hacia la optimización de procesos, la automatización, la digitalización documental, el fortalecimiento del talento digital y la adopción de prácticas modernas de gestión del cambio. La modernización tecnológica debe acompañar y habilitar esta evolución cultural y operativa.

5.2. Estructura organizacional

La estructura organizacional de la **Empresa** define las instancias de dirección, coordinación y ejecución que orientan la operación institucional y soportan el cumplimiento de los objetivos estratégicos. Su conocimiento es fundamental para la formulación del **PETI**, ya que permite identificar los roles responsables de la toma de decisiones, la gestión de proyectos, la administración de la información y el despliegue de capacidades tecnológicas.

La **Empresa de Renovación y Desarrollo Urbano de Bogotá, D.C.** cuenta con una estructura que incluye órganos de gobierno, niveles directivos, oficinas asesoras, dependencias misionales y áreas de apoyo, articuladas para garantizar la ejecución de los proyectos estratégicos, la revitalización urbana, la gestión operativa y la modernización institucional. Esta organización también permite identificar los flujos de información y las responsabilidades clave que deben considerarse en la planeación tecnológica.

A continuación, se presenta la estructura organizacional vigente:

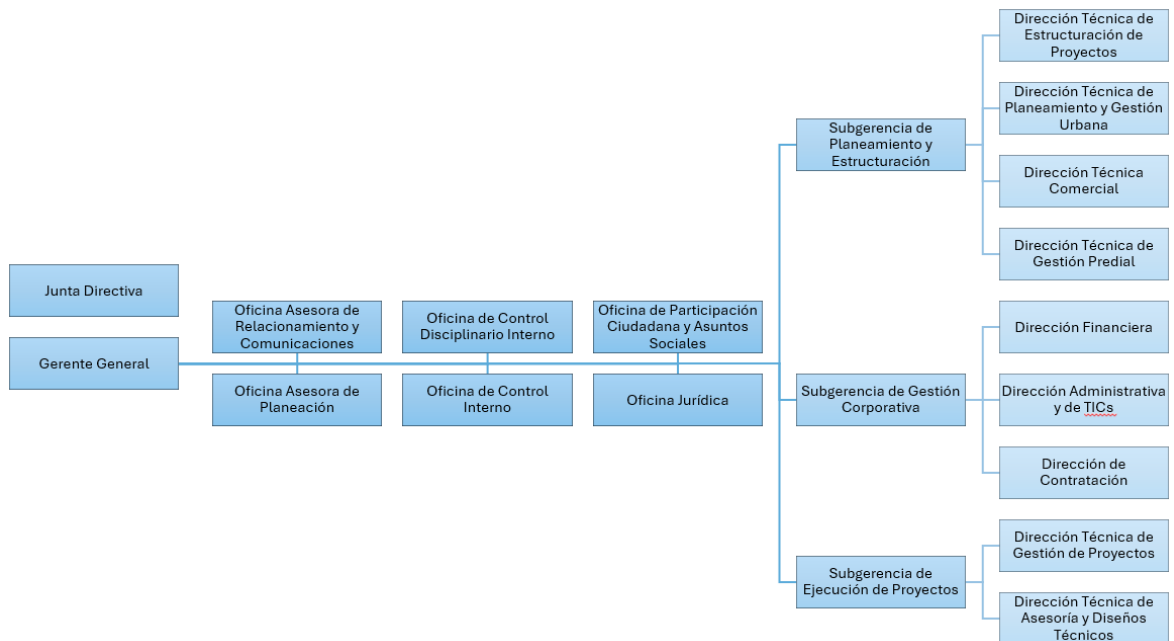


Ilustración 3 - Estructura organizacional

5.3. Modelo operativo

El modelo operativo de la **Empresa** establece la forma en que la Empresa organiza sus capacidades institucionales, procesos y recursos para cumplir su mandato estratégico y generar valor público. Este modelo se estructura alrededor de tres pilares fundamentales que orientan la operación y el direccionamiento estratégico: **Retorno social y sostenibilidad**, **Crecimiento financiero** y **Gestión de Suelo**, **Gestión Inmobiliaria y Portafolio de Servicios** y **Excelencia Operacional**.

5.3.1. Pilares

5.3.1.1. Retorno social y sostenibilidad

Enfocado en promover la revitalización urbana, la participación ciudadana y la sostenibilidad ambiental del territorio, por medio de la maximización del valor social de las intervenciones urbanas.

5.3.1.2. Crecimiento financiero

Dirigido a fortalecer la sostenibilidad institucional mediante el desarrollo de nuevos negocios, la eficiencia operativa y la diversificación de ingresos. Este pilar es particularmente dependiente del soporte tecnológico para habilitar sistemas de gestión comercial, analítica de datos, automatización de procesos y canales digitales eficientes.

5.3.1.3. Gestión de suelo, gestión inmobiliaria, portafolio de servicios y excelencia operacional

Agrupar las capacidades misionales vinculadas a la estructuración, gestión y ejecución de proyectos estratégicos, gestión predial y provisión de servicios para la transformación urbana.

La tecnología, como habilitador transversal de este modelo operativo, debe fortalecer estos pilares, especialmente: el crecimiento financiero, mediante canales digitales eficientes, sistemas de gestión de relaciones con clientes y plataformas que automaticen procesos.

De este modo, el **PETI** debe fortalecer particularmente:

- La disponibilidad y calidad de la información territorial y predial.
- Los sistemas de gestión de proyectos y seguimiento operativo.
- La automatización de procesos críticos.

- La gestión de relaciones con ciudadanos y actores del territorio.
- El desarrollo y sostenimiento de canales digitales que soporten el crecimiento financiero y el relacionamiento institucional.

5.3.2. Mapa de procesos institucional

El mapa de procesos representa la forma en que la Empresa organiza su operación y estructura la cadena de valor institucional. Este modelo se centra en la generación de valor para los grupos de interés y garantiza la articulación entre las funciones estratégicas, misionales, de apoyo y de evaluación.

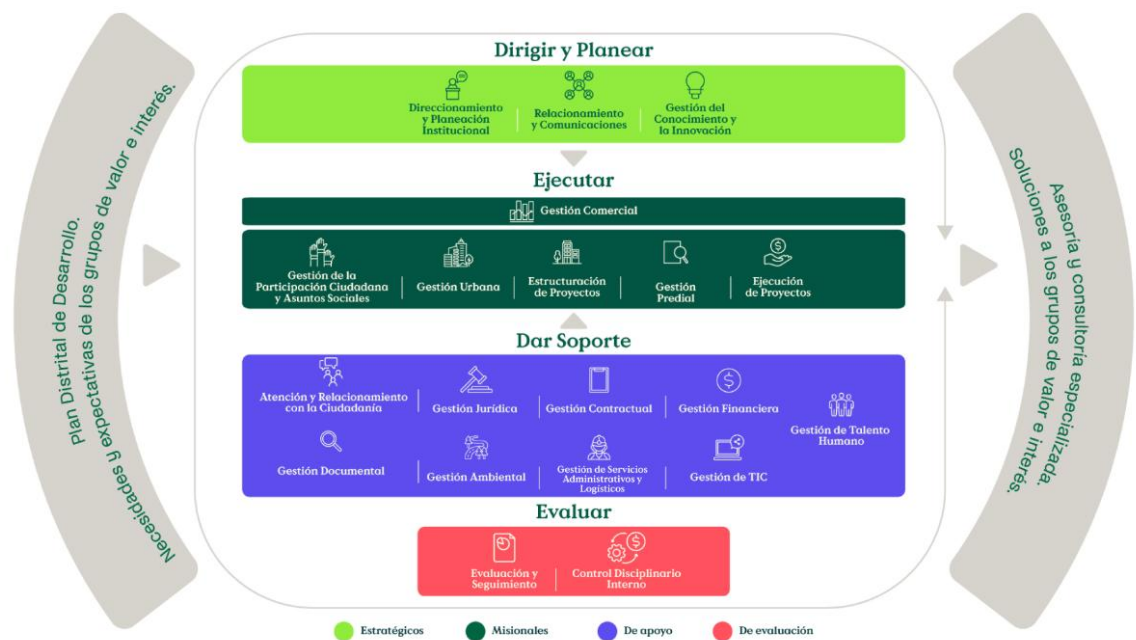


Ilustración 4 - Mapa de procesos

Los procesos que lo conforman son de tipo:

1. Estratégicos.

2. Misionales.
3. De apoyo.
4. De evaluación.

5.3.2.2. Estratégicos:

Definen la orientación institucional, establecen lineamientos y aseguran coherencia entre la estrategia, la gestión de recursos y la toma de decisiones.

5.3.2.3. Misionales:

Materializan la razón de ser de la Empresa. Incluyen la gestión urbana, la estructuración y ejecución de proyectos, la gestión predial, la participación ciudadana y demás procesos que producen el valor principal para la ciudad.

5.3.2.4. De apoyo:

Proveen capacidades esenciales para el funcionamiento de los procesos misionales, entre ellos la gestión jurídica, financiera, ambiental, contractual, logística, documental y tecnológica.

5.3.2.5. De evaluación:

Permiten monitorear el desempeño institucional, identificar oportunidades de mejora y garantizar la transparencia y el cumplimiento normativo mediante actividades de control disciplinario, auditoría y seguimiento.

5.3.3. Descripción de los procesos institucionales

Tipo de Proceso	Nombre del Proceso	Objetivo Principal
Estratégico	Oficina Asesora de Planeación	Liderar el direccionamiento estratégico y la gestión institucional, asegurando la formulación, operación y seguimiento del MIPG para promover la mejora continua.
Estratégico	Oficina Asesora de Relacionamiento y Comunicaciones	Diseñar y ejecutar las políticas y estrategias de relacionamiento y comunicaciones que fortalezcan la imagen institucional y la articulación con los grupos de interés.
Misional	Oficina de Participación Ciudadana y Asuntos Sociales	Dirigir la formulación e implementación de políticas y acciones de gestión social y participación ciudadana que garanticen el involucramiento efectivo de la comunidad.
Misional	Subgerencia de Ejecución de Proyectos	Garantizar la ejecución integral de los proyectos asignados, asegurando cumplimiento técnico, normativo y operativo en todas sus fases.
Misional	Dirección Técnica de Gestión de Proyectos	Supervisar y coordinar técnicamente los proyectos bajo su responsabilidad, asegurando calidad, oportunidad y alineación con los estándares institucionales.

Tipo de Proceso	Nombre del Proceso	Objetivo Principal
Misional	Dirección Técnica de Asesoría y Diseños Técnicos	Garantizar la calidad técnica de los contratos y diseños mediante supervisión, asesoría y control conforme a la normatividad y lineamientos corporativos.
Misional	Subgerencia de Planeamiento y Estructuración	Liderar políticas y estrategias de gestión urbana, predial, ambiental, comercial y de estructuración de proyectos para orientar el desarrollo urbano sostenible.
Misional	Dirección Técnica de Planeamiento y Gestión Urbana	Dirigir el planeamiento y la gestión urbana de los proyectos, aplicando los instrumentos normativos y técnicos vigentes.
Misional	Dirección Técnica de Gestión Predial	Dirigir y ejecutar los procesos de gestión y adquisición de suelo necesarios para el desarrollo de los proyectos urbanos.
Misional	Dirección Técnica Comercial	Diseñar e implementar estrategias comerciales para identificar oportunidades de negocio y gestionar la comercialización de bienes y servicios institucionales.
Misional	Dirección Técnica de Estructuración de Proyectos	Dirigir la estructuración integral de proyectos conforme a criterios técnicos y a los lineamientos de la Subgerencia de Planeamiento y Estructuración.

Tipo de Proceso	Nombre del Proceso	Objetivo Principal
Evaluación y Control	Oficina de Control Interno	Ejecutar funciones de evaluación, auditoría, asesoría y seguimiento que soporten la toma de decisiones y el mejoramiento institucional.
Evaluación y Control	Oficina de Control Disciplinario Interno	Adelantar investigaciones disciplinarias, garantizando imparcialidad, rigor jurídico y cumplimiento de la normatividad aplicable.
De Apoyo	Oficina Jurídica	Dirigir y asesorar a la Empresa en asuntos jurídicos, emitiendo conceptos y realizando la revisión normativa necesaria para el soporte institucional.
De Apoyo	Subgerencia de Gestión Corporativa	Orientar la administración institucional mediante lineamientos estratégicos en materia administrativa, organizacional y de gestión corporativa.
De Apoyo	Dirección Financiera	Dirigir la planeación financiera, la gestión presupuestal, la tesorería, la contabilidad y los análisis financieros que soportan la sostenibilidad institucional.
De Apoyo	Dirección Administrativa y TIC	Dirigir la gestión administrativa, tecnológica, documental, ambiental y del talento humano que soportan la operación institucional.

Tabla 3 - Descripción de los Procesos Institucionales

6. Fase 2. Análisis de la situación actual y oportunidades de mejora

6.1. Alineación estratégica del PETI con el Plan Estratégico Institucional

El *Plan Estratégico de Tecnologías de la Información (PETI)* se articula directamente con los objetivos y prioridades del Plan Estratégico Institucional (*PEI*) de la *Empresa de Renovación y Desarrollo Urbano de Bogotá, D.C.*, garantizando que las inversiones tecnológicas potencien la misión institucional y habiliten la transformación operativa, digital y urbana. Esta alineación se fundamenta en los lineamientos del *Marco de Arquitectura Empresarial (MAE v3)* y del *Modelo de Seguridad y Privacidad de la Información (MSPI)*. De este modo se asegura: coherencia, gobernanza del dato y maduración progresiva de capacidades digitales.

El *PETI* se orienta a generar habilitadores tecnológicos que soporten los pilares misionales del *PEI*, de modo que las soluciones de *TI* contribuyan al crecimiento financiero, la revitalización urbana, la sostenibilidad, la innovación y la eficiencia institucional.

6.1.1. Tabla 4: Objetivos Estratégicos de TI (OE-TI)

Prioridad estratégica PEI	Objetivo institucional	Estrategia asociada
Revitalización urbana	Gestionar 3.000 hectáreas	Implementar proyectos integrales de renovación urbana
Crecimiento financiero	Incrementar ingresos institucionales	Diversificación de negocios y monetización de activos
Sostenibilidad ambiental	Garantizar sostenibilidad urbana	Integrar criterios ambientales en los proyectos
Modernización	Optimizar procesos y cultura	Digitalización, automatización y mejora continua
Nuevos negocios	Ampliar portafolio de servicios	Innovación y desarrollo de canales digitales

Tabla 4: Objetivos Estratégicos de TI (OE-TI)

6.2. Alineación de TI con los procesos

El análisis de la situación actual muestra un **bajo nivel de alineación** entre los procesos institucionales y los sistemas de información existentes, especialmente en los procesos misionales. Esta brecha tecnológica afecta:

- la eficiencia operativa,
- la trazabilidad de la información,
- la capacidad de análisis y toma de decisiones,

- el cumplimiento del PEI,
- y la creación de valor público.

La Tabla 5 presenta el nivel de cubrimiento tecnológico por proceso, los sistemas actualmente implementados y las oportunidades de mejora identificadas, de acuerdo con la revisión del inventario de activos tecnológicos y del mapa de procesos.

6.2.1. Tabla 5: Nivel de cubrimiento tecnológico por proceso

Tipo de proceso	Nombre del proceso	Sistemas de Información	Cubrimiento	Oportunidad de mejora
Estratégico	Oficina Asesora de Planeación	ERP - Modulo Planeación Presupuestal	Parcial	Desarrollo o adquisición de un Sistema para el proceso de seguimiento y evaluación de planes y programas de Acción
Estratégico	Oficina Asesora de Relacionamento y Comunicaciones	Redes sociales: X, Facebook, Instagram, YouTube	Parcial	Adquisición de un sistema administrador de redes sociales
Misional	Oficina de Participación Ciudadana y Asuntos Sociales	Sistema de Gestión Documental	Parcial	Desarrollo o adquisición de un Sistema para gestionar los datos misionales levantados con la comunidad
Misional	Subgerencia de Ejecución de Proyectos	N/A	Sin cobertura	Desarrollo de un Sistema Misional

Tipo de proceso	Nombre del proceso	Sistemas de Información	Cubrimiento	Oportunidad de mejora
Misional	Dirección Técnica de Gestión de Proyectos	N/A	Sin cobertura	Desarrollo de un Sistema Misional
Misional	Dirección Técnica de Asesoría y Diseños Técnicos	N/A	Sin cobertura	Desarrollo de un Sistema Misional
Misional	Subgerencia de Planeamiento y Estructuración	N/A	Sin cobertura	Desarrollo de un Sistema Misional
Misional	Dirección Técnica de Planeamiento y Gestión Urbana	N/A	Sin cobertura	Desarrollo de un Sistema Misional
Misional	Dirección Técnica de Gestión Predial	N/A	Sin cobertura	Desarrollo de un Sistema Misional
Misional	Dirección Técnica Comercial	N/A	Sin cobertura	Desarrollo de un Sistema Misional
Misional	Dirección Técnica de Estructuración de Proyectos	N/A	Sin cobertura	Desarrollo de un Sistema Misional
Evaluación y control	Oficina de Control Interno	N/A	Sin cobertura	Desarrollo de un sistema de gestión de información de auditorías
Evaluación y control	Oficina de Control Disciplinario Interno	Sistema de Gestión Documental	Parcial	

Tipo de proceso	Nombre del proceso	Sistemas de Información	Cubrimiento	Oportunidad de mejora
De apoyo	Oficina Jurídica	N/A	Sin cobertura	Implementación de interoperabilidad con sistemas de bases de datos jurídicos
De apoyo	Subgerencia de Gestión Corporativa	ERP - Sistema de Gestión Documental	Parcial	Implementación de interoperabilidad con sistemas de reporte con Entes de Control
De apoyo	Dirección Financiera	Módulo contable y presupuestal ERP, no misional	Parcial	Desarrollar un sistema para temas contables y presupuestales para proyectos misionales
De apoyo	Dirección Administrativa y TIC	ERP - Sistema de Gestión Documental	Parcial	Desarrollo o adquisición de un Sistema para la gestión de talento humano
De apoyo	Dirección de Contratación	Módulo contractual en ERP procesos internos	Parcial	Desarrollo o adquisición de un Sistema para la gestión contractual con terceros

Tabla 5 - Alineación de TI con los procesos institucionales

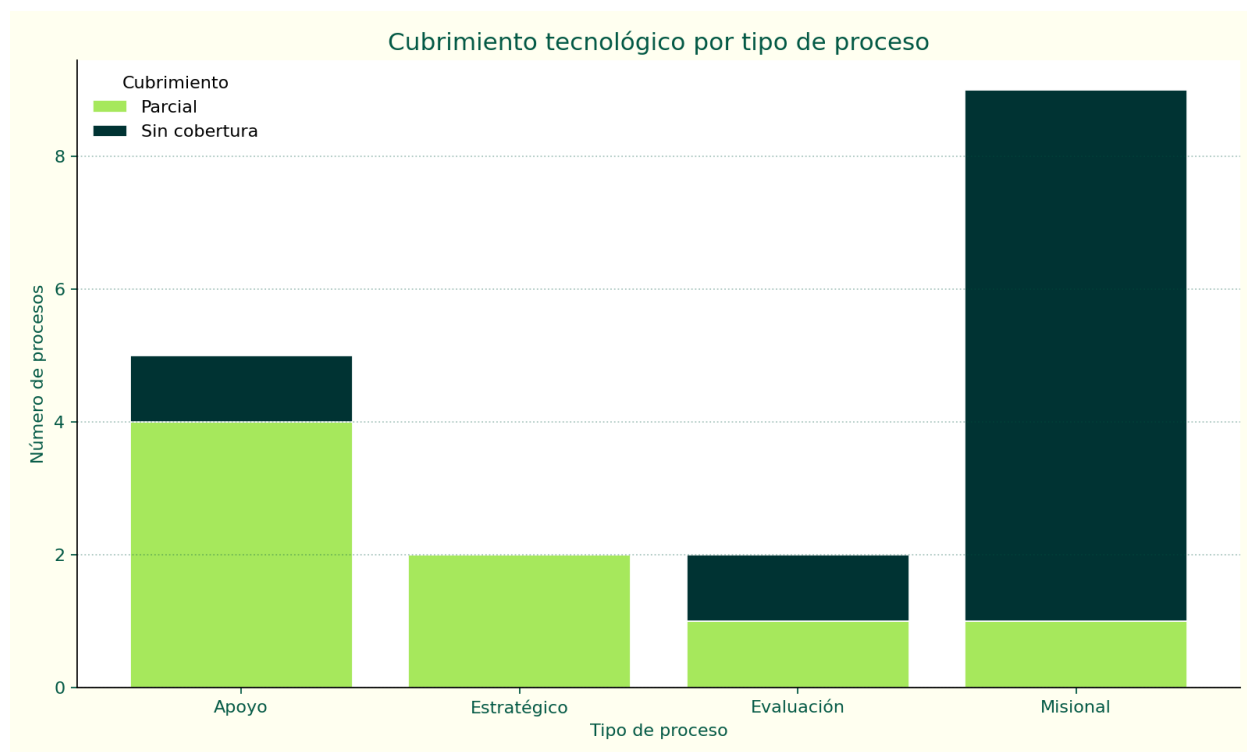


Ilustración 5: Cubrimiento tecnológico por tipo de proceso

A partir del análisis, se identifican los hallazgos relevantes descritos a continuación.

6.2.2. Hallazgos clave

6.2.2.1. Procesos Estratégicos

Las áreas de **Planeación** y **Comunicaciones** presentan un cubrimiento parcial mediante herramientas genéricas (ERP y redes sociales). Sin embargo:

- No existe un sistema especializado para gestión, seguimiento y evaluación de planes, programas y proyectos.
- La gestión de comunicaciones carece de una plataforma integrada que permita trazabilidad, analítica, programación, automatización y gestión multicanal.

Esto limita la capacidad de reportes estratégicos, control de metas, narrativa pública y eficiencia institucional.

6.2.2.2. Procesos Misionales

Los procesos misionales presentan el **mayor rezago tecnológico** de la entidad. Entre los hallazgos:

- Ninguna subgerencia o dirección misional dispone de sistemas especializados para la operación misional (e.g.: proyectos, territorio, diseños, predial, estructuración, gestión comercial, relacionamiento social).
- La operación depende mayormente de herramientas ofimáticas, documentos aislados y procedimientos manuales.
- La ausencia de un ***Sistema Misional*** Integral afecta:
 - Trazabilidad de la información.
 - Integridad del dato.
 - Cierre financiero misional.
 - Gestión de cronogramas.
 - Analítica para toma de decisiones.
 - Consolidación y reporte a entes de control.

Esto genera:

- Reprocesos y duplicidad de información
- Baja trazabilidad

- Limitada capacidad de analítica
- Riesgos operativos y de calidad de información

6.2.2.3. Procesos de *Evaluación y Control*

Los procesos de *Evaluación y Control* presentan brechas significativas debido a la ausencia de sistemas especializados que soporten la gestión institucional.

Entre los hallazgos se destacan:

- La **Oficina de Control Interno** opera sin sistemas dedicados para la gestión de auditorías, riesgos y planes de mejoramiento. Esto representa un riesgo para la trazabilidad, el seguimiento y el cumplimiento del **MIPG**.
- La **Oficina de Control Disciplinario Interno** utiliza únicamente el **Sistema de Gestión Documental** para el manejo de expedientes, sin funcionalidades especializadas para la administración del ciclo disciplinario, control de términos, notificaciones o caducidades.

La ausencia de herramientas tecnológicas en estas áreas limita la eficiencia, la transparencia y la capacidad institucional para ejercer control interno y disciplinario conforme a los estándares normativos.

6.2.2.4. Procesos de apoyo

A pesar de que estas áreas disponen de **ERP** y del **Sistema de Gestión Documental**, la tecnología es insuficiente para la complejidad de sus funciones. En particular, cabe destacar que:

- No existe interoperabilidad interna ni externa.
- **Jurídica** requiere integración con bases jurídicas y herramientas de análisis.
- **Financiera** requiere un sistema para gestión contable y presupuestal de proyectos misionales.

- **Administración y Talento Humano** requieren automatización de nómina, hojas de vida, desempeño y formación.
- **Contratación** requiere un sistema especializado para gestionar ciclos contractuales con terceros y proveedores.

6.3. Interpretación estratégica del diagnóstico

El diagnóstico realizado constituye la base del **PETI 2026–2029** y evidencia tres conclusiones críticas que orientan la transformación digital de la **Empresa**:

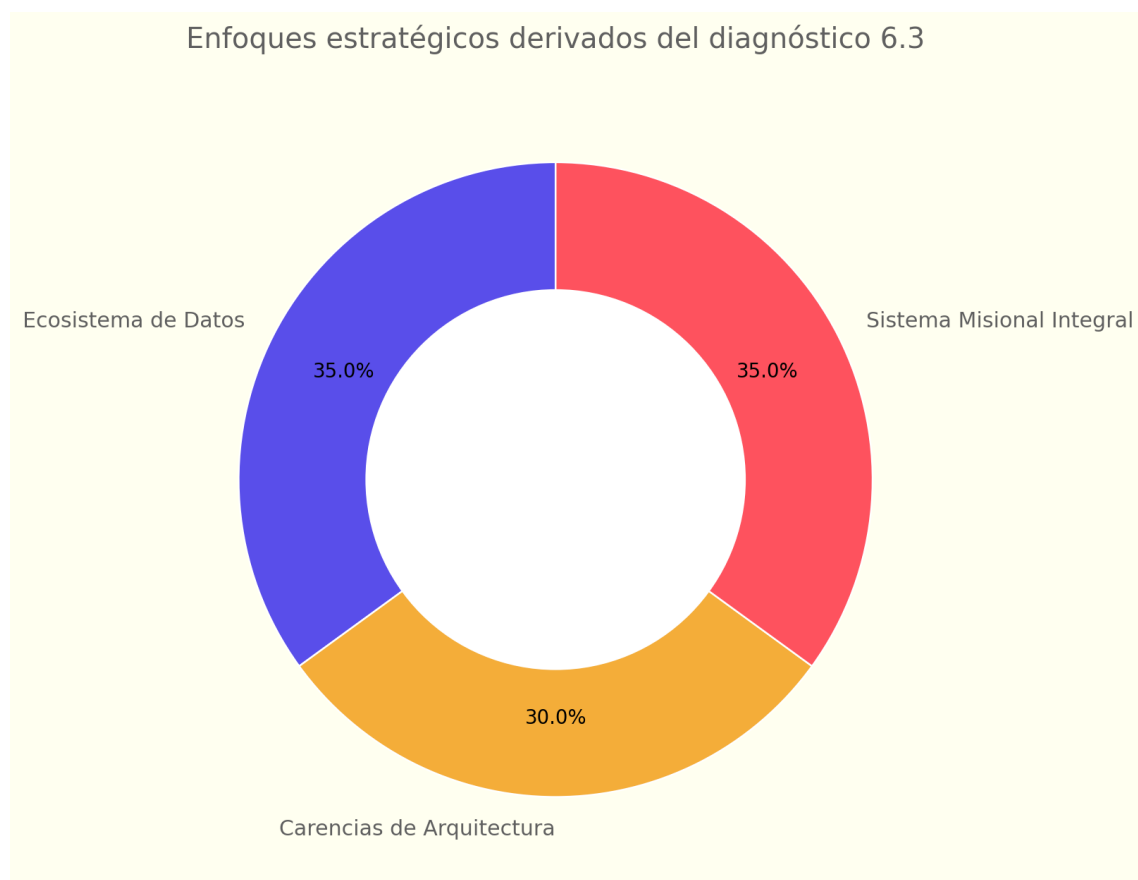


Ilustración 6: Enfoques estratégicos del diagnóstico

- **Necesidad de un Ecosistema de datos institucional:** que unifique la información misional, garantice calidad del dato y habilite la analítica avanzada.
- **Carencias estratégicas en la arquitectura actual,** derivadas de la ausencia de sistemas especializados y de la baja integración entre procesos.
- **Justificación de un Sistema Misional Integral y una Plataforma de Negocio Digital,** como habilitadores clave del crecimiento urbano, territorial y financiero.

En concordancia con el lineamiento **EO 02 – Tecnología**, la entidad prioriza:

1. la actualización, estandarización y resiliencia de la infraestructura tecnológica para garantizar disponibilidad;
2. la implementación del **SGSI** conforme a la **ISO/IEC 27001:2022**, cerrando brechas mediante la ejecución del **SOA 2022**, el **Plan de Tratamiento de Riesgos**, y políticas de cifrado en tránsito y reposo; y
3. la realización periódica de **pruebas DRP**, incluyendo restauración de **ERP/JSP7**, correo institucional, **SGDEA/TAMPUS** y simulación de **ransomware**, con criterios de aceptación y evidencia técnica documentada.

Estas conclusiones refuerzan la necesidad de adoptar una arquitectura moderna, interoperable y centrada en el dato, que permita a la **Empresa a** avanzar hacia una operación más eficiente, trazable y orientada a resultados misionales.

6.3.1. Necesidad de un Ecosistema de datos institucional

El análisis evidencia que los sistemas que soportan los procesos misionales presentan limitaciones significativas y oportunidades de mejora. Aunque existe infraestructura tecnológica básica, se requiere optimización para garantizar integración, automatización y alineación con la estrategia institucional.

La ausencia de sistemas misionales integrados impide:

- Consolidación de información territorial, predial, ambiental, de proyectos y social.
- Analítica para toma de decisiones.
- Interoperabilidad entre áreas misionales y de apoyo.
- Gobernanza del dato (alineado al MAE v3).

Se requiere una plataforma centralizada de datos y servicios, que funcione como eje articulador del negocio.

6.3.2. Carencias estratégicas en la arquitectura actual

Los procesos misionales cuentan con soporte parcial mediante herramientas ofimáticas y sistemas generales (**ERP**, gestión documental), pero carecen de soluciones especializadas e integradas para su operación **end-to-end**.

Los procesos estratégicos como: **Planeación** y **Comunicaciones**: Tienen un cubrimiento parcial. Utilizan herramientas básicas como módulo de presupuesto del **ERP** y redes sociales, pero carecen de sistemas especializados como un sistema de seguimiento a planes o un administrador de redes sociales.

Procesos de apoyo: **Jurídica**, **Corporativa**, **Financiera**, **Contratación**, entre otros, tienen un cubrimiento parcial: dependen del **ERP** y del **Sistema de Gestión Documental** para tareas internas.

El análisis muestra que:

- Los procesos misionales no cuentan con sistemas que soporten su operación **end-to-end**.
- Los procesos estratégicos tienen automatización limitada.
- Los procesos de apoyo dependen casi exclusivamente del ERP, sin herramientas especializadas.
- No existe integración entre procesos, lo que genera duplicidad de esfuerzos, reprocesos y baja trazabilidad.

Esto confirma la necesidad de evolucionar la arquitectura empresarial hacia un modelo más moderno y escalable.

6.3.3. Justificación de un Sistema misional integral y una Plataforma de negocio digital

La brecha más significativa es que ningún proceso misional dispone de un sistema especializado.

Esto afecta:

- Gestión urbana
- Gestión predial
- Estructuración de proyectos
- Ejecución de proyectos
- Gestión social
- Comercialización de servicios
- Planeamiento y estructuración

Por ello, todos los procesos misionales convergen en la misma necesidad: desarrollar un **Sistema Misional Integral**, conectado a un ecosistema de datos y servicios digitales interoperables.

Esto constituye el corazón del **PETI 2026–2029**.

6.3.4. Nota importante

A TIC se le ha dado un rol de apoyo. debe encontrarse entre los procesos estratégicos. Sin embargo, si se quiere que hay una mejora real y significativa, se hace necesario darle esa posibilidad de manejo trascendental en la organización, así como las correspondientes herramientas.

Oportunidades de mejora Claras: La tabla identifica necesidades específicas que el ERP actual no sule:

- Gestión de talento humano para ***Dirección Administrativa y TIC.***
- Gestión contractual con terceros para ***Contratación.***
- Sistemas contables para proyectos misionales para ***Dirección Financiera.***

Existen puntos ciegos: ***Control interno y Jurídica.*** De modo similar al caso de los procesos misionales, la ***Oficina de Control Interno*** y la ***Oficina Jurídica*** operan sin cobertura, dependiendo de un sistema de gestión de auditorías e interoperabilidad jurídica que no existen.

6.3.5. Ecosistema de datos

La falta de un ***sistema misional*** es precisamente el problema que el macroproyecto Ecosistema de Datos busca resolver. La **Empresa de Renovación y Desarrollo Urbano de Bogotá, D.C.** no requiere 8 sistemas aislados, sino una plataforma centralizada que dé servicio a todos estos procesos misionales.

6.3.6. Carencias estratégicas

La falta de sistemas en ***Planeación y Control Interno*** refuerza el resultado del análisis, relacionado con las carencias de la entidad en cuanto a ***Arquitectura empresarial y Definición de políticas.***

6.3.7. Plataforma de negocio digital

La necesidad de un Sistema para la gestión contractual con terceros y temas contables para proyectos misionales son los cimientos de la futura plataforma de **e-Commerce** y monetización de activos.

Esta tabla es el estado actual que sirve como punto de partida. Demuestra que la **Empresa de Renovación y Desarrollo Urbano de Bogotá, D.C.** opera con una brecha tecnológica severa en su Core de negocio, y valida la necesidad urgente de los macroproyectos de transformación definidos para **2026-2029**.

6.4. Estrategia y Gobierno de TI

La elaboración del presente **PETI** se fundamentó en el análisis de los **autodiagnósticos de Gobierno Digital** y los resultados del formulario **FURAG**. Asimismo, integra las acciones correctivas de los planes de mejoramiento derivados de las auditorías de control interno, asegurando una estrategia alineada con el cumplimiento normativo y la realidad institucional.

Actualmente, la función de TI en la Entidad cumple principalmente un rol de apoyo operativo. No obstante, para lograr una mejora sostenible y un mayor impacto en el cumplimiento de los objetivos institucionales, resulta necesario fortalecer su participación como habilitador estratégico, proporcionando soporte técnico, herramientas y capacidades que faciliten la ejecución de las decisiones estratégicas definidas por la organización.

Gobierno de TI

No existe actualmente una **Mesa de Trabajo de Control de Cambios**, la cual es necesaria para garantizar la trazabilidad técnica, el análisis de impacto y la coordinación operativa respecto de modificaciones en

sistemas, infraestructura y plataformas. Esta mesa actúa como instancia técnica, mientras que las decisiones institucionales continúan a cargo del Comité Institucional de Gestión y Desempeño.

Para soportar la operación del SGSI y asegurar la coordinación técnica requerida para los dominios de TI, se establecen **mesas de trabajo especializadas** en reemplazo de las figuras de comités técnicos. Estas mesas incluyen la **Mesa de Trabajo de Seguridad de la Información**, la **Mesa de Trabajo Operativa/Táctica de TI** y la **Mesa de Trabajo de Gobierno de Datos**, las cuales funcionan como instancias técnicas de análisis, coordinación y seguimiento.

Las decisiones institucionales continúan elevándose al **Comité Institucional de Gestión y Desempeño**, autoridad formal definida por el MIPG.

Las mesas de trabajo especializadas de TI sustituyen formalmente a los comités técnicos operativos. Estas mesas actúan como instancias de análisis, coordinación y ejecución técnica del SGSI, la gestión de cambios, la operación TI y el gobierno del dato. Todas las decisiones estratégicas, de aprobación, asignación de recursos y emisión de políticas continúan siendo competencia exclusiva del Comité Institucional de Gestión y Desempeño, garantizando trazabilidad, cumplimiento del MIPG, los lineamientos del **MSPI** y la alineación con **ISO/IEC 27001:2022**.

El fortalecimiento del Gobierno de TI no implica la creación de nuevas instancias normativas desde el área de TI, sino la formalización de espacios de coordinación y soporte técnico que permitan una mejor articulación con la Alta Dirección y las áreas estratégicas, asegurando coherencia, trazabilidad y ejecución efectiva de las decisiones institucionales en materia tecnológica.

6.4.1. Diagnóstico estratégico de TI (AS-IS)

El análisis realizado evidencia un **déficit crítico en capacidades tecnológicas y de gobernanza**, que impacta la alineación entre TI y los objetivos institucionales. Los hallazgos se agrupan en cinco dimensiones:

1. Procesos misionales

- Ausencia total de sistemas especializados para la operación end-to-end (gestión urbana, predial, estructuración, ejecución de proyectos, gestión social y comercial).
- Dependencia de herramientas ofimáticas y procedimientos manuales, lo que genera reprocesos, baja trazabilidad y riesgos de integridad del dato.

2. Procesos estratégicos y de apoyo

- Cobertura parcial mediante ERP y sistemas documentales, sin interoperabilidad ni automatización avanzada.
- Carencia de sistemas para gestión contractual con terceros, talento humano y seguimiento a planes estratégicos.

3. Gobernanza y capacidades estratégicas

- TI opera con fortaleza técnica, pero carece de capacidades para gestionar arquitectura empresarial y definir políticas, lo que limita su rol como habilitador estratégico.
- No existen comités propios de TI ni gobierno de datos formalizado.

4. Infraestructura y continuidad

- Obsolescencia marcada en servidores locales y ausencia de mecanismos automatizados de recuperación.

- Continuidad gestionada mediante pruebas DRP.

5. Seguridad y gestión del riesgo

- SGSI en transición hacia ISO / IEC 27001:2022, con brechas en controles críticos (clasificación y etiquetado de información, cifrado en tránsito y reposo, gestión de vulnerabilidades, seguridad en nube).
- Riesgos prioritarios: pérdida de información, vulnerabilidad de sistemas e indisponibilidad de servicios.

6.4.2. Procesos de TI:

Existen procesos documentados ***PD-71 Administración de Acceso Lógico, PD-51 Copias de respaldo*** que reflejan la realidad operativa, priorizando la eficiencia sobre la adopción estricta de todos los estándares ***ITIL / COBIT***.

6.4.3. Principio de gobernanza de políticas (rol de TI):

La Dirección Administrativa y TIC no emite ni modifica políticas corporativas; su rol es apoyar su formulación, socialización, monitoreo de cumplimiento y provisión de evidencia técnica. Las Oficinas Asesora de Planeación, Jurídica y Alta Dirección son las instancias que lideran la aprobación y publicación. Se formaliza la participación de TI en el Comité Institucional de Gestión y Desempeño y en el nuevo Mesa de Trabajo SGSI como instancia de soporte técnico y verificación.

6.5. Sistemas de información

6.5.1. Sistema misional

Se ha tomado la decisión de no continuar con la herramienta que soporta el sistema misional anterior. La implementación futura se basará en **NocoBase**.

6.5.2. Sistema ERP

El sistema administrativo y financiero - **JSP7** y el **Sistema de Gestión Documental - TAMPUS** están migrados y alojados en la nube.

6.5.3. Integración

La configuración previa de ambientes de intercambio ha sido sustituida. El último análisis arrojó que la integración se realizará mediante **APIs**, donde los proveedores construyen los **endpoints** y **TIC** implementa las conexiones a través de un **Entorno Común de Datos**. Se identificó que **Tampus** usa **SOAP**; se requiere la conversión a formato **API** para la interoperabilidad.

6.6. Infraestructura de TI

6.6.1. Infraestructura

Existe una obsolescencia significativa en los servidores físicos locales: 1 (un) servidor en **Datacenter ETB** y 9 (nueve) en la **Sede administrativa**. A pesar de que estos legados se han repotenciado y modernizado, siguen constituyendo una brecha de obsolescencia.

6.6.2. Continuidad

La continuidad se gestionará a través de:

- Estrategias de **respaldo y restauración (DRP)** sobre servicios en nube y locales
- **Pruebas técnicas de recuperación** periódicas (restauración de ERP, correo, SGDEA, simulación de ransomware)
- Comunicación y trazabilidad del SGSI.

Nota: Las fechas, responsables y cronograma detallado de pruebas y actividades se encuentran en el documento **“Plan de Acción proceso gestión de TI 2026.xlsx”** y consolidan todas las actividades del contrato.

6.7. Servicios de TI

ID	001
Nombre	Acceso a internet por WIFI
Descripción	Acceso a la red de colaboradores de la Entidad de manera inalámbrica a través de dispositivos móviles y computadores portátiles. La velocidad de 400 MB y soporta máximo usuarios conectados concurrentemente

Tabla 6 - Servicio 001 Acceso a Internet por Wifi

ID	002
Nombre	Acceso a la intranet
Descripción	Acceso a la red protegida de la Entidad para el uso de los recursos tecnológicos. (Sistemas, impresoras, Telefonía IP, etc.)

Tabla 7 - Servicio 002 Acceso a la intranet

ID	003
Nombre	Acceso a la red interna por VPN
Descripción	Todos los funcionarios y contratistas de la entidad

Tabla 8 - Servicio 003 Acceso a la red interna

ID	004
Nombre	Correo electrónico junto con las herramientas colaborativas
Descripción	Basado en Google Workspace con un buzón de almacenamiento de 1TB, almacenamiento en drive y acceso a aplicaciones de ofimática de Google.

Tabla 9 - Servicio 004 Correo electrónico y herramientas colaborativas

ID	005
Nombre	Gemini
Descripción	Basado en Google con modelos Flash y Pro

Tabla 10 - Servicio 005 Inteligencia artificial generativa

ID	006
Nombre	Servicio de entrenamiento y capacitación uso de las soluciones de TI
Descripción	Servicio que suministra capacitación y entrenamiento sobre las funciones de los sistemas de información que maneja la entidad.

Tabla 11 - Servicio 006 Entrenamiento y capacitación

ID	007
Nombre	Comunicaciones inteligentes
Descripción	Servicio de comunicaciones telefónicas entre usuarios internos externos de la institución, basado en plataforma Zoom .

Tabla 12 - Servicio 007 Comunicaciones inteligentes

ID	008
Nombre	Plataforma de Mesa de servicio
Descripción	Plataforma para registro, consulta y respuesta de peticiones, quejas, reclamos, sugerencias y denuncias.

Tabla 13 - Servicio 008 Plataforma de mesa de servicio

ID	009
Nombre	Gestión de red interna colaboradores.
Descripción	Gestión de la administración y configuración centralizada de la seguridad de la red institucional (internet e intranet).

Tabla 14 - Servicio 009 Gestión de red interna colaboradores

ID	010
Nombre	Gestión de red de infraestructura tecnológica.
Descripción	Gestión de la administración y configuración centralizada de la seguridad de la red que usan los Sistemas de información.

Tabla 15 - Servicio 010 Gestión de red de infraestructura tecnológica

ID	011
Nombre	Antivirus
Descripción	Software que detecta y elimina virus y otras amenazas informáticas en la red, sistemas de información, PC, dispositivos móviles y demás.

Tabla 16 - Servicio 011 Antivirus

ID	012
Nombre	Gestión de equipos de cómputo
Descripción	Adquisición, instalación, configuración y mantenimientos preventivos y correctivos de hardware y software de los equipos asignados a los funcionarios y contratistas de la Entidad

Tabla 17 - Servicio 012 Gestión de equipos de cómputo

ID	013
Nombre	Instalación de software en Equipos de computo
Descripción	Instalación de software por demanda en los equipos de cómputo de los funcionarios o contratistas

Tabla 18 - Servicio 013 Instalación de Software en equipo de computo

ID	014
Nombre	Videollamadas
Descripción	Acceso de servicio de video llamada a través de Meet de Google con posibilidad de grabación.

Tabla 19 - Servicio 014 Videollamadas

ID	015
Nombre	Soporte aplicaciones
Descripción	Gestión de incidentes y/o problemas presentados en las aplicaciones

Tabla 20 - Servicio 015 Soporte de aplicaciones

ID	016
Nombre	Configuración de ambientes de desarrollo, pruebas, capacitación y preproducción
Descripción	Preparación y configuración de ambientes para desarrollos, procesos de aseguramiento de calidad y capacitaciones en los diferentes sistemas de información

Tabla 21 - Servicio 016 Configuración de ambientes de desarrollo, pruebas, capacitación, preproducción

ID	017
Nombre	Despliegue de software en producción
Descripción	Preparación, configuración y despliegue de las soluciones generadas por el área de TI.

Tabla 22 - Servicio 017 Despliegue de software en producción

ID	018
Nombre	Gestión de infraestructura de TI
Descripción	Administración y monitoreo de servidores, servidores de aplicaciones, servidores web, sistemas de información, herramientas de software, soluciones en la nube y demás elementos de infraestructura de TI

Tabla 23 - Servicio 018 Gestión de Infraestructura de TI

ID	019
Nombre	Adquisición de licencias de software
Descripción	Servicio de adquisición de licencias de software requeridas para usar en los diferentes procesos de la organización

Tabla 24 - Servicio 019 Adquisición de licencias de software

ID	020
Nombre	Mantenimiento de aplicaciones desarrolladas in house
Descripción	<ul style="list-style-type: none"> • Servicio que se encarga de realizar cambios en los sistemas de información para: • Corregir errores recurrentes • Actualizar software base • Aumentar la capacidad funcional de la aplicación

Tabla 25 - Servicio 020 Mantenimiento de aplicaciones

ID	021
Nombre	Administración de bases de datos
Descripción	Servicio que se encarga de la administración de las bases de datos que maneja la entidad

Tabla 26 - Servicio 021 Administración de bases de datos

ID	022
Nombre	Gestión de <i>backup (respaldos)</i>
Descripción	Servicio que se encarga de generar respaldo de datos de los sistemas de información o datos de gestión locales y seguimiento a proveedores externos.

Tabla 27 - Servicio 022 Gestión de *backup*

ID	023
Nombre	Gestión de proyectos de TI
Descripción	Servicio que permite planear, ejecutar y realizar seguimiento a proyectos que afectan los procesos o elementos de la arquitectura de TI

Tabla 28 - Servicio 023 Gestión de proyectos de TI

ID	024
Nombre	Gestión de identidades – Acceso lógico
Descripción	Servicio que permite asignar recursos organizacionales a los funcionarios y contratistas de la entidad, así mismo, provee los mecanismos de autenticación y autorización para el acceso a estos recursos

Tabla 29 - Servicio 024 Gestión de identidades – Acceso lógico

ID	025
Nombre	DNS
Descripción	Servicio que permite asignar nombre de dominio a los diferentes elementos que hacen parte de la red.

Tabla 30 - Servicio 025 DNS

ID	026
Nombre	Servicio de Virtualización de servidores
Descripción	Servicio que permite virtualizar servidores físicos en varias máquinas virtuales, las cuales pueden proveer a su vez servicios de hosting a las diferentes soluciones de software.

Tabla 31 - Servicio 026 Virtualización de servidores

ID	027
Nombre	Aseguramiento de la calidad del software QA
Descripción	Servicio que permite asegurar la calidad de las soluciones de software.

Tabla 32 - Servicio 027 Aseguramiento de la calidad del software

ID	028
Nombre	Servicio de supervisión de proveedores de TI
Descripción	Servicio que permite asegurar que los proveedores cumplan con las obligaciones contractuales.

Tabla 33 - Servicio 028 Servicio de Supervisión de proveedores de TI

6.8. Capacidades de TI.

Categoría	Capacidad	Cuenta con la capacidad en la entidad
Estrategia	Gestionar arquitectura empresarial	NO
	Gestionar Proyectos de TI	SI
	Definir políticas de TI	NO
Gobierno	Gestionar Procesos de TI	SI
Información	Administrar modelos de datos	SI
	Gestionar flujos de información	SI
Sistemas de Información	Definir arquitectura de Sistemas de Información	SI
	Administrar Sistemas de Información	SI
	Interoperar	SI
Infraestructura	Gestionar disponibilidad	SI
	Realizar soporte a usuarios	SI
	Gestionar cambios tecnológicos	SI
	Administrar infraestructura tecnológica	SI
Uso y apropiación	Apropiar TI	SI
	Capacitaciones en TI	SI
Seguridad	Gestionar seguridad de la información	SI

Tabla 34 - Capacidades de TI

Estas capacidades evidencian que TI opera con fortaleza en áreas técnicas, pero carece de capacidades estratégicas (arquitectura empresarial y definición de políticas). Este hallazgo justifica la creación de instancias de gobierno y el cambio de modelo operativo hacia 'Aliado de Negocio', como se detalla en la sección Estrategia y Gobierno de TI.

Las brechas identificadas en capacidades estratégicas no deben interpretarse como una reasignación de responsabilidades institucionales, sino como la necesidad de fortalecer las capacidades técnicas y metodológicas de TI para apoyar de manera más efectiva los procesos de arquitectura empresarial, planeación y definición de lineamientos, liderados por las instancias correspondientes.

La tabla muestra que la entidad si cuenta con la capacidad en todas las áreas operativas clave como:

- **Infraestructura.** Realizar soporte, gestionar cambios y administrar la tecnología.
- **Seguridad.** Gestionar la seguridad.
- **Sistemas e Información.** Administrar sistemas, interoperar, administrar modelos de datos y gestionar flujos.

La tabla revela la verdadera causa de los problemas estratégicos. La entidad no cuenta con la capacidad en dos áreas críticas de la categoría "Estrategia". Gestionar arquitectura empresarial y Definir políticas de TI y se debe a que el proceso gestión de TIC es netamente operativo.

No se puede esperar una ejecución del 100% del **PETI** si la entidad no tiene la capacidad de "Gestionar la arquitectura empresarial" que alinea esos proyectos.

El déficit de capacidad no es solo una falta de personal, sino una falta de dirección estratégica. Sin arquitectura ni políticas claras, los proyectos se vuelven más difíciles de ejecutar, generando reprocesos y desalineación.

Existe una contradicción reveladora: la entidad si puede gestionar proyectos de TI, pero no puede gestionar la arquitectura empresarial. Esto crea un área de TI reactiva que actúa como un tomador de pedidos, pero que carece de la capacidad proactiva para diseñar cómo esos proyectos deben encajar en una visión tecnológica unificada.

6.9. Indicadores de TI

Nombre	Tipo de indicador	Unidad de medida	Responsable	Periodo	Valor	Interpretación
Ejecución del PETI	Gestión	Porcentaje	Director Activo y TIC	anual	74%	Intermedio
Dificultades por capacidad en proyectos de TI	Gestión	Porcentaje	Director Activo y TIC	anual	26%	Alto
Disponibilidad de Información Institucional en <i>ownCloud</i>	Eficacia	Porcentaje	Director Activo y TIC	Mensual	92,8	Bueno
Oportunidad en la atención de servicios de soporte tecnológico de nivel 1	Eficacia	Horas	Director Activo y TIC	Mensual	4,2	Satisfactorio
Oportunidad en la atención de servicios de soporte tecnológico de nivel 2	Eficacia	Días hábiles	Director Activo y TIC	Mensual	4,48	Bueno

Tabla 35 - Control de indicadores

KPI	Tipo	Fórmula	Línea Base 2025	Meta 2026	Meta 2029	Fuente	Responsable
% proyectos PETI ejecutados	Gestión	$(\text{Proyectos ejecutados} / \text{Total}) \times 100$	74%	85%	≥95%	Tablero TI	Dir. Adm. y TIC
% riesgos críticos SGSI mitigados	Seguridad	$(\text{Riesgos} > 15 \text{ mitigados} / \text{Total} > 15) \times 100$	N/A*	≥50%	≥90%	Matriz SGSI	Seguridad Información
% controles ISO 27001:2022 implementados	Seguridad	$(\text{Controles "Implementados"} / 93) \times 100$	N/A*	≥40%	≥90%	SOA 2022	Seguridad Información
MTTD / MTTR incidentes	Seguridad	Horas promedio detección / respuesta	N/A*	MTTD ≤4h / MTTR ≤16h	MTTD ≤2h / MTTR ≤8h	GLPI/Comité	Coordinación TIC
% cifrado en tránsito y reposo	Seguridad	$(\text{Sistemas con TLS} + \text{DB/backup cifrado} / \text{Total sistemas}) \times 100$	N/A*	≥60%	≥95%	Evidencia técnica	Seguridad Información
% pruebas de restauración exitosas	Continuidad	$(\text{Restauraciones exitosas} / \text{Pruebas}) \times 100$	N/A*	≥80%	≥95%	Backups	Infraestructura

Tabla 36 - KPIs estratégicos PETI

Los **KPIs** definidos se entienden como indicadores progresivos, cuyo cumplimiento está condicionado al fortalecimiento gradual de las capacidades de TI y a la implementación de los proyectos estructurantes del PETI. Estos indicadores no buscan generar sobrecarga operativa, sino permitir el seguimiento y la toma de decisiones informadas sobre la evolución del rol habilitador de TI en la Entidad.

El análisis de los indicadores de 2025 revela una **división clara en el desempeño de TI**: la organización es eficaz en la gestión operativa diaria y la gobernanza de datos de gestión, pero enfrenta un déficit crítico en su capacidad para ejecutar proyectos estratégicos.

Se identifica un **problema central**: Déficit de Capacidad Estratégica. El principal hallazgo proviene de la correlación directa entre los dos indicadores de Gestión. La ejecución del PETI alcanzó solo un 74%, dejando una cuarta parte del plan estratégico sin completar.

La causa de este incumplimiento se explica en el **indicador**: Dificultades por capacidad en proyectos de TI, que registra un 26%. La suma de estos dos 74% + 26% sugiere que la falta de capacidad ya sea de personal, tiempo o presupuesto; es el factor directo que impide el 100% de la ejecución estratégica. Por otro lado, las **Fortalezas** están en la operación y gobernanza de datos de gestión. En contraste, los indicadores de "Eficacia" son positivos y demuestran control sobre las operaciones y los activos de información de gestión, así:

- **Soporte Operativo**: La gestión de incidencias diarias funciona bien. El soporte de Nivel 1 se atiende en 4,2 horas que se encuentra dentro de la interpretación Satisfactorio y el de Nivel 2 en 4,48 días hábiles calificado como **Bueno**.
- **Gobernanza de Datos de Gestión (ownCloud)**: El indicador "Disponibilidad de Información Institucional en **ownCloud**" con un 92,8% que se encuentra en la calificación de **Bueno**, es un éxito. Demuestra un alto nivel de cumplimiento por parte de los usuarios al almacenar la información de gestión en el repositorio centralizado y protegido, en lugar de en silos de riesgo como escritorios locales o nubes personales.

Es así como, la **Dirección de Administrativa y TIC** es competente para administrar el presente soporte y protección de datos, pero carece de la capacidad necesaria para construir el futuro como se ve en la ejecución de proyectos del **PETI**.

Las acciones de mejora se proponen en los siguientes capítulos del presente Plan y se enfocan en resolver el déficit de capacidad y cerrar las brechas de cumplimiento en materia de ser aliado de negocio y constituirse en un área estratégica.

6.10. Riesgos

Como instrumento para el gobierno de las TIC, el 29 de enero de 2025 se implementó una matriz de riesgos orientada a identificar y gestionar las principales categorías y eventos de riesgo institucional relacionados con las TIC. Actualmente, esta matriz se encuentra en proceso de actualización para incorporar los lineamientos del contrato de implementación del Sistema de Gestión de Seguridad de la Información (SGSI), garantizando su alineación con la norma **ISO / IEC 27001:2022** y el Modelo de Seguridad y Privacidad de la Información del MinTIC.

Identificación del riesgo				Evaluación del riesgo - Valoración de los controles					Plan de Acción	
Proceso	Descripción del Riesgo	Observación n de criterio	Impacto Inherente	No. Control	Descripción del Control	Afectación	Impacto Residual	Tratamiento	Acción de tratamiento	Acción de Contingencia ante posible
Gestión de TIC	Posibilidad de afectación reputacional por pérdida de información institucional debido a una infraestructura de protección y contingencia desactualizada, junto con deficiencias en el proceso de realizar copias de seguridad.	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	1	El profesional responsable del proceso de Gestión de TIC verifica una vez al mes que la copia automática del sistema JSP7 Gobierno, TRAMPUS, GLPI, Intranet y de la información contenida en los servidores de la Empresa con una periodicidad de cada 12 horas, quede almacenada en los repositorios correspondientes, con el propósito de contar con información actualizada en caso de que se presente una falla. En caso de encontrar que no se realizó de manera automática, se solicita al proveedor justificación por escrito la razón por la cual no se realizó ese backup y paralelamente se ejecute la instrucción de lanzar un backup manual de forma inmediata sin interrumpir la programación de los backups automatizados.	Probabilidad	Moderado	Reducir (mitigar)	Verificar diariamente en los repositorios que los backups se realicen de la forma adecuada.	Solicitar una copia de seguridad de la fecha anterior más reciente del día de materialización del evento.
				2	Los profesionales del proceso de Gestión de TIC, realizan un monitoreo diario de la infraestructura de TI de la entidad, utilizando herramientas de monitoreo, protección y tableros de control, ingresando a la plataforma o revisando que no hayan enviado alertas de correo electrónico sobre fallos en los sistemas, una vez revisado se generan reportes mensuales los cuales son trasladados a los expedientes contractuales. El proveedor también realiza revisión de alertas e informa inmediatamente al profesional de sistemas si se encuentran alguna anomalía.	Probabilidad	Moderado	Reducir (mitigar)	Realizar seguimiento a la contratación de los servicios de mantenimiento preventivo y correctivo del hardware de la Empresa a través del Plan de Adquisiciones.	Realizar mantenimiento correctivo.
Gestión de TIC	Posibilidad de afectación reputacional por la vulnerabilidad de los sistemas de información, debido a la debilidad en la actualización del hardware, software y claves de confidencialidad de acceso a funcionarios y contratistas.	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	1	El profesional encargado del directorio activo generará un mensaje de advertencia que su contraseña va a caducar para que el usuario realice el cambio de la contraseña.	Probabilidad	Moderado	Reducir (mitigar)	Realizar seguimiento a la contratación de los servicios de mantenimiento preventivo y correctivo del hardware de la Empresa a través del Plan de Adquisiciones.	Mantenimiento correctivo.
				2	El profesional del proceso de gestión de TIC mensualmente realizará actualizaciones de los servidores instalando update de seguridad en el software, sistemas operativos para minimizar las brechas de vulnerabilidades.	Probabilidad	Moderado	Reducir (mitigar)	Realizar seguimiento al contrato que soporta los servicios de TI, capacitar al personal del proceso de Gestión de TIC de acuerdo con la necesidad.	Aplicar los ANS con proveedor y restablecer servicio.
Gestión de TIC	Posibilidad de afectación reputacional por indisponibilidad de los servicios o infraestructura de TI debido a cortes de redes eléctricas, de datos, voz e Internet imprevistos por tiempos prolongados y equipos obsoletos que no soportan eficientemente el software adquirido.	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o	Mayor	1	El profesional en cargo de TIC en el tema de redes de internet deberá asegurar la disponibilidad de los servicios con los proveedores de forma mensual con informes de indisponibilidad del servicio.	Probabilidad	Mayor	Reducir (mitigar)	Realizar seguimiento a la contratación de los servicios de mantenimiento preventivo y correctivo del hardware de la Empresa a través del Plan de Adquisiciones.	Mantenimiento correctivo.
				2	El aplicativo ENTUTY de manera permanente realiza monitoreo web a la infraestructura tecnológica compuesta por canales de datos, canal internet y equipos tipo servidor, para verificar la disponibilidad y el estado del funcionamiento de los aplicativos, al encontrar una falla envía un correo de alerta al proceso Gestión de TIC para adelantar las acciones que correspondan.	Probabilidad	Mayor	Reducir (mitigar)	Realizar seguimiento al contrato que soporta los servicios de TI, capacitar al personal del proceso de Gestión de TIC de acuerdo con la necesidad.	Aplicar los ANS con proveedor y restablecer servicio.

Ilustración 7 - Matriz de riesgos TI

En la matriz se puede evidenciar la gestión de 3 riesgos orientados a evitar las fallas en los pilares básicos de la seguridad y operación de **TI** pueden dañar la imagen de la organización. Las causas principales son:

- **Pérdida de Información:** Provocada por una infraestructura de protección "desactualizada" y "deficiencias en el proceso de realizar copias de seguridad".
- **Vulnerabilidad de Sistemas:** Causada por la "debilidad en la actualización del hardware, software y claves", lo que expone los sistemas a ataques o brechas de seguridad.
- **Indisponibilidad de Servicios:** Originada por "cortes de redes eléctricas, de datos" e "equipos obsoletos" que no soportan el software, impidiendo que los usuarios accedan a los servicios.

Es así como el enfoque es gestionar los riesgos operativos de TI como la falta de disponibilidad, integridad y confidencialidad para prevenir un daño a la reputación e imagen de la entidad.

Nota sobre BCP y medidas compensatorias

- **Decisión institucional:** Para la vigencia analizada, no se implementará un **BCP** formal; la decisión se documenta en el **"Anexo al PETI con acta de no BCP"**
- **Medida compensatoria:** Se gestionará la continuidad mediante **pruebas técnicas de recuperación (DRP)** programadas (restauración de ERP, correo institucional, SGDEA TAMPUS y simulación de ransomware), con criterios de aceptación y evidencias técnicas
- **Trazabilidad:** Las **fechas, responsables y cronograma detallado** de estas pruebas se encuentran en el documento **"Plan de Acción proceso gestión de TI 2026.xlsx"**
- **Alineación normativa:** Las medidas **DRP** se integran con los **hitos SGSI** del PETI (SOA 2022, Plan de Tratamiento, política de cifrado) y mantienen el enfoque en **confidencialidad, integridad y disponibilidad** aplicado en esta sección

(Ver continuidad del servicio en 5.4.2 y los hitos SGSI, incluyendo la ejecución de pruebas de continuidad en la Fase 3)

6.11. Gestión financiera de TI

Macroproyecto	2025
Fortalecimiento de Gobierno y estructura organizacional de TI.	\$ 135.000.000
Sistemas de Información.	\$ 201.933.334
Seguridad y Privacidad de la Información	\$ 450.473.845
Infraestructura y Operación de TI	\$1.225.999.724
Total	\$2.013.406.903

Tabla 37 - Gestión financiera TI – 2025

La gestión financiera del **PETI** de la **Empresa** para 2025 asciende a \$2.013.406.903. El análisis de su distribución revela las prioridades estratégicas de la **Empresa** para este período, marcadas por un fuerte enfoque en la consolidación de la infraestructura.

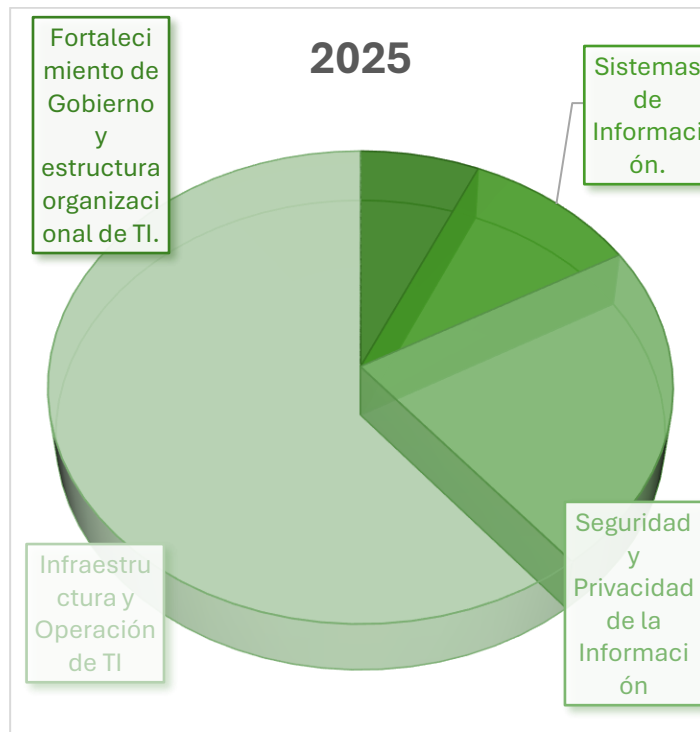


Ilustración 8: Gestión financiera TI - 2025 por Macroproyecto

El foco dominante en Infraestructura con el 60.9% del presupuesto total, se evidencia en la asignación para Infraestructura y Operación de TI. Esto indica que el PETI 2025 cierra el ciclo 2022-2025 con un enfoque primario en cimentar la base tecnológica compuesta por hardware, redes, nube y operaciones diarias. Es una inversión para garantizar el funcionamiento operacional y modernizar la plataforma.

Se observa una alta prioridad en Seguridad con el 22.4%, siendo la Seguridad y Privacidad de la Información el segundo rubro más importante. En conjunto, Infraestructura y Seguridad representan más del 83% del presupuesto de TI, lo que demuestra una fuerte conciencia del riesgo y una estrategia defensiva para proteger los activos de información de la entidad.

Por el contrario, existe una inversión moderada en Sistemas y Gobierno con 16.7%. Los macroproyectos que impulsan nuevas funcionalidades de negocio, como Sistemas de Información 10% y Gobierno de TI 6.7%,

reciben una porción menor, lo que sugiere que su desarrollo a gran escala será una prioridad en el siguiente plan estratégico.

Como conclusión estratégica, el presupuesto 2025 de la **Empresa** no fue un plan de expansión de aplicaciones, sino uno de fortalecimiento, estabilización y aseguramiento. La estrategia principal es consolidar y proteger la infraestructura base, sentando así las bases para los proyectos de transformación digital del próximo **PETI 2026-2029**.

6.12. Políticas TI

Las políticas son directrices o principios establecidos para guiar decisiones y lograr resultados coherentes.

En el PETI, se identifican las políticas y lineamientos vigentes, ajustados conforme al Acta del Comité Institucional de Gestión y Desempeño (diciembre 2025), que eliminó políticas obsoletas y aprobó la adopción del **Manual de lineamientos de seguridad y privacidad de la información**.

Categoría	Nombre de la política o principio	Tipo / Propósito principal
Vigente	Manual de lineamientos de seguridad y privacidad de la información	Las políticas vigentes se consolidan en el Manual de lineamientos de seguridad y privacidad de la información, que establece principios, controles y responsabilidades para garantizar la protección de la información en todos los procesos institucionales. Este manual se articula con el SGSI (ISO/IEC 27001:2022) y el MSPI, asegurando defendibilidad ante auditoría y trazabilidad normativa.

Categoría	Nombre de la política o principio	Tipo / Propósito principal
		Se eliminan referencias a documentos obsoletos, manteniendo como base única el manual actualizado aprobado en Comité Institucional (Acta diciembre 2025).
Vigente	Manual de Roles y responsabilidades	Define los roles y responsabilidades requeridos en la estructura organizacional para facilitar la implementación del MSPI y el SGSI.
Vigente	Plan de seguridad y privacidad de la información (versión ajustada)	Establece las actividades contempladas en el MSPI y los lineamientos para su implementación en la Empresa, alineado con la Norma ISO/IEC 27001:2022, las políticas de Gobierno Digital y Seguridad Digital, continuidad del servicio y protección de datos personales.
Vigente	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Documento actualizado que contiene lineamientos para la gestión integral de riesgos, articulado con la Declaración de Aplicabilidad (SOA) ISO/IEC 27001:2022 y el contrato vigente.

Tabla 38 - Políticas vigentes de TI

6.13. Procedimientos documentados vigentes

Los procedimientos son conjuntos interrelacionados de actividades que transforman insumos en productos o servicios finales. Los siguientes son los procedimientos documentados que gestionan aspectos críticos de la operación de TI en la **Empresa de Renovación y Desarrollo Urbano de Bogotá, D.C.**

Código del procedimiento	Nombre del procedimiento	Descripción del alcance
PD-71	Administración de Acceso Lógico V5	Documenta aspectos críticos de la operación y gestión de TI, específicamente la administración de accesos.
PD-52	Mantenimiento de equipos de TI V3	Documenta aspectos críticos de la operación y gestión de TI, específicamente el mantenimiento de equipos.
PD-50	Adquisición de Infraestructura Tecnológica V3	Documenta aspectos críticos de la operación y gestión de TI, específicamente la adquisición de infraestructura tecnológica.
PD-51	Copias de respaldo V3	Documenta aspectos críticos de la operación y gestión de TI, específicamente el respaldo de datos (versión V3). (Se menciona que existe una versión anterior V2 que se debe actualizar).
PD-70	Soporte técnico y mantenimiento correctivo de dispositivos TI V3	Documenta aspectos críticos de la operación y gestión de TI, específicamente el soporte técnico y mantenimiento correctivo.
No Codificado	Procedimiento de control de cambios	Documento requerido para garantizar la trazabilidad y seguridad en actualizaciones, implementaciones o cambios sobre la infraestructura tecnológica, alineado con los lineamientos del SGSI (ISO/IEC 27001:2022) y el MSPI. Su formalización se realizará en el SIG conforme a la política institucional.

Tabla 39 - Procedimientos documentados vigentes

Es fundamental que los procesos documentados y formalizados reflejen la realidad operativa de la **Empresa**, evitando la implementación de estándares que no se ajusten a su contexto, aunque sean recomendados por marcos como **ITIL** y **COBIT**. La **Dirección Administrativa y de TIC** también reconoce que la documentación actual de los procesos críticos requiere una actualización y formalización que refleje las necesidades y prácticas reales de la Empresa y poder prepararse para los retos que se establecen en el nuevo **PETI 2026-2029**.

6.14. Estructura y organización humana de TI

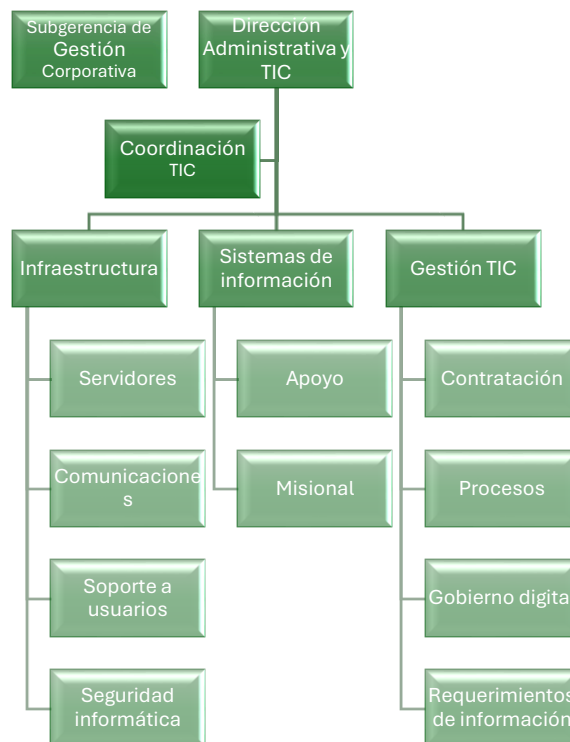


Ilustración 9 - Estructura de TI

De acuerdo con esta distribución, actualmente, el equipo de **TI** cuenta con 4 trabajadores oficiales, incluido el **Director Administrativo y de TIC** quien cumple con la función de **CIO**.

El equipo cuenta también con 13 contratistas organizados de la siguiente forma:

- 2 **Técnicos** contratistas para soporte a usuarios.
- 1 Secretaria de planta para apoyo contratos, informes y paz y salvos.
- 1 profesional contratista **backend**
- 1 profesional contratista **frontend**
- 1 Profesional contratista para Seguridad Perimetral.
- 1 Profesional contratista para infraestructura.
- 1 Profesional contratista para procesos de contratación.
- 1 Profesional contratista para gestión del proyecto Sistema Misional.
- 1 Profesional contratista para levantamiento de flujos de trabajo base para el Sistema Misional.
- 1 Profesional de planta Gestor junior 3, - seguridad de la información - Gobierno Digital.
- 1 Director administrativo y TIC - CIO de planta.
- 1 Profesional especializado contratista para tareas de coordinación del grupo contratistas y liderazgo del proceso TIC.
- 1 Profesional de planta Gestor senior I, supervisión contratos, - Gobierno Digital.

6.15. Sistemas de información

6.15.1. Catálogo de sistemas de información

Nombre aplicación	Sistema ERP administrativa, contable, financiero y nómina
Descripción Funcional	<p>Sistema que soporta todas las actividades contables, financieras, presupuestales, gestión post contractual, tesorería, contratistas de la empresa y dentro de las funciones principales se encuentra:</p> <ul style="list-style-type: none"> • Gestionar órdenes contables • Gestionar documentos contables • Gestionar activos • Gestionar cuentas por pagar • Gestionar cuentas por cobrar • Gestionar compras y gastos • Gestionar movimientos bancarios • Gestionar facturas • Gestionar las metas institucionales del Plan de Desarrollo Distrital. • Gestionar el Plan de Adquisiciones. • Gestionar el proceso de pago a Contratistas. • Gestionar la nómina.
Información que gestiona	<ul style="list-style-type: none"> • Orden contable. • Cuenta por cobrar. • Cuenta por pagar. • Entidad financiera. • Compra. • Gasto. • Factura. • Activo. • Movimiento bancario. • Documento contable. • Balance General. • Estado de resultados. • Estado de flujo de caja. • Avances de actividades del plan de acción institucional. • Registro de la programación presupuestal y la gestión de los egresos asociados a los proyectos presupuestales. • Información de las actividades que desarrollan los contratistas y documentos de cuenta de cobro. • Información de nómina de los empleados públicos y trabajadores oficiales.

Tipo de software	Software como Servicio.
Estado	Productivo.
Esquema de licenciamiento	Usuarios ilimitados y asociado a contrato de soporte y mantenimiento.
Fabricante	ASP Solutions.
Integraciones con otros sistemas	No.
Debilidades o hallazgos estructurales	Ninguna.

Tabla 40 - Caracterización sistema **ERP JSP7**

Nombre aplicación	SECOP 2
Descripción Funcional	Plataforma transaccional para gestionar en línea todos los Procesos de Contratación, con cuentas para entidades y proveedores; y vista pública para cualquier tercero interesado en hacer seguimiento a la contratación pública.
Información que gestiona	<ul style="list-style-type: none"> • Contratos • Documentos de soporte • Procesos pre-contractuales • Proponentes • Oferentes • Licitaciones • Subastas
Tipo de software	Software como servicio
Estado	Productivo
Esquema de licenciamiento	Libre para entidades públicas
Fabricante	Agencia Nacional de Contratación Pública – Colombia Compa Eficiente
Integraciones con otros sistemas	No
Debilidades o hallazgos estructurales	Ninguna

Tabla 41 - Caracterización sistema SECOP 2

Nombre aplicación	SIGEP
Descripción Funcional	El SIGEP es un Sistema de Información y Gestión del Empleo Público al servicio de la administración pública y de los ciudadanos. Contiene información de carácter institucional tanto nacional como territorial, relacionada con: tipo de entidad, sector al que pertenece, conformación, planta de personal, empleos que posee, manual de funciones, salarios, prestaciones, etc.; información con la cual se identifican las instituciones del Estado Colombiano.
Información que gestiona	<ul style="list-style-type: none"> • Información de funcionarios • Manual de funciones • Entidades del Estado • Hojas de vida • Declaración de bienes y rentas • Plan institucional de capacitación • Evaluación de desempeño
Tipo de software	Software como Servicio
Estado	Productivo
Esquema de licenciamiento	Software libre para entidades públicas
Integraciones con otros sistemas	Ninguna
Debilidades o hallazgos estructurales	

Tabla 42 - Caracterización Sistema **SIGEP**

Nombre aplicación	Sistema de Gestión Documental - TAMPUS
Descripción Funcional	Sistema donde se alojan las tablas de retención documental, así como los expedientes y documentos relacionados con los procesos de la Entidad
Información que gestiona	<ul style="list-style-type: none"> • Tablas de retención documental • Expedientes • Todos los documentos en formato digital
Tipo de software	Software como Servicio.
Estado	Productivo.
Esquema de licenciamiento	Software como servicio 370 licencias de usuarios
Integraciones con otros sistemas	Bogotá te escucha PQRS
Debilidades o hallazgos estructurales	No cuenta con APIs de integración, trabaja con SOAP

Tabla 43 - Caracterización sistema de gestión documental

Nombre aplicación	Página web de la Empresa de Renovación y Desarrollo Urbano de Bogotá, D.C.
Descripción Funcional	Sitio web institucional disponible a los ciudadanos que integra información sobre servicios institucionales, trámites, noticias, eventos de interés, políticas y normatividad.
Información que gestiona	<ul style="list-style-type: none"> • Licencias • Normatividad • Noticias • Servicios institucionales • Trámites • Información organizacional
Tipo de software	Gestión de contenido
Estado	Productivo – nube privada
Esquema de licenciamiento	Software libre
Integraciones con otros sistemas	Ninguno
Debilidades o hallazgos estructurales	No cuenta con APIs de integración

Tabla 44 - Caracterización sistema página web

Nombre aplicación	Intranet de la Empresa de Renovación y Desarrollo Urbano de Bogotá, D.C.
Descripción Funcional	Sitio web institucional disponible a los Colaboradores de la Empresa que integra información sobre servicios institucionales, trámites, noticias, eventos de interés, políticas, normatividad, Sistema Integrado de Gestión.
Información que gestiona	<ul style="list-style-type: none"> • Normatividad • Noticias • Servicios institucionales • Información organizacional
Tipo de software	Gestión de contenido
Estado	Productivo
Esquema de licenciamiento	Software libre
Integraciones con otros sistemas	Ninguno
Debilidades o hallazgos estructurales	<ul style="list-style-type: none"> • Sistema operativo Debian desactualizado • No cuenta con certificado SSL • No cuenta con APIs de integración

Tabla 45 - Caracterización sistema Intranet

Nombre aplicación	Mesa de ayuda GLPI
Descripción Funcional	Plataforma web institucional que centraliza la gestión de servicios TI y procesos administrativos, permitiendo manejar solicitudes e incidencias mediante un sistema de mesa de ayuda
Información que gestiona	<ul style="list-style-type: none"> • Soporte técnico nivel 1 • Soporte técnico nivel 2 • Gestión de salas de reuniones • Paz y salvos
Tipo de software	Cliente – servidor aplicaciones Web
Estado	Productivo
Esquema de licenciamiento	Software libre
Integraciones con otros sistemas	Directorio activo
Debilidades o hallazgos estructurales	Sistema operativo Debian desactualizado

Tabla 46 - Caracterización sistema GLPI

Nombre aplicación	Sistema de Gestión Documental - ERUDITA
Descripción Funcional	Sistema donde se alojaron las tablas de retención documental, así como los expedientes y documentos relacionados con los procesos de la Entidad de octubre de 2016 a diciembre de 2020.
Información que gestiona	<ul style="list-style-type: none"> • Tablas de retención documental • Expedientes • Documentos en formato digital
Tipo de software	Aplicación Web

Estado	Histórico.
Esquema de licenciamiento	Software libre
Integraciones con otros sistemas	Ninguna
Debilidades o hallazgos estructurales	Montado sobre infraestructura obsoleta.

Tabla 47 - Caracterización sistema Erudita

Nombre aplicación	Sistema de Gestión Contable y presupuestal - Apoteosys
Descripción Funcional	Sistema donde se alojó información contable y presupuestal de la Empresa ERU antes del año 2016.
Información que gestiona	<ul style="list-style-type: none"> • Cuenta por cobrar. • Cuenta por pagar. • Entidad financiera. • Compra. • Gasto. • Factura. • Activo. • Movimiento bancario. • Documento contable. • Balance General. • Estado de resultados. • Estado de flujo de caja.
Tipo de software	Cliente servidor
Estado	Histórico.
Esquema de licenciamiento	12 usuarios.
Integraciones con otros sistemas	Ninguna

Debilidades o hallazgos estructurales	<ul style="list-style-type: none"> • Montado sobre infraestructura obsoleta. • Sigue consultándose por parte del área contable.
---------------------------------------	---

Tabla 48 - Caracterización sistema Apoteosys

Nombre aplicación	Sistema de Gestión Contable y presupuestal – JSP6
Descripción Funcional	Sistema donde se alojó información contable y presupuestal de la Empresa Metrovivienda antes del año 2016.
Información que gestiona	<ul style="list-style-type: none"> • Cuenta por cobrar. • Cuenta por pagar. • Entidad financiera. • Compra. • Gasto. • Factura. • Activo. • Movimiento bancario. • Documento contable. • Balance General. • Estado de resultados. • Estado de flujo de caja.
Tipo de software	Cliente servidor
Estado	Histórico.
Esquema de licenciamiento	Ilimitado
Integraciones con otros sistemas	Ninguna
Debilidades o hallazgos estructurales	<ul style="list-style-type: none"> • Montado sobre infraestructura obsoleta. • Sigue consultándose por parte del área contable.

Tabla 49 - Caracterización sistema JSP6

7. Infraestructura

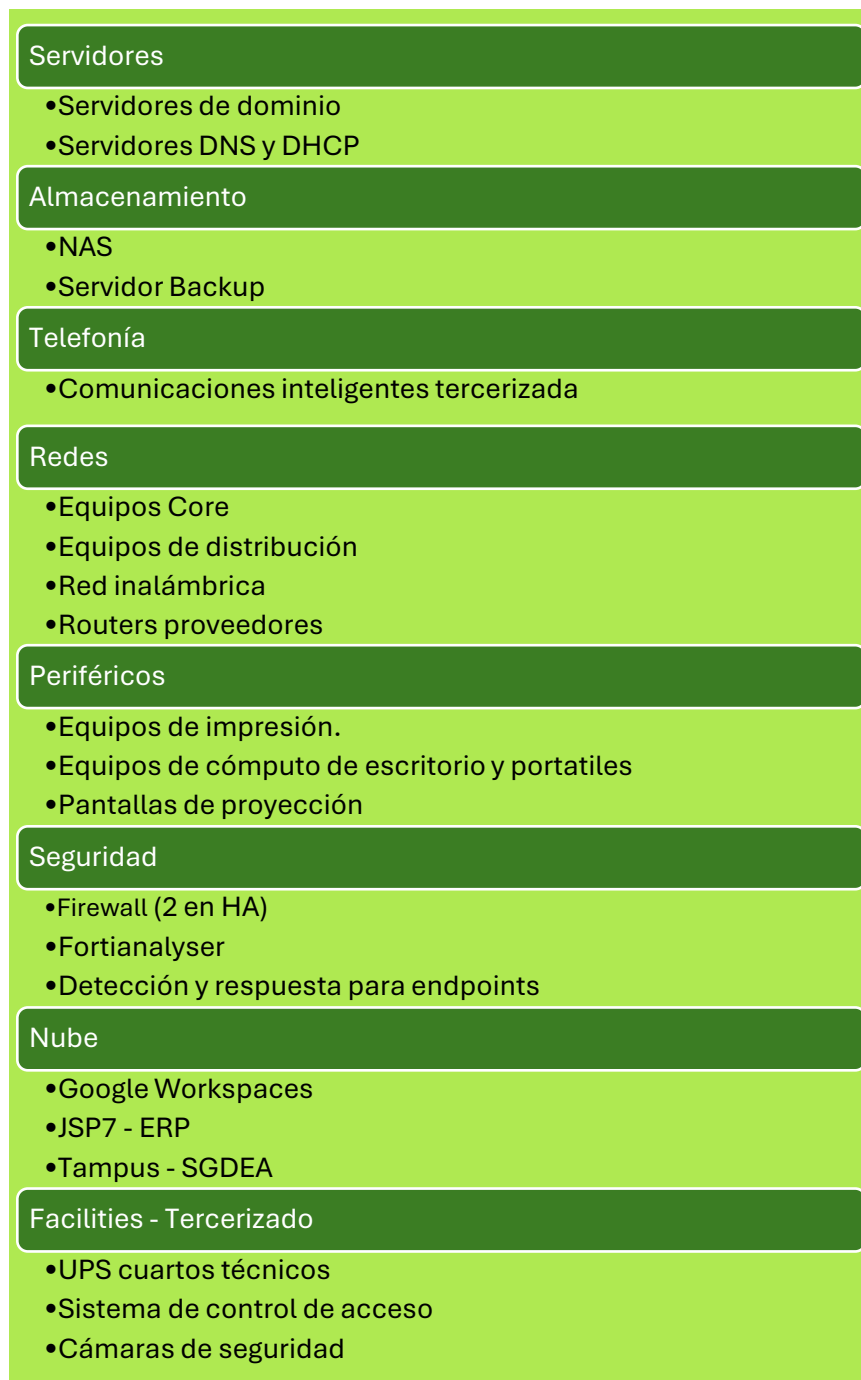


Ilustración 10 - Vista conceptual de Infraestructura de TI

7.1. Arquitectura de infraestructura tecnológica

Servicio de infraestructura	Descripción
Nube	Servicio de nube pública donde se aloja la página web de la Empresa Servicios de nube privada donde se alojan los sistemas: <ul style="list-style-type: none"> • JSP7. • TAMPUS. • Sistema georeferenciación.
Redes	Servicio WAN que permite la conectividad a internet. Servicio LAN que le permite a los usuarios de la entidad a acceder a los sistemas de información local y servidores de archivos
Seguridad	Servicio de seguridad perimetral que permite controlar el tráfico de red desde y a hacia Internet y aporta protección contra ataques externos. Servicio de monitoreo de la seguridad perimetral Fortianalyser. EDR (Detección y respuesta de endpoints) es una solución de ciberseguridad que monitorea y analiza la actividad de los puntos de conexión para detectar amenazas y responder a ellas automáticamente.
Servidores	Servicio de infraestructura de hardware para el alojamiento de aplicaciones históricas y posibles desarrollos propios.
Almacenamiento	Servicio de infraestructura de hardware para el almacenamiento de información. El almacenamiento de la información de gestión se realiza al interior de la Empresa en servidores propios. El almacenamiento referente al Sistema de Gestión Documental se realiza en la nube a través del sistema TAMPUS.
Telefonía	Servicio comunicaciones inteligentes donde se centraliza y gestiona todas las consultas y peticiones relacionadas con la telefonía fija y móvil, en la nube.
Facilities	Servicio tercerizado: UPS en cuartos técnicos respaldan equipos de conectividad y servidores. Sistema de vigilancia y control de acceso biométrico a las instalaciones de la Empresa
Periféricos	Servicios de soporte nivel 1 y 2. Solución de incidentes y requerimientos en sitio y remoto a todos los colaboradores de la Empresa. Acompañamiento a equipos de salas de reuniones.

Tabla 50 - Servicios de Infraestructura de TI

7.2. Administración de la operación

La operación de servicios tecnológicos la entidad busca garantizar la disponibilidad y continuidad de los servicios tecnológicos por medio de procesos, procedimientos, actividades y herramientas.

Identificador	Descripción	Sí	No
Monitoreo de la infraestructura de TI	Herramientas, actividades o procedimiento de monitoreo para e identificar, monitorear y controlar el nivel de consumo de la infraestructura de TI	X	
Capacidad de la infraestructura tecnológica	Se realizan planes de capacidades que permiten proyectar las capacidades de la infraestructura a partir de la identificación de las capacidades actuales	X	
Disposición de residuos tecnológicos	Se cuenta con procesos y procedimientos para una correcta disposición final de los residuos tecnológicos	X	

Tabla 51 - Operación de los servicios tecnológicos

La entidad implementa los procesos de soporte y mantenimiento preventivo y correctivo de los servicios tecnológicos, de acuerdo con las necesidades de su operación.

Identificador	Descripción	Sí	No
Acuerdos de Nivel de Servicios	Se han establecido Acuerdos de Nivel de Servicios y se vela por el cumplimiento	X	
Mesa de Servicio	Se tienen herramientas, procedimientos y actividades para atender requerimientos e incidentes de infraestructura tecnológica	X	
Planes de mantenimiento	Se generan y ejecutan planes de mantenimiento preventivo y evolutivo sobre toda la infraestructura de TI.	X	

Tabla 52 - Matriz de mantenimientos

7.3. Seguridad

No.	Tema / Control ISO 27001:2022	Calificación actual	Calificación objetivo	Evaluación
1	Organizacional (5.1 – 5.37)	70	100	Gestionado
2	Personas (6.1 – 6.8)	80	100	Gestionado
3	Físico (7.1 – 7.14)	76	100	Gestionado
4	Tecnológico (8.1 – 8.34)	68	100	Gestionado
Promedio		73,5	100	

Tabla 53 - Evaluación de efectividad de los controles

Las brechas críticas del SGSI, identificadas en la Declaración de Aplicabilidad (SOA), se atenderán conforme al Plan de Tratamiento y a los hitos SGSI del PETI (Q2–Q4 2026; Q1–Q2 2027). Ver **Anexo 8** para el resumen y el repositorio para la SOA completa.

8. Fase 3. Situación deseada u objetivo

8.1. Estrategia de TI: Visión y Misión 2029.

El modelo operativo de TI al que debe apuntar a la **Empresa de Renovación y Desarrollo Urbano de Bogotá, D.C.** es el de "**Aliado de Negocio**". Esto requiere una transformación cultural y estructural para apoyar los objetivos comerciales y de crecimiento financiero.

- Misión de TI 2029: Ser el habilitador tecnológico que apoya la generación de valor económico y la excelencia operacional de la **Empresa**, mediante el uso estratégico de la información, la provisión de plataformas seguras y la implementación eficiente de soluciones alineadas con la estrategia institucional.
- Visión de TI 2029: En el año 2029, la Dirección de TI de la Empresa será reconocida interna y externamente como un socio clave en la generación de valor económico y la optimización de procesos, mediante la aplicación de Arquitectura Empresarial, la adopción de analítica predictiva y la prestación de servicios digitales de clase mundial.

8.2. Objetivos estratégicos de TI (OE-TI)

Los objetivos de TI se alinean directamente con los pilares del Plan Estratégico Institucional.

8.2.1. OE-TI 1. Habilitación de ingresos y gestión comercial

Proveer soluciones tecnológicas que diversifiquen las fuentes de ingresos y optimicen la gestión de suelo y negocios inmobiliarios, mediante automatización, integración de datos y plataformas transaccionales seguras alineadas con el pilar de Crecimiento Financiero.

8.2.2. OE-TI 2. Transformación de datos y análisis estratégico

Implementar capacidades de gestión de datos, gobierno, interoperabilidad y analítica avanzada para convertir la información institucional en un activo estratégico que soporte decisiones predictivas y proactivas.

8.2.3. Fortalecimiento de la resiliencia y la seguridad digital

Garantizar la confidencialidad, integridad y disponibilidad de la información institucional mediante la consolidación del **SGSI** bajo **ISO / IEC 27001:2022**, la operación del **PTRSPI**, la gestión de incidentes con métricas **MTTD / MTTR**, la implementación de controles técnicos críticos (cifrado en tránsito y reposo, gestión de vulnerabilidades, control de acceso), la protección avanzada de **endpoints** y **EDR**, así como la seguridad integral de la arquitectura de nube híbrida (**cloud baseline, hardening**, logging, segmentación y continuidad SaaS). Esto incluye realizar pruebas **DRP** recurrentes con evidencia, asegurar la operación en entornos híbridos y fortalecer la infraestructura tecnológica conforme al EO0203 del Plan Estratégico Institucional.

8.2.4. OE-TI 4. Excelencia y eficiencia operacional de TI

Fortalecer la gobernanza de TI y madurar los procesos de soporte y gestión de servicios conforme a *ITIL* y *COBIT* para asegurar una operación: confiable, escalable y eficiente.



Ilustración 11 - Objetivos estratégicos de TI alineados con los pilares institucionales

8.3. Sistemas de Información

La arquitectura futura debe estar centrada en el cliente y la omnicanalidad.

8.3.1. Autogestión y comercial

Desplegar una estrategia digital con énfasis en la autogestión, unificando los servicios y productos de la Empresa en una plataforma portal web única (sede electrónica) para optimizar el *marketing social* y los servicios directos al cliente.

- **Gestión de Cliente:** Implementar un bloque arquitectónico dedicado que funcione como la base de datos única de clientes, administrando las interacciones y suministrando información a los demás bloques.
- **Infraestructura (Cloud Híbrida):** Mantener la estrategia de centro de datos y contingencia en nube (Modelo Híbrido), implementando una estrategia de replicación activa/activa o activa/pasiva y asegurando la capacidad y disponibilidad mediante el monitoreo continuo de la obsolescencia y los requisitos no funcionales. Se debe realizar un proceso de contratación de servicios en la Nube que reemplace la infraestructura obsoleta.
- **Gestión Misional: SIM-NocoBase:** El núcleo de la operación. Debe soportar los requerimientos Financieros como: costeo, viabilidad, flujos de caja y Contratación como; trazabilidad, pólizas, proveedores.
- **Gestión de la Integración (CDE y APIs):** Será el punto central de comunicaciones, asegurando que ningún sistema se integre directamente con otro mediante la implementación de una plataforma especializada tipo API Management para que actúe como punto central de comunicaciones, asegurando la consistencia y seguridad del intercambio de datos internos y externos.
- **Entorno Común de Datos (CDE):** Este es un componente clave para la Interoperabilidad. Servirá como un repositorio central de archivos y asegurará la trazabilidad mediante el historial de revisiones y la visualización de modelos BIM/planos.



Ilustración 12 - Estrategia digital de la Empresa

8.4. Infraestructura TI: Arquitectura objetivo

Arquitectura Objetivo: Debe evolucionar a un modelo donde la información sea el activo más estratégico.

Se requiere un bloque de **Autogestión** unificado (portal web), un bloque de **Gestión de Cliente** como base de datos única de clientes, y un bloque de **Gestión de la Integración** tipo API Management como punto central de comunicaciones para garantizar la consistencia de los datos.



Ilustración 13 - Bloques de arquitectura objetivo

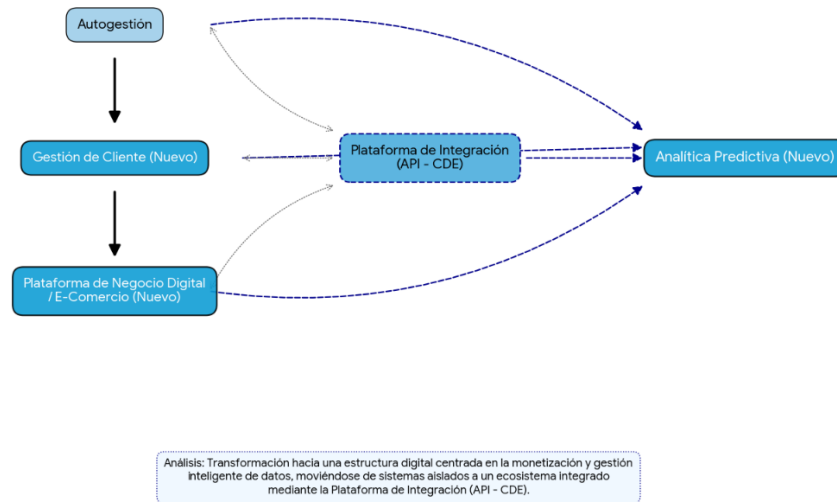


Ilustración 14 - Evolución de la arquitectura de sistemas – Objetivo 2029

La figura resalta los nuevos componentes comerciales y sus flujos. El flujo Comercial: Muestra la conexión directa desde Autogestión -> Gestión de Cliente -> Plataforma de Negocio Digital. La integración: La Plataforma de Integración (API - CDE) se muestra como el conector central que permite la comunicación entre estos sistemas. Como resultado deseado está el análisis de datos: Se visualiza cómo todos los componentes (los comerciales y el de integración) alimentan el nuevo bloque de Analítica Predictiva, centralizando la gestión inteligente de datos.

9. Hoja de ruta y portafolio de proyectos 2026-2029

La Hoja de Ruta del PETI 2026-2029 articula los macroproyectos ya definidos en la vigencia 2025 para cerrar las brechas encontradas en Gobierno, Infraestructura y Seguridad con **tres nuevos macroproyectos** enfocados explícitamente en la generación de ingresos y el cumplimiento del pilar de Crecimiento Financiero.



Ilustración 15 - Hoja de ruta consolidada 2026-2029

La figura presenta el cronograma general de implementación del PETI y los macroproyectos de TI hasta 2029. Se evidencia que los proyectos fundacionales —Infraestructura y Seguridad— constituyen la base durante el periodo 2026-2027, creando las condiciones necesarias para que los proyectos orientados a la generación de ingresos se desplieguen y alcancen su madurez entre 2027 y 2029.

EO0201 se incorpora mediante el despliegue del **SIM – NocoBase** para procesos misionales, la **arquitectura de integración API-Management y CDE**, y la modernización de la **omnicanalidad** (portal único). **EO0202** se integra al **macroproyecto de seguridad y privacidad**, migrando y operando el **SGSI en ISO/IEC 27001:2022** y ejecutando **DRP** con criterios de aceptación y evidencias.

Macroproyecto	Énfasis 2026-2029: Maduración y cierre de brechas
1. Fortalecimiento de Gobierno y Estructura Organizacional de TI	Posicionar la función de TI como Estratégica. Formalizar instancias de decisión internas Mesa de trabajo Operativo/Táctico, Mesa de trabajo de control de cambios TI. Implementación completa de procesos de gestión de proyectos, proveedores, y arquitectura empresarial.
2. Sistemas de Información	Integración Total de la Cadena de Valor (End-to-End): Implementación de la arquitectura de integración API- CDE y completar el ciclo de vida de los sistemas misionales, incluyendo el desarrollo y migración total del sistema misional en la herramienta NocoBase.
3. Seguridad y Privacidad de la Información	Operación Continua del SGSI: Pruebas de vulnerabilidad recurrentes, aseguramiento de la nube y fortalecimiento de la cultura de seguridad, alcanzando altos niveles de cumplimiento normativo (FURAG). Implementación del SGSI (ISO 27001:2022), Control de Acceso a la Red (NAC), y estrategia de Gestión de Identidades y Accesos (Single Sign On). Este macroproyecto incorpora explícitamente los lineamientos obligatorios de la Circular 07 de 2024 de la Consejería Distrital de TIC – Bogotá para PETI distritales (accesibilidad de sistemas de información y web; seguridad de la información), exigidos por los entes de control internos y externos, y articulados con el Programa de Transparencia y Ética Pública 2026 en su componente de accesibilidad. En coherencia, se integran actividades y evidencias para asegurar la defendibilidad normativa del PETI y la trazabilidad con el SGSI (ISO/IEC 27001:2022) y el MSPI.
4. Infraestructura y Operación de TI	Resiliencia y Nube Híbrida Avanzada: Migración completa de servicios locales obsoletos a la nube e infraestructura local actualizada. Implementación de mecanismos automatizados de continuidad y recuperación en la nube

Tabla 54 - Macroproyectos que se mantienen y buscan maduración

9.1. Macroproyectos estratégicos 2026-2029 con enfoque en generación de ingresos que puede apoyar TI

Estos proyectos están diseñados para impactar directamente en el pilar de Crecimiento Financiero de la Empresa y la prioridad de Nuevos Negocios que podrían ser apoyados por TI ya sea realizando implementaciones de herramientas o desarrollos particulares adaptados a las necesidades.

Nuevo Macroproyecto (2026-2029)	Alineación Estratégica (PEI)	Objetivo de Ingreso/Valor
5. Plataforma de Negocio Digital y Comercialización (C-F)	Crecimiento Financiero - Gestión Inmobiliaria y Portafolio de Servicios.	Optimizar la venta de suelo y servicios, reducir la dependencia de intermediarios, y crear un nuevo canal de ingresos por transacciones digitales.
6. Inteligencia de Negocios y Analítica Predictiva (C-F/R-S)	Crecimiento Financiero y Retorno Social	Identificar oportunidades de negocio rentables por nuevas áreas de intervención, antes que la competencia y optimizar la gestión de 3.000 hectáreas. Mejora en la eficiencia y la reducción de riesgos en la toma de decisiones.
7. Ecosistema Digital de Colaboración Urbana (R-S/Nuevos Negocios)	Retorno Social, Revitalización Urbana y Nuevos Negocios	Generar valor agregado al Portafolio de Servicios, mediante herramientas colaborativas B2B (Business-to-Business) y B2C (Business-to-Citizen) que faciliten la participación de promotores e interesados en los proyectos de revitalización.

Tabla 55 - Macroproyectos

C-F = Crecimiento Financiero; R-S= Retorno Social

9.2. Detalle de los nuevos proyectos (2026-2029)

9.2.1. Macroproyecto: Plataforma de Negocio Digital y Comercialización

- **Proyecto 1.1: Implementación de Gestor de Clientes y Promotores:** Adquisición e implementación de un sistema de Gestión de Clientes que centralice toda la información de los grupos de interés: ciudadanos, inversores, promotores. Debe ser compatible con la venta de suelo y la promoción de 5.000 viviendas.
- **Proyecto 1.2: Plataforma de E-Comercio y Subastas Digitales de Activos:** Desarrollo de un portal seguro para la venta en línea de bienes en el marco de Gestión Inmobiliaria y la gestión de arrendamientos comerciales. Debe permitir la automatización de flujos de pago y la generación de ingresos directos.

9.2.2. Macroproyecto: Inteligencia de Negocios y Analítica Predictiva

- **Proyecto 2.1: Desarrollo del Ecosistema de Datos:** Creación de un repositorio centralizado para consolidar datos internos como Sistemas Misionales, JSP7, Georreferenciación y externos como catastro, demografía, mercado inmobiliario. Esto supera la brecha de Analítica actual.
- **Proyecto 2.2: Implementación de Tableros de Control Predictivos:** Desarrollo de visualizaciones (BI) y modelos de análisis descriptivos - predictivos que permitan a la alta dirección tomar decisiones basadas en datos sobre riesgos, tendencias de mercado, y la priorización de nuevas áreas de Revitalización Urbana.

Macroproyecto: Ecosistema Digital de Colaboración Urbana

- **Proyecto 3.1: Modernización de Servicios al Ciudadano - Omnicanalidad:** Fortalecer los canales de comunicación y servicio. Web, intranet, chat, videollamadas para una experiencia totalmente digital, mejorando los servicios misionales y de apoyo.
- **Proyecto 3.2: Portal de Interacción con Promotores (B2B):** Creación de una plataforma digital para facilitar a los aliados externos como promotores y desarrolladores, el acceso a información técnica BIM, georreferenciación, viabilidad técnica y la presentación de propuestas de vinculación público-privada.

9.3. Matriz de alineación entre objetivos de TI y macroproyectos

OE-TI	Descripción	Macroproyectos que lo soportan	Justificación técnica y normativa
OE-TI 1. Habilitación de ingresos y gestión comercial	Soluciones que diversifiquen ingresos y optimicen procesos de gestión de suelo y negocios inmobiliarios.	MP5. Plataforma de Negocio Digital MP7. Ecosistema Digital de Colaboración Urbana MP2. Sistemas de Información (SIM-NocoBase)	La plataforma comercial habilita ventas digitales, subastas y portafolio; el SIM provee datos misionales unificados para la gestión inmobiliaria. Se alinea con MAE v3 (dominios Información y Sistemas de Información).
OE-TI 2. Transformación de	Convertir datos en activos estratégicos para	MP6. Inteligencia de Negocios y Analítica Predictiva	El macroproyecto BI habilita tableros, modelos predictivos, gobierno del dato y analítica; el

OE-TI	Descripción	Macroproyectos que lo soportan	Justificación técnica y normativa
datos y análisis estratégico	decisiones informadas y predictivas.	MP2. Sistemas de Información MP1. Gobierno y Arquitectura TI	SIM unifica datos misionales; la arquitectura empresarial asegura interoperabilidad y trazabilidad (MAE v3, dominio Información).
OE-TI 3. Resiliencia y seguridad digital	Consolidar el SGSI y asegurar la información y la infraestructura.	MP3. Seguridad y Privacidad de la Información MP4. Infraestructura y Operación de TI	MP3 implementa controles ISO 27001:2022 (cifrado, gestión de incidentes, EDR, vulnerabilidades, clasificación); MP4 moderniza infraestructura para asegurar disponibilidad (ISO 27001; MSPI).
OE-TI 4. Excelencia y eficiencia operacional de TI	Gobernanza, procesos ITIL/COBIT y eficiencia en servicios.	MP1. Gobierno y Estructura TI MP4. Infraestructura y Operación TI	MP1 formaliza procesos, mesas de trabajo, RACI y control de cambios según Decreto 338/2022 y MSPI; MP4 asegura continuidad, soporte, ANS y estandarización operacional.
OE-TI 5. Seguridad y resiliencia (ISO 27001:2022)	Confidencialidad, integridad y disponibilidad; cifrado; MTTD/MTTR; DRP.	MP3. Seguridad y Privacidad de la Información MP4.	MP3 operacionaliza SGSI, DRP y pruebas; MP4 soporta continuidad mediante nube híbrida, backups, restauraciones técnicas y plataformas seguras.

OE-TI	Descripción	Macroproyectos que lo soportan	Justificación técnica y normativa
		Infraestructura y Operación TI	

Tabla 56 - 9.3. Matriz de alineación entre objetivos de TI y macroproyectos

10. Proyección financiera año 2026

Macroproyecto	2026
Fortalecimiento de Gobierno y estructura organizacional de TI.	\$ 875.056.800
Sistemas de Información.	\$ 878.602.307
Seguridad y Privacidad de la Información	\$ 439.301.018
Infraestructura y Operación de TI	\$ 928.589.206
Total	\$ 3.121.549.331

Tabla 57 - Proyección financiera TI 2026

Mensualmente se revisan los reportes de ejecución del presupuesto, se toman decisiones al respecto y de ser necesario evalúan la gestión de adiciones/ajustes al presupuesto.

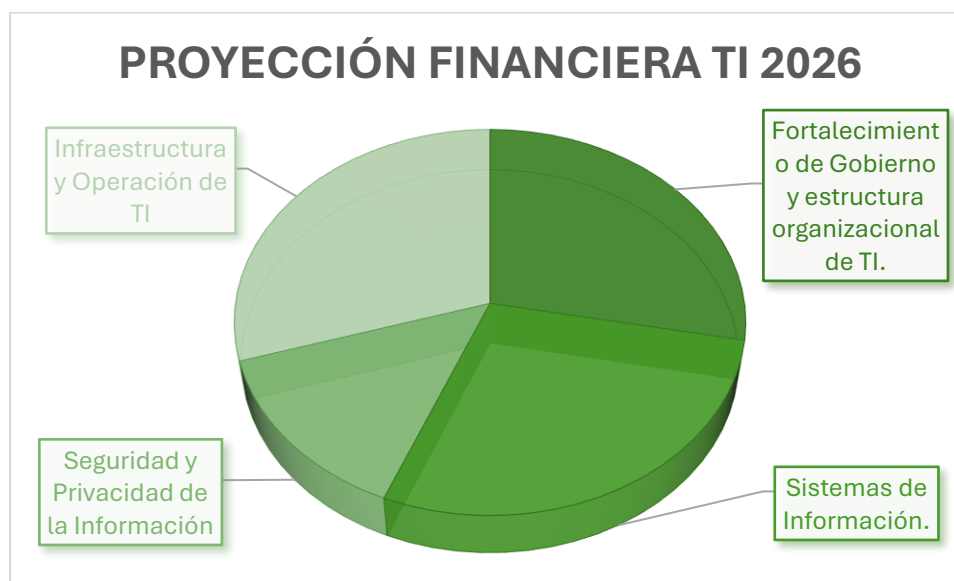


Ilustración 16: Proyección financiera TI 2026

11. Estrategia de Comunicación del PETI

La comunicación del PETI es esencial para la apropiación por parte de los directivos y colaboradores. El plan de comunicaciones se mantendrá, con énfasis en la difusión del rol estratégico de TI como facilitador del crecimiento financiero y la Excelencia Operacional.

11.1. Glosario

Sigla / Término	Definición
PETI	Plan Estratégico de Tecnologías de la Información
MAE v3	Marco de Arquitectura Empresarial versión 3 del MinTIC, que orienta la articulación entre estrategia, procesos, información y tecnología
MSPI	Modelo de Seguridad y Privacidad de la Información (Resolución MinTIC 448 de 2022)
SGSI	Sistema de Gestión de Seguridad de la Información, basado en la norma ISO/IEC 27001:2022
ISO/IEC 27001	Norma internacional para la gestión de la seguridad de la información
ISO/IEC 27002	Código de prácticas para controles de seguridad de la información
DRP	Disaster Recovery Plan: Plan de Recuperación ante Desastres
BCP	Business Continuity Plan: Plan de Continuidad del Negocio

Sigla / Término	Definición
API	Interfaz de Programación de Aplicaciones, conjunto de reglas para la interoperabilidad entre sistemas
CDE	Entorno Común de Datos , repositorio central para gestión colaborativa de información
ERP	Enterprise Resource Planning : Sistema integrado de gestión administrativa y financiera
BI	Business Intelligence : Herramientas para análisis y visualización de datos
FURAG	Formulario Único de Reporte de Avance en Gestión , instrumento de evaluación del MIPG
MIPG	Modelo Integrado de Planeación y Gestión , marco de gestión pública en Colombia
NAC	Network Access Control : Control de acceso a la red
SSO	Single Sign-On : Autenticación única para múltiples sistemas
TLS	Transport Layer Security : Protocolo de cifrado para comunicaciones seguras
PIA	Privacy Impact Assessment : Evaluación de impacto en privacidad
DLP	Data Loss Prevention : Controles para prevenir fuga de información
EDR	Endpoint Detection and Response : Solución para detección y respuesta ante amenazas en dispositivos
ITIL	Information Technology Infrastructure Library : Buenas prácticas para gestión de servicios TI
COBIT	Control Objectives for Information and Related Technologies : Marco para gobierno y gestión de TI

Tabla 58 - Glosario

12. Anexos

12.1. Anexo 1: Fase 1 – Planear

Esta sección documenta las actividades iniciales del proyecto **PETI** de acuerdo con la **Guía MGGTI.GE.ES.01 v3.0**: conformación del equipo y **stakeholders**, presupuesto para la elaboración del **PETI** y plan/cronograma del trabajo.

Actividad	Entregable	Responsable	Estado
Conformar equipo y stakeholders	Lista de equipo y matriz de comunicaciones	CIO / Planeación	En curso
Presupuesto para elaboración del PETI	Nota técnica o estudios previos	CIO / Financiera	Completado
Plan y cronograma del trabajo PETI	Cronograma Gantt	Planeación / CIO	Pendiente

12.2. Anexo 2: Stakeholders y comunicaciones

Stakeholder / Rol	Proceso o dominio	Responsable (Nombre/Rol)	Canales	Frecuencia	Objetivo de comunicación
Dirección Administrativa y TIC – CIO	Gobierno de TI / Estrategia	Director Adm. y TIC (CIO)	Correo, reuniones mesas de trabajo, intranet	Mensual	Decisión y seguimiento del PETI
Oficina Asesora de Planeación	Estrategia / Alineación PEI	Jefe Planeación	Correo, sesiones de trabajo	Quincenal	Alineación estratégica y cronograma PETI
Subgerencia de Gestión Corporativa	Gobierno / Recursos	Subgerente Gestión Corporativa	Correo, actas	Mensual	Asignación de recursos y priorización
Oficina Jurídica	Apoyo / Cumplimiento normativo	Jefe Jurídica	Correo, minutas	Mensual	Conceptos normativos y contratos
Dirección Financiera	Apoyo / Gestión financiera TI	Director Financiero	Correo, reportes BI	Mensual	Presupuesto y ejecución de inversiones TI

Stakeholder / Rol	Proceso o dominio	Responsable (Nombre/Rol)	Canales	Frecuencia	Objetivo de comunicación
Dirección de Contratación	Apoyo / Contratación TI	Director de Contratación	Correo, SECOP, reuniones	Quincenal	Procesos pre/contractuales de proyectos TI
Oficina de Control Interno	Evaluación y control	Jefe Control Interno	Correo, auditorías	Bimestral	Seguimiento de riesgos y controles
Oficina de Relacionamiento y Comunicaciones	Estrategia de socialización	Jefe Comunicaciones	Correo, intranet, piezas	Quincenal	Plan de socialización del PETI
Subgerencia de Ejecución de Proyectos	Misional	Subgerente	Correo, talleres	Quincenal	Requerimientos del SIM – NocoBase
Dirección Técnica de Gestión de Proyectos	Misional	Director Técnico	Correo, talleres	Quincenal	Flujos y KPIs misionales

12.3. Anexo 3: Planes externos y obligaciones

Plan/Norma	Año	Obligación TI/Datos	Área líder	Plazo (objetivo)	Estado
Decreto 767 – Política de Gobierno Digital	2022	Alinear PETI, Portal Único, SCD, TD y MAE v3.0	CIO + Planeación	2026–2028	Pendiente de integración completa
Decreto 88 – Digitalización de trámites	2022	Digitalizar/automatizar trámites y servicios	CIO + Misionales	2026–2027	En diagnóstico
Resolución 460 – PNID	2022	Adopción Hoja de Ruta PNID / Infraestructura de datos	CIO + Información	2026–2028	Planificación
Decreto 338 – Seguridad Digital	2022	Modelo de gobernanza de seguridad digital	CIO + Seguridad Información	2026	En curso (SGSI)
Resolución 746 – Seguridad y Privacidad	2022	Lineamientos adicionales MSPI	CIO + Seguridad Información	2026	En curso

Plan/Norma	Año	Obligación TI/Datos	Área líder	Plazo (objetivo)	Estado
Resolución 1117 – Territorios inteligentes	2022	Lineamientos de TD para territorios inteligentes	CIO + Misionales	2027–2029	Planificación

12.4. Anexo 4: Mapa de integraciones

Sistema Origen	Sistema Destino	Propósito	Protocolo	Seguridad	Frecuencia	Estado
SGDEA TAMPUS	ERP JSP7	Intercambio documental → contable	SOAP→REST API	TLS, token app, IP allow-list	Diaria	Planificada (conversión requerida)
ERP JSP7	BI / Analytics	Extracción contable/presupuestal para tableros	REST API	OAuth2, TLS	Diaria	En diseño
GLPI (Mesa de ayuda)	BI / Analytics	Indicadores ANS y soporte	REST API	Token, TLS	Semanal	Planificada
Página Web	Portal Único / SCD	Omnicanalidad y autogestión	HTTPS REST	OAuth2, TLS	En tiempo real	Planificada

SECOP 2	ERP JSP7	Consulta estado contractual y trazabilidad	Servicios SaaS / APIs	HTTPS, autenticación plataforma	Eventual	Por definir
---------	----------	--	-----------------------	---------------------------------	----------	-------------

12.5. Anexo 5: Hojas de vida de indicadores

Indicador	Definición	Fórmula	Línea base 2025	Meta 2026	Meta 2029	Fuente	Responsable	Periodicidad
Ejecución del PETI	% de iniciativas del PETI ejecutadas	$(\text{Proyectos ejecutados} / \text{Total}) \times 100$	74%	85%	≥95%	Tablero TI	Dir. Adm. y TIC	Anual
Dificultades por capacidad en proyectos TI	% de iniciativas afectadas por falta de capacidad	$(\text{Iniciativas con dificultad} / \text{Total}) \times 100$	26%	≤15%	≤5%	Tablero TI	Dir. Adm. y TIC	Anual

Indicador	Definición	Fórmula	Línea base 2025	Meta 2026	Meta 2029	Fuente	Responsable	Periodicidad
Disponibilidad de info en ownCloud	% de documentos de gestión en repositorio central	(Docs en ownCloud/Docs totales) x 100	92,8%	95%	≥98%	ownCloud	Dir. Adm. y TIC	Mensual
Oportunidad soporte nivel 1	Horas promedio atención de soporte N1	Promedio horas por ticket	4,2 h	≤3,5 h	≤2,5 h	GLPI	Coordinación TIC	Mensual
Oportunidad soporte nivel 2	Días hábiles promedio soporte N2	Promedio días por caso	4,48 días	≤3,5 días	≤2,5 días	GLPI	Coordinación TIC	Mensual

12.6. Anexo 6: Matriz RACI

Proceso	CIO	Planeación	Infraestructura	Sistemas de Información	Seguridad Info	Jurídica	Financiera	Contratación	Comunicaciones	Control Interno	Misionales
Gestión de proyectos TI	A	C	R	R	C	I	C	R	I	I	C
Control de cambios TI	A	I	R	R	R	C	I	C	I	C	I
Interoperabilidad / APIs / CDE	A	C	R	R	C	I	I	C	I	I	C
Gestión de Seguridad (SGSI)	A	I	C	C	R	C	I	I	I	C	I
Gobierno de datos y BI	A	R	I	C	C	I	I	I	I	I	C

Proceso	CIO	Planeación	Infraestructura	Sistemas de Información	Seguridad Info	Jurídica	Financiera	Contratación	Comunicaciones	Control Interno	Misionales
Socialización y comunicaciones	I	C	I	I	I	I	I	I	R	I	C
Arquitectura empresarial	A	R	C	C	C	I	I	I	I	I	C
Intranet y página web	I	I	I	I	I	I	I	I	R	I	I

12.7. Anexo 7: Acta modelo de aprobación

ACTA MODELO DE APROBACIÓN DEL PETI

Entidad: Empresa de Renovación y Desarrollo Urbano de Bogotá, D.C.

Comité: Comité Institucional de Gestión y Desempeño

Acta No.: _____

Fecha: ____ / ____ / ____

ORDEN DEL DÍA

1. Presentación del PETI 2026–2029.
2. Discusión de ajustes y observaciones.
3. Decisión sobre aprobación.

DECISIÓN

☐ Aprobado

☐ Aprobado con ajustes

☐ No aprobado

COMPROMISOS

Responsable

Actividad / Ajuste

Fecha límite

Evidencia esperada

PUBLICACIÓN

URL sitio web institucional / intranet: _____

Fecha de publicación: ____ / ____ / ____

Medio de difusión: ☐ Intranet ☐ Web ☐ Circular interna

FIRMAS

Nombre

Cargo

Firma

12.8. Anexo 8: Tabla brechas ISO 27001:2022

Este anexo complementa la **fase Analizar (AS-IS)** del PETI, aportando el detalle de las **brechas identificadas frente a la norma ISO/IEC 27001:2022** y su relación con el **Modelo de Seguridad y Privacidad de la Información (MSPI)** del MinTIC. Su propósito es:

- **Evidenciar el diagnóstico normativo** realizado sobre los controles aplicables al SGSI institucional.
- **Justificar las acciones correctivas** incluidas en la hoja de ruta del PETI y en el Plan de Tratamiento de Riesgos.
- **Asegurar trazabilidad contractual** con el Contrato 459-2025 y los lineamientos MSPI (Decreto 1078/2015, Decreto 338/2022, Resolución 746/2022).
- **Proveer defendibilidad ante auditoría externa**, mediante la Declaración de Aplicabilidad (SOA) y las evidencias esperadas por control.

Este anexo se articula con los contenidos del Capítulo 6: Análisis de la situación actual y oportunidades de mejora, específicamente en los apartados de Riesgos, Seguridad y Políticas TI, y constituye la base para los hitos SGSI definidos en la hoja de ruta (Q2–Q4 2026; Q1–Q2 2027).

Las brechas priorizadas responden al lineamiento **EO 02** y se cierran con la operación del **SGSI en ISO/IEC 27001:2022: SOA, plan de tratamiento, cifrado, EDR, gestión de vulnerabilidades y seguridad en la nube**, con evidencias verificables.

ISO	Control	Estado	Brecha / Justificación	Acción propuesta	Evidencia esperada
5.9	Inventario de información y activos asociados	Parcial	Aplica por obligatoriedad del Contrato 459-2025 (Cl. Quinta), lineamientos MSPI MinTIC (Dec. 1078/2015; Dec. 338/2022; Res. 746/2022) y la Política General de Seguridad y Privacidad de la Información (versión 2025). Cumplimiento Contractual 459-2025 – Cl. Quinta – Fase I, numeral 11: Inventario y clasificación de activos de información.	Levantar y mantener inventario de información y activos (CMDB), asignar propietarios y ciclo de vida.	CMDB publicada; actas de revisión; propietarios asignados.

ISO	Control	Estado	Brecha / Justificación	Acción propuesta	Evidencia esperada
5.11	Devolución de activos	Parcial	Aplica por obligatoriedad del Contrato 459-2025 (Cl. Quinta), lineamientos MSPI MinTIC (Dec. 1078/2015; Dec. 338/2022; Res. 746/2022) y la Política General de Seguridad y Privacidad de la Información (versión 2025).	Formalizar procedimiento de devolución de activos con checklist y evidencias en mesa de ayuda.	Procedimiento aprobado; tickets de devolución con evidencia.
5.12	Clasificación de la información	Parcial	Aplica por obligatoriedad del Contrato 459-2025 (Cl. Quinta), lineamientos MSPI MinTIC (Dec. 1078/2015; Dec. 338/2022; Res. 746/2022) y la Política General de Seguridad	Definir política y esquema de clasificación (pública/interna/confidencial), capacitar y auditar.	Política de clasificación publicada; registros de aplicación en documentos.

ISO	Control	Estado	Brecha / Justificación	Acción propuesta	Evidencia esperada
			y Privacidad de la Información (versión 2025).		
5.13	Etiquetado de la información	Parcial	Aplica por obligatoriedad del Contrato 459-2025 (Cl. Quinta), lineamientos MSPi MinTIC (Dec. 1078/2015; Dec. 338/2022; Res. 746/2022) y la Política General de Seguridad y Privacidad de la Información (versión 2025).	Implementar etiquetado y metadatos; integrar con DLP y flujo documental.	Etiquetas aplicadas; reportes de DLP; auditoría de metadatos.
5.17	Información de autenticación	Parcial	Aplica por obligatoriedad del Contrato 459-2025 (Cl. Quinta), lineamientos MSPi MinTIC (Dec. 1078/2015; Dec.	Política de credenciales y secretos; MFA; rotación y custodia en vault.	Política de contraseñas; MFA operativa; registros de rotación en vault.

ISO	Control	Estado	Brecha / Justificación	Acción propuesta	Evidencia esperada
			338/2022; Res. 746/2022) y la Política General de Seguridad y Privacidad de la Información (versión 2025).		
5.23	Seguridad en servicios en la nube	Parcial	Aplica por obligatoriedad del Contrato 459-2025 (Cl. Quinta), lineamientos MSPI MinTIC (Dec. 1078/2015; Dec. 338/2022; Res. 746/2022) y la Política General de Seguridad y Privacidad de la Información (versión 2025). Cumplimiento Contractual 459-2025 – Cl. Quinta – Fase I, numerales	Baseline de seguridad cloud; cifrado en reposo y tránsito; logging y hardening CSP.	Checklist de baseline cloud; cifrado habilitado; logs centralizados.

ISO	Control	Estado	Brecha / Justificación	Acción propuesta	Evidencia esperada
			20–21: arquitectura segura/segmentación; uso de servicios en la nube con requisitos de seguridad.		
5.34	Privacidad y protección de PII	Parcial	Aplica por obligatoriedad del Contrato 459-2025 (Cl. Quinta), lineamientos MSPi MinTIC (Dec. 1078/2015; Dec. 338/2022; Res. 746/2022) y la Política General de Seguridad y Privacidad de la Información (versión 2025). Cumplimiento Contractual 459-2025 – Cl. Vigésima Octava	Actualizar políticas de PII; realizar PIAs; registros de tratamiento y evaluación de terceros.	PIAs elaboradas; registro de actividades de tratamiento; contratos con cláusulas de PII.

ISO	Control	Estado	Brecha / Justificación	Acción propuesta	Evidencia esperada
			(Confidencialidad); Cl. Cuarta, numerales 7 y 17: uso adecuado y reserva de información.		
8.6	Gestión de la capacidad	Parcial	Aplica por obligatoriedad del Contrato 459-2025 (Cl. Quinta), lineamientos MSPi MinTIC (Dec. 1078/2015; Dec. 338/2022; Res. 746/2022) y la Política General de Seguridad y Privacidad de la Información (versión 2025).	Establecer plan de capacidad con monitoreo y umbrales; reportes mensuales.	Tableros de capacidad; umbrales y acciones documentadas.
8.7	Protección contra malware	Parcial	Aplica por obligatoriedad del Contrato 459-2025 (Cl.	Endurecimiento, EDR/antimalware unificado; campañas de concienciación.	Cobertura EDR; reporte de firmas/empresas;

ISO	Control	Estado	Brecha / Justificación	Acción propuesta	Evidencia esperada
			Quinta), lineamientos MSPI MinTIC (Dec. 1078/2015; Dec. 338/2022; Res. 746/2022) y la Política General de Seguridad y Privacidad de la Información (versión 2025). Cumplimiento Contractual 459-2025 – Cl. Quinta – Fase II, numeral 1: protección antimalware/EDR.		campañas de concienciación.
8.8	Gestión de vulnerabilidades técnicas	Parcial	Aplica por obligatoriedad del Contrato 459-2025 (Cl. Quinta), lineamientos MSPI MinTIC (Dec. 1078/2015; Dec. 338/2022; Res. 746/2022) y la	Proceso de gestión de vulnerabilidades; escaneo programado y SLAs de remediación.	Informe de escaneo; tickets de remediación; cumplimiento de SLAs.

ISO	Control	Estado	Brecha / Justificación	Acción propuesta	Evidencia esperada
			Política General de Seguridad y Privacidad de la Información (versión 2025). Cumplimiento Contractual 459-2025 – Cl. Quinta – Fase I, numerales 12 y 19: evaluación técnica y validación de vulnerabilidades.		

Tabla 59: Tabla brechas ISO 27001:2022

Las fechas, responsables y cronograma detallado para la implementación de estas acciones se encuentran en el documento **Plan de Acción proceso gestión de TI 2026.xlsx**, que consolida todas las actividades del contrato.

12.9. Anexo 9: Revisión y validación de la implementación IPv6

Verificar la correcta implementación de IPv6 realizada en años anteriores, asegurando que las políticas y configuraciones continúan activas tras el cambio de firewall y que los servicios críticos mantienen compatibilidad.

Fase	Actividad	Estado	Responsable
Revisión documental	Validar actas, reportes y evidencias de la implementación inicial de IPv6	Pendiente	Infraestructura
Verificación técnica	Comprobar configuración IPv6 en routers, firewalls y equipos críticos	Pendiente	Infraestructura
Validación de políticas	Revisar que las políticas de IPv6 y reglas de seguridad continúan activas tras el cambio de firewall	Pendiente	Seguridad Información
Pruebas funcionales	Ejecutar pruebas de conectividad y servicios críticos bajo IPv6	Pendiente	Infraestructura
Informe final	Generar reporte de validación con hallazgos y recomendaciones	Pendiente	CIO / Infraestructura

Tabla 60: Verificación de implementación de IPv6

Las fechas, responsables y cronograma detallado para la implementación de estas acciones se encuentran en el documento **Plan de Acción proceso gestión de TI 2026.xlsx**, que consolida todas las actividades del contrato.

12.10. Anexo 10: Plan de socialización

Actividad	Canal	Público objetivo	Responsable	Métrica
Presentación PETI en Comité	Sesión presencial/virtual	Alta Dirección	CIO	Acta aprobatoria
Kickoff por procesos	Intranet + reunión	Líderes misionales	CIO + Planeación	% participaciones líderes
Cápsulas informativas	Intranet / correo	Todos colaboradores	Comunicaciones	Tasa apertura >60%
Publicación web	Sitio institucional	Ciudadanía	Comunicaciones	URL publicada
Seguimiento de indicadores	Tablero BI	Alta Dirección	CIO	Reporte mensual

Tabla 61: Plan de socialización

Las fechas, responsables y cronograma detallado para la implementación de estas acciones se encuentran en el documento **Plan de Acción proceso gestión de TI 2026.xlsx**, que consolida todas las actividades del contrato.

12.11. Anexo 11: DOFA

Este anexo complementa la **fase Analizar (AS-IS)** del PETI, aportando el análisis **DOFA (Fortalezas, Oportunidades, Debilidades y Amenazas)** por dominios estratégicos de TI. Su propósito es:

- **Evidenciar el diagnóstico estratégico** realizado sobre la función de TI, identificando factores internos y externos que impactan la ejecución del PETI.
- **Justificar las acciones priorizadas** incluidas en la hoja de ruta y en los objetivos estratégicos de TI (OE-TI), orientadas a cerrar brechas y aprovechar oportunidades.
- **Asegurar trazabilidad** con los hallazgos del Capítulo 6 (Estrategia, Gobierno, Información, Sistemas, Infraestructura, Seguridad y Uso/Apropiación), vinculando cada elemento DOFA con iniciativas del PETI.
- **Proveer defendibilidad ante auditoría**, mostrando cómo las acciones estratégicas del PETI responden a debilidades y amenazas identificadas en el diagnóstico.

Este anexo se articula con los contenidos del **Capítulo 6: Análisis de la situación actual y oportunidades de mejora**, especialmente en los apartados de **Interpretación estratégica del diagnóstico** y **Estrategia y Gobierno de TI**, y constituye insumo clave para la definición de los **macroproyectos 2026–2029** y la priorización de iniciativas.

12.11.1. Estrategia de TI

Fortalezas	Debilidades
Misión y Visión TI 2029 claras y alineadas a pilares institucionales.	Metas SMART por objetivo aún no detalladas.
Hoja de ruta con macroproyectos 2026-2029.	Diagnóstico por dominios sin DOFA formal.
Portafolio con foco en crecimiento financiero y transformación digital.	Dependencia de TI percibida más operativa que estratégica.

Oportunidades	Amenazas
Incorporar tendencias tecnológicas (IA, RPA, IoT, API Mgmt).	Posible observación de órganos de control si no se aprueba/publica PETI.
Vincular entregables del Contrato SGSI a la hoja de ruta PETI.	Riesgo de sobrecarga de proyectos si no se priorizan con brechas, costos y tiempos.
Alinear iniciativas con obligaciones externas (Gobierno Digital, PNID).	

12.11.1.1. Acciones priorizadas

- Definir metas SMART por OE-TI y tablero BI.
- Completar DOFA por dominio y catálogo de brechas.
- Adjuntar acta de Comité o Mesa de trabajo y URL de publicación como evidencia.

12.11.2. Gobierno de TI

Fortalezas	Debilidades
Políticas vigentes y procedimientos documentados.	No existen comités propios de TI. Carencia crítica de capacidades estratégicas.
Oportunidades	Amenazas
Formalizar Mesa de trabajo Operativo/Táctico TI y Gobierno de Datos.	Cambios sin control formal. Incumplimientos normativos si no se actualiza SGSI.

12.11.2.1. Acciones priorizadas

- Crear instancias de gobierno y publicar matriz RACI.
- Actualizar procedimientos y evidencias.

12.11.3. Información

Fortalezas

ownCloud con alta disponibilidad de información.

- Integración prevista vía APIs y CDE.

Debilidades

Conversión pendiente SOAP→REST.

Falta de Modelo de Gobierno de Datos.

Oportunidades

Ecosistema de Datos y Analítica Predictiva.

Adopción de API Management y MDM.

Amenazas

Riesgo de pérdida de información por backups deficientes.

Exposición de datos sin cifrado robusto.

12.11.3.1. Acciones priorizadas

- Plan de Gobierno de Datos.
- Roadmap SOAP→REST y especificación de APIs.
- Endurecer políticas de backup y restauración.

12.11.4. Sistemas de Información

Fortalezas	Debilidades
Decisión de implementar SIM (NocoBase).	Procesos misionales que requieren mejoras y optimizaciones.
Catálogo de SI y servicios caracterizados.	Intranet/Web sin SSL y desactualizada.
Oportunidades	Amenazas
Plataforma de autogestión omnicanal y Gestión de Cliente.	Operación misional manual/ofimática.
API-CDE como conector central.	Integraciones frágiles y dependencia de sistemas obsoletos.

12.11.4.1. Acciones priorizadas

- Desarrollar SIM-NocoBase por flujos misionales.
- Modernizar Intranet/Web.
- Implementar API-Management + CDE.

12.11.5. Infraestructura de TI

Fortalezas	Debilidades
Estrategia de continuidad apalancada en nube.	Obsolescencia marcada en servidores locales.
Catálogo y operación de servicios TI.	Carencia de monitoreo/capacidad formal.
Oportunidades	Amenazas
Migración a nube híbrida avanzada.	Indisponibilidad por cortes eléctricos/datos.
Sustitución de infraestructura obsoleta.	Persistencia del riesgo si no se ejecuta modernización.

12.11.5.1. Acciones priorizadas

- Programa de refresh y cloud landing zone.
- Monitoreo y planes de mantenimiento.
- Checklist IPv6 y endurecimiento de perímetro.

12.11.6. Uso y Apropiación

Fortalezas	Debilidades
Indicadores de soporte N1/N2 con desempeño positivo.	Ausencia de metas de adopción.
Plan de socialización y cápsulas informativas.	Equipo TI con capacidad estratégica limitada.
Oportunidades	Amenazas
Omnicanalidad y autogestión.	Baja adopción del SIM/API-CDE si no hay gestión del cambio.
Programas de formación en seguridad y datos.	Observaciones por falta de publicación y evidencias.

12.11.6.1. Acciones priorizadas

- Definir KPIs de adopción.
- Ejecutar campañas y kick-off por procesos.
- Integrar formación SGSI al plan de comunicaciones.

12.11.7. Seguridad

Fortalezas	Debilidades
Políticas y planes de seguridad vigentes.	Evaluación de controles en formato 2013.
Presupuesto robusto para Seguridad y Privacidad.	Falta de plan de pruebas de seguridad y KPIs .
Oportunidades	Amenazas
Contrato SGSI: entrega SOA 27001:2022 y Plan de Tratamiento .	Pérdida de información, vulnerabilidad e indisponibilidad.
Implementación de NAC/SSO y seguridad cloud .	Observaciones por no migrar evaluación a 27001:2022.

12.11.7.1. Acciones priorizadas

- Migrar evaluación a **ISO/IEC 27001:2022** y generar **SOA**.
- Plan de pruebas y criterios de aceptación.
- Cifrado robusto y **hardening**.

El PETI integra la operación continua del **SGSI** y la migración plena a **ISO/IEC 27001:2022**, articulando controles prioritarios con los **macroproyectos** vigentes y el presupuesto. Las brechas críticas (criptografía, continuidad, gestión de incidentes, relaciones con proveedores) se atienden mediante hitos anuales, evidencias verificables y KPIs de eficacia. (Ver **Macroproyecto 3** Seguridad y Privacidad; **Infraestructura/Nube**; y **Gobierno de TI**).

Hitos SGSI integrados en la Hoja de Ruta (2026–2027):

- **Hito 3.1:** SOA 2022 publicado y aprobado en Mesa de trabajo (Q2-2026).
- **Hito 3.2:** Plan de Tratamiento de Riesgos con costos/plazos y criterios de aceptación (Q3-2026).
- **Hito 3.3:** Política de cifrado en tránsito y reposo operativa (TLS en intranet, bases de datos y backup) (Q4-2026).
- **Hito 3.4:** Pruebas de continuidad (DRP): Ejecución de **pruebas DRP** (restauración ERP, correo, SGDEA y simulación de ransomware) sobre servicios en nube y locales, con criterios de aceptación y evidencias técnicas.

Nota: La planificación detallada (fechas y responsables) se consolida en “Plan de Acción proceso gestión de TI 2026.xlsx”

- **Hito 3.5:** Proceso de gestión de incidentes con métricas MTTD/MTTR y reporte mensual a Alta Dirección (Q2-2027).

Conexión con presupuesto: Los rubros 2026 para **Seguridad y Privacidad, Sistemas e Infraestructura** soportan estos hitos (ver Tabla 22).

12.12. Anexo 12: plan de implementación del PETI

Este anexo complementa la **fase Construir (TO-BE y hoja de ruta)** del PETI, detallando la **implementación operativa** de las iniciativas estratégicas mediante **cronograma, responsables (RACI), KPIs, evidencias esperadas y mecanismos de seguimiento**. Su propósito es:

- **Operativizar la hoja de ruta 2026–2029** y los objetivos estratégicos de TI, definiendo **fases, actividades, entregables y responsables** conforme a la metodología PETI (MGGTI.GE.ES.01 v3) y a la estructura de gobierno adoptada en el documento base.
- **Asegurar trazabilidad y defendibilidad** con un conjunto de **KPIs** (ISO/IEC 27001:2022, continuidad y seguridad) y **evidencias verificables** por actividad, alineados al tablero de control del PETI y al Mesa de trabajo de Seguridad de la Información.
- **Integrar el cronograma detallado 2026** (actividades, fechas, responsables y entregables), incrustado en el anexo como **resumen ejecutivo** y referenciado al archivo maestro de planificación, en coherencia con la sección de **fases del plan** y su marco temporal (Inicio, Ejecución, Seguimiento).
- **Vincular responsabilidades** a la **Matriz RACI** y a las instancias de gobernanza de TI (CIO, Planeación, Infraestructura, Seguridad de la Información, Jurídica, Financiera, Contratación), garantizando coordinación interáreas y cumplimiento normativo

12.12.1. Introducción

En cumplimiento del lineamiento **EO 02 Tecnología** y de los objetivos estratégicos de **seguridad y resiliencia**, se definen los siguientes **indicadores clave (KPIs)** para monitorear la implementación del **SGSI bajo ISO/IEC 27001:2022**, la **ejecución de pruebas DRP** y el fortalecimiento del **cifrado y la infraestructura tecnológica**. Estos KPIs se integrarán al **tablero de control del PETI** y serán objeto de **seguimiento periódico** por las instancias de **gobierno de TI** y el **Mesa de trabajo de Seguridad de la Información**. Se adopta el mismo **formato de hojas de vida de indicadores** utilizado en el PETI (nombre, definición, fórmula, línea base, metas, fuente, responsable y periodicidad) para asegurar consistencia y trazabilidad con las secciones de indicadores (6.5) y Anexo 5 de este documento.

Indicador	Definición	Fórmula	Línea base 2025	Meta 2026	Meta 2029	Fuente	Responsable	Periodicidad
% controles ISO/IEC 27001:2022 implementados	Porcentaje de controles del SGSI implementados conforme a la SOA 2022 (catálogo de 93 controles de referencia)	$\left(\frac{\text{Controles "Implementados"} / 93}{100} \right) \times 100$	N/A *	≥40 %	≥90 %	SOA 2022 aprobada en Mesa de trabajo	Seguridad de la información	Trimestral
% pruebas de restauración (DRP) exitosas	Porcentaje de pruebas de DRP ejecutadas con éxito sobre	$\left(\frac{\text{Restauraciones exitosas} / \text{Total pruebas}}{100} \right) \times 100$	N/A *	≥80 %	≥95 %	Informes técnicos y evidencias DRP	Infraestructura	Semestral

	servicios críticos (ERP/JSP7, correo, SGDEA/TAM PUS, simulación ransomware)							
% cifrado en tránsito y reposo	Porcentaje de sistemas con TLS habilitado en tránsito y cifrado de bases de datos/backups en reposo	(Sistemas con TLS + DB/backup cifrado / Total sistemas) × 100	N/A *	≥60 %	≥95 %	Evidencia técnica (configuraciones y reportes)	Seguridad de la información	Trimestral
MTTD / MTTR incidentes	Tiempo promedio de detección (MTTD) y	Horas promedio de detección / respuesta	N/A *	MTTD ≤4h / MTT	MTTD ≤2h / MTT	GLPI / reportes a Mesa de Trabajo SGSI	Coordinación TIC	Mensual

	respuesta (MTTR) de incidentes de seguridad registrados			R ≤16 h	R ≤8h			
--	--	--	--	---------------	----------	--	--	--

Tabla 62 - KPIs- EO 02

12.12.2. Objetivo

Definir las fases, actividades, responsables y evidencias para la ejecución del PETI 2026–2029, asegurando trazabilidad, cumplimiento normativo y defendibilidad ante auditoría externa.

12.12.3. Fases del plan

El plan de implementación del PETI se estructura en tres fases principales que garantizan la trazabilidad, el cumplimiento normativo y la defendibilidad ante auditoría externa:

Fase	Descripción	Entregables claves
Inicio	Conformación del equipo, aprobación del PETI, asignación de recursos	Acta de Comité, Matriz RACI, cronograma
Ejecución	Implementación de macroproyectos, gestión de riesgos, seguimiento de KPIs	Reportes mensuales, tableros BI, evidencias
Seguimiento	Auditoría interna, control de cambios, cierre de brechas ISO 27001:2022	Informes de auditoría, actas de mesa de trabajo

Ilustración 17 - Fase de implementación del PETI

Actividad	Inicio	Fin
Aprobación PETI y socialización	Feb 2026	Mar 2026
Implementación macroproyectos fundacionales	Abr 2026	Dic 2027
Implementación proyectos generadores de valor	Ene 2028	Dic 2029
Auditorías y cierre de brechas SGSI	Jun 2026	Dic 2027

Tabla 63 - Resumen de cronograma



Ilustración 18 - Cronograma Grantt (Resumen)

Los hitos de continuidad (**Pruebas DRP**) y el **detalle operativo del cronograma (fechas y responsables)** se encuentran consolidados en “**Plan de Acción proceso gestión de TI 2026.xlsx**”. Este PETI conserva el nivel estratégico y las evidencias requeridas.

12.12.4. Responsables (según Matriz RACI)

La ejecución del PETI 2026–2029 requiere una asignación clara de responsabilidades para garantizar la trazabilidad, la coordinación interáreas y el cumplimiento normativo. Los roles se definen conforme a la **Matriz RACI** y a las instancias establecidas en el Modelo de Gobernanza de TI, asegurando que cada actividad cuente con un responsable directo, un apoyo estratégico y mecanismos de control.

- **CIO:** Aprobación y liderazgo estratégico.
- **Planeación:** Alineación con PEI y cronograma.

- **Infraestructura:** Migración a nube híbrida, IPv6.
- **Seguridad Información:** Implementación SGSI, controles ISO.
- **Jurídica:** Cumplimiento normativo y contractual.
- **Financiera:** Gestión presupuestal.
- **Contratación:** Procesos precontractuales y contractuales.

12.12.5. Evidencias esperadas

La implementación del **PETI** debe generar evidencias verificables que permitan demostrar el cumplimiento de los objetivos estratégicos, la trazabilidad de las actividades y la conformidad con los estándares normativos (ISO / IEC 27001:2022, MinTIC, MAE v3). Estas evidencias son esenciales para auditorías internas, externas y para los órganos de control.

Las evidencias se clasifican en cuatro categorías:

1. Aprobación y socialización

- Acta del Comité Institucional de Gestión y Desempeño que aprueba el PETI.
- Publicación del documento en intranet y sitio web institucional.
- Registro fotográfico y minutas de las sesiones de socialización.

2. Ejecución de macroproyectos

- Reportes mensuales de avance por proyecto.
- Tableros BI con indicadores de ejecución (% proyectos PETI ejecutados).
- Evidencias de integración tecnológica (API Management, CDE).

3. Cumplimiento normativo y SGSI

- Declaración de Aplicabilidad (SOA) ISO/IEC 27001:2022.
- Plan de Tratamiento de Riesgos con costos, plazos y responsables.
- Evidencias técnicas: cifrado en tránsito y reposo, pruebas de restauración, registros de gestión de incidentes.

4. Seguimiento y auditoría

- Informes de auditoría interna y actas de cierre.
- KPIs estratégicos validados (seguridad, continuidad, adopción tecnológica).
- Documentación de control de cambios y trazabilidad contractual.

Actividad	Evidencia
Aprobación PETI	Acta de Comité Institucional
Socialización	Publicación en intranet y web
Implementación macroproyectos	Reportes mensuales, tableros BI
Cumplimiento SGSI	SOA ISO 27001:2022, Plan de Tratamiento, KPIs
Auditorías internas	Informes y actas de cierre

Tabla 64 – Resumen de evidencias esperadas

12.13. Anexo 13: Acta de no implementación del BCP

Entidad: Empresa de Renovación y Desarrollo Urbano de Bogotá, D.C.

Comité: Comité Institucional de Gestión y Desempeño

Acta No.: _____

Fecha: ____ / ____ / ____

Orden del día

- Presentación del PETI 2026–2029
- Discusión sobre continuidad y BCP
- Decisión sobre implementación de BCP

Decisión

Por acuerdo institucional, se decide **no implementar un Plan de Continuidad del Negocio (BCP)** formal durante la vigencia del PETI 2026–2029.

En su lugar, se gestionará la continuidad mediante **pruebas técnicas de recuperación (DRP)** programadas, conforme a los hitos del SGSI y al documento **“Plan de Acción proceso gestión de TI 2026.xlsx”**.

La aprobación del PETI 2026–2029 implica la aprobación automática de este anexo, conforme a lo acordado en el Comité Institucional de Gestión y Desempeño.

Compromisos

- Documentar la decisión en el PETI y anexos
- Ejecutar pruebas DRP (restauración ERP, correo, SGDEA, simulación de ransomware) con criterios de aceptación y evidencias
- Mantener trazabilidad en el cronograma consolidado (Excel)

Publicación

URL sitio web institucional / intranet: _____

Fecha de publicación: ____ / ____ / ____

Medio de difusión: ____ Intranet ____ Web ____ Circular interna

Firmas

Presidente del Comité: _____

Secretario técnico: _____

Director Administrativo y TIC (CIO): _____

12.14. Anexo 14: Autodiagnósticos Gobierno Digital y Seguridad

Digital

Este anexo complementa la **fase Analizar (AS-IS)** del PETI, aportando los resultados de los **autodiagnósticos 2025** realizados sobre las políticas de **Gobierno Digital** y **Seguridad Digital**, conforme a los lineamientos del **MinTIC** y los instrumentos de evaluación del **Modelo Integrado de Planeación y Gestión (MIPG)**. Su propósito es:

- **Evidenciar el nivel de madurez institucional** frente a los componentes de Gobierno Digital (arquitectura empresarial, interoperabilidad, datos abiertos, accesibilidad) y Seguridad Digital (MSPI, gestión de riesgos, protección de datos personales).
- **Justificar las acciones estratégicas** incluidas en el PETI para cerrar brechas detectadas en los autodiagnósticos y cumplir con los requisitos normativos (Decreto 767 de 2022, Decreto 338 de 2022, Resolución 746 de 2022).

- **Asegurar trazabilidad** con los planes de mejoramiento vigentes y con las metas del **FURAG**, integrando los hallazgos a la hoja de ruta tecnológica y a los macroproyectos priorizados.
- **Proveer defendibilidad ante auditoría y entes de control**, demostrando que el PETI responde a las brechas identificadas en los diagnósticos oficiales y que articula las acciones correctivas con evidencias verificables.

Este anexo se articula con los contenidos del **Capítulo 6: Análisis de la situación actual y oportunidades de mejora**, especialmente en los apartados de **Estrategia y Gobierno de TI** y **Interpretación estratégica del diagnóstico**, y constituye insumo clave para la definición de los **macroproyectos 2026–2029**, la priorización de iniciativas y el cumplimiento de los lineamientos distritales y nacionales en materia de transformación digital y seguridad de la información.

12.14.1. Introducción

Este anexo presenta los **resultados 2025** de los autodiagnósticos de **Gobierno Digital** y **Seguridad Digital** aplicados a la Empresa, conforme a la **Guía PETI v3 MGGTI.GE.ES.01** y a la **Política de Gobierno Digital (Decreto 767 de 2022)**, que definen responsabilidades, componentes y estándares de referencia para la planeación de TI en entidades públicas. Adicionalmente, se integra la gobernanza de **Seguridad Digital** establecida por el **Decreto 338 de 2022**, como marco de roles y articulación institucional para el aseguramiento de la información y la continuidad de servicios.

12.14.2. Objetivos

- **Determinar el nivel de madurez** de la Empresa en los componentes de **Gobierno Digital** (arquitectura, interoperabilidad, datos, accesibilidad, servicios digitales) y **Seguridad Digital** (MSPI, riesgos, protección de datos, continuidad).

- **Identificar brechas y acciones correctivas** que se integran a la **hoja de ruta del PETI** y a los **macroproyectos** priorizados (Sistemas Misionales, Integración/API-CDE, Seguridad/SGSI, Infraestructura/Nube), asegurando trazabilidad con controles ISO/IEC 27001:2022 y con la estrategia distrital (PTEP, accesibilidad).

12.14.3. Alcance

Este autodiagnóstico cubre:

- **Gobierno Digital:** dominios y lineamientos de la política nacional (planeación/arquitectura, interoperabilidad, seguridad y privacidad, servicios ciudadanos digitales, accesibilidad y datos abiertos).
- **Seguridad Digital:** gobernanza, gestión de riesgos, protección de datos personales, continuidad y respuesta (MSPI/SGSI), conforme al modelo nacional y las responsabilidades del Decreto 338/2022.

12.14.4. Metodología

- **Instrumentos de referencia:** Guía **MGGTI.GE.ES.01 v3** (MinTIC) y marcos de la **Política de Gobierno Digital** (Decreto 767/2022); se valoran capacidades y evidencias por dominio y se asignan niveles de madurez (Inicial/Parcial/Definido/Gestionado/Optimizado).
- **Seguridad Digital (Gobernanza):** se verifican roles, comités, mesas de trabajo y responsabilidades según **Decreto 338/2022** (instancias de gobierno, coordinación interáreas).
- **Fuentes internas:** Capítulo 6 del PETI (alineación TI–procesos, hallazgos misionales, infraestructura, seguridad, riesgos), anexos de brechas ISO (Anexo 8: Tabla brechas ISO 27001:2022) y DOFA (Anexo 11: DOFA) como evidencias complementarias del diagnóstico AS-IS.

12.14.5. Resultados de Gobierno Digital (2025)

12.14.5.1. Arquitectura y planeación de TI

- **Madurez:** Parcial → Existe metodología PETI y visión TO-BE, pero se identifica **déficit de capacidades estratégicas** en arquitectura empresarial y definición de políticas (impacto en alineación integral y ejecución).
- **Brecha clave:** Instancias de gobierno de TI no formalizadas (mesas de trabajo propios, gobierno de datos).
- **Acción PETI:** Fortalecimiento de Gobierno de TI (comités, Mesas de trabajo, RACI, proceso de control de cambios formal en SIG; Anexo 6/16).

12.14.5.2. Interoperabilidad y datos (API-CDE)

- **Madurez:** Inicial/Parcial → No existe plataforma central de **API Management**; **TAMPUS** opera con **SOAP** y requiere conversión a **REST**; falta **CDE** para trazabilidad de archivos y modelos (brecha de integración end-to-end).
- **Acción PETI:** Macroproyecto de **Integración/API-CDE** (Cap. 8–9); mapa de integraciones (Anexo 4: Mapa de integraciones).

12.14.5.3. Servicios digitales y accesibilidad

- **Madurez:** Parcial → La **intranet** presenta **SO desactualizado** y **sin TLS/SSL**; la **web** carece de **APIs** y debe alinearse a estándares de **accesibilidad** (WCAG 2.1 AA) y transparencia distrital (PTEP).
- **Acción PETI:** Omnicanalidad/Portal único, actualización de intranet/web (certificados, hardening, accesibilidad).

12.14.5.4. Datos abiertos y gobierno del dato

- **Madurez:** Parcial → Avances en repositorio **ownCloud**, pero sin **modelo de gobierno de datos** institucional ni MDM; alto potencial para analítica e infraestructura de datos (PNID).
- **Acción PETI:** Ecosistema de datos y **BI/analítica predictiva**, con política de datos y catálogo institucional.

12.14.6. Resultados de seguridad digital (2025)

12.14.6.1. Gobernanza de seguridad digital y MSPI

- **Madurez:** Parcial → El manual vigente define las pautas, directrices y reglas para garantizar la seguridad y protección de la información en todos los procesos institucionales, alineado con los controles ISO/IEC 27001:2022 y los lineamientos del MSPI. Aunque las políticas están vigentes y el SGSI en operación, las evaluaciones de efectividad aún transitan del formato 2013 al 2022; falta plan de pruebas formal y KPIs de seguridad (MTTD/MTTR).
- **Acción PETI:** Migración completa a **ISO/IEC 27001:2022** (SOA y plan de tratamiento), KPIs EO-02 y mesas de trabajo de seguridad.

12.14.6.2. Gestión de riesgos y continuidad (DRP)

- **Madurez:** Parcial → Se define operar continuidad vía **DRP** (restauraciones ERP, correo, SGDEA, simulación ransomware) con criterios de aceptación; **BCP** no implementado por decisión institucional (Anexo 13: Acta de no implementación del BCP).
- **Acción PETI:** Pruebas **DRP** periódicas con evidencias; evaluación de viabilidad de **BCP** a 2027.

12.14.6.3. Protección de datos personales y controles técnicos

- **Madurez:** Parcial → Brechas en **clasificación/etiquetado** de información, **información de autenticación (MFA/vault)** y **seguridad en nube** (línea base, cifrado en reposo y tránsito) identificadas en **SOA 2022** (Anexo 8: Tabla brechas ISO 27001:2022).
- **Acción PETI:** Política de cifrado integral, **EDR**, gestión de vulnerabilidades y línea base cloud, con evidencias verificables.

12.14.6.4. Matriz de brechas y plan de acciones

Propósito: Consolidar las **brechas del SGSI** identificadas frente a **ISO/IEC 27001:2022** y definir el **plan de acciones** para su cierre con **cronograma, responsables (RACI), KPIs y evidencias**, articulado con la **hoja de ruta del PETI** y el Anexo 12 (Anexo 12: plan de implementación del PETI). Esta matriz se deriva de la **Declaración de Aplicabilidad (SOA 2022)** y de los lineamientos **MSPI MinTIC** y decisiones contractuales del período 2025–2027.

Componente	Brecha 2025 (AS-IS)	Acción PETI 2026–2027	Evidencia esperada
Arquitectura y gobierno TI	Falta comités propios y capacidad de arquitectura	Mesa de trabajo Operativo/Táctico TI, Gobierno de Datos; Matriz RACI	Actas de mesas de trabajo; RACI publicada; control de cambios formal (SIG)
Interoperabilidad/API	Integraciones puntuales; SOAP sin REST; sin API Mgmt	Implementación API Management, conversión SOAP→REST, CDE	Endpoints, políticas API; bitácora de

Componente	Brecha 2025 (AS-IS)	Acción PETI 2026–2027	Evidencia esperada
			integraciones; auditoría CDE
Servicios/Accesibilidad	Intranet sin TLS, SO desactualizado; web sin APIs	Hardening, TLS/SSL, WCAG 2.1 AA; portal único/omnicanalidad	Escaneo de seguridad; certificado vigente; informe accesibilidad
Datos/Gobierno del dato	Sin modelo de gobierno; repositorio sin MDM	Política de datos; catálogo; Ecosistema de datos + BI/Analytics	Política publicada; diccionario de datos; tableros BI
Seguridad/SGSI	Evaluación 2013; faltan KPIs; brechas SOA 2022	SOA 2022 aprobada; plan de tratamiento; KPIs EO-02	SOA y plan aprobado; reportes MTDD/MTTR; cifrado aplicado
Continuidad (DRP)	DRP parcial; BCP no implementado	Pruebas DRP semestrales; criterios de aceptación	Informes técnicos; evidencias de restauración; mejoras

Tabla 65 - Brechas - planes de acción

12.14.6.5. Indicadores (KPIs) y metas

- **% cierres de brechas Gobierno Digital** = (Brechas cerradas / brechas priorizadas) × 100

Meta: ≥60% (2026), ≥90% (2029) – Fuente: tableros BI y actas de mesa de trabajo.

- **% integraciones gestionadas por API Mgmt** = (Integraciones vía API Mgmt / total integraciones) × 100

Meta: ≥40% (2026), ≥85% (2029).

- **% sistemas con TLS y cifrado en reposo** = $(\text{Sistemas con TLS} + \text{DB/backup cifrado} / \text{total sistemas}) \times 100$

Meta: ≥60% (2026), ≥95% (2029) – coherente con KPIs EO-02 del PETI (Seguridad/Continuidad).

- **MTTD/MTTR incidentes**

Meta: MTTD ≤4h / MTTR ≤16h (2026); MTTD ≤2h / MTTR ≤8h (2029).

12.14.6.6. Trazabilidad normativa

- **Guía PETI v3 MGGTI.GE.ES.01:** define fases y evidencias por fase, articulando diagnóstico con construcción y socialización (Planear–Analizar–Construir–Socializar).
- **Decreto 767 de 2022** (Política de Gobierno Digital): establece lineamientos y responsabilidades para la adopción de TIC en entidades públicas, incluyendo arquitectura, interoperabilidad y seguridad.
- **Decreto 338 de 2022** (Gobernanza de Seguridad Digital): define instancias y roles para la gestión de seguridad en el Distrito, fortaleciendo gobernanza y coordinación de SGSI/MSPI.
- **Lineamientos distritales de integridad y transparencia (PTEP):** refuerzan accesibilidad y apertura de información como componentes exigibles en planeación estratégica y PETI, a articular con portal e intranet de la entidad.

12.14.6.7. Relación con el PETI (capítulos y anexos)

- **Cap. 6:** Alineación TI–procesos, hallazgos clave, seguridad, riesgos (AS-IS) – base del presente anexo.
- **Cap. 8–9:** Arquitectura objetivo y hoja de ruta – acciones correctivas y proyectos vinculados.
- **Anexo 8:** Brechas ISO/IEC 27001:2022 – insumo de seguridad para plan de tratamiento.
- **Anexo 11:** DOFA – insumo estratégico (fortalezas/debilidades/amenazas/oportunidades).

- **Anexo 12:** Plan de implementación – cronograma, RACI, KPIs y evidencias.
- **Anexo 10:** Socialización – publicaciones y difusión del PETI.

12.14.6.8. Conclusiones

El autodiagnóstico evidencia **brechas críticas** en arquitectura/gobierno, interoperabilidad/API-CDE, accesibilidad y seguridad/SGSI que justifican la **priorización** de macroproyectos y KPIs EO-02 ya definidos en el PETI, garantizando **trazabilidad** con la **Política de Gobierno Digital** y la **Gobernanza de Seguridad Digital**. Su ejecución reforzará la **defendibilidad** del PETI ante auditorías y entes de control, y habilitará la **transformación digital** orientada a valor público en 2026–2029.

12.15. Anexo 15: Brechas FURAG

12.15.1. Introducción

Este anexo consolida las brechas identificadas en los autodiagnósticos del Formulario Único de Reporte de Avance en Gestión (FURAG) relacionadas con Gobierno Digital y Seguridad Digital, y las vincula con el PETI 2026–2029. Se estructura para asegurar trazabilidad normativa, acciones de cierre, responsables (RACI), KPI medibles y evidencias verificables, coherentes con el SGSI (ISO/IEC 27001:2022), el MSPI y el MAE v3.

12.15.2. Alcance

Cubre dominios de Gobierno Digital (arquitectura y planeación de TI, interoperabilidad y datos – APICDE, servicios ciudadanos digitales, accesibilidad y datos abiertos) y Seguridad Digital (gobernanza MSPI, gestión

de riesgos, protección de datos personales, continuidad – DRP/BCP, controles técnicos). Las brechas se traducen en acciones priorizadas del PETI con metas 2026–2029.

12.15.3. Trazabilidad normativa

- Decreto 767 de 2022 – Política de Gobierno Digital: adopción de arquitectura empresarial, interoperabilidad y servicios digitales.
- Decreto 88 de 2022 – Digitalización y automatización de trámites en línea.
- Resolución 460 de 2022 – Plan Nacional de Infraestructura de Datos (PNID) y hoja de ruta.
- Decreto 338 de 2022 – Gobernanza de la seguridad digital (instancias y roles).
- Resolución 746 de 2022 – Lineamientos adicionales del MSPI.
- Resolución 448 de 2022 – MSPI (Modelo de Seguridad y Privacidad de la Información).
- ISO/IEC 27001:2022 e ISO/IEC 27002:2022 – SGSI y código de prácticas de seguridad.
- Guía MinTIC MGGTI.GE.ES.01 v3 – Metodología PETI (Planear, Analizar, Construir, Socializar).

12.15.4. Metodología de autodiagnóstico y valoración

Se emplea la escala de madurez FURAG (Inicial, Parcial, Definido, Gestionado, Optimizado) y se formula el riesgo por brecha en términos de Impacto (I) y Probabilidad (P) en escala 1–5; el Nivel de riesgo (NR) = $I \times P$. Cada brecha se vincula a una acción del PETI, un responsable según la matriz RACI y una evidencia esperada.

12.15.5. Matriz de brechas y plan de acciones

Componente FURAG	Criterio (referencia)	Descripción del criterio	Madurez actual	Hallazgo ASIS	Impacto	Probabilidad	Nivel de riesgo	Acción PETI 2026–2027	Responsable (RACI)	Plazo	Evidencia esperada	KPI asociado
Arquitectura y planeación TI	GD-AP	Instancias de gobierno y definición de políticas de TI	Parcial	No existen comités o mesas de trabajo propios de TI ni gobierno de datos; déficit de capacidades estratégicas	4	3	12	Formalizar Mesa de trabajo Operativo/Táctico TI y de Gobierno de Datos; publicar matriz RACI y proced	CIO (A), Planeación (R), Seguridad (C), Jurídica (C), Misionales (C)	Q2 – Q3 2026	Actas de comité, RACI publicada, procedimientos de control de cambios en SIG	% mesas de trabajo o TI formalizados, % procedimientos actualizados

Componente FURAG	Criterio (referencia)	Descripción del criterio	Madurez actual	Hallazgo ASIS	Impacto	Probabilidad	Nivel de riesgo	Acción PETI 2026–2027	Responsable (RACI)	Plazo	Evidencia esperada	KPI asociado
								imiento de control de cambios				
Interoperabilidad y datos (APICDE)	GD-INT	Plataforma central de integración (API Mgmt) y CDE	Inicial /Parcial	Sistema documental operacon SOAP; no hay API Mgmt ni CDE; integraciones puntuales	4	4	16	Implementar API Management; convertir SOAP →REST ; desplegar	Sistemas (R), Infraestructura (R), Seguridad (C), CIO (A)	Q3 – Q4 2026	Endpoints REST operativos, políticas gestionadas por API Mgmt	% integraciones gestionadas por API Mgmt

Componente FURAG	Criterio (referencia)	Descripción del criterio	Madurez actual	Hallazgo ASIS	Impacto	Probabilidad	Nivel de riesgo	Acción PETI 2026–2027	Responsable (RACI)	Plazo	Evidencia esperada	KPI asociado
								CDE como repositorio y trazabilidad de archivos			bitácora de integridad	
Servicios digitales y accesibilidad	GD-SDA	Portal/intranet seguros y accesibles (TLS/SSL, WCAG 2.1 AA)	Parcial	Intranet sin TLS/SSL y SO desactualizado; web sin APIs e interoperabilidad	4	3	12	Hardening de servidores; habilitar TLS/SSL; modernizar	Infraestructura (R), Comunicaciones (R), Seguridad	Q2 – Q4 2026	Escaneos de seguridad, certificados vigentes, informes	% sistemas con TLS y cifrado; cumplimiento o WCAG

Componente FURAG	Criterio (referencia)	Descripción del criterio	Madurez actual	Hallazgo ASIS	Impacto	Probabilidad	Nivel de riesgo	Acción PETI 2026–2027	Responsable (RACI)	Plazo	Evidencia esperada	KPI asociado
								intrane t/web y cumpli r WCAG 2.1 AA; avanza r a portal único	(C), CIO (A)		me de accesi bilida d, public ación de portal único	
Gobernanza MSPI / SGSI	SD- GOB	SOA 27001:20 22 y plan de tratamien to de riesgos	Parcial	Evaluación de controles aún en formato 2013; faltan	4	3	12	Publicar SOA 2022; aprobar plan de tratami	Seguridad de la información (R), CIO	Q2 – Q3 202 6	SOA aprobada en mesa de trabaj	% contro les 27001 imple menta dos;

Componente FURAG	Criterio (referencia)	Descripción del criterio	Madurez actual	Hallazgo ASIS	Impacto	Probabilidad	Nivel de riesgo	Acción PETI 2026–2027	Responsable (RACI)	Plazo	Evidencia esperada	KPI asociado
				KPIs y plan de pruebas formal				ento con costos/plazos; definir KPIs (MTTD /MTTR , , cifrado , DRP)	(A), Infraestructura (C)		o, plan de tratamiento, tablero de KPIs	MTTD /MTTR
Gestión de riesgos TI	SD-RIES	Matriz de riesgos TI alineada a SGSI y PETI	Definido/En actualización	Matriz implementada con foco en pérdida de info, vulnerabil	3	3	9	Actualizar matriz con criterios 2022; vincula	Seguridad (R), Coordinación TIC (R),	Q2 – Q4 2026	Matriz revisada y aprobada, umbr	% riesgos críticos mitigados

Componente FURAG	Criterio (referencia)	Descripción del criterio	Madurez actual	Hallazgo ASIS	Impacto	Probabilidad	Nivel de riesgo	Acción PETI 2026–2027	Responsable (RACI)	Plazo	Evidencia esperada	KPI asociado
				idades e indisponibilidad; actualización en curso				r riesgos de integración (APIs/CDE) y cloud; definir umbrales y tratamiento	CIO (A)		ales y reportes mensuales	dos (>15)
Continuidad (DRP / BCP)	SD-DRP	Pruebas DRP periódicas y criterios de	Parcial	Continuidad vía DRP (restauración	4	3	12	Ejecución semestral de prueba	Infraestructura (R), Seguri	Se mensura (20	Informes técnicos, evidencias	% pruebas DRP exitosas

Componente FURAG	Criterio (referencia)	Descripción del criterio	Madurez actual	Hallazgo ASIS	Impacto	Probabilidad	Nivel de riesgo	Acción PETI 2026–2027	Responsable (RACI)	Plazo	Evidencia esperada	KPI asociado
		aceptación; decisión institucional sobre BCP		ERP/corrección/SGDEA, simulación ransomware); BCP no implementado por decisión institucional				s. DRP con evidencias; evaluar viabilidad de BCP a 2027	dad (C), CIO (A)	26–2029)	ncias de restauración y mejoras	
Protección de datos personales	SD-PIL	Clasificación/etiquetado, MFA y custodia de secretos	Parcial	Brechas en clasificación/etiquetado; MFA y	4	3	12	Política y esquema de clasificación;	Seguridad (R), Jurídica (C), Coordi	Q3 – Q4 2026	Políticas a publicadas, evidencias	% documentos clasificados y

Componente FURAG	Criterio (referencia)	Descripción del criterio	Madurez actual	Hallazgo ASIS	Impacto	Probabilidad	Nivel de riesgo	Acción PETI 2026–2027	Responsable (RACI)	Plazo	Evidencia esperada	KPI asociado
				administración de credenciales/secretos				etiquetado con metadatos; MFA y vault con rotación de secretos	nación TIC (R)		de etiquetado, registros de MFA y rotación en vault	etiquetados; % MFA habilitado
Gobierno del dato / PNID	GD-DAT O	Catálogo de datos, diccionario y ecosistema de	Parcial	Repositorio institucional con alta disponibilidad	3	3	9	Publicar política de datos y catálogo	Planeación (R), Sistemas (R), Seguridad	Q3 2026 – Q2 2027	Política y catálogo público, %	% catálogo de datos público; %

Componente FURAG	Criterio (referencia)	Descripción del criterio	Madurez actual	Hallazgo ASIS	Impacto	Probabilidad	Nivel de riesgo	Acción PETI 2026–2027	Responsable (RACI)	Plazo	Evidencia esperada	KPI asociado
		BI/analítica		idad, sin modelo formal de gobierno de datos/MDM				o; habilitar ecosistema de datos y BI/analítica con tableros estratégicos	dad (C), CIO (A)		tableros BI	tableros BI operativos
Gestión de proveedores TI	GD-PROV	Supervisión contractual y cumplimiento	Definido/Parcial	Supervisión de proveedores TI existente;	3	3	9	Actualizar minutas y SLAs	Contratación (R), Seguridad	Q2 – Q3 2026	Minutas actualizadas,	% proveedores con cláusulas

Componente FURAG	Criterio (referencia)	Descripción del criterio	Madurez actual	Hallazgo ASIS	Impacto	Probabilidad	Nivel de riesgo	Acción PETI 2026–2027	Responsable (RACI)	Plazo	Evidencia esperada	KPI asociado
		ento de requisitos de seguridad		fortalecer requisitos de seguridad en contratos y SLAs				con cláusulas de seguridad, privacidad y continuidad; seguimiento con métricas	(C), Jurídica (R)		evidencias de cumplimiento y reportes	las de seguridad y continuidad

Tabla 66 - Matriz de brechas y plan de acciones - FURAG

12.15.6. KPIs para el cierre de brechas FURAG

Indicador	Definición	Fórmula	Línea a bas e 202 5	Met a 202 6	Meta 2029	Fuente	Responsabl e	Periodicid ad
% cierres de brechas FURAG	% de brechas priorizadas cerradas	(Brechas cerradas / Brechas priorizadas) × 100	N/A *	≥60 %	≥90 %	Tablero BI / Actas de mesa de trabajo	CIO / Planeación	Trimestral
% integraciones vía API Mgmt	% de integraciones gestionadas por API Mgmt	(Integraciones API Mgmt / Integraciones totales) × 100	N/A *	≥40 %	≥85 %	Bitácora de integraciones / API Mgmt	Sistemas / Infraestructura	Mensual
% sistemas con TLS y cifrado	% de sistemas con TLS en tránsito y	(Sistemas con TLS + DB/backup cifrado / Total	N/A *	≥60 %	≥95 %	Evidencia técnica / Configuraciones	Seguridad de la información	Trimestral

Indicador	Definición	Fórmula	Línea a bas e 202 5	Met a 202 6	Meta 2029	Fuente	Responsabl e	Periodicid ad
	cifrado en reposo	sistemas) × 100						
MTTD / MTTR incidentes	Tiempo medio de detección y respuesta de incidentes	Horas promedio detección / respuesta	N/A *	MTT D ≤4h / MTT R ≤16 h	MTT D ≤2h / MTT R ≤8h	GLPI / Mesa de Trabajo SGSI	Coordinació n TIC	Mensual
% pruebas DRP exitosas	% de pruebas DRP ejecutadas con éxito	(Restauracio nes exitosas / Pruebas ejecutadas) × 100	N/A *	≥80 %	≥95 %	Informes técnicos DRP	Infraestruct ura	Semestral

Indicador	Definición	Fórmula	Línea base 2025	Meta 2026	Meta 2029	Fuente	Responsable	Periodicidad
% documentos clasificados y etiquetados	% de documentos con clasificación y etiquetado aplicado	(Docs clasificados y etiquetados / Docs totales) × 100	N/A *	≥70 %	≥95 %	Auditoría documental / DLP	Seguridad de la información	Trimestral
% catálogo de datos publicado	% de conjuntos de datos con definición en catálogo	(Conjuntos con ficha / Conjuntos totales) × 100	N/A *	≥60 %	≥95 %	Catálogo institucional / PNID	Planeación / Información	Trimestral
% proveedores con	% de contratos TI con	(Contratos con cláusulas /	N/A *	≥80 %	≥100 %	SECOP / Jurídica Contratación	Jurídica / Contratación	Semestral

Indicador	Definición	Fórmula	Línea a bas e 202 5	Met a 202 6	Meta 2029	Fuente	Responsabl e	Periodicid ad
cláusulas de seguridad y continuida d	requisitos de seguridad y continuida d	Contratos TI totales) × 100						

Tabla 67 - KPIs para el cierre de brechas FURAG

12.15.7. Evidencias verificables

- Actas de Mesa de Trabajo de Gobierno de TI y Seguridad de la Información
- Matriz RACI publicada y procedimiento de control de cambios formal en el SIG
- Políticas, minutas contractuales y documentos aprobados (seguridad, privacidad, datos)
- Evidencias técnicas de TLS/SSL, cifrado de bases de datos y backups, hardening de servidores
- Bitácora y políticas de API Management; auditoría del CDE
- SOA 27001:2022 aprobada y Plan de Tratamiento de Riesgos con costos y plazos
- Informes de pruebas DRP con criterios de aceptación y resultados
- Tableros BI con indicadores y reportes periódicos a la Alta Dirección

12.15.8. Relación con el PETI (capítulos y anexos)

- Cap. 6 – Diagnóstico ASIS: hallazgos en alineación TI–procesos, seguridad, riesgos e infraestructura
- Cap. 8–9 – Arquitectura objetivo y hoja de ruta: integraciones API/CDE, SIM–NocoBase, omnicanalidad
- Anexo 8 – Brechas ISO/IEC 27001:2022: insumo para SOA y plan de tratamiento
- Anexo 11 – DOFA: insumo estratégico para priorización de acciones
- Anexo 12 – Plan de implementación: cronograma, RACI, KPIs y evidencias
- Anexo 14 – Autodiagnósticos Gobierno Digital y Seguridad Digital: base para este anexo

12.16. Anexo 16: Matriz de trazabilidad de hallazgos y planes de mejoramiento

Id hallazgo/NC	Fuente	Descripción del hallazgo/NC	Plan de mejoramiento vigente (Actividades)	Acción estratégica PETI asociada	Control ISO/IEC 27001:2022 aplicable	Responsable (RACI)	Fecha compromiso	Evidencia requerida	Estado
NC 1	Auditoría Interna	Plan Estratégico de TI (PETI) no ajustado a característica requeridas (GDO-TIC-FM-025, MGGTI.GE.ES.03).	1. Actualizar PETI 2025 incorporando lineamiento s planear, analizar, construir. 2. Presentar para	EO02: Tecnología: Aumentar la eficiencia operativa. Proyect: Fortalecimiento de Gobierno y estructura organizacional de TI.	5.1 Liderazgo y compromiso: La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información. A.5.8 Seguridad de	Director Administrativo y de TIC / Gestor senior 1 Gestión TIC	31/12/2025	PETI 2025 formulado bajo metodología a MINTIC y aprobado por CIGD. Informes de seguimiento.	En Curso

		Corresponde más a un diagnóstico que a un plan estratégico. No alineado con objetivos estratégicos actuales. No cuenta con información para evaluar estado de desarrollo de programas 2022-2024.	aprobación del CIGD. 3. Ejecutar PETI 2025 asegurando cumplimiento de fases. 4. Realizar seguimiento a fases y proyectos TI. 5. Realizar seguimiento a ejecución de cada proyecto TI.		la información en la gestión de proyectos: La seguridad de la información debe integrarse en la gestión de proyectos.				
--	--	--	---	--	---	--	--	--	--

NC 2	Auditoría Interna	Plan de comunicación del PETI no disponible. No contar con estrategia de comunicaciones conlleva a desconocimiento sobre proyectos TI y su impacto.	1. Formular el plan de comunicaciones del PETI 2022-2025. 2. Ejecutar el plan de priorizando divulgación de hoja de ruta y avances. 3. Realizar seguimiento a la fase socializar.	Fase IV PETI: Plan de comunicaciones. Tarea 9.2: Socializar el PETI.	A.5.4 Responsabilidades de la gestión: La dirección debe exigir a todos los empleados que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos. (Comunicación y concientización son clave).	Director Administrativo y de TIC / Gestor senior 1 proceso Gestión TIC	31/12/2025	Plan de comunicaciones formulado. Informe de resultados de evaluación fase socializar.	En Curs o
------	-------------------	--	---	---	---	---	------------	--	-----------

NC 3	Auditoría Interna	<p>Ausencia de identificación de actividades de dinamización para optimizar procesos misionales (Estructuración, Gestión Predial, Ejecución).</p> <p>No se identifican actividades</p>	<p>1. Documentar matriz de necesidades TI para procesos misionales.</p> <p>2. Realizar mesa técnica para identificación y priorización.</p> <p>3. Elaborar plan de trabajo act.</p>	<p>EO0201: Fortalecer los sistemas de información estratégicos, misionales y transversales.</p>	<p>A.5.14 Transferencia de información: Deben existir reglas, procedimientos y acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia. (Relacionado con dinamización y flujo de información misional).</p>	<p>Director Administrativo y de TIC / Gestor senior 1 proceso Gestión TIC</p>	<p>14/02/2025</p>	<p>Matriz de necesidades TI documentada. Informe técnico de identificación y priorización. Plan de trabajo. Comunicación interna.</p>	<p>En Curs o</p>
------	-------------------	--	---	---	---	---	-------------------	---	------------------

		para logro de objetivos específicos del PETI.	dinamización. 4. Comunicar actividades prioritizadas 2025.						
NC 4	Auditoría Interna	Información incompleta relacionada con continuidad del negocio (migración nube, security, backup,	1. Realizar mesas técnicas plan continuidad 2025. 2. Formular plan de trabajo por fases BCP	EO0202: Implementar buenas prácticas ISO 27001 y Plan de recuperación de desastres (22301).	5.29 Seguridad de la información durante una interrupción: La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante una	Director Administrativo y de TIC / Gestor senior 1 proceso Gestión TIC	31/12/2025	Plan de continuidad (BCP) formulado y aprobado. Informes de seguimiento trimestrales.	En Curs o

		DRP). No disponibilida d del documento Plan de Recuperación ante Desastres (DRP).	2025. 3. Presentar a mesa de trabajo BCP 2025. 4. Ejecutar actividades plan BCP 2025. 5. Hacer seguimiento documenta ción actividades.		interrupción. 5.30 Preparación de las TIC para la continuidad del negocio: La organización debe asegurar la disponibilidad de la información y otros activos asociados durante una interrupción.				
NC 5	Audito ría	No se cuenta con información	1. Realizar mesas de trabajo	EO0203: Fortalecer la capacidad de la	A.5.25 Evaluación de eventos de seguridad de la	Director Administra tivo y de	31/12/20 25	Informe técnico identificació	En Curs o

		Intern a	para evaluar informe de cierre de brechas (PETI 2022). Incertidumbr e sobre actividades realizadas para cierre de brechas.	levantamien to necesidades TI. 2. Realizar mesa técnica priorización necesidades TI 2025. 3. Ejecutar actividades priorizadas 2025. 4. Elaborar informe cierre de	infraestructura tecnológica. Identificación de brechas: Sección 8.1.10 del PETI.	información: Los eventos de seguridad de la información se deben evaluar y decidir si se clasifican como incidentes de seguridad de la información. (Relacionado con monitoreo y cierre de brechas/vulnerabili dades).	TIC / Gestor senior 1 proceso Gestión TIC		n y priorización necesidades TI. Informe cierre de brechas.	
--	--	-------------	--	---	--	--	---	--	--	--

			brechas 2025.						
NC 6	Auditoría Interna	No se dispone de información para evaluar estado actual y resultados seguimiento a 4 indicadores de operación TI. Incertidumbre sobre estado de	1. Identificar acciones estratégicas PETI que orientan indicadores. 2. Realizar reuniones técnicas mesas de trabajo autoevaluación para evaluar	Sección 8.1.12: Indicadores y plan de seguimiento del PETI.	9.1 Seguimiento, medición, análisis y evaluación: La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión.	Director Administrativo y de TIC / Gestor senior 1 proceso Gestión TIC	31/12/2025	Informe de acciones estratégicas PETI. Actas de reuniones de mesa de trabajo.	En Curs o

		implementación.	avance indicadores.						
--	--	-----------------	---------------------	--	--	--	--	--	--

13. Referencias

13.1. Referencias generales

- Chiavenato, I. (2017). *Introducción a la teoría general de la administración* (8.ª ed.). McGraw-Hill.
- David, F. R., & David, F. R. (2017). *Administración estratégica: Conceptos y casos* (15.ª ed.). Pearson Education.
- Elkington, J. (1997). *Cannibals with Forks: The Triple Bottom Line of 21st Century Business*. Oxford: Capstone.
- Harvard Business School. (1960s). Herramienta clásica de planificación estratégica.
- Johnson, G., Scholes, K., & Whittington, R. (2017). *Dirección estratégica: Teoría y aplicación* (10.ª ed.). Pearson Education.
- Kim, W. C., & Mauborgne, R. (2015). *La estrategia del océano azul: Cómo crear un espacio no disputado en el mercado y hacer que la competencia sea irrelevante* (Edición ampliada). Empresa Activa.
- Kotler, P., & Keller, K. L. (2016). *Dirección de marketing* (15.ª ed.). Pearson Education.
- Monk, E., & Wagner, B. (2012). *Concepts in Enterprise Resource Planning*. Boston, MA: Cengage Learning.
- Ohno, T. (1988). *Toyota Production System: Beyond Large-Scale Production*. Cambridge, MA: Productivity Press.
- Osterwalder, A., & Pigneur, Y. (2011). *Generación de modelos de negocio: Un manual para visionarios, revolucionarios y retadores*. Deusto.
- Porter, M. E. (1985). *Competitive Advantage: Creating and Sustaining Superior Performance*. Nueva York: Free Press.
- Porter, M. E. (2008). **Las cinco fuerzas que dan forma a la estrategia competitiva**. Harvard Business Review, 86(1), 78-93.
- Porter, M. E. (1999). *Ventaja competitiva: Creación y sostenimiento de un desempeño superior*. CECSA.

13.2. Normatividad nacional aplicable

Ministerio de Tecnologías de la Información y las Comunicaciones. (2022). Decreto 767 de 2022:

Por el cual se actualiza la Política de Gobierno Digital del país. Tomado de:
https://www.mintic.gov.co/portal/715/articles-210461_recurso_1.pdf (Consulta: 2025)

Ministerio de Tecnologías de la Información y las Comunicaciones. (2022). Decreto 88 de 2022:

Por el cual se establecen los lineamientos para la digitalización y automatización de trámites y su realización en línea. Tomado de:
https://www.mintic.gov.co/portal/715/articles-198550_decreto_88_24_enero_2022.pdf (Consulta: 2025)

Presidencia de la República de Colombia. (2022). Decreto 338 de 2022: Por el cual se establecen

lineamientos para fortalecer la gobernanza de la seguridad digital. Tomado de:
<https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%20338%20DEL%208%20DE%20MARZO%20DE%202022.pdf> (Consulta: 2025)

Ministerio de Tecnologías de la Información y las Comunicaciones. (2022). Resolución 460 de

2022: Por la cual se expide el Plan Nacional de Infraestructura de Datos (PNID). Tomado de:
https://www.mintic.gov.co/portal/715/articles-198952_resolucion_00460_2022.pdf (Consulta: 2025)

Ministerio de Tecnologías de la Información y las Comunicaciones. (2022). Resolución 746 de

2022: Por la cual se fortalecen los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI). Tomado de: https://www.mintic.gov.co/portal/715/articles-208143_recurso_1.pdf (Consulta: 2025)

Ministerio de Tecnologías de la Información y las Comunicaciones. (2022). Resolución 1117 de

2022: Por la cual se establecen lineamientos de transformación digital para ciudades y territorios inteligentes. Tomado de: https://www.mintic.gov.co/portal/715/articles-208739_recurso_1.pdf (Consulta: 2025)

13.3. Marcos y estándares internacionales

AXELOS. (2019). ITIL Foundation: ITIL 4 Edition. AXELOS Global Best Practice.

ISACA. (2019). COBIT 2019 Framework: Governance and Management Objectives. Information Systems Audit and Control Association.

ISO/IEC. (2013). ISO/IEC 27001:2013 — Information Security Management Systems. International Organization for Standardization.

ISO/IEC. (2022). ISO/IEC 27001:2022 — Information Security Management Systems. International Organization for Standardization.

ISO/IEC. (2022). ISO/IEC 27001:2022 — Tecnologías de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Tomado de: <https://www.iso.org/standard/27001> (Consulta: 2025)

ISO/IEC. (2022). ISO/IEC 27002:2022 — Tecnologías de la información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. Tomado de: <https://www.iso.org/standard/27002> (Consulta: 2025)

13.4. Referentes técnicos del Ministerio TIC

Ministerio de Tecnologías de la Información y las Comunicaciones. (2020). *Marco de Arquitectura Empresarial – MAE v3.0.*

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). *Modelo de Seguridad y Privacidad de la Información – MSPI.*

Ministerio de Tecnologías de la Información y las Comunicaciones. (s.f.). *Guía MGGTI.GE.ES.01 v3.0 — Guía para la formulación del PETI.*

Presidencia de la República de Colombia. (2022). Decreto 338 de 2022: Por el cual se establecen lineamientos para fortalecer la gobernanza de la seguridad digital. Tomado de: <https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%20338%20DEL%208%20DE%20MARZO%20DE%202022.pdf> (Consulta: 2025)

13.5. Políticas internas vigentes de la Empresa

Empresa de Renovación y Desarrollo Urbano de Bogotá D.C. – RenoBo. (2025). Plan de seguridad y privacidad de la información.

Empresa de Renovación y Desarrollo Urbano de Bogotá D.C.– RenoBo. (2025). Plan de tratamiento de riesgos de seguridad y privacidad de la información.

13.6. Procedimientos internos utilizados como referencia

(2025). *PD-71 Administración de Acceso Lógico (V5)*.

(2025). *PD-51 Copias de respaldo (V3)*.

(2025). *PD-52 Mantenimiento de equipos de TI (V3)*.

(2025). *PD-50 Adquisición de infraestructura tecnológica (V3)*.

(2025). *PD-70 Soporte técnico y mantenimiento correctivo de dispositivos TI (V3)*.

(2025). *Procedimiento de control de cambios (sin codificación)*.

13.7. Plataformas y herramientas tecnológicas citadas

Google LLC. (s.f.). *Google Workspace*.

Zoom Video Communications. (s.f.). *Zoom Unified Communications Platform*.

Teclib Group. (s.f.). *GLPI ITSM Platform*.

NocoBase. (s.f.). *NocoBase Low-code Platform*.

Índice de ilustraciones

Ilustración 1: Metodología de formulación del PETI	23
Ilustración 2: Relación PETI-MAE v3 y MSPI	29
Ilustración 3 - Estructura organizacional	33
Ilustración 4 - Mapa de procesos	35
Ilustración 5: Cubrimiento tecnológico por tipo de proceso	45
Ilustración 6: Enfoques estratégicos del diagnóstico.....	48
Ilustración 7 - Matriz de riesgos TI	73
Ilustración 8: Gestión financiera TI - 2025 por Macroproyecto.....	76
Ilustración 9 - Estructura de TI.....	80
Ilustración 10 - Vista conceptual de Infraestructura de TI.....	91
Ilustración 11 - Objetivos estratégicos de TI alineados con los pilares institucionales	98
Ilustración 12 - Estrategia digital de la Empresa	100
Ilustración 13 - Bloques de arquitectura objetivo.....	100
Ilustración 14 - Evolución de la arquitectura de sistemas – Objetivo 2029.....	101
Ilustración 15 - Hoja de ruta consolidada 2026-2029.....	102
Ilustración 16: Proyección financiera TI 2026	109
Ilustración 17 - Fase de implementación del PETI	147
Ilustración 18 - Cronograma Grantt (Resumen).....	148

Índice de tablas

Tabla 1 – Normatividad	21
Tabla 2 - Relación anexos - fase	25
Tabla 3 - Descripción de los Procesos Institucionales.....	39

Tabla 4: Objetivos Estratégicos de TI (OE-TI)	41
Tabla 5 - Alineación de TI con los procesos institucionales	44
Tabla 6 - Servicio 001 Acceso a Internet por Wifi	59
Tabla 7 - Servicio 002 Acceso a la intranet.....	59
Tabla 8 - Servicio 003 Acceso a la red interna	59
Tabla 9 - Servicio 004 Correo electrónico y herramientas colaborativas	60
Tabla 10 - Servicio 005 Inteligencia artificial generativa	60
Tabla 11 - Servicio 006 Entrenamiento y capacitación	60
Tabla 12 - Servicio 007 Comunicaciones inteligentes	61
Tabla 13 - Servicio 008 Plataforma de mesa de servicio	61
Tabla 14 - Servicio 009 Gestión de red interna colaboradores	61
Tabla 15 - Servicio 010 Gestión de red de infraestructura tecnológica	62
Tabla 16 - Servicio 011 Antivirus	62
Tabla 17 - Servicio 012 Gestión de equipos de cómputo	62
Tabla 18 - Servicio 013 Instalación de Software en equipo de computo	63
Tabla 19 - Servicio 014 Videollamadas.....	63
Tabla 20 - Servicio 015 Soporte de aplicaciones.....	63
Tabla 21 - Servicio 016 Configuración de ambientes de desarrollo, pruebas, capacitación, preproducción	64
Tabla 22 - Servicio 017 Despliegue de software en producción	64
Tabla 23 - Servicio 018 Gestión de Infraestructura de TI	64
Tabla 24 - Servicio 019 Adquisición de licencias de software	65
Tabla 25 - Servicio 020 Mantenimiento de aplicaciones	65
Tabla 26 - Servicio 021 Administración de bases de datos	65
Tabla 27 - Servicio 022 Gestión de backup	66

Tabla 28 - Servicio 023 Gestión de proyectos de TI.....	66
Tabla 29 - Servicio 024 Gestión de identidades – Acceso lógico	66
Tabla 30 - Servicio 025 DNS.....	67
Tabla 31 - Servicio 026 Virtualización de servidores	67
Tabla 32 - Servicio 027 Aseguramiento de la calidad del software	67
Tabla 33 - Servicio 028 Servicio de Supervisión de proveedores de TI.....	67
Tabla 34 - Capacidades de TI	68
Tabla 35 - Control de indicadores.....	70
Tabla 36 - KPIs estratégicos PETI	71
Tabla 37 - Gestión financiera TI – 2025	75
Tabla 38 - Políticas vigentes de TI.....	78
Tabla 39 - Procedimientos documentados vigentes.....	79
Tabla 40 - Caracterización sistema ERP JSP7	83
Tabla 41 - Caracterización sistema SECOP 2.....	83
Tabla 42 - Caracterización Sistema SIGEP	84
Tabla 43 - Caracterización sistema de gestión documental.....	85
Tabla 44 - Caracterización sistema página web	86
Tabla 45 - Caracterización sistema Intranet	87
Tabla 46 - Caracterización sistema GLPI	88
Tabla 47 - Caracterización sistema Erudita	89
Tabla 48 - Caracterización sistema Apoteosys.....	90
Tabla 49 - Caracterización sistema JSP6	90
Tabla 50 - Servicios de Infraestructura de TI	92
Tabla 51 - Operación de los servicios tecnológicos	93

Tabla 52 - Matriz de mantenimientos	94
Tabla 53 - Evaluación de efectividad de los controles	95
Tabla 54 - Macroproyectos que se mantienen y buscan maduración	103
Tabla 55 - Macroproyectos.....	104
Tabla 56 - 9.3. Matriz de alineación entre objetivos de TI y macroproyectos	108
Tabla 57 - Proyección financiera TI 2026	109
Tabla 58 - Glosario	111
Tabla 59: Tabla brechas ISO 27001:2022	132
Tabla 60: Verificación de implementación de IPv6	133
Tabla 61: Plan de socialización.....	134
Tabla 62 - KPIs- EO 02.....	147
Tabla 63 - Resumen de cronograma	148
Tabla 64 – Resumen de evidencias esperadas.....	150
Tabla 65 - Brechas - planes de acción	158
Tabla 66 - Matriz de brechas y plan de acciones - FURAG.....	171
Tabla 67 - KPIs para el cierre de brechas FURAG	175

Control de cambios

Versión	Fecha	Descripción
1.0	23/01/2026	Formulación. Aprobado en Comité Institucional de Gestión y Desempeño.