# POLÍTICA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

2023



Secretaría de Gestión Humana y Desarrollo Organizacional

Subsecretaría de TIC

Secretaria de Gestión Humana y Desarrollo Organizacional
**Carolina Tejada Marín**

Subsecretario de TIC
**Harlem Augusto Ramírez**

Profesional Universitario
**Wilson Libardo López**
Profesional Universitario
**Juan Sebastian Abril**
Profesional Universitario
**Deivis Carrillo**

Profesional Universitario
**David Alejandro Machado**
Profesional Universitario
**Leidy Paola Pérez**
Profesional Universitario
**Luis Antonio Ruiz**

Colaboradores contratistas
**Bladimir Villada, Dairo Ayala**
**Fabián Arbeláez, Julián Arbeláez, Giovanni Piedrahita, Andrés Ruiz**

CONTENIDO

# 1 INTRODUCCIÓN

En la actualidad, el gobierno colombiano reconoce la información como un activo valioso y a medida que los sistemas de información apoyan cada vez más los procesos de misión, se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos.

Por esta razón, el Ministerio de tecnologías de la información y las telecomunicaciones por medio del decreto 1078 de 2015 da la directriz para que, entre otros ejes, se implemente el eje de seguridad y privacidad de la información basado en la norma técnica NTC-ISO-IEC27001 “Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información”.

También se considera el Modelo Integrado de Planificación y Gestión MIPG y su actualización mediante el decreto 1499 de 2017, en su articulado 2.2.22.1.5 “Articulación y complementariedad con otros sistemas de gestión”. Establece que: “El Sistema de Gestión se complementa y articula, entre otros, con los sistemas nacional de servicio al ciudadano, de gestión de la seguridad y salud en el trabajo, de gestión ambiental y de Seguridad de la Información”.

Por lo anterior y consciente de sus necesidades actuales, el Municipio de Rionegro implementará el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) como una herramienta de gestión que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales y regulatorios vigentes.

# 2 OBJETIVOS

## 2.1 Objetivo General

Establecer la política general del Sistema de Gestión de Seguridad de la Información (SGSI) y proveer una guía respecto a la seguridad de los sistemas de información y privacidad de los datos personales en el Municipio de Rionegro.

### 2.2 Objetivos específicos

- Establecer el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI)
- Definir el marco políticas específicas de Seguridad y Privacidad de la Información en el Municipio de Rionegro
- Establecer lineamientos para la revisión, mantenimiento y actualización de este plan.

## 3 ALCANCE

Las política general de gestión de seguridad de la información contenida en este plan aplican para todos los usuarios internos del Municipio de Rionegro en todos los niveles jerárquicos y todos los usuarios externos como aprendices, practicantes, proveedores y demás partes interesadas.

## 4 POLÍTICA GENERAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Municipio de Rionegro, entendiendo la importancia de una adecuada gestión de la información, se compromete con la implementación de un Sistema de Gestión de Seguridad de la Información buscando fortalecer la confianza en el ejercicio de sus deberes con los grupos de interés, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la organización.

Para el Municipio de Rionegro, la protección de la información busca la disminución del impacto generado sobre sus activos por los riesgos identificados de manera sistemática, con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

Los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Cumplir con los principios de la función administrativa.
- Cumplir con los principios de seguridad de la información.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.

- Establecer las políticas específicas, procedimientos e instructivos en materia de seguridad de la información.
- Minimizar el riesgo de los procesos misionales de la entidad.
- Garantizar la continuidad del negocio frente a incidentes de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del Municipio de Rionegro
- Mantener la confianza de los usuarios, funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.

El Municipio de Rionegro establece los siguientes principios de seguridad que soportan el SGSI:

1. Definir, implementar, operar y mejorar de forma continua un sistema de gestión de seguridad de la información, soportado en lineamientos claros, alineados a las necesidades del negocio y a los requerimientos regulatorios que le aplican a su naturaleza.
2. Proteger la información generada, procesada, transmitida o resguardada por los procesos de negocio y su infraestructura tecnológica, del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
3. Proteger la información generada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de ésta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
4. Proteger la información de las amenazas originadas por parte del personal.
5. Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
6. Controlar la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y de las redes de datos.
7. Implementar controles de acceso a la información, sistemas y recursos de red.
8. Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
9. Garantizar, a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información, una mejora efectiva de su modelo de seguridad.
10. Garantizar la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos adversos de seguridad.
11. Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

12. Las responsabilidades frente a la seguridad de la información deben ser definidas, compartidas y publicadas por la organización y aceptadas por cada uno de los empleados, contratistas, proveedores, socios de negocio y terceros.

Esta política de seguridad y privacidad de la información se complementará con políticas específicas, procedimientos, normas y guías específicas para orientar su implementación.

El incumplimiento de la política de seguridad y privacidad de la Información acarrea las consecuencias legales que apliquen a la normativa de la organización, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a seguridad y privacidad de la Información se refiere.

# 5 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

## 5.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El Comité Institucional del Gestión y Desempeño debe definir y documentar los roles y responsabilidades que las personas, procesos y dependencias deben asumir frente a la seguridad de la información en la entidad.

## 5.2 GESTIÓN DE ACTIVOS DE INFORMACIÓN

La Subsecretaría de TIC debe:

1. Identificar los activos de información al interior de la entidad
2. Clasificar los activos de información de acuerdo a los requisitos legales.
3. Etiquetar e inventariar los activos de información
4. Proporcionar herramientas como sistemas y formatos para apoyar la devolución de los activos de información por los funcionarios, contratistas y terceros tras la terminación del empleo, acuerdo o contrato que tenían con la entidad.
5. Garantizar la adecuada disposición de activos de información físicos y digitales una vez sean dados de baja.
6. Coordinar la gestión del inventario de activos tecnológicos con la Subsecretaría de Desarrollo Organizacional.
7. Determinar las políticas de conexión de dispositivos móviles a las redes inalámbricas de la entidad.

## 5.3 CONTROL DE ACCESO

La Subsecretaría de TIC debe documentar los procedimientos y controles necesarios para:

1. Controlar el acceso a los activos de información mediante usuario y contraseña.
2. Suministrar el control de acceso a los activos de información a los usuarios autorizados.
3. Gestionar las contraseñas de acceso a los activos de información.
4. Asegurar los perímetros físicos de seguridad de los cuartos de cableado y procesamiento de información.

## 5.4 NO REPUDIO

La Subsecretaría de TIC debe establecer los procedimientos y controles necesarios para realizar la trazabilidad de las acciones de los usuarios en los sistemas de información de la entidad.

## 5.5 PRIVACIDAD Y CONFIDENCIALIDAD

Con el fin de dar cumplimiento a la Ley 1581 de 2012, el Municipio de Rionegro debe establecer, implementar, difundir y actualizar periódicamente una política de tratamiento de datos personales.

## 5.6 INTEGRIDAD

Todos los funcionarios, contratistas y/o terceros que establezcan una vinculación contractual con la entidad deben aceptar y dar cumplimiento a la siguiente cláusula contractual, denominada Clausula de integridad de la información:

“Toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.”

## 5.7 DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

La Subsecretaría de TIC debe definir para cada servicio, con la participación de los líderes de cada proceso cliente, las siguientes características del servicio:

1. Niveles de disponibilidad
2. Planes de recuperación
3. Interrupciones

4. Acuerdos de Nivel de Servicio
5. Segregación de Ambientes
6. Gestión de Cambios

### 5.8 REGISTRO Y AUDITORIA

La Subsecretaría de TIC debe definir, con la participación la Oficina de Control Interno, una política que vele por el mantenimiento de las evidencias de las actividades y acciones que afecten los activos de información y contenga:

1. Responsabilidad
2. Almacenamiento de Registros
3. Normatividad
4. Garantía cumplimiento
5. Periodicidad

### 5.9 GESTIÓN DE INCIDENTES

La subsecretaría de TIC cuenta con una política general de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información.

### 5.10 CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

La Subsecretaría de TIC debe documentar, con la participación la Subsecretaría de Talento Humano, una política de capacitación y sensibilización del personal en seguridad y privacidad de la información.

## 6 REVISIÓN, MANTENIMIENTO Y ACTUALIZACIÓN DE ESTE PLAN

El Comité Institucional de Gestión y Desempeño debe revisar y actualizar esta política semestralmente o cada vez que sea usada para dar respuesta a la materialización de un riesgo y también cuando se presente uno de los siguientes eventos:

- Cambios normativos
- Adquisición de infraestructura tecnológica o sistemas de información
- Cambios en la estructura organizacional

Los objetivos de la revisión y actualización de esta política son:

- Revisar la adecuación a requisitos legales

- Agregar aspectos no considerados dentro de la política general
- Actualizar los planes y políticas.

## 7 DOCUMENTOS ASOCIADOS

- Políticas específicas de seguridad de la información.
- Plan de gestión de seguridad de la información
- Matriz de aplicabilidad de los dominios según ISO 27001.
- Plan de tratamiento de riesgos de la seguridad de la información

## 8 CONTROL DE CAMBIOS

| FECHA | VER. | PROYECTÓ | REVISÓ | APROBÓ | DESCRIPCIÓN |
|---|---|---|---|---|---|
| 24/01/2019 | 1.0 | Oscar Franco Catalina Martínez | Héctor Fabio Orjuela | Comité Institucional de Gestión y Desempeño | Versión inicial |
| 17/05/2022 | 2.0 | Juan Abril | Héctor Fabio Orjuela | Comité Institucional de Gestión y Desempeño | Primera versión, actualización de ISO 27001 |