RESOLUCIÓN NÚMERO 072

DICIEMBRE 30 DE 2025

"POR LA CUAL SE ADOPTA EL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PSPI) DEL FONDO DE DESARROLLO SOCIAL DEL MUNICIPIO DE EL RETIRO – FONDESER PARA EL PERIODO 2025–2027"

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 de Colombia, la Ley 87 de 1993, la Ley 489 de 1998, la Ley 1581 de 2012, la Ley 1712 de 2014, la Ley 594 de 2000, el Decreto 1377 de 2013, el Decreto 1078 de 2015 –Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones–, el Decreto 612 de 2018, el CONPES 3975 de 2019, y demás normas concordantes y complementarias,

CONSIDERANDO:

Que el artículo 209 de la Constitución Política dispone 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.

Que la Ley 87 de 1993 establece la obligación de implementar sistemas de control interno orientados a la prevención y mitigación de riesgos que puedan afectar la operación y los activos institucionales, incluyendo los de información y comunicación.

Que la Ley 489 de 1998 señala que las entidades descentralizadas deben garantizar el cumplimiento de los fines del Estado mediante una administración eficiente, transparente y controlada, haciendo uso responsable de los recursos públicos y tecnológicos.

Que la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013 fijan las disposiciones para la protección de los datos personales y exigen la adopción de medidas técnicas, humanas y administrativas que aseguren su confidencialidad, integridad y disponibilidad.

Que la Ley 1712 de 2014 garantiza el derecho de acceso a la información pública y ordena implementar mecanismos de seguridad que garanticen la integridad y disponibilidad de la información bajo custodia de las entidades estatales.

Que la Ley 594 de 2000 regula la gestión documental y la conservación del patrimonio documental, lo que implica adoptar medidas que aseguren la protección de la información física y electrónica institucional.

Que el Decreto 1078 de 2015 y el Decreto 612 de 2018 establecen las directrices para la implementación de la Política de Gobierno Digital, la seguridad de la información y la gestión tecnológica en el sector público.

Que el Documento CONPES 3975 de 2019 define la Política Nacional de Seguridad Digital, la cual orienta a las entidades públicas hacia una gestión integral de los riesgos digitales y la protección de los activos de información del Estado.

Que el Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER, en cumplimiento de dichas disposiciones y en articulación con el Modelo Integrado de Planeación y Gestión (MIPG) y el Plan Estratégico de Tecnologías de la Información (PETI 2025–2027), ha formulado el Plan de Seguridad y Privacidad de la Información (PSPI) 2025–2027, como instrumento de gestión que orienta la planeación, implementación y mejora continua de los controles y mecanismos de seguridad y privacidad de la información institucional.

Que el PSPI busca garantizar la protección integral de los activos de información, prevenir incidentes de seguridad, fortalecer la cultura institucional en materia de protección de datos, y asegurar el cumplimiento de los estándares internacionales ISO/IEC 27001 y 27701, así como las buenas prácticas promovidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Que en mérito de lo expuesto, se considera procedente adoptar formalmente el Plan de Seguridad y Privacidad de la Información (PSPI) 2025–2027 como instrumento técnico y estratégico de obligatorio cumplimiento en FONDESER.

RESUELVE:

ARTÍCULO PRIMERO. ADOPCIÓN DEL PSPI.
Adóptese el Plan de Seguridad y Privacidad de la Información (PSPI) 2025–2027 del Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER, como instrumento de planeación, gestión y control orientado a la protección de los activos de información institucional y los datos personales bajo su custodia.

ARTÍCULO SEGUNDO. OBJETIVO.
El PSPI tiene como objetivo establecer los lineamientos, políticas, roles, controles y mecanismos necesarios para preservar la confidencialidad, integridad, disponibilidad, autenticidad y privacidad de la información que gestiona FONDESER en el ejercicio de sus funciones crediticias, contractuales y administrativas.

ARTÍCULO TERCERO. ALCANCE Y APLICABILIDAD.
El presente Plan será de aplicación obligatoria para todos los funcionarios, contratistas y colaboradores de FONDESER que, en el desarrollo de sus actividades, accedan, procesen o administren información institucional o datos personales.
Las dependencias deberán implementar las medidas y controles definidos en el PSPI dentro de sus procedimientos, sistemas de información, archivos físicos y entornos digitales.

ARTÍCULO CUARTO. IMPLEMENTACIÓN Y DIVULGACIÓN.
La Gerencia, con el apoyo del área de Tecnologías de la Información, Talento Humano y la Oficina de Control Interno, será responsable de implementar y divulgar el PSPI mediante:

- Publicación del documento en la página web institucional de FONDESER.
- Jornadas de capacitación y sensibilización dirigidas a funcionarios y contratistas.
- Emisión de circulares y comunicados que promuevan la cultura de seguridad y privacidad de la información.

ARTÍCULO QUINTO. SEGUIMIENTO Y EVALUACIÓN.
La Oficina de Control Interno y el responsable de Tecnologías de la Información realizarán el seguimiento semestral y la evaluación anual del PSPI, de acuerdo con los indicadores definidos en el plan.
Los resultados deberán integrarse en los informes de auditoría, control interno y gestión institucional, así como en los componentes de Gobierno Digital y del MIPG.

ARTÍCULO SEXTO. MEJORA CONTINUA.
El PSPI será revisado y actualizado anualmente o cuando se presenten cambios normativos, tecnológicos o institucionales que lo requieran, garantizando la mejora continua en la gestión de la seguridad y privacidad de la información.

ARTÍCULO SÉPTIMO. VIGENCIA.
La presente resolución rige a partir de la fecha de su publicación y tendrá vigencia durante el período 2025–2027, sin perjuicio de las actualizaciones que se realicen para su fortalecimiento.

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 DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025–2027

Tabla de Contenido

1. Introducción

El Fondo de Desarrollo Social del Municipio de El Retiro – **FONDESER** es una entidad descentralizada de carácter industrial y comercial del Estado, adscrita a la Alcaldía de El Retiro, Antioquia. Su misión es impulsar el desarrollo económico y social del municipio mediante la **otorgación de créditos**, la **ejecución de interventorías y consultorías**, y la **gestión y desarrollo de proyectos de infraestructura**, asegurando una administración eficiente y transparente de los recursos públicos y sociales.

En un entorno institucional progresivamente más digital, la **seguridad y la privacidad de la información** se consolidan como pilares estratégicos para mantener la **confianza de la ciudadanía, los contratistas, los aliados institucionales y los entes de control**. El manejo responsable de los datos y la consolidación de una cultura organizacional orientada a la seguridad de la información son factores esenciales para garantizar la **continuidad operativa**, la **transparencia** y la **integridad de la gestión pública**.

El **Plan de Seguridad y Privacidad de la Información 2025–2027 (PSPI)** establece un **marco integral de gestión**, orientado a proteger los activos de información de FONDESER frente a amenazas internas y externas. Este plan promueve el **cumplimiento normativo**, la **mejora continua** y la **sostenibilidad institucional**, en articulación con los objetivos definidos en el **Plan Estratégico de Tecnologías de la Información – PETI FONDESER 2025–2027**, así como con las políticas nacionales de **seguridad digital** y **protección de datos personales**.

Su implementación busca **mitigar los riesgos tecnológicos, operativos y de privacidad**, fortalecer el **Sistema de Control Interno** y consolidar una cultura organizacional basada en la **transparencia, la responsabilidad y la confianza ciudadana**.

1.1 Objetivos

Objetivos Generales

Establecer un marco estratégico, técnico y normativo que garantice la **confidencialidad, integridad, disponibilidad y privacidad** de la información administrada por FONDESER, asegurando su correcta protección frente a amenazas o incidentes que puedan comprometer los datos institucionales o personales.

Objetivos Específicos

- Proteger los activos de información críticos para la misión institucional.
- Cumplir con las normas nacionales e internacionales de seguridad y privacidad.
- Prevenir y mitigar riesgos asociados al uso de tecnologías de la información.
- Promover la cultura de seguridad digital en todos los funcionarios y contratistas.
- Establecer mecanismos de seguimiento, control y mejora continua del sistema de seguridad de la información.

1.2 Alcance

El Plan de Seguridad y Privacidad de la Información de FONDESER aplica a **todas las áreas, procesos, sistemas de información, contratistas y empleados** que manejen, procesen o custodien información institucional, financiera, técnica o personal.

El alcance incluye:

- **Activos de Información:** Documentos físicos y digitales, bases de datos de créditos, contratos, informes técnicos, sistemas financieros y registros administrativos.
- **Personas:** Personal de planta, contratistas por prestación de servicios, interventores, asesores, proveedores, usuarios y aliados estratégicos.
- **Procesos:** Actividades relacionadas con la recolección, almacenamiento, procesamiento, transmisión y disposición de información en los ámbitos administrativo, financiero y técnico.
- **Infraestructura tecnológica:** Equipos de cómputo, redes, servidores, sistemas de respaldo, plataformas contables y de crédito, correos institucionales y dispositivos móviles de trabajo.
- **Normativa:** Cumplimiento de la Ley 1581 de 2012 (Protección de Datos Personales), Ley 1273 de 2009 (Delitos Informáticos), Ley 1712 de 2014 (Transparencia y Acceso a la Información Pública), Decreto 1377 de 2013 y Decreto 1078 de 2015.
- **Gestión de Incidentes:** Acciones de prevención, detección y respuesta frente a amenazas que puedan afectar la confidencialidad, integridad o disponibilidad de los datos institucionales.

2. BASE LEGAL Y NORMATIVA APLICABLE

El **Plan de Seguridad y Privacidad de la Información del Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER** se fundamenta en el marco jurídico colombiano y en las mejores prácticas internacionales de ciberseguridad, gestión de la información y protección de datos personales.

Su cumplimiento es obligatorio para todos los funcionarios, contratistas, proveedores y terceros que participen en actividades relacionadas con el tratamiento, manejo, almacenamiento o transmisión de información de la entidad.

- ### 2.1 Normativa Nacional

- **Ley 489 de 1998 – Organización y Funcionamiento de las Entidades del Orden Nacional:** Establece el marco general de la función administrativa y la estructura de las entidades descentralizadas, definiendo principios de eficiencia, economía y control interno aplicables a FONDESER como entidad de carácter industrial y comercial del Estado.

- **Ley 1581 de 2012 – Protección de Datos Personales:** Define los principios y disposiciones generales para garantizar el derecho fundamental al *habeas data*. Regula las obligaciones de FONDESER como responsable y encargado del tratamiento de datos personales de usuarios, contratistas y funcionarios.

- **Decreto 1377 de 2013 – Reglamentario de la Ley 1581 de 2012:** Detalla los procedimientos para la obtención de autorizaciones, la administración de bases de datos y las condiciones para el tratamiento de información personal en entidades públicas y mixtas.

- **Ley 1266 de 2008 – Habeas Data Financiero:** Regula el manejo de información crediticia y financiera, siendo esencial para FONDESER por su función de otorgamiento de créditos, evaluación de riesgo financiero y reporte de información a centrales de riesgo.

- **Ley 1273 de 2009 – Protección de la Información y los Datos:** Crea el bien jurídico de la "protección de la información y de los datos" y establece sanciones por delitos informáticos, aplicable a los sistemas de información crediticia y de gestión documental de FONDESER.

- **Ley 1712 de 2014 – Transparencia y Derecho de Acceso a la Información Pública:** Obliga a FONDESER a garantizar la publicación, acceso y veracidad de la información institucional, financiera y contractual, fomentando la transparencia en el uso de recursos públicos.

- **Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector TIC:** Compila las disposiciones sobre Gobierno Digital y seguridad de la información, orientando la implementación de buenas prácticas tecnológicas en la gestión de datos e infraestructura informática de la entidad.

- **Ley 594 de 2000 – Ley General de Archivos:** Regula la gestión documental y la conservación del patrimonio archivístico. FONDESER debe asegurar la integridad, custodia y trazabilidad de los documentos relacionados con créditos, contratos y proyectos de obra pública.

- **Ley 1474 de 2011 – Estatuto Anticorrupción:** Establece mecanismos de control, prevención y sanción de la corrupción, y exige a entidades como FONDESER adoptar controles administrativos y tecnológicos para garantizar la transparencia en procesos de crédito e interventoría.

- **Ley 80 de 1993 – Estatuto General de Contratación de la Administración Pública:** Aplica a los procesos contractuales que adelanta FONDESER en el marco de sus labores de interventoría, consultoría y obras públicas, garantizando la selección objetiva, la eficiencia y la transparencia.

- **Ley 1150 de 2007 – Reforma al Estatuto de Contratación:** Introduce mecanismos de selección abreviada y procedimientos electrónicos de contratación, relevantes para la gestión de proyectos e interventorías de FONDESER.

- **Ley 2015 de 2020 – Historia Laboral Electrónica:** Regula la digitalización y conservación electrónica de historias laborales y demás documentos

administrativos, aplicable a la gestión de personal de planta y contratistas de FONDESER.

- **Circular Externa 005 de 2017 – Superintendencia de Industria y Comercio (SIC):**
  Establece lineamientos sobre gestión de incidentes de seguridad y violaciones de datos personales, aplicables a los sistemas que administra FONDESER para el manejo de información crediticia y administrativa.

2.2 Normativa Internacional y Estándares de Referencia

- **ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información (SGSI):** Define los requisitos para implementar un sistema de gestión que garantice la confidencialidad, integridad y disponibilidad de la información crediticia, financiera y técnica de FONDESER.

- **ISO/IEC 27701 – Extensión de Privacidad de la Información:** Proporciona directrices para la protección de datos personales dentro del SGSI, alineada con la Ley 1581 de 2012 y aplicable a los registros de beneficiarios, contratistas y empleados.

- **ISO/IEC 27002 – Controles de Seguridad de la Información:** Ofrece buenas prácticas para la implementación de controles administrativos, físicos y tecnológicos en los sistemas de información de FONDESER.

- **Reglamento General de Protección de Datos (GDPR) – Unión Europea:** Aunque no es de aplicación directa, sirve como referencia para reforzar las prácticas de consentimiento informado, transparencia y gestión de derechos de los titulares de datos personales.

- **NIST SP 800-53 – Controles de Seguridad y Privacidad:** Proporciona un marco técnico internacional para estructurar controles de ciberseguridad y gestión de riesgos tecnológicos aplicable al entorno digital de FONDESER.

2.3 Normativa Local e Instrumentos Institucionales

- **Política de Seguridad Digital de Colombia (CONPES 3975 de 2019):** Establece los lineamientos de la estrategia nacional de seguridad digital, que orientan a FONDESER en la gestión del riesgo cibernético, la protección de la información pública y la continuidad operativa.

- **Plan Estratégico de Tecnologías de la Información – PETI FONDESER 2025–2027:** Documento institucional que define las líneas estratégicas en materia de transformación digital, seguridad informática, interoperabilidad y sostenibilidad tecnológica.

- **Manual de Políticas de Seguridad de la Información de FONDESER:** Instrumento interno que establece los controles, roles y responsabilidades para el manejo seguro de la información financiera, crediticia y contractual.

- **Manual de Procesos y Procedimientos Administrativos y Financieros:** Documento que regula los procesos de crédito, interventoría y gestión administrativa, integrando prácticas de control interno y seguridad documental.

- **Código de Ética de FONDESER:** Define los deberes de los funcionarios y contratistas respecto al uso adecuado de la información, los recursos tecnológicos y la confidencialidad institucional.

- **Plan Anticorrupción y de Atención al Ciudadano de FONDESER:** Instrumento que operacionaliza los principios de transparencia, rendición de cuentas y participación ciudadana en la gestión de los recursos públicos y la información institucional.

2.4 Definiciones y Términos Clave

Activo de Información:

Cualquier dato, documento, archivo o sistema que posea valor para FONDESER y que requiera protección, incluyendo información física y digital.

Amenaza:
Cualquier evento o circunstancia que pueda afectar negativamente los activos de información de la entidad.

Confidencialidad:
Propiedad que garantiza que la información solo sea accesible a las personas autorizadas.

Disponibilidad:
Condición mediante la cual la información, los servicios y los sistemas se mantienen accesibles y operativos cuando se requieran.

Integridad:
Propiedad que asegura que los datos no sean alterados o modificados de forma no autorizada.

Datos Personales: Cualquier información vinculada o asociable a una persona natural identificada o identificable, tales como nombres, números de identificación, direcciones o datos financieros.

Datos Sensibles: Aquellos que afectan la intimidad del titular, como datos de salud, orientación política, creencias religiosas o información biométrica.

Incidente de Seguridad: Evento que compromete la confidencialidad, integridad o disponibilidad de la información institucional o personal.

Riesgo de Seguridad: Posibilidad de que una amenaza aproveche una vulnerabilidad y genere impacto negativo sobre los activos de información.

Sistema de Gestión de Seguridad de la Información (SGSI): Marco estructurado de políticas, procedimientos y controles, basado en estándares como la ISO/IEC 27001, para gestionar de forma eficaz los riesgos de seguridad.

Privacidad: Derecho fundamental que garantiza que los datos personales sean tratados con consentimiento y bajo las condiciones establecidas por la ley.

Usuario Autorizado: Persona a la que se le han concedido permisos para acceder y usar la información o los sistemas de FONDESER bajo las políticas de seguridad institucionales.

3. MARCO ESTRATÉGICO

El **Marco Estratégico del Plan de Seguridad y Privacidad de la Información de FONDESER 2025–2027** define los principios, objetivos y lineamientos que orientan la gestión integral de la seguridad y privacidad de la información en la entidad.

Este marco se fundamenta en el reconocimiento de la información como un activo institucional de alto valor, esencial para el cumplimiento de la misión social y financiera de FONDESER, y busca garantizar que todas las decisiones y acciones se adopten bajo criterios de responsabilidad, legalidad y mejora continua.

3.1 Principios Rectores

Los siguientes principios orientan las acciones y decisiones de FONDESER en materia de seguridad y privacidad de la información:

- **Confidencialidad:** Garantizar que la información sensible, técnica, contractual y personal solo sea accesible a usuarios autorizados.
- **Integridad:** Preservar la exactitud, completitud y confiabilidad de la información a lo largo de su ciclo de vida.
- **Disponibilidad:** Asegurar que los sistemas, aplicaciones, bases de datos y documentos estén accesibles cuando se requieran para las funciones institucionales.
- **Legalidad:** Cumplir con las leyes, decretos, políticas y normas nacionales e internacionales que regulan la seguridad de la información y la protección de datos personales.
- **Responsabilidad y Transparencia:** Promover el uso ético, seguro y responsable de la información pública, en coherencia con los valores institucionales y los principios del Código de Integridad del Servidor Público.
- **Mejora Continua:** Implementar procesos permanentes de evaluación, auditoría y fortalecimiento de los controles de seguridad y privacidad.

3.2 Relación con el Plan Estratégico de Tecnologías de la Información (PETI)

El **Plan de Seguridad y Privacidad de la Información (PSPI)** se articula directamente con el **Plan Estratégico de Tecnologías de la Información (PETI) de FONDESER 2025–2027**, asegurando la protección de los sistemas y datos que soportan las funciones institucionales.

Esta integración busca:

- Incorporar la seguridad como componente transversal en todos los proyectos tecnológicos.
- Garantizar que la innovación digital se realice con criterios de protección de datos y ciberseguridad.
- Mitigar los riesgos asociados a la implementación y operación de tecnologías.
- Fortalecer la gobernanza de la información mediante la interoperabilidad segura con la Alcaldía de El Retiro y otras entidades aliadas.

El PSPI se constituye, así, en un **pilar complementario del PETI**, contribuyendo al cumplimiento de los objetivos estratégicos institucionales de eficiencia, transparencia y confianza ciudadana.

3.3 Compromiso de la Alta Dirección

La Gerencia del **Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER** reafirma su compromiso con la protección de la información y la privacidad de los datos personales, garantizando la asignación de los recursos humanos, financieros y tecnológicos necesarios para la implementación y sostenimiento del presente plan.

El compromiso directivo se refleja en:

- **Liderazgo institucional:** Integrar la seguridad y privacidad como valores organizacionales.
- **Asignación de recursos:** Disponer de herramientas tecnológicas, personal capacitado y presupuesto específico para la gestión de seguridad.
- **Supervisión y seguimiento:** Evaluar periódicamente los avances del PSPI y adoptar medidas correctivas o de mejora.
- **Cumplimiento normativo:** Asegurar la observancia de las leyes y estándares aplicables.
- **Cultura organizacional:** Fomentar entre servidores y contratistas el uso responsable de la información y los medios tecnológicos.

3.4 Objetivos Estratégicos de Seguridad y Privacidad

1. Proteger los activos de información críticos para la gestión institucional y financiera de FONDESER.
2. Garantizar la confidencialidad, integridad y disponibilidad de la información.

3. Cumplir con las normas nacionales e internacionales sobre seguridad digital y protección de datos personales.
4. Promover la sensibilización y capacitación continua del personal en temas de seguridad y privacidad.
5. Reducir los riesgos y vulnerabilidades tecnológicas mediante la implementación de controles adecuados.
6. Asegurar la continuidad operativa ante incidentes, fallas o desastres tecnológicos.
7. Incorporar la seguridad de la información como elemento transversal del Sistema de Control Interno.

3.5 Gestión de Seguridad de la Información

La **Gestión de Seguridad de la Información** en FONDESER comprende el conjunto de políticas, procedimientos y controles destinados a proteger los activos de información de la entidad frente a riesgos internos y externos.

Se basa en el ciclo de mejora continua **(Planear – Hacer – Verificar – Actuar)**, conforme a la norma ISO/IEC 27001, e integra la gestión de riesgos como proceso central para la toma de decisiones en materia de seguridad.

Esta gestión incluye:

- Inventario y clasificación de activos de información.
- Identificación, evaluación y tratamiento de riesgos.
- Implementación de controles preventivos, detectivos y correctivos.
- Monitoreo de incidentes de seguridad.
- Cumplimiento normativo y auditorías internas.

3.6 Política de Seguridad de la Información

La **Política de Seguridad de la Información de FONDESER** tiene como propósito proteger los datos institucionales y personales de acuerdo con la legislación vigente y las mejores prácticas internacionales.

Sus lineamientos principales son:

- La información es un activo estratégico de FONDESER y debe ser protegida adecuadamente.
- Todos los funcionarios, contratistas y terceros con acceso a información institucional son responsables de su correcto uso.
- Se deben implementar controles proporcionales al nivel de riesgo de cada activo.
- El acceso a la información estará restringido y basado en roles y privilegios definidos.

- Toda actividad que involucre tratamiento de datos personales debe realizarse con consentimiento informado y bajo los principios de legalidad, finalidad y proporcionalidad.
- Las violaciones o incidentes de seguridad deberán ser reportadas de inmediato a la Gerencia y a Control Interno.

3.7 Roles y Responsabilidades

FONDESER establece roles específicos para garantizar una gestión efectiva de la seguridad y privacidad de la información:

3.7.1 Responsable de Seguridad de la Información:
La **Gerencia de FONDESER** liderará la implementación, supervisión y actualización del PSPI, coordinando acciones con el área de apoyo tecnológico y con la Oficina de Control Interno del Municipio de El Retiro.

3.7.2 Propietarios de la Información:
Cada dependencia administrativa o técnica será responsable de la integridad, disponibilidad y actualización de los datos que genera o gestiona (ej. cartera de créditos, interventorías, informes financieros, convenios, etc.).

3.7.3 Usuarios de la Información:
Funcionarios y contratistas que acceden a los sistemas o documentos institucionales deberán hacerlo conforme a las políticas de seguridad, garantizando la confidencialidad y uso adecuado de la información.

3.7.4 Proveedores y Contratistas:
Toda persona natural o jurídica que preste servicios a FONDESER deberá firmar cláusulas de confidencialidad y cumplir con las disposiciones del presente plan.

3.8 Análisis y Gestión de Riesgos

FONDESER adopta un modelo de gestión de riesgos que identifica, analiza y mitiga las amenazas que pueden comprometer los activos de información.

El proceso incluye:

1. **Identificación de activos de información** (documentos, sistemas, bases de datos, archivos físicos y digitales).
2. **Valoración de amenazas y vulnerabilidades** (errores humanos, ciberataques, pérdida de equipos, manipulación indebida, siniestros, etc.).
3. **Evaluación del impacto** en términos de confidencialidad, integridad y disponibilidad.
4. **Diseño de medidas de control** para prevenir o mitigar los riesgos detectados.
5. **Seguimiento y mejora continua** con apoyo de la Oficina de Control Interno y el área TIC.

A continuación, se presenta una muestra de los activos más representativos de FONDESER y su gestión de riesgos:

Tabla 1. Activos de Información – FONDESER

N.º	Activo de Información	Descripción
1	Base de datos de créditos y beneficiarios	Contiene información personal, financiera y crediticia de los usuarios atendidos por FONDESER.
2	Informes de interventoría y consultoría	Documentos técnicos con datos de obras, contratistas y supervisión de proyectos.
3	Contratos de prestación de servicios	Acuerdos jurídicos con profesionales y entidades aliadas.
4	Estados financieros y contables	Información sobre ingresos, egresos, cartera y resultados operativos.
5	Correspondencia y comunicaciones oficiales	Documentos internos y externos que reflejan la gestión institucional.
6	Historias laborales y hojas de vida	Información confidencial del personal vinculado a la entidad.
7	Convenios con la Alcaldía de El Retiro	Acuerdos interadministrativos para ejecución de proyectos.
8	Informes de gestión y de control interno	Evidencian el desempeño institucional y cumplimiento de metas.
9	Documentación de proyectos de infraestructura	Planos, presupuestos, informes de avance y soportes técnicos.
10	Manuales, políticas y procedimientos internos	Normas internas para la gestión administrativa y técnica.

3.9 Evaluación de Amenazas, Vulnerabilidades e Impacto

Tabla 2. Riesgos Identificados y Controles Propuestos

N.º	Riesgo	Descripción	Impacto	Control o Acción Preventiva
1	Pérdida de información de créditos por fallas técnicas	Daños en equipos o servidores pueden afectar bases de datos financieras.	Alto	Copias de seguridad semanales en almacenamiento externo seguro.

N.º	Riesgo	Descripción	Impacto	Control o Acción Preventiva
2	Acceso no autorizado a datos personales	Usuarios sin privilegios podrían acceder a información sensible.	Alto	Control de accesos con contraseñas seguras y autenticación multifactor.
3	Manipulación indebida de documentos físicos	Riesgo de alteración o pérdida de documentos en archivo.	Medio	Capacitación y supervisión permanente en gestión documental.
4	Ciberataques o malware	Intentos externos de vulnerar los sistemas de FONDESER.	Alto	Antivirus actualizado, cortafuegos, monitoreo de red y políticas de respaldo.
5	Divulgación no autorizada de información institucional	Filtración de datos a terceros o redes sociales.	Alto	Políticas de confidencialidad y sanciones disciplinarias.
6	Errores humanos en el manejo de información	Omisiones o uso inadecuado por parte de funcionarios.	Medio	Capacitación periódica y doble verificación de procesos.
7	Siniestros o daños físicos (incendios, inundaciones)	Destrucción de archivos físicos o equipos.	Alto	Plan de contingencia y almacenamiento en lugares seguros.

4. CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

La información gestionada por el **Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER** constituye un activo esencial para el cumplimiento de su misión institucional. Por ello, su clasificación y manejo deben regirse por criterios uniformes de seguridad, confidencialidad y trazabilidad.

4.1 Clasificación de la Información

Toda la información que se genera, recibe o administra en FONDESER se clasifica en cuatro niveles:

Nivel	Tipo de Información	Descripción	Acceso
1. Pública	Información de libre acceso	Datos que pueden ser conocidos por cualquier ciudadano (p. ej., informes de gestión, contratos publicados en SECOP, informes financieros consolidados).	Libre acceso conforme a la Ley 1712 de 2014.
2. Interna	Información de uso institucional	Datos utilizados dentro de la entidad para procesos administrativos o técnicos, sin ser confidenciales.	Solo empleados y contratistas autorizados.

Nivel	Tipo de Información	Descripción	Acceso
3. Confidencial	Información restringida	Contiene datos personales, financieros o estratégicos. Su divulgación puede afectar la entidad o a terceros.	Acceso limitado según roles y autorización.
4. Reservada	Información crítica o sensible	Involucra secretos industriales, datos de seguridad informática o información protegida por ley.	Acceso exclusivo de la Gerencia y Control Interno.

4.2 Manejo de la Información

- Toda la documentación deberá registrarse y custodiarse conforme a las **Tablas de Retención Documental (TRD)** aprobadas por FONDESER.
- La digitalización de archivos se realizará bajo protocolos de **seguridad, trazabilidad y respaldo**.
- Los documentos físicos deben almacenarse en lugares seguros, con control de acceso y condiciones ambientales adecuadas.
- Los archivos digitales deben conservarse en servidores institucionales con **copias de seguridad y acceso autenticado**.
- Se prohíbe la copia o traslado de información institucional a dispositivos personales o no autorizados.
- Toda eliminación de información debe realizarse de forma **segura e irreversible**, conforme a los procedimientos de eliminación segura definidos por la entidad.

5. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Los **controles de seguridad de la información de FONDESER** comprenden un conjunto de medidas **administrativas, técnicas y operativas** orientadas a proteger los activos informáticos, garantizar la continuidad del servicio y cumplir con las disposiciones legales y normativas.

5.1 Controles Administrativos

Estos controles están enfocados en la estructura organizacional, la gestión del talento humano y la adopción de políticas internas de seguridad.

5.1.1 Políticas y Procedimientos

- Implementación de una **Política Institucional de Seguridad y Privacidad** actualizada anualmente.
- Procedimientos claros para la creación, clasificación, manejo, transferencia y eliminación de la información.
- Inclusión de cláusulas de confidencialidad y seguridad en todos los contratos laborales y de prestación de servicios.

5.1.2 Gestión de Roles y Responsabilidades

- Asignación formal de roles de seguridad y privacidad en cada dependencia.
- Responsabilidad compartida entre la Gerencia, Control Interno y el área de apoyo administrativo y financiero.
- Seguimiento al cumplimiento mediante auditorías internas.

5.1.3 Concienciación y Capacitación

- Realización de programas anuales de capacitación sobre **seguridad digital, ciberseguridad y protección de datos personales**.
- Sensibilización sobre los riesgos del phishing, malware y pérdida de información.
- Divulgación de guías prácticas y boletines informativos.

5.1.4 Gestión de Riesgos

- Identificación continua de vulnerabilidades mediante revisiones semestrales.
- Actualización del mapa de riesgos del PETI y del Sistema de Control Interno.
- Ejecución de planes de tratamiento de riesgos tecnológicos y de privacidad.

5.1.5 Gestión de Proveedores

- Inclusión de cláusulas de seguridad en los contratos con terceros que manejen información o infraestructura tecnológica.
- Auditorías o revisiones aleatorias a proveedores con acceso a información crítica.
- Evaluación de cumplimiento normativo antes de la suscripción de contratos.

5.2 Controles Técnicos

Estos controles están orientados al uso de tecnologías seguras, protección de redes, bases de datos, sistemas y equipos informáticos.

5.2.1 Control de Accesos

- Implementación de políticas de **contraseñas robustas** y renovables cada 90 días.
- Aplicación del principio de **privilegio mínimo**: los usuarios solo tendrán acceso a la información necesaria para sus funciones.
- Autenticación multifactor (MFA) para el ingreso a sistemas críticos.

5.2.2 Seguridad en Redes

- Uso de **firewalls, antivirus corporativos y filtros antimalware**.
- Segmentación de redes para proteger los ambientes administrativos, contables y financieros.
- Prohibición de acceso remoto no autorizado a los sistemas institucionales.

5.2.3 Protección de Endpoints

- Instalación y actualización constante de antivirus y herramientas antimalware.
- Bloqueo automático de sesiones inactivas.

- Supervisión del estado de los equipos mediante inventarios y revisiones periódicas.

5.2.4 Cifrado de Información

- Encriptación de datos sensibles almacenados o transmitidos por medios digitales.
- Cifrado de dispositivos portátiles y medios removibles utilizados por la entidad.

5.2.5 Copias de Seguridad (Backups)

- Realización de copias de seguridad semanales, almacenadas en medios seguros fuera de la red principal.
- Pruebas periódicas de restauración para garantizar la disponibilidad de los datos.

5.2.6 Monitoreo y Auditoría

- Implementación de registros de actividad (logs) en los sistemas institucionales.
- Revisión de accesos, modificaciones y eliminaciones de información sensible.
- Auditorías semestrales de seguridad tecnológica.

5.2.7 Gestión de Vulnerabilidades

- Escaneo periódico de vulnerabilidades en equipos y sistemas.
- Aplicación oportuna de parches y actualizaciones de seguridad.
- Evaluación técnica de nuevos sistemas antes de su puesta en marcha.

5.3 Controles Operativos

Estos controles se orientan a garantizar la operación segura y continua de los procesos institucionales.

5.3.1 Gestión de Incidentes de Seguridad

- Creación de un protocolo interno de reporte y atención de incidentes.
- Registro y análisis de todos los eventos relacionados con la pérdida, alteración o divulgación de información.
- Comunicación inmediata a la Gerencia y Control Interno.

5.3.2 Continuidad del Negocio y Recuperación ante Desastres

- Elaboración y actualización anual del **Plan de Continuidad del Negocio (PCN)**.
- Copias redundantes de información crítica en medios físicos y digitales.
- Pruebas semestrales de restauración y simulacros de contingencia.

5.3.3 Gestión del Cambio

- Control sobre las modificaciones de hardware, software y redes.
- Registro de todos los cambios con autorización de la Gerencia.
- Verificación de impacto antes de implementar cambios tecnológicos.

5.3.4 Control de Movilidad

- Regulación del uso de equipos portátiles, memorias USB y dispositivos móviles institucionales.

- Configuración de políticas de acceso remoto seguro mediante VPN.
- Prohibición del almacenamiento de información institucional en dispositivos personales.

5.3.5 Eliminación Segura de Información

- Eliminación de datos mediante **borrado criptográfico** o destrucción física de medios.
- Documentación del proceso de eliminación para efectos de auditoría.
- Supervisión por parte del área administrativa o Control Interno.

5.4 Control de Privacidad

Los controles de privacidad buscan garantizar el cumplimiento de la **Ley 1581 de 2012** y las políticas internas de tratamiento de datos personales.

5.4.1 Principios de Protección de Datos

- Legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.
- Tratamiento de datos únicamente con el consentimiento informado del titular.

5.4.2 Consentimiento y Autorización

- Obtención de autorizaciones escritas o electrónicas antes del tratamiento de datos personales.
- Conservación de los registros de autorización en formato físico o digital.

5.4.3 Derechos de los Titulares

- Garantía del derecho de los titulares a acceder, corregir, suprimir o revocar la autorización sobre sus datos.
- Atención oportuna a solicitudes a través de los canales institucionales de FONDESER.

5.4.4 Evaluaciones de Impacto en la Privacidad (PIA)

- Evaluación de riesgos en proyectos o procesos que involucren tratamiento de datos personales.
- Adopción de medidas preventivas y correctivas en función del nivel de riesgo identificado.

5.4.5 Transferencia Segura de Información

- Verificación de que toda transferencia de datos personales a terceros cumpla con los requisitos legales.
- Establecimiento de acuerdos de confidencialidad con entidades receptoras.

6. PROTECCIÓN DE LA PRIVACIDAD

El **Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER**, en cumplimiento de la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás normas complementarias, garantiza la protección integral de los datos personales que administra,

asegurando que su tratamiento se realice bajo los principios de legalidad, transparencia y responsabilidad.

6.1 Principios para el Tratamiento de Datos Personales

FONDESER se compromete a garantizar los siguientes principios en la gestión de la información personal:

- **Legalidad:** El tratamiento de los datos personales se realizará conforme a las disposiciones legales vigentes.
- **Finalidad:** Los datos personales serán recolectados y tratados únicamente para fines legítimos, específicos y previamente informados al titular.
- **Libertad:** El tratamiento se efectuará solo con el consentimiento previo, expreso e informado del titular.
- **Veracidad:** La información será veraz, completa, exacta, actualizada y comprobable.
- **Transparencia:** Se garantizará a los titulares el derecho a conocer, en cualquier momento, la información que se haya recolectado sobre ellos.
- **Acceso y Circulación Restringida:** El tratamiento estará limitado al cumplimiento de los fines autorizados.
- **Seguridad:** Se adoptarán medidas técnicas, humanas y administrativas para evitar pérdida, alteración o uso indebido de la información.
- **Confidencialidad:** Toda persona con acceso a datos personales deberá mantener reserva sobre ellos incluso después de terminada su relación con la entidad.

6.2 Derechos de los Titulares de la Información

FONDESER garantiza a los titulares de datos personales el ejercicio de los siguientes derechos:

1. Conocer, actualizar y rectificar sus datos personales.
2. Solicitar prueba de la autorización otorgada para su tratamiento.
3. Ser informado sobre el uso que se ha dado a sus datos.
4. Presentar quejas ante la Superintendencia de Industria y Comercio en caso de infracción.
5. Revocar la autorización y/o solicitar la supresión del dato.
6. Acceder de manera gratuita a sus datos personales tratados por la entidad.

6.3 Políticas y Procedimientos para la Protección de la Privacidad

6.3.1 Política de Tratamiento de Datos Personales

FONDESER cuenta con una **Política de Tratamiento de Datos Personales** que establece los lineamientos sobre recolección, almacenamiento, uso, circulación y supresión de

información personal.
Esta política es pública y se encuentra disponible en los medios institucionales.

6.3.2 Consentimiento Informado
El tratamiento de datos personales requiere la autorización previa, expresa e informada del titular, mediante documentos físicos o electrónicos debidamente firmados o verificados.

6.3.3 Avisos de Privacidad
FONDESER publica y comunica a los titulares los **avisos de privacidad**, informando las finalidades específicas del tratamiento y los derechos de los titulares.

6.3.4 Evaluación de Impacto en la Privacidad (PIA)
En todos los proyectos tecnológicos o administrativos que impliquen tratamiento de datos personales, se realiza una **Evaluación de Impacto** que permita anticipar riesgos y definir medidas de mitigación.

6.3.5 Gestión Segura de la Información Personal
Los datos personales se almacenan en servidores institucionales bajo mecanismos de seguridad, acceso restringido, cifrado y respaldo periódico.

6.3.6 Transferencia y Comunicación de Datos Personales
Las transferencias o transmisiones de datos personales a terceros nacionales o internacionales deberán cumplir los principios y requisitos establecidos por la ley y contar con autorización del titular.

6.3.7 Eliminación Segura de Datos
Una vez cumplida la finalidad del tratamiento, o cuando el titular solicite la eliminación de sus datos, estos serán suprimidos de forma segura, sin posibilidad de recuperación.

6.4 Medidas de Seguridad en la Protección de Datos Personales

FONDESER implementa medidas tecnológicas y administrativas para garantizar la seguridad de los datos personales, tales como:

- Cifrado de la información almacenada y transmitida.
- Autenticación multifactor en el acceso a sistemas que contengan datos personales.
- Registro de accesos, consultas y modificaciones.
- Auditorías internas periódicas sobre la gestión de la información.
- Formación continua en protección de datos personales para funcionarios y contratistas.

6.5 Respuesta a Incidentes de Privacidad

FONDESER establece un protocolo de actuación ante incidentes de seguridad o violaciones de datos personales que comprende las siguientes etapas:

1. **Detección:** Identificación del incidente y su impacto.
2. **Notificación:** Comunicación inmediata al responsable de seguridad y a la Gerencia.

3. **Contención:** Medidas inmediatas para detener la exposición o pérdida de información.
4. **Investigación:** Análisis de causas y responsables.
5. **Mitigación:** Acciones correctivas y preventivas.
6. **Comunicación a los titulares y autoridades:** Cuando el incidente afecte datos personales sensibles.

6.6 Cumplimiento Legal y Normativo

FONDESER asegura el cumplimiento de las normas nacionales e internacionales aplicables, incluyendo:

- **Ley 1581 de 2012 y Decreto 1377 de 2013.**
- **Ley 1273 de 2009 (Delitos Informáticos).**
- **ISO/IEC 27701 (Gestión de Privacidad de la Información).**
- **Circulares de la Superintendencia de Industria y Comercio (SIC).**

7. CAPACITACIÓN Y SENSIBILIZACIÓN

FONDESER reconoce que la gestión de la seguridad y privacidad de la información requiere la participación activa de todo el personal.

Por tanto, se desarrollarán programas de **capacitación y sensibilización** dirigidos a empleados, contratistas y aliados estratégicos, enfocados en:

- Buenas prácticas de ciberseguridad y manejo de información.
- Políticas institucionales de seguridad digital y confidencialidad.
- Uso responsable de correos electrónicos, contraseñas y dispositivos móviles.
- Manejo adecuado de datos personales conforme a la ley.
- Simulacros de respuesta ante incidentes tecnológicos o de privacidad.

La Gerencia y el área de Control Interno harán seguimiento anual al cumplimiento de estos programas.

8. EVALUACIÓN Y MEJORA CONTINUA

El seguimiento y control del presente plan estará articulado con el **Plan Estratégico de Tecnologías de la Información (PETI) 2025–2027** y con el **Sistema de Control Interno de FONDESER**.

La evaluación se realizará mediante:

- **Revisiones semestrales** del nivel de cumplimiento de los objetivos del plan.

- **Auditorías internas** en materia de seguridad de la información y protección de datos.
- **Actualización del mapa de riesgos tecnológicos** conforme a los resultados del seguimiento.
- **Indicadores de gestión**, tales como:
    - Porcentaje de incidentes atendidos y solucionados.
    - Nivel de cumplimiento de los planes de respaldo y contingencia.
    - Grado de implementación de controles de acceso y cifrado.
    - Cumplimiento de capacitaciones programadas.

Los resultados serán documentados y presentados a la Gerencia y a la Oficina de Control Interno, promoviendo la mejora continua.

9. ANEXOS

Anexo 1. Mapa de Riesgos de Seguridad y Privacidad de la Información – FONDESER 2025.
Anexo 2. Tablas de Retención Documental y Clasificación de Información.
Anexo 3. Política de Tratamiento de Datos Personales.
Anexo 4. Procedimiento de Atención de Incidentes de Seguridad de la Información.

(Los anexos podrán ser actualizados anualmente según los cambios tecnológicos o normativos.)

10. REFERENCIAS

- Consejo Nacional de Política Económica y Social. (2019). *CONPES 3975 de 2019: Política Nacional de Seguridad Digital.* Departamento Nacional de Planeación.
- Congreso de la República de Colombia. (2000). *Ley 594 de 2000: Por la cual se dicta la Ley General de Archivos.* Diario Oficial No. 44.093.
- Congreso de la República de Colombia. (2009). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado – la protección de la información y de los datos.* Diario Oficial No. 47.223.
- 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.
- Congreso de la República de Colombia. (2014). *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.
- Ministerio de Tecnologías de la Información y las Comunicaciones. (2024). *Manual de Gobierno Digital.* República de Colombia.

- Presidencia de la República de Colombia. (2013). *Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.* Diario Oficial No. 48.834.

- Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER. (2025). *Plan Estratégico de Tecnologías de la Información 2025–2027 (PETI FONDESER).* El Retiro, Antioquia.

- International Organization for Standardization. (2013). *ISO/IEC 27001:2013 – Information security management systems — Requirements.* ISO.

- International Organization for Standardization. (2019). *ISO/IEC 27701:2019 – Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.* ISO.

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