PERSONERÍA DE RIONEGRO

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

VERSIÓN 1

PERSONERÍA MUNICIPAL
RIONEGRO, ANTIOQUIA
2025

CONTENIDO

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2025

La Personería municipal de Rionegro distingue el papel fundamental que tiene la información en el cumplimiento de los procesos, por esta razón, se desarrollan las acciones necesarias para un manejo adecuado y una protección idónea de los activos. Estas acciones incluyen la prevención de amenazas que violenten los principios fundamentales de confidencialidad, integridad y disponibilidad de la información. Por ende, el plan de tratamientos de riesgos se realiza con la finalidad de conocer cómo se realizará la implementación de los lineamientos de Gobierno digital, definidos por MinTIC, que buscan dar protección a los datos de las personas tanto jurídicas como naturales, brindando una seguridad en la información que se da a conocer y sobre todo asumiendo los retos que trae la tecnología día a día, actualizando los planes de acción a la era digital.

1. OBJETIVO GENERAL

Identificar y analizar los riesgos de seguridad y privacidad de la información que se relacionen con los procesos que existen en la Personería Municipal de Rionegro, definiendo acciones que promuevan la prevención y control para evitar su materialización.

2. ALCANCE

El presente plan regirá y se aplicará a todos los procesos que conforman el Sistema Integrado de Gestión de la Personería Municipal de Rionegro.

3. MARCO NORMATIVO

REFERENTE NORMATIVO	TEMÁTICA
Políticas técnicas de	Busca proteger los activos de información (grupos de valor, información, procesos, tecnologías de información incluido el hardware y el software), mediante el establecimiento de lineamientos generales para la aplicación de la seguridad de

REFERENTE NORMATIVO	TEMÁTICA
seguridad de la información Función Pública	la información en la gestión de los procesos internos, bajo el marco del Modelo Integrado de Planeación y Gestión.
Decreto 103 de 2015	Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.
Decreto 1008	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
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.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Constitución Política de Colombia 1991	Artículo 15. Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.
Norma técnica colombiana NTC - ISO/IEC 27001	Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa.

4. DESARROLLO DEL PLAN

4.1. Recursos

- Personal: personero municipal, personeros delegados, líderes de los procesos, contratistas.
- Físico: implementos de trabajo, computadores y equipos de comunicaciones.

4.2. Identificación de activos de información

Tipo de activo	Información
Información	El principal activo de la Personería es la información, la cual puede estar en forma física como documentos impresos o escritos a mano, en medios

Tipo de activo	Información
	electrónicos almacenados en discos duros externos, memorias USB, en los equipos de cómputo o en la nube
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
Hardware	Equipos físicos de cómputo
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa.
Servicios	Servicio brindado por parte de la Personería para el apoyo de las actividades de los procesos.
Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para los procesos, son considerados activos de información: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la Personería

4.3. Identificación de los riesgos

El objetivo de la identificación de los riesgos es conocer los incidentes o eventos que pueden causar pérdidas o alteraciones en el funcionamiento de la Personería Municipal de Rionegro y pueden afectar la confidencialidad, integridad y disponibilidad de la información.

Riesgos	Causas	Efectos
Pérdida, robo o fuga de información	- Prestar los equipos informáticos a personal no autorizado. - Acceso no autorizado a las oficinas. - Conectar dispositivos externos a los equipos.	- Mala imagen - Pérdida de información - Multas, sanciones y pérdidas económicas.

Riesgos	Causas	Efectos
	- Falta de equipos electrónicos para copias de respaldos - Falta de equipos institucionales	
Daño en los equipos tecnológicos	- Manejo inadecuado de los equipos - Falta de mantenimiento o mala conexión de estos en las instalaciones eléctricas - Falta de ambiente adecuado para los equipos	- Pérdida de información - Pérdida de los equipos informáticos - Interrupción en la prestación del servicio
Perdida de conectividad	- Daño en el Internet	- Pérdida temporal del servicio

4.4. Identificación de amenazas

Una amenaza se identifica como un evento, persona, situación o fenómeno, que puede causar daño a los activos de la Personería, las amenazas pueden ser de origen humano o ambiental.

Amenaza	Tipo
Polvo, corrosión	Evento natural
Inundación	Evento natural
Incendios	Evento natural
Fenómenos sísmicos	Evento natural
Perdida el suministro de energía	Daño físico
Fallas del equipo	Fallas técnicas

5. SEGUIMIENTO

Se realiza seguimiento trimestral a la gestión de amenazas y de los riesgos de seguridad y privacidad de la información identificados, definiendo acciones de mejora de ser necesario.

6. CONTROL DE CAMBIOS

VERSIÓN	FECHA	CAMBIO
1	31/01/2025	Creación del documento