RESOLUCIÓN NÚMERO 086
DICIEMBRE 30 DE 2025

"POR LA CUAL SE ADOPTA EL PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (PETI) DEL FONDO DE DESARROLLO SOCIAL DEL MUNICIPIO DE EL RETIRO – FONDESER"

El Gerente del Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER, en uso de sus atribuciones constitucionales, legales y estatutarias, en especial las conferidas por la Constitución Política, la Ley 87 de 1993, la Ley 489 de 1998, la Ley 1341 de 2009, la Ley 1474 de 2011, el Decreto 1078 de 2015 –Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones–, el Decreto 612 de 2018 –por el cual se establecen los lineamientos generales para la adopción e implementación del PETI en las entidades públicas–, y demás normas concordantes y complementarias,

CONSIDERANDO:

Que el artículo 209 de la Constitución Política establece que la función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones.

Que la Ley 489 de 1998, en sus artículos 3 y 4, dispone que la administración pública debe orientarse a la satisfacción de las necesidades colectivas, mediante la coordinación y uso racional de los recursos, con criterios de eficiencia y eficacia.

Que el Decreto 612 de 2018 determina los lineamientos para la formulación, adopción, implementación, seguimiento y evaluación del Plan Estratégico de Tecnologías de la Información (PETI), como instrumento que orienta el uso y la gestión de las TIC en las entidades públicas, con el fin de garantizar la alineación con el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo de Seguridad y Privacidad de la Información (MSPI), el Modelo de Gobierno Digital y los objetivos misionales de cada entidad.

Que el PETI constituye una herramienta de planeación estratégica que permite a FONDESER integrar las Tecnologías de la Información y las Comunicaciones al cumplimiento de su misión institucional, promoviendo la eficiencia administrativa, la

transparencia en la gestión pública, la toma de decisiones basada en datos y la optimización del servicio a los ciudadanos.

Que el Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER, en cumplimiento de la normatividad vigente, ha elaborado su Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI 2025–2028), bajo los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones y el Departamento Administrativo de la Función Pública, en articulación con el Plan de Desarrollo Municipal y el Modelo Integrado de Planeación y Gestión (MIPG).

Que el PETI de FONDESER define los objetivos estratégicos, líneas de acción, políticas, programas y proyectos tecnológicos necesarios para fortalecer los procesos internos, promover la interoperabilidad institucional, asegurar la protección de la información y mejorar la relación entre la entidad y la ciudadanía a través del uso eficiente y responsable de las TIC.

Que en virtud de lo anterior, se hace necesario adoptar formalmente dicho instrumento, con el fin de garantizar su implementación y seguimiento conforme a la normativa vigente y a los principios de planeación, eficacia, eficiencia, transparencia y mejora continua de la gestión pública.

RESUELVE:

ARTÍCULO PRIMERO. ADOPCIÓN DEL PETI. Adóptese el Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI) del Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER, como instrumento de planeación y gestión institucional para el periodo 2025–2028, el cual hace parte integral de la presente resolución.

ARTÍCULO SEGUNDO. OBJETIVO. El PETI tiene como propósito definir la ruta estratégica para el uso, fortalecimiento y aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en FONDESER, asegurando su alineación con los objetivos misionales, el Plan de Desarrollo Municipal y el Modelo Integrado de Planeación y Gestión (MIPG).

ARTÍCULO TERCERO. APLICABILIDAD. El presente Plan será de cumplimiento obligatorio para todos los funcionarios y contratistas de FONDESER, quienes deberán

incorporarlo en la planeación, ejecución y seguimiento de los procesos institucionales que involucren tecnologías de la información y comunicaciones.

ARTÍCULO CUARTO. IMPLEMENTACIÓN Y SOCIALIZACIÓN. La Gerencia, con el apoyo del área administrativa y de control interno, será responsable de la implementación, divulgación y seguimiento del PETI. Su socialización se efectuará mediante:

- Publicación en la página web institucional https://www.fondeser.com.co/.
- Reuniones de capacitación y sensibilización con funcionarios y contratistas.
- Divulgación de los objetivos y proyectos estratégicos en medios institucionales y espacios físicos de la entidad.

ARTÍCULO QUINTO. SEGUIMIENTO Y EVALUACIÓN. La Gerencia y el área de Control Interno establecerán indicadores de gestión y resultados que permitan medir el avance, cumplimiento y efectividad del PETI. Los resultados del seguimiento deberán incorporarse a los informes de gestión y ser objeto de revisión periódica en el marco del MIPG.

ARTÍCULO SEXTO. VIGENCIA. La presente resolución rige a partir de la fecha de su publicación y tendrá vigencia durante el periodo de ejecución del PETI (2025–2028), sin perjuicio de las actualizaciones o ajustes que resulten necesarios conforme a la evolución tecnológica o las directrices del Gobierno Nacional.

Dado en las instalaciones del Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER, a los 30 días del mes de diciembre de 2025.

COMUNÍQUESE Y CÚMPLASE.

Carlos Mauricio Yepes Bedoya
Gerente
Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER

ANEXO

PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (PETI)

FONDESER — Periodo 2025-2028

ÍNDICE

1. INTRODUCCIÓN

El avance de las Tecnologías de la Información y las Comunicaciones (TIC) ha transformado la manera en que las entidades públicas planifican, ejecutan y evalúan su gestión institucional. En este contexto, el **Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER**, como entidad descentralizada de naturaleza industrial y comercial del Estado, reconoce la necesidad de fortalecer su capacidad tecnológica y de gestión digital como pilar para el cumplimiento eficiente, transparente y sostenible de su misión institucional.

El presente **Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI) 2025–2027** constituye la hoja de ruta que orientará las acciones y decisiones relacionadas con el uso, la gestión y la inversión en tecnología dentro de la entidad. Este plan busca garantizar que las TIC aporten valor estratégico al desarrollo de los procesos misionales —particularmente en la gestión de créditos, interventoría y ejecución de obras— y a los procesos de apoyo administrativo, financiero y de control interno.

El PETI se formula en coherencia con las directrices establecidas por el **Modelo de Gobierno Digital del Estado Colombiano**, las políticas de **Seguridad y Privacidad de la Información**, y las normas que regulan la gestión tecnológica en el sector público. Su propósito es consolidar un ecosistema tecnológico moderno, seguro, eficiente y alineado con los objetivos institucionales de FONDESER, promoviendo la transformación digital, la transparencia y la optimización de recursos.

La metodología aplicada contempla el diagnóstico de la situación actual, la identificación de brechas tecnológicas, la formulación de estrategias de corto y mediano plazo, la definición de proyectos priorizados y la proyección presupuestal para su ejecución. Así mismo, incorpora un modelo de seguimiento y evaluación que permitirá medir los avances, garantizar la sostenibilidad de las acciones y asegurar la continuidad operativa de los servicios críticos.

Con este plan, FONDESER reafirma su compromiso con la **innovación, la eficiencia administrativa y la mejora continua**, entendiendo las TIC como un habilitador esencial para fortalecer la gestión pública, mejorar la atención al ciudadano y generar valor social a través de la tecnología.

El presente **Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI)** define la hoja de ruta que orientará la gestión tecnológica de **FONDESER** durante el periodo 2025–2027, con el propósito de fortalecer el uso estratégico de las TIC como herramienta clave para el cumplimiento de la misión institucional.

Este plan busca que las Tecnologías de la Información y las Comunicaciones se conviertan en un factor determinante para **optimizar la gestión del otorgamiento de créditos**, mejorar los procesos de **interventoría y ejecución de obras**, y consolidar la eficiencia en los **procesos administrativos, financieros y de gestión humana**.

De igual manera, el PETI se orienta a garantizar la **disponibilidad, integridad, confidencialidad y trazabilidad de la información**, promoviendo la modernización tecnológica, la eficiencia operativa y la toma de decisiones basada en datos.

Finalmente, este instrumento contribuye al fortalecimiento de la **transparencia institucional y la rendición de cuentas**, asegurando el uso responsable de los recursos públicos y el acceso equitativo a los servicios que ofrece FONDESER a la comunidad del municipio de El Retiro.

2. JUSTIFICACIÓN:

El PETI 2025–2027 define la ruta estratégica de las TIC en FONDESER para garantizar la eficiencia, la transparencia y la continuidad operativa de los procesos misionales y de apoyo. Este documento busca asegurar que las inversiones tecnológicas estén alineadas con la planeación institucional y contribuyan directamente a los objetivos de desarrollo económico y social del municipio de El Retiro.

3. OBJETIVOS

General

Formular e implementar el **Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI)** de **FONDESER** para el periodo **2025–2027**, con el propósito de **modernizar la infraestructura tecnológica**, garantizar la **continuidad operativa de los servicios institucionales**, fortalecer la **seguridad y protección de la información**, y potenciar la **analítica de datos y la gestión documental digital**, en coherencia con los objetivos estratégicos de la entidad.

Objetivos Específicos

1. **Optimizar la infraestructura tecnológica y los sistemas de información** de FONDESER mediante la implementación de soluciones modernas, seguras y escalables que soporten las operaciones misionales y de apoyo.
2. **Fortalecer la ciberseguridad, la privacidad y la integridad de los datos institucionales**, mediante la adopción de políticas, controles y buenas prácticas alineadas con el Modelo de Seguridad y Privacidad de la Información (MSPI).
3. **Promover la transformación digital y el desarrollo de competencias TIC** en los funcionarios y contratistas, garantizando la apropiación tecnológica, la eficiencia en los procesos y la mejora continua en la prestación de los servicios.

4. ALCANCE

El presente **Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI)** aplica a todas las **dependencias, funcionarios y contratistas** que utilizan o administran recursos tecnológicos de **FONDESER**.

Su alcance comprende la **planificación, gestión y fortalecimiento** de los componentes tecnológicos que soportan los procesos misionales, administrativos y de control, incluyendo:

- El **inventario y administración de hardware y software** institucional.
- La gestión de **servicios en la nube y locales (on-premise)**.
- La **gobernanza y seguridad de la información**.
- La **continuidad operativa y respaldo de datos**.
- La **formación tecnológica del talento humano**.
- La **interoperabilidad con la Alcaldía, proveedores y entidades financieras**.

- El **plan de comunicaciones y presupuesto** del periodo **2025–2027**.

Con ello, el PETI busca garantizar la eficiencia operativa, la transparencia y la sostenibilidad tecnológica de FONDESER.

5. DEFINICIONES

Para efectos de este Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI), se adoptan las siguientes definiciones y términos clave:

- **TIC (Tecnologías de la Información y las Comunicaciones):** Conjunto de recursos, herramientas, equipos, programas y sistemas utilizados para gestionar, almacenar, procesar y transmitir información de manera digital.
- **PETI (Plan Estratégico de Tecnologías de la Información):** Instrumento de planeación que define los objetivos, estrategias y proyectos tecnológicos necesarios para fortalecer la gestión institucional.
- **SLA / ANS (Service Level Agreement / Acuerdo de Nivel de Servicio):** Compromiso formal entre FONDESER y un proveedor o dependencia interna, que establece los tiempos y condiciones de prestación de un servicio tecnológico.
- **MSPI (Modelo de Seguridad y Privacidad de la Información):** Marco que orienta la implementación de controles, políticas y procedimientos para garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de la información.
- **GDPR / Normativa de Protección de Datos Personales:** Conjunto de disposiciones (nacionales e internacionales) que regulan el tratamiento adecuado de la información personal. En Colombia se rige por la **Ley 1581 de 2012** y sus decretos reglamentarios.
- **Backups / Copias de seguridad:** Procesos mediante los cuales se realiza la duplicación y almacenamiento seguro de la información institucional, con el fin de garantizar su recuperación ante pérdida o daño.
- **Gobierno Digital:** Política pública que busca fortalecer la gestión estatal mediante el uso estratégico de las TIC, fomentando la eficiencia, transparencia, participación y servicio al ciudadano.
- **Transformación Digital:** Proceso de cambio organizacional que integra las tecnologías digitales en todas las áreas de la entidad, mejorando la gestión, la productividad y la atención a los usuarios.
- **Interoperabilidad:** Capacidad de los sistemas y entidades para intercambiar información de manera eficiente, segura y comprensible, favoreciendo la coordinación con la Alcaldía y otros actores externos.
- **Ciberseguridad:** Conjunto de medidas técnicas, organizativas y humanas orientadas a proteger los activos digitales de la entidad frente a amenazas o ataques informáticos.

- **Infraestructura tecnológica:** Conjunto de recursos físicos y virtuales (servidores, redes, equipos, software y servicios en la nube) que soportan los sistemas de información institucionales.
- **Continuidad del negocio:** Estrategias y procedimientos que permiten mantener las operaciones críticas de la entidad ante contingencias o interrupciones tecnológicas.
- **Talento TIC:** Personal con competencias técnicas y administrativas para la gestión, soporte y desarrollo de los recursos tecnológicos institucionales.
- **Gestor documental:** Sistema de información diseñado para administrar, controlar y digitalizar los documentos institucionales, garantizando su conservación, trazabilidad y consulta segura.
- **Analítica de datos / Business Intelligence (BI):** Conjunto de herramientas y metodologías que permiten analizar información para apoyar la toma de decisiones estratégicas.
- **Mesa de ayuda (Help Desk):** Servicio encargado de atender, registrar y dar solución a los incidentes y requerimientos tecnológicos de los usuarios internos.

6. MARCO NORMATIVO

El presente **Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI)** de **FONDESER** se fundamenta en el marco legal y normativo que regula la gestión de las Tecnologías de la Información en el sector público colombiano. A continuación, se relacionan las principales disposiciones aplicables:

Normatividad Nacional

1. **Ley 1341 de 2009 – Ley TIC** Define los principios y conceptos generales sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones en Colombia. Promueve el acceso, uso y apropiación de las TIC para el desarrollo social, económico y cultural del país.
2. **Decreto Único Reglamentario 1078 de 2015 – Sector TIC** Compila las disposiciones reglamentarias del sector de Tecnologías de la Información y las Comunicaciones, incluyendo los lineamientos sobre el uso eficiente de las TIC, la seguridad digital, la interoperabilidad y la implementación del Gobierno Digital.
3. **Ley 1581 de 2012 – Protección de Datos Personales** Establece las disposiciones generales para la protección de los datos personales y regula el tratamiento de la información que contenga datos de carácter privado, garantizando el derecho fundamental al habeas data.
4. **Decreto 1377 de 2013 – Reglamentación de la Ley 1581 de 2012** Regula aspectos relacionados con la autorización, recolección y tratamiento de datos personales, así como los mecanismos de protección y actualización de la información.
5. **Política de Gobierno Digital – Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)** Define los lineamientos para que las entidades públicas transformen digitalmente su gestión, promoviendo la eficiencia

administrativa, la transparencia y la participación ciudadana mediante el uso estratégico de las TIC.

6. **Política Nacional de Seguridad Digital (CONPES 3995 de 2020)** Establece la estrategia nacional de seguridad digital para fortalecer la protección de los activos de información del Estado, prevenir riesgos cibernéticos y promover una cultura de ciberseguridad en las entidades públicas.
7. **Modelo de Seguridad y Privacidad de la Información (MSPI)** Herramienta técnica del MinTIC que orienta la implementación de controles, políticas y procedimientos para salvaguardar la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional.
8. **Guía para la Implementación del Modelo de Gobierno Digital (MinTIC)** Documento técnico que orienta a las entidades públicas en la adopción de prácticas de planeación, gestión, seguridad, interoperabilidad y servicios ciudadanos digitales, garantizando el cumplimiento del marco normativo TIC.
9. **Ley 1712 de 2014 – Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional** Promueve la transparencia activa y pasiva de la información pública, estableciendo la obligación de las entidades de divulgar información y facilitar el acceso ciudadano por medios tecnológicos.
10. **Ley 527 de 1999 – Comercio Electrónico y Firmas Digitales** Regula el uso de los mensajes de datos, el comercio electrónico y las firmas digitales, otorgando validez jurídica a los documentos y transacciones electrónicas.
11. **Ley 594 de 2000 – Ley General de Archivos** Define las disposiciones generales para la organización y conservación de los archivos públicos, incluyendo los lineamientos para la gestión documental electrónica y la preservación digital de la información institucional.
12. **Decreto 1008 de 2018 – Política de Seguridad Digital y Gobierno Digital** Establece la articulación entre las políticas de Gobierno Digital y Seguridad Digital, definiendo responsabilidades de las entidades en la gestión segura de la información y el uso de tecnologías.
13. **Ley 1266 de 2008 – Habeas Data Financiero** Regula la administración de la información financiera, crediticia y comercial, relevante para los procesos de gestión de créditos y análisis de cartera de FONDESER.
14. **Ley 1474 de 2011 – Estatuto Anticorrupción** Dispone mecanismos para prevenir, investigar y sancionar actos de corrupción en la administración pública, promoviendo la transparencia y el control ciudadano, aplicables también a la gestión tecnológica.

Normatividad Institucional

- **Manual de Contratación de FONDESER:** Define los procedimientos internos para la adquisición de bienes y servicios tecnológicos, garantizando la transparencia y la eficiencia en la ejecución de recursos.
- **Manual de Control Interno:** Establece las políticas y procedimientos de control, evaluación y seguimiento de los procesos institucionales, incluyendo la gestión tecnológica.

- **Política Interna de Seguridad de la Información (en formulación):** Busca asegurar la protección, uso responsable y disponibilidad de los activos de información y sistemas tecnológicos de la entidad.

7. RUPTURAS ESTRATÉGICAS

Para transformar la gestión mediante TIC, FONDESER debe impulsar las siguientes rupturas estratégicas:

- **Considerar las TIC como aporte directo a la sostenibilidad y transparencia del negocio de microcréditos y obras**
  Las TIC deben dejar de verse como un soporte operativo y convertirse en un **motor estratégico** para fortalecer la eficiencia y trazabilidad de los procesos misionales de FONDESER. A través de sistemas integrados y reportes digitales, se mejora el control de los recursos, la gestión de cartera y la rendición de cuentas. Esto contribuye a una mayor **transparencia**, confianza ciudadana y sostenibilidad financiera en la ejecución de los proyectos de crédito y obra pública

- **Potenciar la gobernanza y control documental digital (cero papel, trazabilidad de documentos y facturas)**
  La digitalización de la documentación institucional permite avanzar hacia un modelo **"cero papel"**, en el cual los documentos, contratos y facturas puedan ser gestionados de forma electrónica, con trazabilidad y respaldo seguro. Esto optimiza los tiempos de respuesta, reduce riesgos de pérdida de información y facilita las auditorías internas y externas. Además, fortalece la gobernanza de la información y la eficiencia administrativa.

- **Implementar analítica de datos para seguimiento de cartera, tasas de recupero y desempeño de proyectos**
  La analítica de datos permite transformar la información operativa de FONDESER en **conocimiento estratégico** para la toma de decisiones. A través de tableros de control y herramientas de Business Intelligence (BI), se podrá realizar seguimiento en tiempo real a la cartera, tasas de recuperación, cumplimiento de metas y ejecución de obras. Esto impulsa la mejora continua y la gestión basada en evidencia.

- **Externalizar o contratar servicios especializados donde sea más eficiente (Data Center, seguridad, soporte)**
  Dado el tamaño y estructura operativa de FONDESER, resulta más eficiente contratar ciertos servicios tecnológicos a proveedores especializados, como alojamiento en Data Center, ciberseguridad o soporte técnico. Esta estrategia reduce costos de infraestructura local, asegura disponibilidad permanente y garantiza el cumplimiento de estándares de calidad y seguridad exigidos por el Gobierno Digital.

- **Implementar políticas de seguridad y privacidad robustas y verificables**
  La información es uno de los activos más valiosos de FONDESER, por lo que requiere medidas de protección sólidas y sostenibles. La implementación del **Modelo de Seguridad y Privacidad de la Información (MSPI)** permitirá establecer políticas, controles de acceso, respaldo de datos y gestión de incidentes. De esta manera, se asegura la confidencialidad, integridad y disponibilidad de la información institucional y de los datos personales de los usuarios.

- **Fortalecer capacidades del personal y contratistas en uso de herramientas digitales**
  El éxito del PETI depende del talento humano. Por ello, es fundamental fortalecer las competencias digitales de los funcionarios y contratistas, promoviendo el uso adecuado de las plataformas tecnológicas, la cultura de seguridad digital y la apropiación del cambio tecnológico. Un equipo capacitado genera procesos más eficientes, reduce errores y aumenta la productividad institucional.

8. ANÁLISIS DE LA SITUACIÓN ACTUAL

8.1 Contexto institucional

FONDESER es una entidad descentralizada adscrita a la **Alcaldía de El Retiro**, cuyo objeto principal es **otorgar créditos sociales**, realizar **interventorías, consultorías y obras de infraestructura** en beneficio de la comunidad. La entidad cuenta con una estructura administrativa pequeña, conformada por **2 funcionarios de planta** y aproximadamente **12 contratistas por prestación de servicios**.
Esta composición institucional limita la capacidad técnica interna y exige una **estrategia TIC basada en soluciones escalables, seguras, de bajo mantenimiento y alto retorno operativo**, que reduzcan la dependencia tecnológica y garanticen la continuidad de los servicios.

8.2 Infraestructura y conectividad

Actualmente, FONDESER dispone de una **red de Internet corporativa** con capacidad estimada entre **100 y 200 GB mensuales**, utilizada principalmente para labores administrativas y misionales. Sin embargo, **no cuenta con un sistema de seguridad de red robusto** ni con un cumplimiento completo en las políticas de acceso segmentado, lo que incrementa los riesgos de exposición y vulnerabilidad de la información institucional.

Toda la operación tecnológica se realiza **por medio de conexión Wi-Fi**, sin puntos de red cableados dedicados a cada equipo, lo que dificulta el control de tráfico, la trazabilidad de conexiones y la estabilidad del servicio.

FONDESER cuenta con un **servidor físico local** que actualmente es utilizado por uno de los empleados para sus labores cotidianas, práctica que representa un **riesgo significativo para la seguridad y la integridad de los datos institucionales**, pues el servidor debería destinarse exclusivamente a servicios de red, bases de datos o almacenamiento seguro.

El **backup o copia de seguridad** solo se realiza sobre el sistema **SAIMYR**, dejando por fuera la información restante alojada en el servidor, lo cual genera una vulnerabilidad crítica ante posibles pérdidas de datos o fallas de hardware. Se recomienda implementar una **política integral de respaldo de toda la información del servidor**, con copias automáticas y almacenadas también en la nube.

8.3 Inventario de hardware y software (HW/SW)

La infraestructura tecnológica actual de FONDESER se compone de:

- **6 equipos de escritorio**, propiedad de la entidad.
- **3 equipos portátiles**, también institucionales.

- **Servidor físico** local en la sede administrativa.
- **Software administrativo SAIMYR**, licenciado y en uso.
- **Licencias de Microsoft Office 365** para los equipos institucionales.

Es importante señalar que algunos **contratistas por prestación de servicios** utilizan **equipos personales sin licenciamiento oficial**, los cuales tienen **acceso directo a las carpetas compartidas y a la información de la entidad**, lo que **aumenta el riesgo de filtraciones, pérdida o modificación no autorizada de información**. Se recomienda restringir accesos por roles, utilizar cuentas institucionales y aplicar políticas de control de dispositivos.

8.4 Sistemas de información y servicios críticos

- Sistema administrativo y contable (**SAIMYR**).
- Sistema de gestión de cartera y créditos.
- Gestión documental (en fase inicial, se recomienda implementar un gestor documental centralizado).
- Correo institucional y herramientas colaborativas (Microsoft Office 365).
- Página web institucional e intranet para comunicación interna.
- Copias de seguridad locales (solo para SAIMYR, requiere ampliación).

Se recomienda que los sistemas críticos (SAIMYR, gestión documental y correo institucional) sean **migrados a un entorno de Data Center o nube segura**, con respaldo automatizado y monitoreo continuo.

8.5 Gestión humana y competencias TIC

FONDESER no cuenta actualmente con un **área formal de tecnología** ni con un **responsable TIC exclusivo**. La gestión tecnológica se realiza de forma compartida entre funcionarios administrativos, lo cual limita el seguimiento técnico y el control de la infraestructura.
Se recomienda crear el rol de **Coordinador TIC o soporte externo permanente**, encargado de implementar políticas de seguridad, gestionar accesos y monitorear la red. Asimismo, es prioritario **capacitar a todo el personal y contratistas** en temas de **seguridad de la información, uso de herramientas colaborativas, gestión documental digital y buenas prácticas de protección de datos personales.**

8.6 Análisis FODA TIC

Fortalezas	**Oportunidades**
- Tamaño institucional reducido que permite agilidad en la toma de decisiones.	- Posibilidad de **migrar servicios críticos a la nube** y contratar soporte especializado.
- Existencia de software administrativo licenciado (SAIMYR).	- Apoyo y articulación con la Alcaldía de El Retiro para proyectos tecnológicos.
Debilidades	**Amenazas**
- Ausencia del cumplimiento de políticas de seguridad digital y segmentación de accesos.	**- Ciberataques, pérdida o manipulación de información sensible.**
- Uso inadecuado del servidor por personal operativo.	**- Obsolescencia tecnológica y vulnerabilidad de equipos.**
- Falta de respaldo integral del servidor y datos institucionales.	**- Accesos no controlados de contratistas externos.**
- Conectividad débil y no segura (Wi-Fi sin puntos de red cableados).	**- Dependencia de terceros sin acuerdos de nivel de servicio (ANS/SLA).**

9. ENTENDIMIENTO ESTRATÉGICO

9.1 Misión TIC

Garantizar la gestión eficiente, segura y transparente de la información institucional mediante el uso estratégico de las Tecnologías de la Información y las Comunicaciones (TIC), apoyando los procesos misionales de FONDESER —especialmente el otorgamiento de créditos, la interventoría y la ejecución de obras— y contribuyendo al cumplimiento de los objetivos institucionales, la transparencia y la rendición de cuentas ante la comunidad del municipio de El Retiro.

9.2 Visión TIC (2027)

Para el año 2027, FONDESER será una entidad **tecnológicamente fortalecida**, con **infraestructura moderna, servicios alojados en entornos seguros y políticas de seguridad digital plenamente implementadas**, que garanticen la disponibilidad, integridad y confidencialidad de la información institucional. Las TIC serán un eje estratégico para la eficiencia administrativa, la transformación digital y la generación de valor público.

9.3 Principios Orientadores

Las acciones del PETI se desarrollarán bajo los siguientes principios:

- **Transparencia:** Toda gestión tecnológica estará orientada a garantizar el acceso, trazabilidad y rendición de cuentas.
- **Seguridad de la información:** La protección de los datos institucionales será prioritaria en la planificación y operación de todos los servicios.
- **Eficiencia y sostenibilidad:** Se promoverán soluciones tecnológicas con bajo costo de mantenimiento y alto impacto institucional.
- **Interoperabilidad:** Se garantizará la integración tecnológica con el personal de planta, contratistas y entidades con quien se tenga diferentes tipos de vinculos.
- **Cumplimiento normativo:** Las decisiones TIC se ajustarán a las leyes nacionales, políticas del MinTIC y lineamientos institucionales vigentes.

9.4 Principios Orientadores

FONDESER **cuenta con políticas internas de seguridad de la información**, sin embargo, su **implementación y seguimiento aún no se cumplen en su totalidad**. Existen brechas relacionadas con el control de accesos, la segmentación de red, los respaldos de datos, el manejo de equipos personales y la administración de usuarios. Por ello, el PETI establece como prioridad **consolidar la aplicación efectiva del Modelo de Seguridad y Privacidad de la Información (MSPI)**, asegurando que las políticas no solo estén formalizadas, sino también **operativas, monitoreadas y verificables** mediante controles y auditorías periódicas.

9.5 Alineación con los objetivos institucionales de FONDESER

El PETI se articula directamente con los objetivos estratégicos de la entidad, de la siguiente manera:

Objetivo Institucional	**Aporte Estratégico del PETI**
Fortalecer la gestión del otorgamiento de créditos.	Implementación de sistemas integrados de información y analítica de datos para seguimiento de cartera y recuperación.
Garantizar la transparencia y eficiencia en la ejecución de obras.	Digitalización documental y trazabilidad de procesos mediante gestión documental electrónica.
Mejorar la atención al ciudadano y la eficiencia administrativa.	Servicios digitales y herramientas colaborativas para comunicación y trámites internos.

Objetivo Institucional	Aporte Estratégico del PETI
Consolidar la sostenibilidad financiera y operativa.	Migración a la nube, reducción de costos locales y políticas de seguridad estandarizadas.
Promover el bienestar y desarrollo del talento humano.	Capacitación permanente en competencias TIC y seguridad digital.

9.6 Iniciativas Estratégicas Prioritarias

Cumplimiento integral de las políticas de seguridad digital y adopción plena del MSPI.

1. **Implementación de un gestor documental electrónico** con trazabilidad de facturas, contratos y soportes de crédito.
2. **Migración gradual de servicios críticos a la nube o Data Center** con respaldo automatizado.
3. **Fortalecimiento del control de accesos y segmentación de red.**
4. **Modernización de equipos y puntos de conexión cableada** para mejorar la estabilidad y seguridad.
5. **Implementación de herramientas de analítica de datos (BI)** para seguimiento de cartera y proyectos.
6. **Capacitación continua en ciberseguridad y uso responsable de la información.**

10. MODELO DE GESTIÓN Y GOBIERNO DE TI

10.1 Estructura organizacional y roles TIC

Dada la estructura administrativa y el tamaño operativo de FONDESER, la gestión de las Tecnologías de la Información se desarrolla bajo un **modelo mixto**, que combina la responsabilidad interna de coordinación con la **contratación externa de servicios especializados** para soporte, mantenimiento y seguridad.

Los roles principales se definen así:

Cargo / Rol	Responsabilidades Principales
Gerente General	Define lineamientos estratégicos, aprueba el PETI y el presupuesto TIC. Supervisa el cumplimiento de las políticas de seguridad y transformación digital.
Secretaria Ejecutiva	Supervisa la ejecución presupuestal, gestiona las adquisiciones tecnológicas y hace seguimiento a los contratos de soporte y licenciamiento.

Cargo / Rol	Responsabilidades Principales
Coordinador TIC (funcionario o contratista especializado)	Responsable de la administración tecnológica, monitoreo de red, gestión de incidentes, respaldo de información, control de accesos y cumplimiento del MSPI.
Proveedor externo de soporte / Data Center	Encargado del mantenimiento preventivo y correctivo de equipos, soporte técnico remoto, seguridad perimetral y gestión de copias de seguridad.
Usuarios internos y contratistas	Deben cumplir las políticas institucionales de seguridad, uso aceptable de TIC y protección de datos personales. Reportan incidentes y requerimientos a la mesa de ayuda.

Nota: Se recomienda formalizar la figura del *Coordinador TIC institucional* mediante contrato o cargo permanente, con funciones específicas de planeación, control y seguimiento al cumplimiento del PETI.

10.2 Modelo de Gobierno de TI

El **Gobierno de TI** en FONDESER se basa en la definición de responsabilidades, políticas y procesos que aseguren que la tecnología se utilice de manera efectiva, segura y alineada con los objetivos institucionales.

El modelo se estructura sobre los siguientes ejes:

1. **Dirección estratégica:** el PETI define prioridades, inversiones y metas tecnológicas alineadas con el Plan Estratégico Institucional.
2. **Gestión y control:** la Subgerencia y la Coordinación TIC realizan seguimiento continuo a la ejecución de proyectos, presupuesto y cumplimiento de políticas.
3. **Seguridad y cumplimiento:** se aplican las políticas internas de seguridad de la información, el MSPI y la Ley 1581 de 2012, priorizando la protección de los datos y la continuidad operativa.
4. **Rendición de cuentas:** se generarán informes semestrales de avance del PETI, incidentes de seguridad y estado de los proyectos TIC para la Gerencia y la Junta Directiva.

10.3 Políticas institucionales TIC vigentes

FONDESER cuenta con **políticas internas de seguridad de la información y uso aceptable de recursos TIC**, las cuales, aunque formuladas, presentan un **nivel de cumplimiento parcial**. El PETI busca fortalecer su aplicación práctica mediante acciones de seguimiento, capacitación y control.

Las políticas prioritarias son:

- **Política de Uso Aceptable de TIC (PUA):** regula el empleo responsable de los equipos, software, internet y correo institucional.

- **Política de Seguridad de la Información:** define los controles de acceso, respaldo de datos y protección de información sensible.
- **Política de Backup y Continuidad Operativa:** establece la obligación de realizar copias completas y automáticas de los sistemas y servidores.
- **Política de Gestión de Incidentes:** determina los procedimientos de reporte, análisis y mitigación de incidentes tecnológicos.
- **Política de Control de Dispositivos y Accesos:** regula el uso de equipos personales y el acceso remoto a la información institucional.
- **Política de Renovación y Actualización Tecnológica:** orienta la reposición de equipos, licencias y servicios de manera planificada.

El cumplimiento de estas políticas será evaluado trimestralmente por la Coordinación TIC, con reportes a la Subgerencia Administrativa y a la Gerencia General.

10.4 Modelo de prestación de servicios TIC (SLA / ANS)

Con el fin de garantizar la eficiencia y calidad en la atención tecnológica, FONDESER adoptará un **modelo de prestación de servicios basado en Acuerdos de Nivel de Servicio (ANS / SLA)**, tanto para soporte interno como externo.

Catálogo de servicios básicos:

- Soporte técnico presencial y remoto.
- Administración de red, servidores y respaldo.
- Actualización de software y licencias.
- Gestión de incidentes y requerimientos.
- Capacitación en herramientas TIC y seguridad digital.
- Mantenimiento preventivo y correctivo de equipos.

Tiempos de atención recomendados:

Prioridad del incidente	**Tiempo máximo de respuesta**	**Tiempo estimado de solución**
Crítico (caída de sistema o red)	2 horas	8–24 horas
Alto (problemas funcionales graves)	4 horas	24–48 horas
Medio (fallas parciales o de usuario)	8 horas	48–72 horas
Bajo (requerimientos menores o consultas)	24 horas	3–5 días hábiles

Los incidentes se registrarán mediante un **sistema de tickets o base de datos de seguimiento**, que permitirá generar indicadores mensuales sobre tiempos de atención, reincidencias y causas raíz.

10.5 Seguimiento y mejora continua

El PETI establece un esquema de **monitoreo y mejora continua** de la gestión tecnológica, bajo los siguientes mecanismos:

- **Informes de avance semestrales** sobre cumplimiento del PETI, ejecución presupuestal y cumplimiento de políticas TIC.
- **Revisiones anuales del inventario tecnológico** (hardware, software, licencias y usuarios).
- **Auditorías internas y externas** sobre seguridad digital y cumplimiento normativo.
- **Indicadores de desempeño (KPI)** para medir la disponibilidad de servicios, atención de incidentes, calidad del soporte y efectividad de los respaldos.
- **Revisión y actualización anual de las políticas de seguridad**, incorporando las lecciones aprendidas y los hallazgos de control interno.

11. RIESGOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y CONTROLES ASOCIADOS

El análisis de riesgos tecnológicos de FONDESER evidencia brechas significativas en materia de seguridad, respaldo de información, control de accesos y uso de infraestructura. Estos riesgos pueden afectar la **confidencialidad, integridad y disponibilidad** de los datos institucionales, así como la continuidad operativa de los procesos misionales.

A continuación, se presentan los principales riesgos identificados y los controles propuestos para su mitigación:

No.	Riesgo Identificado	Descripción y Causa Raíz	Impacto Potencial	Controles Existentes / Propuestos
1	**Uso inadecuado del servidor institucional**	El servidor es utilizado directamente por un empleado para labores operativas, en lugar de destinarse exclusivamente a servicios de red o almacenamiento.	Pérdida de información, daño físico del servidor, exposición de datos críticos.	- Restringir acceso físico y lógico al servidor. - Separar entornos de trabajo y producción. - Configurar políticas de acceso por roles. - Supervisar uso mediante bitácoras y registros.

No.	Riesgo Identificado	Descripción y Causa Raíz	Impacto Potencial	Controles Existentes / Propuestos
2	**Falta de respaldo integral de la información**	Actualmente solo se realiza copia de seguridad del sistema SAIMYR, dejando sin respaldo el resto del servidor y archivos institucionales.	Pérdida total o parcial de información ante fallas, ataques o borrado accidental.	- Implementar política integral de backup automatizado. - Incluir todos los sistemas y carpetas del servidor. - Guardar copias externas (nube y dispositivo externo). - Realizar pruebas de restauración trimestrales.
3	**Acceso no controlado a carpetas institucionales por contratistas externos**	Contratistas con equipos personales sin licencia tienen acceso libre a la información de la entidad.	Riesgo de fuga, modificación o eliminación de datos sensibles.	- Definir niveles de acceso por usuario y función. - Implementar autenticación con cuentas institucionales. - Aplicar política de “mínimo privilegio”. - Monitorear accesos y registrar cambios en archivos.
4	**Red Wi-Fi insegura y sin segmentación**	Toda la operación se realiza sobre conexión Wi-Fi sin configuración de seguridad avanzada ni puntos de red cableados.	Interceptación de datos, pérdida de conectividad o acceso no autorizado.	- Configurar red segura con WPA3 y contraseñas robustas. - Implementar VLAN para separar tráfico administrativo y público. - Instalar puntos de red cableada para equipos fijos.

No.	Riesgo Identificado	Descripción y Causa Raíz	Impacto Potencial	Controles Existentes / Propuestos
				- Activar monitoreo del tráfico de red.
5	**Incumplimiento parcial de las políticas de seguridad de la información**	Las políticas existen, pero su aplicación y seguimiento no son consistentes.	Vulnerabilidad institucional frente a incidentes y auditorías.	- Implementar plan anual de cumplimiento MSPI. - Realizar capacitaciones y simulacros. - Designar responsable TIC para seguimiento. - Generar reportes trimestrales de cumplimiento.
6	**Uso de software sin licencia por parte de contratistas**	Algunos contratistas utilizan equipos personales con programas no autorizados.	Riesgos legales, vulnerabilidades de malware y pérdida de reputación institucional.	- Prohibir el uso de software sin licencia en actividades institucionales. - Verificar cumplimiento mediante auditorías. - Ofrecer acceso remoto seguro a entornos virtuales institucionales.

No.	Riesgo Identificado	Descripción y Causa Raíz	Impacto Potencial	Controles Existentes / Propuestos
7	**Ciberataques y amenazas de ransomware**	Falta de protección avanzada en red, antivirus centralizado y monitoreo de vulnerabilidades.	Pérdida o secuestro de información, interrupción de servicios.	- Instalar soluciones UTM o firewall avanzado. - Actualizar antivirus y parches de seguridad. - Establecer plan de respuesta a incidentes y respaldo externo.
8	**Obsolescencia tecnológica de equipos**	Algunos equipos presentan limitaciones de rendimiento y capacidad.	Lentitud operativa, incompatibilidad con nuevas versiones de software, fallos frecuentes.	- Implementar plan de renovación gradual (cada 3–5 años). - Realizar mantenimiento preventivo semestral. - Incluir reposición en presupuesto anual.
9	**Ausencia de monitoreo y registro de incidentes tecnológicos**	No existe un sistema formal de seguimiento o mesa de ayuda para reportar fallas.	Falta de trazabilidad, tiempos largos de atención y pérdida de control sobre incidentes.	- Implementar sistema de tickets o bitácora digital. - Clasificar incidentes por prioridad (SLA). - Generar informes mensuales de soporte y solución.

No.	Riesgo Identificado	Descripción y Causa Raíz	Impacto Potencial	Controles Existentes / Propuestos
10	**Falta de segmentación de roles y privilegios en sistemas**	Todos los usuarios tienen acceso a información general sin restricciones.	Modificación o eliminación no autorizada de información.	- Definir perfiles de usuario por área. - Activar control de accesos por contraseña y autenticación multifactor (MFA). - Auditar cambios periódicamente.

Plan de mejora continua y monitoreo de riesgos

Para garantizar la mitigación efectiva de los riesgos anteriores, FONDESER adoptará las siguientes acciones permanentes:

1. **Actualización anual del mapa de riesgos TIC**, incorporando nuevos hallazgos y controles.
2. **Ejecución de auditorías semestrales** sobre cumplimiento de políticas y seguridad digital.
3. **Monitoreo de alertas y eventos tecnológicos** mediante registros de servidor y herramientas de red.
4. **Capacitación anual a todo el personal y contratistas** sobre seguridad, privacidad y uso responsable de la información.
5. **Reportes trimestrales de incidentes** y seguimiento al cumplimiento de las medidas de seguridad a la Gerencia General.

12. MODELO DE PLANEACIÓN Y PROGRAMA DE ACCIÓN (2025–2027)

El modelo de planeación del PETI de FONDESER establece las **acciones, proyectos y metas estratégicas** que permitirán fortalecer la infraestructura tecnológica, la seguridad de la información y la eficiencia institucional durante el periodo 2025–2027.

Este plan se enfoca en **cerrar las brechas identificadas en el diagnóstico**, priorizando la **seguridad digital, el control de accesos, el respaldo integral de la información, la mejora de la conectividad y la capacitación del talento humano.**

12.1 Proyectos Estratégicos Prioritarios

Código	Proyecto / Iniciativa	Descripción General	Objetivo Específico	Periodo de Ejecución
P1	**Implementación del Plan de Seguridad Digital y Cumplimiento del MSPI**	Revisión, actualización y aplicación integral de las políticas de seguridad de la información existentes.	Garantizar la protección, integridad y disponibilidad de los datos institucionales mediante controles efectivos y monitoreo continuo.	2025
P2	**Configuración de red cableada y fortalecimiento de la infraestructura de conectividad**	Instalación de puntos de red LAN en los puestos de trabajo y configuración de red segura con VLAN y Wi-Fi corporativo protegido.	Mejorar la estabilidad y seguridad de la red institucional y reducir la dependencia del Wi-Fi abierto.	2025–2026
P3	**Implementación de un sistema de respaldo integral (Backup & Recovery)**	Diseño y ejecución de una política automatizada de copias de seguridad para el servidor completo y los equipos institucionales.	Asegurar la continuidad operativa y la recuperación de información ante pérdidas o ataques cibernéticos.	2025
P4	**Fortalecimiento del control de accesos y segmentación de usuarios**	Implementación de roles, permisos y autenticación institucional (cuentas corporativas y MFA).	Evitar accesos no autorizados y garantizar la trazabilidad de la información.	2025–2026
P5	**Adquisición de licencias y regularización de software institucional**	Verificación, adquisición y legalización de licencias de software para equipos propios y de contratistas.	Cumplir normatividad y reducir riesgos de seguridad y legales.	2025
P6	**Gestor Documental Electrónico (fase I)**	Implementación de un sistema ECM o gestor documental para digitalizar y controlar documentos, contratos y facturas.	Fortalecer la trazabilidad, eficiencia administrativa y transparencia documental.	2026–2027

Código	Proyecto / Iniciativa	Descripción General	Objetivo Específico	Periodo de Ejecución
P7	**Migración de servicios críticos a la nube o Data Center**	Alojamiento seguro de SAIMYR, correos y respaldos en entornos de nube certificada o Data Center externo.	Garantizar disponibilidad, respaldo remoto y continuidad operativa.	2026–2027
P8	**Implementación del Tablero de Control (BI) para seguimiento de cartera y obras**	Desarrollo de un panel de indicadores con información de cartera, tasas de recuperación y avance de proyectos.	Mejorar la toma de decisiones y la gestión basada en datos.	2027
P9	**Capacitación institucional en seguridad digital y herramientas colaborativas**	Formación periódica para funcionarios y contratistas en buenas prácticas TIC, seguridad y productividad digital.	Fomentar la cultura tecnológica y el cumplimiento de políticas TIC.	2025–2027

12.2 Cronograma General de Ejecución (2025–2027)

Proyecto	2025	2026	2027
P1. Plan de Seguridad Digital y MSPI	●		
P2. Red cableada y conectividad segura	●	●	
P3. Sistema de respaldo integral	●		
P4. Control de accesos y autenticación	●	●	
P5. Regularización de licencias	●		
P6. Gestor documental electrónico		●	●
P7. Migración de servicios críticos a la nube		●	●
P8. Tablero de control (BI)			●
P9. Capacitación y sensibilización TIC	●	●	●

(● = Periodo de ejecución o avance significativo)

12.3 Indicadores de Cumplimiento (KPI)

Indicador	Meta / Periodo	Responsable del seguimiento
% de cumplimiento de políticas TIC y MSPI	100% para diciembre de 2025	Coordinador TIC / Gerencia
% de equipos conectados a red segura cableada	80% en 2026	Coordinador TIC / Soporte externo
% de respaldos verificados y recuperables	100% anual	Coordinador TIC
% de sistemas institucionales migrados a nube o Data Center	70% en 2027	Gerencia / Soporte TIC
% de usuarios capacitados en seguridad y TIC	100% anual	Talento Humano / Coordinación TIC
Disponibilidad promedio de servicios críticos	≥99.5%	Proveedor Data Center / Soporte TIC
Tiempo promedio de atención de incidentes (SLA)	≤24 horas	Mesa de Ayuda / Coordinador TIC

12.4 Estrategia de seguimiento y control del PETI

Para garantizar la ejecución efectiva del PETI 2025–2027, se implementará un **mecanismo de seguimiento trimestral**, coordinado por la **Subgerencia Administrativa y Financiera** con apoyo del **Coordinador TIC**, que incluirá:

- Reportes de avance físico y financiero de cada proyecto.
- Revisión de cumplimiento de políticas de seguridad y MSPI.
- Actualización del inventario TIC y de licencias.
- Evaluación de riesgos emergentes y controles aplicados.
- Presentación de resultados y ajustes ante la Gerencia y la Junta Directiva.

13. PRESUPUESTO PROYECTADO (resumen anual en COP)

El presupuesto proyectado del PETI de FONDESER para el periodo **2025–2027** considera las necesidades identificadas en materia de infraestructura, seguridad, licenciamiento, servicios en la nube, soporte técnico y fortalecimiento del talento humano.

Los montos presentados son **estimativos** y deberán ajustarse anualmente según la disponibilidad presupuestal, los costos de mercado y las políticas de contratación pública vigentes.

13.1 Estructura de Inversión Tecnológica

Componente de Inversión	Descripción General
Infraestructura y Conectividad	Adquisición de equipos, instalación de red cableada, mejora de conectividad y puntos de acceso.
Seguridad de la Información y MSPI	Implementación de controles, firewall, autenticación, políticas de backup y plan de contingencia.
Gestión Documental y Digitalización	Implementación de gestor documental electrónico y automatización de procesos administrativos.
Licenciamiento y Software	Regularización y renovación de licencias de software, sistemas operativos y aplicaciones institucionales.
Servicios en la Nube / Data Center	Migración de sistemas críticos (SAIMYR, correo, respaldos) y alojamiento seguro externo.
Soporte Técnico y Mantenimiento	Contratación de soporte interno y externo para equipos, red y sistemas.
Capacitación y Cultura Digital	Formación continua en seguridad, uso de herramientas TIC y apropiación tecnológica.
Contingencias y Reposición de Equipos	Fondo para emergencias, renovación tecnológica y mejoras imprevistas.

13.2 Presupuesto Estimado por Año (en COP)

Componente	2025	2026	2027	Total
1. Infraestructura y conectividad	45,000,000	60,000,000	25,000,000	**130,000,000**
2. Seguridad de la información y MSPI	30,000,000	35,000,000	25,000,000	**90,000,000**
3. Sistema de respaldo integral (backup y recuperación)	20,000,000	10,000,000	10,000,000	**40,000,000**
4. Licenciamiento y software institucional	25,000,000	15,000,000	10,000,000	**50,000,000**
5. Gestor documental electrónico (ECM)	0	80,000,000	20,000,000	**100,000,000**
6. Servicios en la nube / Data Center	10,000,000	40,000,000	50,000,000	**100,000,000**
7. Soporte técnico y mantenimiento	15,000,000	20,000,000	20,000,000	**55,000,000**

Componente	2025	2026	2027	Total
8. Capacitación y cultura digital	10,000,000	15,000,000	15,000,000	**40,000,000**
9. Contingencias y renovación tecnológica	10,000,000	20,000,000	20,000,000	**50,000,000**
TOTAL ANUAL ESTIMADO (COP)	**165,000,000**	**295,000,000**	**195,000,000**	**655,000,000**

13.3 Criterios de Priorización Presupuestal

1. **Seguridad y continuidad operativa:** Los proyectos que garanticen la protección y respaldo de la información tendrán prioridad en la ejecución.
2. **Obligaciones normativas:** Las inversiones relacionadas con el cumplimiento del MSPI, la Ley 1581 de 2012 y las políticas TIC institucionales son de carácter prioritario.
3. **Impacto operativo:** Se priorizarán los proyectos con impacto directo en la eficiencia administrativa y la calidad del servicio.
4. **Sostenibilidad:** Se buscarán soluciones escalables y de bajo costo de mantenimiento, especialmente en servicios de nube y soporte.
5. **Capacitación y cultura digital:** La formación del talento humano será continua y transversal a todos los proyectos.

13.4 Fuentes de Financiación

El desarrollo del PETI podrá financiarse a través de:

- Recursos propios del presupuesto de funcionamiento de FONDESER.
- Aportes y convenios con la Alcaldía de El Retiro.
- Proyectos cofinanciados con el Ministerio TIC o fondos de innovación pública.
- Recursos de inversión aprobados por la Junta Directiva.
- Reasignación presupuestal de gastos operativos hacia modernización tecnológica.

13.5 Plan de Ejecución Presupuestal

El presupuesto será ejecutado de manera **trimestral** y supervisado por la **Subgerencia Administrativa y Financiera**, con control y seguimiento del **Coordinador TIC**, asegurando:

- Cumplimiento de metas físicas y financieras.
- Transparencia en la contratación y adquisición de bienes y servicios.
- Reportes semestrales a la Gerencia General y a la Junta Directiva.

- Ajustes anuales conforme al avance del plan y la disponibilidad de recursos.

14. PLAN DE COMUNICACIONES DEL PETI

El **Plan de Comunicaciones** tiene como propósito asegurar que todas las partes interesadas —funcionarios, contratistas, la Alcaldía de El Retiro, la Junta Directiva y la ciudadanía— conozcan, comprendan y se apropien de los objetivos, avances y resultados del **Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI) 2025–2027**.

La comunicación efectiva permitirá fortalecer la cultura institucional hacia el uso responsable de las TIC, la transparencia en la gestión y el cumplimiento de las políticas de seguridad digital.

14.1 Objetivo del Plan de Comunicaciones

Establecer un modelo de comunicación interna y externa que promueva la **difusión, sensibilización y seguimiento del PETI**, garantizando la participación de todos los actores institucionales y el cumplimiento de los compromisos definidos.

14.2 Públicos Objetivo

Tipo de público	**Descripción / Rol dentro del PETI**
Junta Directiva de FONDESER	Instancia de aprobación, seguimiento y control estratégico del plan.
Gerencia General	Responsable de la dirección y supervisión general del PETI.
Subgerencia Administrativa y Financiera	Encargada del seguimiento presupuestal, adquisiciones y reportes.
Coordinación TIC / Soporte externo	Responsable técnico y operativo de la ejecución del PETI.
Funcionarios de planta	Usuarios directos de las plataformas tecnológicas y garantes del cumplimiento de las políticas TIC.
Contratistas por prestación de servicios	Usuarios externos con responsabilidades en la aplicación de las políticas de seguridad y uso aceptable.
Alcaldía de El Retiro	Entidad articuladora y aliada en proyectos de interoperabilidad y Gobierno Digital.
Ciudadanía	Beneficiarios indirectos, a través de la transparencia, la eficiencia y la mejora de los servicios institucionales.

14.3 Estrategia de Comunicación

La estrategia contempla tres niveles de acción:

1. **Comunicación Interna:** Dirigida a funcionarios y contratistas de FONDESER para informar, sensibilizar y capacitar sobre el contenido y la ejecución del PETI.
    - Socialización formal del plan en reunión general.
    - Envío digital del documento oficial a todos los colaboradores.
    - Capacitación en políticas TIC y seguridad digital.
    - Boletines internos con avances trimestrales.
    - Reuniones periódicas de seguimiento (mínimo trimestrales).
2. **Comunicación Interinstitucional:** Busca mantener coordinación con la **Alcaldía de El Retiro**, proveedores tecnológicos y entidades aliadas.
    - Mesas técnicas semestrales con representantes TIC de la Alcaldía.
    - Informes ejecutivos de avances y requerimientos.
    - Presentación de resultados anuales del PETI a la Junta Directiva.
3. **Comunicación Externa y Transparencia:** Orientada a la ciudadanía y entes de control para divulgar el compromiso de FONDESER con la modernización y la seguridad tecnológica.
    - Publicación del PETI y sus avances en la página web institucional.
    - Sección en la web de **"Transparencia y Gobierno Digital"**.
    - Informes públicos de cumplimiento en rendición de cuentas anual.

14.4 Herramientas y Canales de Comunicación

Canal / Medio	**Uso principal**
Correo institucional	Comunicación oficial interna y difusión de lineamientos TIC.
Reuniones presenciales o virtuales	Presentaciones, capacitaciones y seguimiento de avances.
Boletines digitales / circulares internas	Difusión periódica de avances, logros y recordatorios de cumplimiento.
Intranet o carpeta compartida	Repositorio del PETI, políticas TIC, informes y documentos técnicos.
Página web institucional	Publicación del PETI, informes públicos y avances de gestión tecnológica.

Canal / Medio	Uso principal
Actas de Junta Directiva	Registro formal de seguimiento y aprobación de avances del plan.

14.5 Cronograma de Comunicación (2025–2027)

Actividad	Periodicidad	Responsable
Presentación inicial del PETI ante Junta Directiva	2025 (inicio del plan)	Gerencia General / Coordinación TIC
Socialización del PETI con funcionarios y contratistas	2025	Subgerencia / Coordinador TIC
Boletines internos de avance	Trimestral	Coordinador TIC
Reuniones de seguimiento interno	Trimestral	Gerencia / Subgerencia
Informe ejecutivo a la Junta Directiva	Semestral	Subgerencia / Coordinación TIC
Publicación de avances en página web	Semestral	Comunicaciones / Coordinación TIC
Rendición de cuentas pública	Anual	Gerencia General
Evaluación y actualización del PETI	2027	Gerencia / Junta Directiva

14.6 Resultados Esperados

- Funcionarios y contratistas informados y comprometidos con las políticas TIC.
- Cumplimiento visible y medible del PETI 2025–2027.
- Mayor transparencia y acceso a la información pública.
- Coordinación efectiva con la Alcaldía y entidades aliadas.
- Cultura organizacional orientada a la seguridad digital y la innovación.

15. SISTEMA DE EVALUACIÓN Y SEGUIMIENTO DEL PETI

El **Sistema de Evaluación del Plan Estratégico de Tecnologías de la Información (PETI) 2025–2027** tiene como finalidad medir el cumplimiento de los objetivos, la eficiencia en la ejecución de los proyectos y la efectividad de las acciones implementadas en materia tecnológica y de seguridad digital.

Este sistema busca promover la **cultura de evaluación, autocontrol y mejora continua**, involucrando a todos los funcionarios y contratistas de FONDESER, bajo el acompañamiento técnico del área de **Control Interno**.

15.1 Principios del Sistema de Evaluación

1. **Corresponsabilidad:** la gestión TIC no es exclusiva de un área; todos los integrantes del equipo FONDESER deben contribuir al cumplimiento del PETI.
2. **Transparencia:** los resultados deben ser medibles, verificables y documentados para rendición de cuentas ante la Gerencia y la Junta Directiva.
3. **Mejora continua:** los hallazgos y desviaciones servirán como base para acciones correctivas y actualizaciones del plan.
4. **Evidencia verificable:** toda medición debe sustentarse en documentos, registros y reportes de avance.
5. **Acompañamiento técnico:** el área de Control Interno asesorará el seguimiento, validará la información y apoyará los procesos de evaluación.

15.2 Niveles de Evaluación

Nivel	Enfoque	Frecuencia	Responsable principal
Operativo	Seguimiento a ejecución de actividades, proyectos TIC y cumplimiento de cronogramas.	Trimestral	Coordinador TIC / Subgerencia
Táctico	Evaluación de cumplimiento de metas, uso de recursos y resultados intermedios.	Semestral	Gerencia / Subgerencia / Control Interno
Estratégico	Análisis global de impacto del PETI y logros frente a los objetivos institucionales.	Anual	Gerencia General / Junta Directiva / Control Interno

15.3 Indicadores de Gestión y Evaluación del PETI

Dimensión de Evaluación	Indicador	Meta / Periodo	Fuente de Verificación	Responsable del Seguimiento
Gobernanza TIC	% de cumplimiento de proyectos del PETI ejecutados según cronograma	90% anual	Informes trimestrales / actas de seguimiento	Subgerencia / Coordinador TIC
Seguridad de la información	% de cumplimiento de políticas MSPI y controles implementados	100% a 2026	Auditorías internas / reportes TIC	Coordinador TIC / Control Interno
Respaldo y continuidad operativa	% de copias de seguridad verificadas y restauradas correctamente	100% trimestral	Bitácora de backup / pruebas de restauración	Coordinador TIC / Soporte externo
Infraestructura tecnológica	% de equipos conectados a red segura cableada o VLAN protegida	80% en 2026	Inventario TIC / registros de red	Coordinador TIC
Capacitación y cultura digital	% de funcionarios y contratistas capacitados en seguridad y TIC	100% anual	Listas de asistencia / certificados	Talento Humano / Coordinador TIC
Licenciamiento	% de equipos institucionales y de contratistas con software legalizado	100% a 2025	Auditoría de software / inventario TIC	Subgerencia / Coordinador TIC
Satisfacción del usuario TIC	Nivel de satisfacción con servicios de soporte y tecnología	≥85% anual	Encuesta interna de percepción	Subgerencia / Control Interno
Cumplimiento presupuestal	% de ejecución presupuestal TIC frente al plan aprobado	≥90% anual	Estados financieros / informes de gestión	Subgerencia Administrativa
Transparencia y rendición de cuentas	Publicación semestral de avances del PETI y políticas TIC en web institucional	100% anual	Página web / informes de rendición	Comunicaciones / Gerencia

Dimensión de Evaluación	Indicador	Meta / Periodo	Fuente de Verificación	Responsable del Seguimiento
Mejora continua	Número de acciones correctivas implementadas frente a hallazgos	100% ejecutadas	Planes de mejora / actas de seguimiento	Coordinador TIC / Control Interno

15.4 Mecanismo de Evaluación y Reporte

1. **Reuniones trimestrales de seguimiento** del PETI, lideradas por la Gerencia General y la Subgerencia, con participación del Coordinador TIC, representantes de cada área y Control Interno.
2. **Elaboración de un informe semestral** que consolide los indicadores, avances físicos y financieros, hallazgos y acciones correctivas.
3. **Evaluación anual global** presentada a la Junta Directiva y publicada en el informe de gestión institucional.
4. **Control Interno** verificará el cumplimiento metodológico, la calidad de la información y la ejecución de las medidas correctivas derivadas de los resultados del sistema de evaluación.
5. **Actualización anual del PETI** con base en los resultados del sistema de evaluación, los cambios tecnológicos y las recomendaciones del área de Control Interno.

15.5 Resultados Esperados del Sistema de Evaluación

- Seguimiento permanente y documentado del avance del PETI.
- Cumplimiento verificable de los objetivos estratégicos y de seguridad TIC.
- Participación activa de todas las áreas en la gestión tecnológica.
- Mayor control, transparencia y trazabilidad en la inversión tecnológica.
- Fortalecimiento del Sistema de Control Interno en materia tecnológica.

16. BIBLIOGRAFÍA

- **Congreso de la República de Colombia.** (2009). *Ley 1341 de 2009.* “Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia.” Diario Oficial No. 47.426.
- **Presidencia de la República de Colombia.** (2015). *Decreto Único Reglamentario del Sector TIC – Decreto 1078 de 2015.* Compila las disposiciones reglamentarias relacionadas con la administración, uso y promoción de las TIC en el país.

- **Congreso de la República de Colombia.** (2012). *Ley 1581 de 2012.* "Por la cual se dictan disposiciones generales para la protección de datos personales." Diario Oficial No. 48.587.
- **Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).** (2018). *Política de Gobierno Digital.* Versión actualizada. Bogotá D.C. Recuperado de https://gobiernodigital.mintic.gov.co.
- **Ministerio TIC.** (2020). *Guía para la formulación de Planes Estratégicos de Tecnologías de la Información (PETI) en entidades públicas.* Bogotá D.C.
- **Departamento Administrativo de la Función Pública (DAFP).** (2021). *Modelo Integrado de Planeación y Gestión (MIPG).* Lineamientos para la gestión estratégica y la articulación de políticas institucionales. Bogotá D.C.
- **Ministerio TIC.** (2021). *Modelo de Seguridad y Privacidad de la Información (MSPI).* Guía de implementación para entidades públicas colombianas.
- **Ley 1712 de 2014.** "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional." Diario Oficial No. 49.084.
- **Ley 1266 de 2008.** "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales."

- **Oficina de Naciones Unidas para los Asuntos Económicos y Sociales (ONU–UNDESA).** (2022). *Informe Mundial sobre Gobierno Electrónico.* Nueva York.
- **Control Interno FONDESER.** (2024). *Informe diagnóstico sobre la gestión tecnológica y riesgos de seguridad de la información.* Documento interno.
- **FONDESER.** (2024). *Política de Seguridad de la Información y Uso Aceptable de TIC.* Versión institucional vigente.
- **Ministerio TIC.** (2023). *Política Nacional de Seguridad Digital.* Bogotá D.C.
- **Gobierno de Colombia – MinTIC.** (2024). *Guía de madurez digital y fortalecimiento de capacidades TIC en entidades públicas.*

CARLOS MAURICIO YEPES BEDOYA
Gerente
Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER