RESOLUCIÓN NÚMERO 094
DICIEMBRE 30 DE 2025

"POR LA CUAL SE ADOPTA EL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PTRSPI) 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, la Ley 87 de 1993, la Ley 489 de 1998, la Ley 1581 de 2012, la Ley 1712 de 2014, 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, y demás normas concordantes y complementarias,

CONSIDERANDO:

Que el artículo 209 de la Constitución Política de Colombia 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 las normas para el ejercicio del control interno en las entidades del Estado, exigiendo la implementación de mecanismos de prevención, mitigación y control de riesgos en los procesos institucionales.

Que la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013 regulan la protección de los datos personales, disponiendo la adopción de medidas técnicas, humanas y administrativas necesarias para garantizar su seguridad y evitar su adulteración, pérdida o acceso no autorizado.

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

Que el Decreto 1078 de 2015 y el Decreto 612 de 2018 establecen las directrices para la gestión de la información, la seguridad digital y la implementación de políticas de gobierno digital en el sector público.

Que el Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER, en cumplimiento de la normativa mencionada y en articulación con el Modelo Integrado de Planeación y Gestión (MIPG) y el Plan Estratégico de Tecnologías de la Información (PETI 2025–2028), ha formulado su Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI) 2025–2027, como instrumento de planeación que establece las acciones,

controles, responsables y mecanismos de seguimiento orientados a garantizar la protección integral de la información institucional y de los datos personales bajo su custodia.

Que el PTRSPI permite fortalecer la gestión de riesgos tecnológicos, físicos, humanos y organizacionales, mediante la aplicación de buenas prácticas, la sensibilización del personal y la implementación de controles de seguridad acordes con las normas internacionales ISO/IEC 27001 y las guías del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Que en virtud de lo anterior, se considera pertinente adoptar formalmente el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI) 2025–2027, como instrumento técnico-administrativo de obligatorio cumplimiento en FONDESER.

RESUELVE:

ARTÍCULO PRIMERO. ADOPCIÓN DEL PTRSPI.
Adóptese el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI) 2025–2027 del Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER, como instrumento de planeación, gestión y control para la protección de los activos de información institucional, el cual hace parte integral de la presente resolución.

ARTÍCULO SEGUNDO. OBJETIVO.
El PTRSPI tiene como objetivo establecer las estrategias, acciones y controles necesarios para mitigar, transferir, aceptar o eliminar los riesgos que puedan afectar la seguridad, confidencialidad, integridad, disponibilidad y privacidad de la información en FONDESER.

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 funciones, manejen información institucional o datos personales.
Las dependencias deberán garantizar la aplicación de los controles definidos en el PTRSPI dentro de sus procesos, procedimientos y proyectos tecnológicos**.**

ARTÍCULO CUARTO. IMPLEMENTACIÓN Y SOCIALIZACIÓN.
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 PTRSPI.
Su socialización se realizará mediante:

- Publicación en la página web institucional de FONDESER.
- Capacitaciones y jornadas de sensibilización dirigidas a funcionarios y contratistas.
- Circulares y comunicados institucionales que promuevan la cultura de seguridad de la información.

ARTÍCULO QUINTO. SEGUIMIENTO Y EVALUACIÓN.
La Oficina de Control Interno y el responsable de Tecnología realizarán el seguimiento semestral y la evaluación anual del PTRSPI, conforme a los indicadores definidos en el propio plan.

Los resultados del seguimiento deberán incorporarse en los informes de control interno, auditorías y gestión institucional, así como en el marco del MIPG y el PETI.

ARTÍCULO SEXTO. MEJORA CONTINUA.
El PTRSPI será revisado y actualizado anualmente, o cuando se presenten cambios normativos, tecnológicos o institucionales que lo ameriten, garantizando la mejora continua en la gestión de riesgos de 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 periodo 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 TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – PTRSPI 2025–2027

ÍNDICE

1. INTRODUCCIÓN

El **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI)** es un instrumento estratégico que establece las acciones y controles necesarios para **identificar, evaluar, tratar y mitigar** los riesgos que puedan comprometer la **confidencialidad, integridad y disponibilidad** de la información institucional. Estas tres dimensiones constituyen los **pilares fundamentales de la seguridad de la información**:

- **Confidencialidad:** Garantiza que la información solo sea accesible por las personas autorizadas.
- **Integridad:** Asegura que los datos sean exactos, completos y no se modifiquen de forma indebida.
- **Disponibilidad:** Permite que la información esté accesible y utilizable cuando se necesite.

El **Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER**, como **entidad descentralizada de economía mixta adscrita a la Alcaldía de El Retiro**, tiene entre sus funciones principales la **administración de programas de crédito social**, la **interventoría y consultoría de proyectos**, así como la **ejecución de obras de infraestructura comunitaria**.
En el cumplimiento de estas funciones, la entidad gestiona información de carácter **financiero, técnico, contractual y personal**, la cual es considerada sensible por su relevancia para los ciudadanos, contratistas y la gestión pública.

En este contexto, la **gestión de riesgos en seguridad y privacidad de la información** resulta fundamental para mantener la **confianza ciudadana**, fortalecer la **transparencia institucional** y asegurar la **continuidad de los servicios públicos**.

El presente Plan se fundamenta en metodologías y normas reconocidas a nivel nacional e internacional, entre ellas:

- **MAGERIT v3 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información):** Herramienta desarrollada por el Gobierno de España que orienta el proceso de identificación, evaluación y tratamiento de riesgos asociados a los sistemas de información.
- **ISO/IEC 27001:2013:** Norma internacional emitida por la **Organización Internacional de Normalización (ISO)** y la **Comisión Electrotécnica Internacional (IEC)**, que establece los requisitos para implementar, mantener y mejorar un **Sistema de Gestión de Seguridad de la Información (SGSI)**.
- **Normativa colombiana vigente:** especialmente la **Ley 1581 de 2012** y sus decretos reglamentarios sobre **protección de datos personales**, el **Decreto 1008 de 2018** sobre **seguridad digital**, y los lineamientos del **Modelo de Seguridad y Privacidad de la Información (MSPI)** definidos por el **Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)**.

El PTRSPI constituye, además, un **componente esencial del Plan Estratégico de Tecnologías de la Información (PETI) 2025–2027** y del **Modelo Integrado de Planeación y Gestión (MIPG)**.

- El **PETI** (Plan Estratégico de Tecnologías de la Información) define la hoja de ruta para el uso estratégico y seguro de las tecnologías en la entidad.

- El **MIPG** (Modelo Integrado de Planeación y Gestión) es la política marco del Estado colombiano que integra la planeación, la gestión y la evaluación del desempeño institucional para promover la eficiencia, la transparencia y el servicio al ciudadano.

En conjunto, este plan promueve una **cultura institucional de seguridad, corresponsabilidad y mejora continua**, orientada a proteger los activos de información de FONDESER y garantizar la correcta gestión del conocimiento dentro de todos los procesos de la entidad.

2. ALCANCE

El **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI)** aplica a todos los **procesos, áreas, funcionarios, contratistas y sistemas de información** del **Fondo de Desarrollo Social del Municipio de El Retiro – FONDESER**, que intervienen en la generación, manejo, almacenamiento, transmisión o eliminación de información institucional.

Su alcance comprende los siguientes componentes:

1. **Procesos institucionales:** Incluye los procesos misionales (crédito social, interventoría, consultoría y ejecución de proyectos de infraestructura), así como los procesos de apoyo y de control interno, los cuales involucran la administración y tratamiento de datos sensibles, financieros, técnicos y personales.

2. **Activos de información:** Cubre todos los elementos que poseen valor para la entidad, tales como bases de datos, archivos físicos y digitales, sistemas informáticos, redes de comunicación, aplicaciones, equipos tecnológicos y el conocimiento del talento humano.

3. **Usuarios internos y externos:** Abarca a todos los servidores públicos, contratistas, proveedores y demás actores que tengan acceso a la información institucional o a los sistemas que la soportan, garantizando el cumplimiento de las políticas de seguridad y privacidad establecidas por FONDESER.

4. **Infraestructura tecnológica:** Incluye los equipos, redes, software, plataformas en la nube y servicios tecnológicos utilizados en la operación institucional.

5. **Cumplimiento normativo:** Se alinea con las disposiciones legales y reglamentarias nacionales en materia de protección de datos personales, seguridad digital, gestión documental, gobierno digital y transparencia.

En consecuencia, el PTRSPI es de **obligatorio cumplimiento** para todo el personal vinculado a la entidad, cualquiera sea su modalidad de contratación o nivel jerárquico, y se articula con otros instrumentos institucionales como el **Plan Estratégico de Tecnologías de la Información (PETI)**, el **Modelo Integrado de Planeación y Gestión (MIPG)** y el **Modelo de Seguridad y Privacidad de la Información (MSPI)** del MinTIC.

3. PROPÓSITO

El presente **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI)** tiene como propósito establecer un **marco formal, sistemático, preventivo y permanentemente actualizado** que oriente la **identificación, evaluación, priorización y tratamiento** de los riesgos que puedan afectar la información institucional de FONDESER.

Este plan abarca todos los **activos de información**, entendidos como los recursos que poseen valor para la entidad, incluyendo **datos, documentos, sistemas informáticos, equipos tecnológicos, infraestructura física y conocimiento del personal**. Asimismo, contempla los **procesos operativos, tecnológicos, administrativos y misionales**, asegurando que todos los componentes estratégicos y de soporte estén protegidos frente a posibles vulnerabilidades.

El PTRSPI busca **reducir la probabilidad de ocurrencia y el impacto de los incidentes** relacionados con la seguridad y privacidad de la información, fortaleciendo la **resiliencia institucional** —es decir, la capacidad de la entidad para anticiparse, resistir, responder y recuperarse ante situaciones adversas—.
De esta forma, se garantiza la **continuidad del negocio y la prestación ininterrumpida de los servicios públicos**, incluso ante eventos o amenazas de tipo:

- **Tecnológico:** como ciberataques, virus informáticos, fallas en los sistemas o pérdida de datos.
- **Físico:** como incendios, daños en equipos, cortes de energía o desastres naturales.
- **Humano:** como errores involuntarios, negligencia, mal uso de la información o actos intencionales.
- **Organizacional:** como fallas en los procedimientos, falta de controles internos o deficiencias en la gestión administrativa.

Además, este plan promueve el desarrollo de una **cultura institucional de gestión proactiva del riesgo**, donde cada **servidor público, contratista y colaborador de FONDESER** asuma un rol activo en la **protección de los activos de información** y en la correcta aplicación de las **políticas de seguridad digital y privacidad de los datos**.

En este sentido, el PTRSPI refuerza los **principios de transparencia, legalidad, eficiencia administrativa y responsabilidad pública**, consolidando un entorno organizacional confiable y seguro que respalde la misión social de FONDESER y su compromiso con la comunidad del Municipio de El Retiro.

4. OBJETIVOS

Objetivo General

Establecer las estrategias, medidas y controles necesarios para **gestionar de manera integral los riesgos de seguridad y privacidad de la información** en FONDESER, garantizando la **protección de los activos de información**, el **cumplimiento normativo** y la **continuidad de los procesos institucionales** frente a amenazas internas o externas.

Objetivos Específicos

- **Identificar, analizar y evaluar** los riesgos que puedan afectar la seguridad y privacidad de la información institucional, determinando su probabilidad, impacto y nivel de criticidad, con el fin de establecer controles y acciones de mitigación adecuados.

- **Implementar medidas técnicas, administrativas y organizacionales** que fortalezcan la protección de los activos de información, garanticen la continuidad operativa de los procesos misionales y aseguren el cumplimiento de la normativa vigente en materia de seguridad digital y protección de datos personales.

- **Fomentar una cultura institucional de seguridad y corresponsabilidad**, en la que los servidores públicos, contratistas y aliados estratégicos participen activamente en la gestión del riesgo, promoviendo la transparencia, la eficiencia y la mejora continua en la administración de la información.

5. USUARIOS

- **Gerente General:** Responsable de la aprobación, adopción y supervisión del cumplimiento del plan.

- **Asores Control Interno:** Acompaña la evaluación, seguimiento y mejora continua del PTRSPI.

- **Líderes de proceso:** Identifican riesgos, aplican los controles definidos y reportan incidentes.

- **Contratistas y funcionarios:** Cumplen los lineamientos del plan y protegen la información que manejan.

- **Aliados y proveedores:** Deben garantizar la aplicación de medidas de seguridad acordes con los estándares institucionales.
-

6. MARCO NORMATIVO Y DOCUMENTOS DE REFERENCIA

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI) se fundamenta en el marco jurídico colombiano, así como en estándares internacionales reconocidos que orientan la gestión integral de la seguridad de la información, la protección de datos personales y la transparencia institucional.

Normatividad Colombiana aplicable

- **Ley 1581 de 2012:**
  Por la cual se dictan disposiciones generales para la protección de datos personales.
  Establece los principios, derechos y procedimientos para el tratamiento legítimo de la información personal, garantizando la privacidad y el control de los titulares sobre sus datos.

- **Decreto 1377 de 2013:**
  Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
  Define los lineamientos para la implementación de políticas de tratamiento de datos personales, así como las medidas para la obtención de autorizaciones, manejo de

bases de datos y deberes de los responsables y encargados del tratamiento.

- **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.
  Regula el acceso de los ciudadanos a la información pública, estableciendo obligaciones de publicidad activa y protección de información reservada o clasificada.

- **Decreto 612 de 2018:**
  Por el cual se establecen directrices para la integración de los planes institucionales y estratégicos al Modelo Integrado de Planeación y Gestión (MIPG).
  Dispone la articulación del PTRSPI con los demás instrumentos de gestión institucional, fortaleciendo la planeación estratégica y la rendición de cuentas.

- **Decreto 1078 de 2015:**
  Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones (TIC).
  Compila la normativa relacionada con la gestión de la seguridad digital, la infraestructura tecnológica y la protección de la información pública.

- **Decreto 620 de 2020:**
  Por el cual se actualiza la Política de Gobierno Digital.
  Promueve el uso seguro, eficiente y responsable de las tecnologías de la información en las entidades del Estado, priorizando la protección de los datos personales y la gestión de riesgos digitales.

Referencias técnicas internacionales

- **ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información (SGSI):**
  Norma internacional que establece los requisitos para implementar, mantener y mejorar un sistema de gestión de seguridad de la información, garantizando la confidencialidad, integridad y disponibilidad de los datos.

- **ISO/IEC 27002:2022 – Controles de Seguridad de la Información:**
  Proporciona un conjunto de controles, buenas prácticas y directrices para gestionar los riesgos asociados a la seguridad de la información dentro de las organizaciones.

- **ISO/IEC 27005:2018 – Gestión del Riesgo de Seguridad de la Información:**
  Complementa la norma ISO 27001, proporcionando metodologías para la identificación, evaluación y tratamiento de riesgos relacionados con la información.

- **MAGERIT v3 – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información:**
  Desarrollada por el Gobierno de España, orienta la valoración de activos, amenazas, vulnerabilidades y salvaguardas, sirviendo como referencia para la administración pública en la gestión del riesgo informático.

- **Guía de Seguridad y Privacidad de la Información – MinTIC:**
  Documento técnico del Ministerio TIC que orienta la implementación de controles de seguridad, la gestión de incidentes y la protección de datos personales en entidades del Estado colombiano.

7. DEFINICIONES

Activo de información:
Conjunto de datos, documentos, sistemas, equipos, aplicaciones o recursos que tienen valor para la entidad y deben ser protegidos frente a amenazas o pérdidas.

Amenaza:
Cualquier evento, acción o circunstancia que pueda causar daño a los activos de información, vulnerar su confidencialidad, integridad o disponibilidad.

Análisis de riesgos:
Proceso mediante el cual se identifican, valoran y priorizan los riesgos que afectan la seguridad de la información, con base en su probabilidad e impacto.

Autenticación:
Mecanismo que permite verificar la identidad de un usuario o sistema antes de otorgarle acceso a recursos de información.

Backup (copia de seguridad):
Duplicado de información crítica que se almacena de forma segura para garantizar su recuperación en caso de pérdida, daño o incidente.

Confidencialidad:
Principio de la seguridad de la información que garantiza que los datos solo sean accesibles a las personas autorizadas.

Control:
Medida técnica, administrativa o física implementada para prevenir, detectar o mitigar un riesgo o amenaza.

Ciberseguridad:
Conjunto de prácticas, tecnologías y procesos diseñados para proteger los sistemas informáticos, redes y datos frente a ataques o accesos no autorizados.

Disponibilidad:
Atributo de la información que asegura que los usuarios autorizados puedan acceder a ella cuando sea necesario.

Evaluación de riesgos:
Etapa en la que se analizan los resultados del análisis de riesgos para priorizar las acciones de tratamiento según su nivel de criticidad.

Gestión del riesgo:
Conjunto de actividades coordinadas para dirigir y controlar una organización en relación con los riesgos que pueden afectar sus objetivos.

Incidente de seguridad de la información:
Suceso que compromete o amenaza la confidencialidad, integridad o disponibilidad de la información institucional.

Integridad:
Propiedad que asegura que la información no sea alterada, modificada o destruida de manera no autorizada.

MAGERIT:
Metodología oficial del Gobierno de España para el *Análisis y Gestión de Riesgos en los Sistemas de Información*. Es una herramienta estructurada para identificar y tratar riesgos en entornos tecnológicos.

MinTIC:
Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Entidad que orienta la política pública de transformación digital, seguridad y protección de datos en el Estado.

MIPG:
Modelo Integrado de Planeación y Gestión. Marco de referencia del Estado colombiano que articula la planeación, la gestión y la evaluación institucional para fortalecer la transparencia y la eficiencia pública.

PETI:
Plan Estratégico de Tecnologías de la Información. Instrumento que define la hoja de ruta tecnológica de la entidad, orientando inversiones, proyectos y políticas digitales.

Privacidad de la información:
Derecho de las personas a controlar el uso, acceso y divulgación de sus datos personales.

Protección de datos personales:
Conjunto de medidas legales, técnicas y organizacionales destinadas a garantizar que el tratamiento de los datos de los ciudadanos se realice conforme a la ley y con respeto por sus derechos.

Riesgo:
Posibilidad de que una amenaza explote una vulnerabilidad y cause un impacto negativo en los activos de información o en los procesos de la entidad.

Seguridad de la información:
Conjunto de políticas, procedimientos y controles diseñados para proteger la confidencialidad, integridad y disponibilidad de la información institucional.

SGSI (Sistema de Gestión de Seguridad de la Información):
Modelo estructurado basado en la norma ISO/IEC 27001 que permite gestionar de forma sistemática los riesgos de seguridad de la información en una organización.

Tratamiento del riesgo:
Proceso de selección e implementación de medidas destinadas a modificar, reducir, transferir o aceptar los riesgos identificados.

Vulnerabilidad:
Debilidad o falla en un sistema, procedimiento o control que puede ser aprovechada por una amenaza para afectar la seguridad de la información.

8. METODOLOGÍA DE GESTIÓN DE RIESGOS

La gestión de riesgos de seguridad y privacidad de la información en FONDESER se desarrolla bajo un **enfoque sistemático, estructurado y continuo**, que permite identificar, analizar, valorar y tratar los riesgos que puedan comprometer la información institucional, los activos tecnológicos y los procesos misionales de la entidad.

Esta metodología se fundamenta en los lineamientos de la **norma internacional ISO/IEC 27001:2013** y en la **Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – MAGERIT v3**, reconocidas por su efectividad en la administración del riesgo en entornos tecnológicos y de información.

8.1 Principios Metodológicos

El proceso de gestión de riesgos de seguridad de la información se orienta por los siguientes principios:

- **Integralidad:** considera todos los activos de información, procesos, recursos humanos y tecnológicos de la entidad.
- **Prevención:** prioriza la adopción de medidas que eviten la materialización de incidentes.
- **Proporcionalidad:** asegura que los controles implementados sean coherentes con la magnitud del riesgo y con los recursos institucionales disponibles.
- **Mejora continua:** el proceso se revisa y actualiza periódicamente, conforme a los cambios tecnológicos, organizacionales y normativos.
- **Corresponsabilidad:** reconoce la participación activa de todos los servidores y contratistas en la gestión del riesgo.

8.2 Etapas del Proceso de Gestión de Riesgos

El procedimiento adoptado por FONDESER se estructura en las siguientes etapas:

1. **Identificación de activos de información:**
   Se determinan los activos que poseen valor para la entidad (bases de datos, sistemas informáticos, equipos, documentos, infraestructura tecnológica, entre otros) y se asignan responsables de su custodia y uso.

2. **Identificación de amenazas y vulnerabilidades:**
   Se analizan los factores internos y externos que pueden afectar la seguridad de la información, tales como ataques cibernéticos, errores humanos, fallas técnicas, eventos naturales o deficiencias en los controles administrativos.

3. **Valoración del riesgo:**
   Para cada activo, se evalúa la **probabilidad de ocurrencia** de un incidente y su **impacto potencial** sobre la confidencialidad, integridad o disponibilidad de la información.
   El nivel de riesgo se clasifica según una escala cualitativa (alto, medio o bajo), conforme al modelo propuesto por **MAGERIT v3**.

4. **Tratamiento del riesgo:**
   Una vez valorados los riesgos, se definen las acciones de respuesta más adecuadas, que pueden incluir:

- **Mitigar:** reducir la probabilidad o el impacto mediante controles preventivos o correctivos.
- **Evitar:** eliminar la causa del riesgo o modificar el proceso que lo genera.
- **Transferir:** compartir el riesgo con terceros (por ejemplo, mediante contratos o seguros).
- **Aceptar:** reconocer el riesgo cuando su impacto es mínimo o el costo de mitigación es mayor que el beneficio.

5. **Implementación de controles:**
   Se aplican controles técnicos (por ejemplo, contraseñas, copias de seguridad, antivirus, firewalls) y administrativos (como políticas, manuales, procedimientos y capacitaciones) para minimizar los riesgos detectados.

6. **Monitoreo y revisión:**
   Se realiza seguimiento periódico a los riesgos, a la eficacia de los controles y a la aparición de nuevas amenazas. Los resultados se documentan en informes de seguimiento que sirven de base para la mejora continua del PTRSPI.

8.3 Responsabilidades

La implementación y sostenibilidad del proceso de gestión de riesgos es una tarea compartida. Para tal fin, se establecen las siguientes responsabilidades:

- **Gerencia:** Aprobar el PTRSPI y asignar los recursos necesarios para su ejecución.
- **Líder de Tecnologías de la Información o quien haga sus veces:** Coordinar la identificación y tratamiento de los riesgos, velando por la aplicación de los controles definidos.
- **Oficina de Control Interno:** Realizar seguimiento, verificación y evaluación de la eficacia de los controles implementados, garantizando la mejora continua.
- **Servidores públicos y contratistas:** Cumplir las políticas, procedimientos y controles establecidos, reportando oportunamente cualquier incidente o anomalía que comprometa la seguridad de la información.

9. PLAN DE TRATAMIENTO DE RIESGOS

El **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI)** constituye el conjunto de **acciones, controles y medidas correctivas, preventivas y de mitigación** orientadas a reducir los riesgos identificados durante el proceso de análisis y valoración.

Este plan busca asegurar que los riesgos residuales —es decir, aquellos que permanecen después de aplicar los controles— se mantengan en niveles aceptables para la entidad, garantizando la protección de los activos de información y la continuidad de los procesos institucionales.

9.1 Objetivo del Plan de Tratamiento

Definir e implementar las **acciones específicas** necesarias para **prevenir, mitigar o controlar** los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información administrada por FONDESER, alineando los esfuerzos institucionales con los principios de seguridad digital, transparencia y mejora continua.

9.2 Estrategia General de Tratamiento

El tratamiento de los riesgos se desarrollará bajo los siguientes **enfoques estratégicos**:

1. **Prevención proactiva:** aplicar controles antes de que ocurra el incidente, reduciendo la probabilidad de materialización del riesgo.

2. **Mitigación del impacto:** reducir las consecuencias de los incidentes mediante respuestas oportunas y efectivas.

3. **Fortalecimiento institucional:** consolidar políticas, procedimientos y capacidades internas para responder adecuadamente ante eventos de riesgo.

4. **Cumplimiento normativo:** garantizar que todas las acciones estén en conformidad con la legislación colombiana sobre seguridad digital y protección de datos personales.

9.3 Categorías de Riesgo y Líneas de Acción

El PTRSPI agrupa los riesgos en cuatro categorías principales, cada una con sus respectivas líneas de acción y controles orientativos:

Categoría de Riesgo	**Descripción**	**Líneas de Acción / Controles Recomendados**
Riesgos tecnológicos	Amenazas derivadas del mal uso, falla o ataque a los sistemas, redes y equipos informáticos.	- Implementar antivirus y cortafuegos actualizados. - Realizar copias de seguridad periódicas. - Actualizar software y parches de seguridad. - Restringir el acceso a información sensible mediante autenticación y contraseñas seguras.

Riesgos físicos y ambientales	Incidentes originados por daños en la infraestructura, desastres naturales o pérdida física de la información.	- Asegurar los equipos en lugares protegidos y con control de acceso. - Contar con planes de contingencia ante incendios, inundaciones o cortes de energía. - Digitalizar documentos críticos.
Riesgos humanos u organizacionales	Errores, negligencias o acciones intencionadas de servidores, contratistas o terceros que comprometan la información.	- Capacitar periódicamente al personal en buenas prácticas de seguridad de la información. - Firmar acuerdos de confidencialidad. - Implementar procedimientos disciplinarios ante incumplimientos.
Riesgos normativos o de cumplimiento	Desconocimiento o incumplimiento de la normativa sobre protección de datos y seguridad digital.	- Socializar las políticas internas de seguridad y privacidad. - Alinear los procesos institucionales con la Ley 1581 de 2012 y el Decreto 1008 de 2018. - Garantizar la aplicación del Modelo de Seguridad y Privacidad de la Información (MSPI).

9.4 Plan de Acción Específico

Cada riesgo identificado en el inventario institucional será documentado en una **matriz de tratamiento**, que incluirá los siguientes campos:

Elemento	**Descripción**

Código del riesgo	Identificador único asignado en la matriz institucional de riesgos.
Descripción del riesgo	Resumen claro del evento o amenaza.
Causa	Factores o condiciones que generan el riesgo.
Consecuencia	Impacto potencial sobre los procesos, activos o servicios.
Valoración inicial	Nivel de riesgo antes de aplicar controles (alto, medio o bajo).
Controles existentes	Medidas actualmente implementadas para mitigar el riesgo.
Tratamiento propuesto	Acción adicional a ejecutar (mitigar, evitar, transferir o aceptar).
Responsable	Servidor o área encargada de ejecutar el tratamiento.
Plazo de implementación	Fecha límite para la ejecución del control.
Valoración residual	Nivel de riesgo posterior a la aplicación del tratamiento.
Seguimiento y evidencia	Mecanismos de control, indicadores o registros de cumplimiento.

Esta matriz será actualizada **anualmente** o cada vez que se presente un cambio significativo en los procesos, sistemas o estructura organizacional de FONDESER.

9.5 Responsables del Tratamiento de Riesgos

Rol / Dependencia	**Responsabilidades principales**

Gerencia de FONDESER	Aprobar el PTRSPI, asignar recursos y supervisar su cumplimiento.
Líder de Tecnologías de la Información (o quien haga sus veces)	Coordinar la implementación técnica de los controles y el seguimiento a los incidentes.
Oficina de Control Interno	Realizar la evaluación independiente del plan y emitir recomendaciones de mejora.
Servidores públicos y contratistas	Cumplir las políticas de seguridad y reportar oportunamente cualquier anomalía o incidente.

9.6 Mecanismos de Seguimiento y Mejora

El cumplimiento del PTRSPI se evaluará mediante un **sistema de indicadores de gestión** y un esquema de **seguimiento continuo** que permita verificar:

- La eficacia de los controles implementados.
- La reducción del nivel de riesgo residual.
- El grado de cumplimiento de las acciones programadas.
- La actualización del inventario de activos y riesgos.
- La generación de reportes para la alta dirección y Control Interno.

Los resultados del seguimiento se consolidarán en **informes semestrales**, los cuales servirán de base para los procesos de **auditoría interna** y para la **revisión del Sistema de Gestión de Seguridad de la Información (SGSI)** en FONDESER.

10. APLICABILIDAD DE CONTROLES DE SEGURIDAD

Los controles de seguridad establecidos se basan en la **metodología MAGERIT v3** y los **controles del Anexo A de la norma ISO/IEC 27001:2013**, adaptados al contexto de FONDESER.

Cada riesgo identificado será tratado mediante uno de los siguientes enfoques:

- **AS (Asumir):** Aceptar el riesgo cuando su impacto es bajo o su control es ineficiente económicamente.

- **DC (Definir Controles):** Implementar controles para reducir la probabilidad o impacto.
- **TT (Transferir):** Trasladar el riesgo mediante contratos, seguros o acuerdos con terceros.

El tratamiento seleccionado dependerá del nivel de criticidad del activo, la magnitud del impacto, la capacidad institucional y la disponibilidad presupuestal.

Objetivos principales:

- Garantizar la **confidencialidad, integridad y disponibilidad** de la información.
- Prevenir accesos no autorizados o uso indebido de los datos institucionales.
- Mantener la continuidad operativa de los servicios tecnológicos.
- Cumplir la normatividad vigente en materia de **protección de datos personales y seguridad digital**.

Los controles se agrupan por tipo de activo: datos/información, servicios, software, hardware, comunicaciones, equipos auxiliares e instalaciones.

[D] DATOS / INFORMACIÓN					
Código	Activo	Riesgo	Tratamiento	Salvaguardas	Referencia ISO/IEC 27001
D_BUCKUP	Copias de seguridad de la información contable y crediticia	Pérdida o corrupción de datos	DC	Respaldos automáticos cifrados, pruebas periódicas de recuperación	A.8.2, A.12.3.1
D_DOCUMENTOS	Contratos y actas de supervisión	Divulgación o pérdida de integridad	DC	Cifrado y almacenamiento en nube institucional	A.10.1

D_FINANCIEROS	Estados financieros y reportes de control	Acceso no autorizado o alteración	DC	Control de acceso por roles y auditoría de cambios	A.9.2
D_PERSONALES	Datos personales de beneficiarios	Uso indebido o fuga de datos	DC	Aplicación Ley 1581 de 2012, anonimización y consentimiento informado	A.18.1
D_REGISTROS	Registro de crédito y cartera	Eliminación o duplicidad	DC	Respaldo diario y revisión cruzada con sistema contable	A.12.3
[S] SERVICIOS					
Código	Activo	Riesgo	Tratamiento	Salvaguardas	Referencia ISO
S_MAIL	Correo electrónico institucional	Suplantación o pérdida de información	DC	Uso de dominio institucional, autenticación multifactor	A.13.2.3
S_WEB	Portal institucional y sitio web	Ataques de denegación o alteración	DC	Certificados SSL, firewall web y monitoreo continuo	A.12.6

S_BANCARIOS	Servicios bancarios y pagos electrónicos	Fraude o acceso no autorizado	TT	Seguros antifraude, doble validación de usuarios	A.17.1
S_INTERNOS	Servicios internos (intranet, nube)	Fallos de disponibilidad	DC	Copias de respaldo y redundancia de servicios	A.17.1
[SW] SOFTWARE					
Código	Activo	Riesgo	Tratamiento	Salvaguardas	Referencia ISO
SW_FINANCIEROS	Software contable y financiero	Corrupción de datos o manipulación	DC	Control de versiones y acceso restringido	A.12.2
SW_CARTERA Y CREDITO	Sistema de cartera y crédito	Fuga o pérdida de información	DC	Encriptación de base de datos y autenticación	A.14.2
SW_ANTIVIRUS	Antivirus institucional	Desactualización	DC	Actualización automática y monitoreo	A.12.2.1
SW_OPERATIVOS	Sistemas operativos	Fallas o vulnerabilidades	DC	Parches de seguridad automáticos	A.12.6.1

[HW] HARDWARE					
Código	Activo	Riesgo	Tratamiento	Salvaguardas	Referencia ISO
HW_SERVIDOR	Servidor principal	Daño físico o pérdida total	DC	UPS, control de temperatura y respaldos	A.11.2
HW_COMPUTADORES DE ESCRITORIOS	Computadores de escritorio	Robo o mal uso	DC	Control de inventario y claves personales	A.11.1
HW_COMPUTADORES PORTATILES	Portátiles institucionales	Pérdida o sustracción	TT	Seguros y políticas BYOD seguras	A.11.2
[COM] COMUNICACIONES					
Código	Activo	Riesgo	Tratamiento	Salvaguardas	Referencia ISO
COM_ACCESO A INTERNET	Internet y red LAN	Acceso no autorizado	DC	Firewall perimetral y VLAN por área	A.13.1
COM_WIFI	Red Wi-Fi institucional	Uso indebido	DC	Contraseña segura, filtrado MAC	A.13.2
COM_EXTERNAS	Enlaces externos con la Alcaldía	Interrupción o manipulación	TT	Contrato con proveedor certificado	A.17.1

[AUX] EQUIPO AUXILIAR					
Código	Activo	Riesgo	Tratamiento	Salvaguardas	Referencia ISO
AUX_UPS	Sistema de energía ininterrumpida	Fallo de suministro eléctrico	DC	Mantenimiento semestral	A.11.2
AUX_CABLEADO	Cableado estructurado	Deterioro o corte	DC	Canalización segura y etiquetado	A.11.2.6
[L] INSTALACIONES					
Código	Activo	Riesgo	Tratamiento	Salvaguardas	Referencia ISO
L_OFICINA	Oficina principal FONDESER	Daños físicos o robo	DC	Vigilancia, alarmas y control de acceso	A.11.1
L_DOCUMENTOS ARCHIVADOS	Archivo físico	Pérdida o incendio	DC	Sistema de detección y control de humedad	A.11.2
L_SERVIDORES	Sala de servidores	Sobrecalentamiento	DC	Aire acondicionado y monitoreo ambiental	A.11.2.3

10.1 AMENAZAS

Tecnológicas

- Ciberataques (phishing, malware, ransomware).
- Fallas de hardware y software.
- Desactualización tecnológica.
- Pérdida de respaldos.

Operativas

- Errores humanos o falta de capacitación.
- Ausencia de procedimientos documentados.
- Dependencia de terceros.
- Retrasos en proyectos tecnológicos.

Físicas

- Robo, vandalismo o daño a equipos.
- Inundaciones, incendios o sismos.
- Accesos no autorizados.

Financieras

- Pérdida de recursos por fraude digital.
- Multas por incumplimiento normativo.

Cumplimiento y Reputación

- Violación de normas sobre datos personales.
- Pérdida de confianza ciudadana por incidentes de seguridad.

Estratégicas

- Cambios normativos o presupuestales.
- Falta de alineación con políticas TIC nacionales.

11. TRATAMIENTO DE RIESGOS POR ACTIVO

El tratamiento de riesgos consiste en la aplicación de estrategias y controles que permitan **reducir, transferir, evitar o aceptar los riesgos identificados** sobre los activos de información de FONDESER, de acuerdo con su nivel de criticidad e impacto potencial sobre la entidad.

Cada activo será **registrado, valorado y clasificado** considerando su nivel de confidencialidad, integridad y disponibilidad, así como su relación con los procesos misionales, administrativos y tecnológicos.

Los controles aplicados podrán incluir medidas **técnicas, físicas, administrativas o contractuales**, como el uso de cifrado, copias de respaldo, restricciones de acceso, autenticación multifactor, mantenimiento preventivo, y cláusulas de confidencialidad.

Los principales activos de información de FONDESER son los siguientes:

- **Documentos contractuales:** minutas, actas, convenios y demás instrumentos jurídicos que soportan las relaciones contractuales y los proyectos institucionales.
- **Registros financieros y presupuestales:** soportes contables, registros de ejecución presupuestal, informes financieros y conciliaciones bancarias.
- **Bases de datos de beneficiarios de crédito:** información personal, socioeconómica y financiera de los usuarios de los programas de crédito social.
- **Informes de interventoría y consultoría:** documentos técnicos y administrativos derivados de los procesos de seguimiento y control a obras y servicios.
- **Equipos informáticos, software contable y de cartera:** recursos tecnológicos que soportan la operación administrativa, financiera y técnica de la entidad.
- **Redes de comunicación y servicios digitales:** conexiones, plataformas y sistemas compartidos con la Alcaldía de El Retiro y otras entidades asociadas.

El **responsable de tecnología o el área de Control Interno** realizará anualmente una **evaluación de los activos y de los controles implementados**, actualizando los registros y definiendo las acciones de mejora requeridas.
Asimismo, se mantendrán políticas de respaldo, actualización de software y revisión de accesos para garantizar la continuidad de la operación y la seguridad de la información institucional.

12. CAPACITACIÓN Y SENSIBILIZACIÓN

La capacitación y sensibilización del talento humano son pilares fundamentales para consolidar una **cultura organizacional de seguridad de la información y protección de datos personales** en FONDESER.

Con este propósito, la entidad implementará **programas anuales de formación y concientización**, dirigidos a todos los servidores públicos, contratistas y aliados estratégicos, con el apoyo de la Oficina de Control Interno y la coordinación tecnológica.

Estas acciones formativas tendrán como objetivos principales:

- **Fortalecer las competencias del personal** en el manejo adecuado de la información institucional y el uso responsable de los sistemas tecnológicos.
- **Promover la adopción de buenas prácticas de ciberseguridad**, incluyendo la gestión segura de contraseñas, la prevención de ataques informáticos y el manejo correcto del correo electrónico institucional.
- **Fomentar la identificación y reporte oportuno de incidentes de seguridad**, de acuerdo con los protocolos establecidos en el PTRSPI.
- **Difundir las responsabilidades legales y éticas** que conlleva el tratamiento de datos personales conforme a la Ley 1581 de 2012 y demás normas relacionadas.
- **Generar conciencia sobre la corresponsabilidad institucional**, recordando que la seguridad de la información depende del compromiso de cada integrante de la entidad.

Las capacitaciones podrán desarrollarse mediante **talleres presenciales, cursos virtuales, guías digitales, charlas institucionales y campañas comunicativas**, integrando estrategias pedagógicas que refuercen el aprendizaje continuo y la apropiación de la cultura de seguridad en todos los niveles de FONDESER.

13. SISTEMA DE EVALUACIÓN Y SEGUIMIENTO DEL PTRSPI

El **Sistema de Evaluación y Seguimiento del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI)** tiene como propósito **medir la efectividad, eficiencia y cumplimiento** de las acciones implementadas para la gestión de los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional de **FONDESER**.

Este sistema permite **verificar la eficacia de los controles, la reducción del nivel de riesgo residual y la consolidación de una cultura organizacional de seguridad digital**, garantizando la trazabilidad, la responsabilidad y la mejora continua en la gestión de la información.

El seguimiento y la evaluación se articulan con los mecanismos institucionales del **Modelo Integrado de Planeación y Gestión (MIPG)** y con las estrategias definidas en el **Plan Estratégico de Tecnologías de la Información (PETI) 2025–2027**, asegurando coherencia con los demás instrumentos de planeación y control interno de la entidad.

13.1 Objetivos del Sistema de Evaluación

1. **Verificar** el grado de cumplimiento de las acciones de tratamiento definidas en la matriz de riesgos del PTRSPI, evaluando la implementación efectiva de los controles de seguridad.

2. **Evaluar** la eficacia y eficiencia de las medidas aplicadas, identificando oportunidades de mejora y posibles ajustes en las estrategias de mitigación.

3. **Monitorear** la evolución del nivel de riesgo residual y su permanencia dentro de los límites de tolerancia definidos por la Gerencia.

4. **Fortalecer** la cultura institucional de corresponsabilidad, promoviendo el aprendizaje continuo y la mejora en la gestión de la seguridad y privacidad de la información.

13.2 Enfoque y Metodología de Evaluación

El sistema de evaluación se desarrolla bajo un **enfoque de gestión por resultados**, utilizando **indicadores cuantitativos y cualitativos** que reflejan la eficacia, eficiencia y cumplimiento del plan.

Las tres dimensiones de análisis son:

- **Eficacia:** mide el grado de logro de los objetivos y la reducción efectiva de los riesgos identificados.

- **Eficiencia:** evalúa el uso adecuado de los recursos humanos, financieros y tecnológicos destinados al tratamiento de los riesgos.

- **Cumplimiento:** valora el nivel de ejecución de las acciones, controles y actividades planificadas.

El seguimiento se realizará de manera **semestral**, con reportes consolidados **anualmente**, integrándose al proceso de gestión del riesgo institucional y a los informes de evaluación del MIPG.

13.3 Indicadores de Gestión del PTRSPI

Dimensión	**Indicador**	**Fórmula de Cálculo**	**Meta 2027**	**Periodicidad**	**Responsable del Seguimiento**
Eficacia	Porcentaje de riesgos mitigados	(N° de riesgos mitigados / N° total de riesgos identificados) × 100	≥ 85%	Semestral	Líder de Tecnologías de la Información

Eficiencia	Nivel de cumplimiento del plan de acción	(N° de actividades ejecutadas / N° total de actividades planificadas) × 100	≥ 90%	Trimestral	Coordinación Administrativa / Control Interno
Cumplimiento	Porcentaje de servidores y contratistas capacitados en seguridad de la información	(N° de funcionarios capacitados / N° total de funcionarios y contratistas) × 100	100 %	Anual	Talento Humano / TIC
Mejora Continua	Porcentaje de controles evaluados como eficaces	(N° de controles eficaces / N° total de controles implementados) × 100	≥ 80%	Semestral	Oficina de Control Interno
Resiliencia Institucional	Tiempo promedio de recuperación ante incidentes (en horas)	(Suma de tiempos de recuperación / N° de incidentes atendidos)	≤ 8 horas	Trimestral	TIC / Gerencia

13.4 Mecanismos de Seguimiento y Evaluación

Para garantizar la trazabilidad y sostenibilidad del PTRSPI, se establecen los siguientes mecanismos de control y mejora:

- **Informes semestrales de avance:** elaborados por el Líder de Tecnologías de la Información, en coordinación con la Oficina de Control Interno, donde se reportan avances, desviaciones y recomendaciones.
- **Revisión anual del PTRSPI:** actualización de la matriz de riesgos, controles y responsables, atendiendo a cambios normativos, tecnológicos o estructurales de la entidad.
- **Auditorías internas y externas:** orientadas a verificar la aplicación de los controles y el cumplimiento de las políticas de seguridad de la información.
- **Comités institucionales:** presentación de resultados ante el Comité de Gestión y Desempeño Institucional y/o el Comité de Coordinación de Control Interno,

fortaleciendo la transparencia y la toma de decisiones basada en evidencia.

- **Retroalimentación del personal:** desarrollo de encuestas, reuniones o espacios participativos para identificar oportunidades de mejora en la gestión de la seguridad y la privacidad.

13.5 Compromiso Institucional y Mejora Continua

El éxito del PTRSPI depende del **compromiso activo de todos los funcionarios, contratistas y directivos** de FONDESER, quienes comparten la responsabilidad de salvaguardar la información institucional.

Por ello, la entidad fomentará una **cultura organizacional basada en la corresponsabilidad, la prevención y la ética digital**, asegurando que cada miembro comprenda su rol en la protección de los activos de información y en la continuidad de los procesos misionales.

El Sistema de Evaluación y Seguimiento permitirá una **retroalimentación permanente**, de manera que los resultados obtenidos sirvan como insumo directo para la **actualización de políticas, procedimientos y controles**, garantizando la **vigencia, efectividad y sostenibilidad del PTRSPI durante el período 2025–2027**.

14. CONCLUSIÓN GENERAL

El **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI) 2025–2027** constituye una herramienta estratégica y operativa que fortalece la capacidad institucional de **FONDESER** para proteger sus activos de información, garantizar la continuidad de sus procesos y asegurar la confianza de la ciudadanía en la gestión pública.

A través de la implementación de políticas, controles y acciones de mitigación basadas en estándares internacionales y normativa nacional, el plan promueve una **gestión proactiva y responsable de los riesgos**, asegurando que la información financiera, contractual, técnica y personal sea tratada de manera segura, ética y transparente.

El PTRSPI se integra de forma transversal con el **Plan Estratégico de Tecnologías de la Información (PETI) 2025–2027**, el **Modelo Integrado de Planeación y Gestión (MIPG)** y las políticas institucionales de control interno, convirtiéndose en un componente esencial para la modernización administrativa, la gobernanza digital y la mejora continua de la entidad.

Asimismo, el éxito en su implementación depende del **compromiso activo de todos los servidores públicos, contratistas y directivos**, quienes desempeñan un papel fundamental en la construcción de una cultura organizacional basada en la seguridad, la corresponsabilidad y la ética en el uso de la información.

Con este plan, **FONDESER reafirma su compromiso con la protección de los datos personales, la transparencia institucional y la eficiencia administrativa**, contribuyendo al fortalecimiento de la confianza pública y al cumplimiento de su misión social y comunitaria en el Municipio de El Retiro.

15. BIBLIOGRAFÍA

- Alcaldía de El Retiro – Fondo de Desarrollo Social (FONDESER). *Plan Estratégico de Tecnologías de la Información (PETI) 2025–2027.* El Retiro, Antioquia, 2025.
- Departamento Administrativo de la Función Pública – DAFP. *Guía para la Gestión del Riesgo Institucional y Corrupción en el MIPG.* Bogotá D.C., 2022.
- DAFP. *Guía para la Implementación de la Política de Seguridad y Privacidad de la Información.* Bogotá D.C., 2021.
- ISO/IEC 27001:2022. *Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de Seguridad de la Información – Requisitos.* Organización Internacional de Normalización (ISO).
- ISO/IEC 27005:2018. *Gestión del Riesgo de Seguridad de la Información.*
- MAGERIT v3. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Ministerio de Política Territorial y Función Pública, Gobierno de España, 2012.
- Ley 1581 de 2012. *Por la cual se dictan disposiciones generales para la protección de datos personales.* Congreso de la República de Colombia.
- Decreto 1377 de 2013. *Por el cual se reglamenta parcialmente la Ley 1581 de 2012.*
- Decreto 612 de 2018. *Por el cual se establecen directrices para la integración de los planes institucionales y estratégicos al MIPG.*
- Documento CONPES 3854 de 2016. *Política Nacional de Seguridad Digital.*
- Superintendencia de Industria y Comercio – SIC. *Guía de Responsabilidad Demostrada para el Tratamiento de Datos Personales.* Bogotá D.C., 2021.
- Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). *Política de Seguridad y Privacidad de la Información del Estado Colombiano.* Bogotá D.C., 2020.

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