1. Introducción

La gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación Tecnológica permite al Fondo de Valorización de Medellín – FONVALMED identificar, analizar, evaluar y tratar los eventos que puedan afectar el cumplimiento de sus objetivos estratégicos y misionales.

Este proceso contribuye a la toma oportuna de decisiones orientadas a prevenir la materialización de riesgos, minimizar impactos negativos y fortalecer la confianza en el manejo de la información institucional. Asimismo, facilita la identificación de fortalezas y debilidades a las que se encuentran expuestos los servicios de la entidad durante todo su ciclo de vida.

El presente plan se fundamenta en la normativa colombiana vigente, especialmente los lineamientos del Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, los documentos CONPES 3854 de 2016 y 3995 de 2020, el Decreto 1008 de 2018, las buenas prácticas establecidas en la norma ISO/IEC 27001:2013 y la Política de Administración del Riesgo adoptada por la entidad.

En este contexto, la gestión de riesgos incorpora de manera transversal la protección de los datos personales y la privacidad de la información, garantizando el cumplimiento de los principios, derechos y deberes establecidos en la Ley 1581 de 2012 y sus decretos reglamentarios, así como los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI del MinTIC, asegurando que el tratamiento de la información se realice de forma segura, responsable y conforme a la normatividad vigente.

1.2 Objetivo

Definir y aplicar los lineamientos institucionales para la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de los riesgos asociados a la Seguridad y Privacidad de la Información en el FONVALMED, garantizando la confidencialidad, integridad y disponibilidad de la información, así como la protección de los datos personales y los derechos de los titulares, en concordancia con el MSPI y la normatividad vigente.

1.3 Alcance

El alcance del presente plan comprende todas las etapas del proceso de gestión del riesgo de Seguridad y Privacidad de la Información, desde la identificación y análisis de los riesgos hasta la definición, implementación y seguimiento de los controles establecidos para su tratamiento.

Incluye los riesgos que puedan afectar la seguridad de la información y la privacidad de los datos personales en todos los procesos, sistemas de información, activos tecnológicos, servicios digitales, proveedores, terceros y usuarios, durante todo el ciclo de vida de la información, desde su recolección hasta su disposición final.

2. Definiciones

- **Confidencialidad:** Es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.

- **Integridad:** Es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada.

- **Disponibilidad:** Es una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones.

- **Seguridad de la Información:** Consiste en asegurar que los recursos del Sistema de Información de una empresa se utilicen de la forma que ha sido decidido y el acceso de información se encuentra contenida, así como controlar que la modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización.

- **Activos de información:** Son los elementos que la Seguridad de la Información debe proteger. Por lo que son tres elementos lo que forman los activos:

    - **Información:** Es el objeto de mayor valor para la empresa.
    - **Equipos:** Suelen ser software, hardware y la propia organización.
    - **Usuarios:** son las personas que usan la tecnología de la organización.
    - **Administración/gestión del riesgo:** Actividades coordinadas para dirigir y controlar la organización con relación al riesgo.
    - **Evento:** Ocurrencia o cambio de un conjunto particular de circunstancias.
    - **Control:** Medida que mantiene y/o modifica un riesgo.

- **Consecuencia/impacto:** Resultado de un evento que afecta a los objetivos.
- **Fuente de riesgo:** Elemento que, por si solo o en combinación con otros, tiene el potencial de generar riesgo.
- **Probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
- **Matriz de riesgos:** Documento con la información resultante de la gestión del riesgo.

3. Glosario – MSPI

- **Activo:** Elemento que tiene valor para FONVALMED y que requiere protección.
- **Activo de Información:** Información y recursos que la soportan, relevantes para el cumplimiento de los objetivos institucionales.
- **Amenaza:** Evento potencial que puede causar daño a un activo de información.
- **Análisis de Riesgos:** Proceso para identificar y evaluar riesgos de seguridad y privacidad de la información.
- **Confidencialidad**: Garantía de acceso a la información solo por usuarios autorizados.
- **Control:** Medida administrativa, técnica o física para modificar un riesgo.
- **Dato Personal:** Información asociada o vinculable a una persona natural determinada o determinable.
- **Disponibilidad:** Propiedad que asegura el acceso oportuno a la información.
- **Gestión de Riesgos:** Actividades coordinadas para dirigir y controlar los riesgos.
- **Impacto:** Consecuencia de la materialización de un riesgo.
- **Incidente de Seguridad:** Evento que compromete la seguridad o privacidad de la información.
- **Integridad:** Exactitud y completitud de la información.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información definido por MinTIC.

- **Plan de Tratamiento**: Conjunto de acciones para tratar riesgos identificados.
- **Privacidad:** Protección de los datos personales y derechos de los titulares.
- **Probabilidad:** Posibilidad de ocurrencia de un riesgo.
- **Responsable del Tratamiento:** Quien decide sobre el tratamiento de datos personales.
- **Riesgo:** Posibilidad de que una amenaza afecte un activo.
- **Riesgo Residual:** Riesgo que permanece tras aplicar controles.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad.
- **SGSPI:** Sistema de Gestión de Seguridad y Privacidad de la Información.
- **Tratamiento de Datos:** Operaciones realizadas sobre datos personales.
- **Vulnerabilidad:** Debilidad que puede ser explotada por una amenaza.

4. Marco legal.

- **Ley 1581 de 2012 - Protección de datos "**Establecen el marco general para el tratamiento de datos y derechos de los titulares".
- **Ley 1712 de 2014** "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
- **Decreto 767 de 2022** "Actualiza la Política de Gobierno Digital para mejorar la relación Estado-ciudadano, y la **Resolución 02277 de 2025**, que actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI)
- **Decreto 1263 de 2022** "Establece lineamientos para la Transformación Digital Pública"
- **Decreto 1008 de 2018** "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital"
- **Decreto 1499 de 2017** "Por medio del cual se establece el MIPG".

- **Decreto 103 de 2015** "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones"

- **Decreto 1377 de 2013** "Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.

- **Ley 1581 de 2012** "Por la cual se dictan disposiciones generales para la protección de datos personales."

- **Ley 1273 de 2009**. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- **Resolución 2021-76** Por medio de la cual se adopta la Política de Protección de Datos Personales del ciudadano en el Fondo de Valorización del Municipio de Medellín- FONVALMED.

Estándares y marcos internacionales

- **ISO 27001 de 2013**. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la Información (SGSI). Requisitos.

- **ISO/IEC 27002:2013**. Describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

- **ISO 27005:** Guía para la gestión del riesgo de seguridad de la información.

- **ISO 27000:** Vocabulario y fundamentos.

Guías y Metodologías Locales (Adaptación):

- **Guías del DAFP (Departamento Administrativo de la Función Pública):** Metodologías para la administración del riesgo y diseño de controles en entidades públicas (Colombia).

- **Modelos de Gestión (MIPG):** Integran la gestión del riesgo en la administración pública.

Políticas Internas y Procedimientos (Aplicación):

- **Plan de Tratamiento de Riesgos de Seguridad y Privacidad (PTR):** Documento que define acciones sobre riesgos inaceptables.

Guía vigente de administración del riesgo establecida por la Función Pública y con los lineamientos de la política de protección de datos ***"Por medio de la cual se adopta el manual de políticas y procedimientos para la protección de datos en el Fondo de valorización del distrito de Medellín –FONVALMED***

5. Gestionar los riesgos

La gestión de riesgo es una actividad que está inmersa en las actividades del modelo de operación por procesos de la Entidad y hacen parte de las responsabilidades de la alta dirección y de las 3 líneas de defensa que establece el modelo integrado de planeación y gestión MIPG.

Para el desarrollo del plan de tratamiento de riesgos, FONVALMED se adhiere a los lineamientos que establece la norma para poder identificar, analizar, tratar, valorar, evaluar y monitorear los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y todos aquellos relacionados en la materia.

La gestión de riesgos de Seguridad y Privacidad de la Información se articula con el Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI, permitiendo identificar amenazas y vulnerabilidades que puedan afectar los activos de información y los datos personales, así como definir controles administrativos, técnicos y físicos que reduzcan la probabilidad de ocurrencia y el impacto de los riesgos.

5.1 Establecimiento del contexto

El análisis del contexto considera factores internos y externos que puedan afectar la operación institucional.

- **Factores externos:** Incluyen aspectos políticos, económicos, sociales, culturales, tecnológicos, legales y ambientales, entre otros.

- **Factores internos:** Comprenden variables como disponibilidad y competencias del personal, asignación presupuestal, estructura organizacional, cultura institucional, articulación de procesos, gestión del conocimiento, infraestructura tecnológica, sistemas de información y direccionamiento estratégico.

Asimismo, se identifican los activos de información asociados a cada proceso, tales como aplicaciones, servicios web, redes, información física y digital y tecnologías de la información.

Se pueden analizar variables tales como: diseño del proceso, articulación, procedimientos asociados, liderazgo al interior, activos de TI del proceso, etc.

Dentro del análisis del contexto interno y de proceso se deberán identificar: las aplicaciones, servicios web, redes, información física o digital, tecnologías de la información, que se utilizan en el Instituto con las cuales tenga interacción el proceso o aquellas que sean propias del mismo.

5.2 Identificación del Riesgo:

El Líder del Proceso de Tecnologías de la Información, con el apoyo de su equipo de trabajo, identifica los riesgos que puedan afectar el cumplimiento de los objetivos institucionales, utilizando técnicas como lluvia de ideas y análisis de contexto.

Debe clasificar el riesgo, teniendo como base las tipologías de riesgo establecidas en Política de Administración del Riesgo de FONVALMED, escogiendo la que se considere se ajusta a la naturaleza del evento que se está analizando. Dentro de las tipologías se tienen:

- **Estratégicos:** Son los riesgos asociados a la Administración de FONVALMED, se enfoca a asuntos globales relacionados con la Misión y el cumplimiento de los Objetivos Estratégicos, la definición de Políticas, diseño y conceptualización de la entidad por parte de la Dirección.

- **De imagen:** Relacionado con la percepción y la confianza por parte de nuestros grupos de valor, partes interesadas y comunidad en general, hacia FONVALMED.

- **Operativos:** Riesgo asociado a la estructuración y ejecución de los proyectos.
- **Financieros:** Relacionado con el manejo de recursos que incluyen la Ejecución Presupuestal, la elaboración de los Estados Financieros, modelo financiero, los Pagos, y el Manejo sobre los Bienes.
- **Cumplimiento y conformidad:** Se asocian con la capacidad de FONVALMED para Cumplir con los Requisitos Legales, contractuales, de la política de integridad y transparencia y en general con su compromiso ante la comunidad.
- **Tecnológicos:** Están relacionados con la capacidad tecnológica de la entidad para satisfacer sus necesidades actuales, futuras y el cumplimiento de la Misión.
- **De información:** Se asocia a la calidad, seguridad, oportunidad, pertinencia y confiabilidad de la Información.
- **Administrativos:** Riesgo asociado a la gestión de los procesos dentro del Modelo operación por procesos MOP.

Una vez clasificado el riesgo, se define su descripción, principales causas, los agentes generadores y sus efectos, teniendo en cuenta las siguientes descripciones:

- **Descripción del riesgo:** Es la definición específica de cómo se manifiesta el riesgo, acordado por el respectivo Equipo de Trabajo.
- **Causa:** Son factores generadores del riesgo (debilidades y amenazas). Son los porqués de la ocurrencia del evento riesgoso.
- **Efecto:** Son las consecuencias o el impacto que se genera con la ocurrencia del riesgo.

En la identificación de los riesgos de información se deberán considerar, de manera específica, aquellos relacionados con:

- Acceso no autorizado a la información.
- Pérdida, alteración o divulgación indebida de datos personales.
- Incumplimiento de principios y obligaciones en materia de protección de datos personales.
- Fallas en la seguridad de los sistemas de información y servicios digitales.
- Debilidades en la gestión de proveedores y terceros que tengan acceso a información institucional.

5.3 Calificación preliminar de los Riesgos

En esta etapa el líder del proceso de tecnología de la información determina la probabilidad y el impacto de los riesgos identificados sin tener en cuenta el efecto de los controles que se estén implementando o se puedan implementar para su tratamiento.

La calificación de la probabilidad e impacto se realiza de acuerdo con las siguientes escalas:

Frecuencia-Probabilidad	Impacto
Improbable 1 Posible 2 Frecuente 3	Menor 1 Moderado 2 Catastrófico 3

5.4 Valoración del riesgo después del control:

El líder del proceso de tecnología de la información analiza y describe los controles existentes relacionados directamente con el riesgo identificado y sus principales causas y los documenta en la columna “acciones para el control” del formato Mapa de Riesgos.

Los controles pueden estar definidos en los procedimientos, en la normatividad legal aplicable, o políticas o directrices administrativas, entre otros.

En esta etapa se determina nuevamente la probabilidad y el impacto de los riesgos identificados teniendo en cuenta el efecto de los controles que se estén implementando para mitigar la materialización del riesgo.

Esta valoración determina la calificación del riesgo en una escala de bajo, medio o alto.

5.5 Realizar el tratamiento de los riesgos

Para dar el tratamiento a los riesgos, de acuerdo con la valoración obtenida, el líder del proceso de tecnología y su equipo de trabajo determina los controles propuestos, considerando lo establecido en la "Matriz de Calificación, evaluación y Respuesta a los Riesgos" y teniendo en cuenta la viabilidad técnica y financiera.

El tratamiento de los riesgos de seguridad y privacidad de la información deberá priorizar la implementación de controles orientados a la prevención de incidentes, la protección de los datos personales, la continuidad de los servicios tecnológicos y el cumplimiento de los requisitos legales y regulatorios, de conformidad con el MSPI, la política de protección de datos personales y los estándares internacionales adoptados por el Fondo de valorización de Medellín.

La prioridad para la toma de las acciones depende de la zona de riesgo donde se ubica, considerando lo siguiente:

- **Zona Roja:** Requiere atención inmediata
- **Zona Amarilla (Zona Moderada):** Requiere acciones de control y monitoreo permanente.
- **Zona Verde**: Seguir aplicando los controles existentes y hacer monitoreo periódico.

Teniendo en cuenta la criticidad del riesgo se deja registro en el formato PE-F04 "Acción Correctiva y Preventiva" en el caso de requerir establecer acciones asociadas a los controles propuestos.

6. Análisis de la gestión de riegos y plan de acción

El Fondo de Valorización de Medellín, realizará el análisis de la gestión de los riesgos de Seguridad y Privacidad de la Información con el fin de definir y ejecutar las acciones necesarias ante la materialización de un riesgo, garantizando la protección de los activos de información, los datos personales, la continuidad de los servicios institucionales y el cumplimiento del Modelo de Seguridad y Privacidad de la Información – MSPI y la normatividad vigente.

En caso de materialización de un riesgo de seguridad y/o privacidad de la información, la Entidad procederá de la siguiente manera:

- **Identificación y reporte del evento**

  Una vez se detecte la materialización de un riesgo o la ocurrencia de un evento de seguridad de la información, este deberá ser reportado de manera inmediata al responsable de Seguridad y Privacidad de la Información y al líder del proceso afectado, conforme al procedimiento de gestión de incidentes establecido.

- **Activación de los controles definidos**

  Se activarán los controles preventivos, correctivos y/o de contingencia definidos en el plan de tratamiento del riesgo, con el propósito de contener el evento y reducir su impacto sobre la confidencialidad, integridad y disponibilidad de la información.

- **Análisis del impacto**

  El Fondo de valorización de Medellín realizará el análisis del impacto generado por la materialización del riesgo, identificando los activos de información afectados, los procesos comprometidos, la criticidad del evento y las posibles afectaciones a los datos personales, de acuerdo con los criterios definidos en el MSPI.

- **Ejecución del plan de acción**

  Con base en el análisis realizado, se ejecutarán las acciones correctivas necesarias para mitigar el riesgo materializado, restablecer la operación normal de los procesos y asegurar la continuidad de los servicios institucionales, de conformidad con los procedimientos de respaldo, recuperación y continuidad del negocio.

- **Gestión de incidentes de seguridad y privacidad de la información**

  Cuando la materialización del riesgo constituya un incidente de seguridad de la información o de privacidad de datos personales, este será gestionado conforme al procedimiento institucional, incluyendo su registro, seguimiento, cierre y, de ser aplicable, la notificación a las instancias competentes, en cumplimiento de la normatividad vigente.

- **Evaluación del riesgo residual**

  Una vez controlado el evento, se evaluará el riesgo residual con el fin de determinar la efectividad de los controles aplicados y definir si es necesario actualizar el plan de tratamiento del riesgo o implementar controles adicionales.

- **Mejora continua**

  El Fondo de valorización de Medellín documentará las lecciones aprendidas derivadas de la materialización del riesgo, las cuales serán insumo para la actualización de la matriz de riesgos de seguridad y privacidad de la información, el fortalecimiento del MSPI y la mejora continua del Sistema de Gestión.

Las acciones definidas permitirán fortalecer la capacidad de respuesta institucional ante incidentes de seguridad y privacidad de la información, reducir la probabilidad de recurrencia, asegurar la mejora continua del SGSPI y mantener la confianza de los grupos de valor y partes interesadas.

7. Ejecutar el monitoreo y seguimiento

El monitoreo y seguimiento de los riesgos de seguridad y privacidad de la información permitirá verificar la efectividad de los controles implementados, identificar nuevas amenazas o vulnerabilidades y asegurar la actualización permanente de la matriz de riesgos, en coherencia con los cambios tecnológicos, normativos y organizacionales.

Este se debe realizar de manera permanente y está a cargo del líder de cada proceso quien debe consolidar un seguimiento a la matriz de riesgos y ser enviado a al Líder de Planeación.

Planeación como segunda línea de defensa, consolidará un informe sobre la administración del riesgo a nivel global, utilizando como insumo la información suministrada por cada proceso la resultante de las actividades de acompañamiento desarrolladas. Dicho informe será presentado al Comité Institucional Coordinador de Control Interno.

Para efectos del seguimiento a los riesgos clasificados como de corrupción, se consolidará una matriz propia para la temática, la cual resultará del trabajo de identificación de riesgos a nivel de proceso. También será objeto de auditoría por parte de la Oficina de Control Interno con corte a las siguientes fechas: 30 de marzo, 30 de junio, 30 de septiembre y 30 de diciembre de cada año, tal como lo establece la norma.

8. Anexo

- Matriz de riesgos Proceso de TI

Aprobado por el Comité de Institucional de Gestión y Desempeño
Medellín, 26 de enero de 2026