PERSONERÍA DE RIONEGRO

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VERSIÓN 1

PERSONERÍA MUNICIPAL
RIONEGRO, ANTIOQUIA
2026

CONTENIDO

1. OBJETIVO GENERAL 2

2. ALCANCE 2

3. MARCO NORMATIVO 2

4. ARTICULACIÓN CON MIPG, GOBIERNO DIGITAL Y MSPI 3

5. DIAGNÓSTICO INSTITUCIONAL 3

6. LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN .. 3

7. GESTIÓN Y TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 4

8. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 4

9. SEGUIMIENTO, EVALUACIÓN Y MEJORA CONTINUA 4

10. DESARROLLO DEL PLAN 5

10.1. Recursos 5

10.2. Identificación de activos de información 5

10.3. Identificación de los riesgos 6

10.4. Identificación de amenazas 8

11. SEGUIMIENTO 9

12. CONTROL DE CAMBIOS 9

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2026

La Personería Municipal de Rionegro reconoce la información como un activo estratégico indispensable para el cumplimiento de sus funciones constitucionales y legales. En consecuencia, la entidad adopta medidas orientadas a garantizar su adecuada gestión, protección y uso, con el fin de salvaguardar los principios de **confidencialidad, integridad y disponibilidad**, así como la privacidad de los datos personales de los ciudadanos, servidores públicos y demás partes interesadas.

En atención a los lineamientos del **Modelo de Gobierno Digital**, definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, y en concordancia con las buenas prácticas establecidas en la **norma ISO/IEC 27001**, la Personería Municipal de Rionegro formula el presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026.

1. OBJETIVO GENERAL

Definir y ejecutar las acciones necesarias para tratar los riesgos de seguridad y privacidad de la información identificados en la Personería Municipal de Rionegro, mediante la implementación de controles, medidas preventivas y acciones correctivas que permitan reducir la probabilidad de ocurrencia y el impacto de los riesgos, garantizando la protección de los activos de información institucionales.

2. ALCANCE

El presente Plan aplica a todos los procesos misionales, estratégicos y de apoyo de la Personería Municipal de Rionegro, e involucra a todos los servidores públicos, contratistas y terceros que, en ejercicio de sus funciones, tengan acceso, uso, custodia o administración de activos de información, independientemente del medio en que estos se encuentren (físico o digital).

3. MARCO NORMATIVO

- Constitución Política de Colombia (artículos 15, 20 y 74).
- Ley 1581 de 2012 y decretos reglamentarios – Protección de Datos Personales.

- Ley 1712 de 2014 – Transparencia y Derecho de Acceso a la Información Pública.
- Ley 594 de 2000 – Ley General de Archivos.
- Decreto 1078 de 2015 – Decreto Único Reglamentario del sector TIC.
- Decreto 1008 de 2018 – Política de Gobierno Digital.
- Lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI (MinTIC).
- Modelo Integrado de Planeación y Gestión – MIPG.
- Norma ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información.

Directrices del FURAG y del Índice de Transparencia y Acceso a la Información – ITA.

4. ARTICULACIÓN CON MIPG, GOBIERNO DIGITAL Y MSPI

El presente Plan se articula con la dimensión de Gestión con Valores para Resultados del MIPG, específicamente con la política de Gobierno Digital, integrando el enfoque de gestión del riesgo, control interno y mejora continua. Así mismo, se alinea con el MSPI, promoviendo la protección de la información como un habilitador de la gestión institucional y del servicio al ciudadano.

5. DIAGNÓSTICO INSTITUCIONAL

La Personería Municipal de Rionegro realiza el análisis de su contexto interno y externo, considerando su estructura organizacional, procesos, sistemas de información, activos de información y partes interesadas. Este diagnóstico permite identificar brechas, amenazas y vulnerabilidades, así como el nivel de madurez del Sistema de Seguridad y Privacidad de la Información, sirviendo de base para la definición de acciones de mejora.

6. LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la vigencia 2026, la Personería Municipal de Rionegro adopta y fortalece los siguientes lineamientos:

- Garantizar la protección de los datos personales y de la información sensible conforme a la Ley 1581 de 2012.
- Asegurar la reserva, confidencialidad y custodia de la información asociada a procesos misionales, disciplinarios y administrativos.
- Dar cumplimiento a la Ley de Transparencia mediante la publicación oportuna y veraz de la información en SECOP II.
- Utilizar de manera segura plataformas nacionales como Vivanto, Toma en Línea y SIGEP II.

- Gestionar la información documental a través del aplicativo QF Document, conforme a la Ley General de Archivos.
- Incluir cláusulas de confidencialidad y protección de la información en los contratos suscritos con servidores y contratistas.
- Promover la estrategia de datos abiertos sin afectar la reserva legal ni la privacidad de la información.
- Asegurar el uso responsable y controlado de las redes sociales institucionales.
- Identificar, clasificar y asignar responsables a los activos de información institucionales.

7. GESTIÓN Y TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La gestión de los riesgos de seguridad y privacidad de la información se desarrolla de manera articulada con el Mapa de Riesgos Institucional. Para cada riesgo identificado se define su análisis, evaluación y tratamiento, mediante la implementación de controles técnicos, administrativos y organizacionales, conforme a la Matriz de Tratamiento de Riesgos de Seguridad y Privacidad de la Información vigente.

8. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Personería Municipal de Rionegro adopta la Política de Seguridad y Privacidad de la Información como marco orientador para la protección de la información institucional. Esta política es de obligatorio cumplimiento y busca garantizar el equilibrio entre la transparencia, el acceso a la información pública y la protección de la información sujeta a reserva legal o confidencialidad.

La entidad promueve la sensibilización y responsabilidad de los servidores públicos, y contratistas frente al adecuado uso, manejo y custodia de la información, asegurando los niveles de confidencialidad, integridad y disponibilidad requeridos.

9. SEGUIMIENTO, EVALUACIÓN Y MEJORA CONTINUA

El seguimiento al presente Plan se realizará de manera trimestral, verificando el cumplimiento de los lineamientos y acciones definidas, y dejando evidencia documental para efectos de control interno, auditoría, FURAG e ITA. Al cierre de la vigencia se efectuará una evaluación integral que permitirá definir acciones de mejora para el fortalecimiento continuo del Sistema de Seguridad y Privacidad de la Información.

10. DESARROLLO DEL PLAN

10.1. Recursos

La Personería Municipal de Rionegro dispondrá de los recursos humanos, físicos y tecnológicos necesarios para la adecuada implementación, ejecución, seguimiento y mejora del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, en concordancia con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG) y el Sistema de Gestión de Seguridad de la Información (SGSI – ISO/IEC 27001).

- **Recursos humanos:** El Personero Municipal de Rionegro, los Personeros Delegados, los líderes de los procesos misionales, estratégicos y de apoyo, y contratistas de la entidad, serán responsables de aplicar y cumplir los lineamientos, controles y acciones definidos en el Plan, de acuerdo con sus roles y funciones, contribuyendo a la gestión integral de los riesgos de seguridad y privacidad de la información.

- **Recursos físicos y tecnológicos:** La Personería Municipal de Rionegro contará con la infraestructura física y tecnológica requerida para el desarrollo de sus funciones, que incluye implementos de trabajo, equipos de cómputo, sistemas de información y equipos de comunicaciones, los cuales deberán mantenerse bajo condiciones de seguridad, control y mantenimiento que garanticen la confidencialidad, integridad y disponibilidad de la información institucional.

10.2. Identificación de activos de información

La Personería Municipal de Rionegro identifica y clasifica sus activos de información con el fin de garantizar su adecuada protección, administración y uso, atendiendo a los principios de confidencialidad, integridad y disponibilidad. Los activos de información se reconocen de acuerdo con su naturaleza y función dentro de los procesos institucionales, así:

Tipo de activo	Información
Información	La información constituye el principal activo de la Personería Municipal de Rionegro. Puede encontrarse en formato físico, como documentos impresos o manuscritos, y en formato digital, almacenada en equipos de cómputo, discos duros externos, memorias USB, sistemas de

Tipo de activo	Información
	información o servicios de almacenamiento en la nube, y es esencial para el cumplimiento de las funciones misionales y administrativas de la entidad.
Software	Activos lógicos que incluyen programas, aplicaciones, herramientas ofimáticas y sistemas de información utilizados para la ejecución, apoyo y control de las actividades institucionales.
Hardware	Equipos físicos de cómputo y demás dispositivos tecnológicos empleados para el procesamiento, almacenamiento y transmisión de la información institucional.
Activos Intangibles	Activos inmateriales que aportan valor estratégico a la entidad, entre los cuales se destaca la imagen corporativa, la reputación institucional y el conocimiento organizacional.
Servicios	Servicios prestados por la Personería Municipal de Rionegro, así como aquellos contratados con terceros, que apoyan la operación y el desarrollo de los procesos misionales, estratégicos y de apoyo.
Personas	Servidores públicos y contratistas que, por su conocimiento, experiencia, competencias y nivel de criticidad en los procesos, son considerados activos de información, al tener acceso, manejo o custodia de información relevante para la entidad.
Instalaciones	Espacios físicos e instalaciones destinadas al funcionamiento de la entidad y al alojamiento, custodia y protección de los activos de información considerados críticos para la Personería Municipal de Rionegro.

10.3. Identificación de los riesgos

El objetivo de la identificación de los riesgos es reconocer, analizar y documentar los incidentes, amenazas o eventos que puedan generar pérdidas, afectaciones o alteraciones en el normal funcionamiento de la Personería Municipal de Rionegro, así como impactar la confidencialidad, integridad y disponibilidad de la información. Este proceso se realiza en cumplimiento de la normativa legal vigente y de los lineamientos institucionales en materia de seguridad y privacidad de la información, con el fin de prevenir materializaciones de riesgo y definir oportunamente las acciones de tratamiento correspondientes.

Riesgos	Causas	Efectos
Pérdida, robo o fuga de información	- Uso de equipos institucionales por parte de personal no autorizado. - Acceso no autorizado a las oficinas y áreas restringidas. - Conexión de dispositivos de almacenamiento externos no autorizados. - Ausencia o deficiencia en los mecanismos de respaldo de la información. - Insuficiencia de equipos institucionales para el desarrollo de las actividades**.**	- Afectación a la confidencialidad, integridad y disponibilidad de la información. - Pérdida total o parcial de información institucional. - Deterioro de la imagen y reputación institucional. - Posibles sanciones administrativas, disciplinarias o económicas derivadas del incumplimiento normativo.
Daño en los equipos tecnológicos	- Manejo inadecuado de los equipos por parte de los usuarios. - Falta de mantenimiento preventivo y correctivo. - Deficiencias en las instalaciones eléctricas o conexiones inadecuadas. - Condiciones ambientales no apropiadas para la	- Pérdida de información almacenada en los equipos. - Daños físicos irreparables en los activos tecnológicos. - Interrupción parcial o total de la prestación del servicio. - Afectación al cumplimiento de las funciones misionales y administrativas.

Riesgos	Causas	Efectos
	operación de los equipos.	
Perdida de conectividad	- Fallas en el servicio de internet o en los proveedores de conectividad. - Daños en la infraestructura de red interna.	- Interrupción temporal de los servicios institucionales. - Afectación en el acceso a los sistemas de información y a la atención al ciudadano. - Retrasos en la ejecución de los procesos institucionales.

10.4. Identificación de amenazas

La identificación de amenazas consiste en reconocer los eventos, personas, situaciones o fenómenos que pueden ocasionar daño, pérdida, alteración o indisponibilidad de los activos de información y demás activos asociados de la Personería Municipal de Rionegro. Las amenazas pueden tener origen humano, ambiental, técnico o físico, y pueden afectar la confidencialidad, integridad y disponibilidad de la información, así como la continuidad de los procesos institucionales.

Este ejercicio permite anticipar escenarios de riesgo y constituye un insumo fundamental para la valoración del riesgo y la definición de controles y acciones de tratamiento, en concordancia con la normativa vigente y las buenas prácticas en gestión de la seguridad y privacidad de la información.

A continuación, se relacionan algunas de las principales amenazas identificadas para la entidad:

Amenaza	Tipo
Polvo, corrosión	Evento ambiental
Inundación	Evento ambiental
Incendios	Evento ambiental
Fenómenos sísmicos	Evento ambiental
Perdida el suministro de energía	Daño físico e infraestructura
Fallas del equipo	Falla técnica

11. SEGUIMIENTO

La Personería Municipal de Rionegro realizará seguimiento trimestral a la gestión de las amenazas y de los riesgos de seguridad y privacidad de la información identificados, con el propósito de verificar el cumplimiento y la efectividad de los controles implementados, así como el avance de las acciones definidas en el Plan de Tratamiento de Riesgos. Este seguimiento permitirá identificar desviaciones, oportunidades de mejora y necesidades de ajuste, en concordancia con la normativa vigente y los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG).

Responsables

El seguimiento estará a cargo del Personero Municipal, los Personeros delegados y los líderes de proceso, quienes, de acuerdo con sus competencias y responsabilidades, deberán verificar la correcta implementación de las acciones de tratamiento de riesgos y reportar los resultados correspondientes. Los servidores públicos y contratistas de la entidad deberán suministrar la información requerida para el desarrollo de este proceso.

12. CONTROL DE CAMBIOS

VERSIÓN	FECHA	CAMBIO
2	31/01/2026	Elaboración y adopción del Plan de Seguridad y Privacidad de la Información conforme a normatividad vigente