

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PSPI

MUNICIPIO DE RIOSUCIO – CALDAS

Entidad: Municipio de Riosucio Caldas

Tipo de documento: Plan Institucional

Vigencia: 2026 – 2027

Versión: 1.0

Fecha de adopción: 31 de enero de 2026

Contenido

1. INTRODUCCIÓN	5
2. OBJETIVOS DEL PLAN	6
2.1 Objetivo General	6
2.2 Objetivos Específicos	6
3. ALCANCE	7
4. MARCO NORMATIVO	9
4.1 Normatividad Constitucional	9
4.2 Normatividad Reglamentaria	9
4.3 Políticas públicas y lineamientos institucionales	10
4.4 El PSPI se articula de manera directa con el Modelo Integrado de Planeación y Gestión – MIPG, en particular con:	11
4.5 Normas técnicas y buenas prácticas de referencia	11
5. DEFINICIONES Y CONCEPTOS CLAVES	11
6. PRINCIPIOS DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	14
6.1 Principio de legalidad	14
6.2 Principio de Finalidad	14
6.3 Principio de Confidencialidad	14
6.4 Principio de Seguridad	14
6.5 Principio de Integridad	15
6.6 Principio de Disponibilidad	15
6.7 Principio de responsabilidad y rendición de cuentas	15
6.8 Principio de Transparencia	15
6.9 Principio de gestión de riesgo	15
6.10 Principio de mejora continua	15
7. CLASIFICACION DE LA INFORMACION	16
7.1 Criterios para la clasificación de la información	16
7.2 Niveles de Clasificación de la información	16
7.2.1 Información Publica	16
7.2.2 Información de uso interno	17
7.2.3 Información confidencial	17

7.2.4	Información con datos personales y sensibles	18
7.3	Responsabilidades y Clasificación.....	18
7.4	Actualización de la clasificación	18
8.	ROLES Y RESPONSABILIDADES.....	18
8.1	Alcalde Municipal	19
8.2	Secretaría de Planeación (o quien haga sus veces).....	19
8.3	Oficina de Control Interno	19
8.4	Responsables de Proceso y Jefes de Dependencia.....	20
8.5	Servidores Públicos	20
8.6	Contratistas y Terceros	20
8.7	Área de Sistemas o Soporte Tecnológico (cuando aplique)	21
9.	GESTION DEL RIESGO Y SEGURIDAD DE LA INFORMACION.....	21
9.1.	Objetivo de la Gestión del Riesgo.....	21
9.2.	Metodología para la Gestión del Riesgo	22
9.3.	Identificación de Riesgos de Seguridad de la Información.....	22
9.4.	Tratamiento de los Riesgos	23
9.5.	Articulación con el Mapa de Riesgos Institucional.....	23
9.6.	Seguimiento y Actualización	23
10.	CONTROLES DE SEGURIDAD DE LA INFORMACION	23
10.1.	Controles Administrativos	24
10.1.1.	Políticas de Seguridad de la Información	24
10.1.2.	Control de Accesos	24
10.1.3.	Gestión del Talento Humano	24
10.2.	Controles Técnicos	24
10.2.1.	Seguridad de Contraseñas.....	24
10.2.2.	Protección de Equipos y Sistemas.....	25
10.2.3.	Respaldo de la Información (Backups).....	25
10.3.	Controles Físicos.....	25
10.3.1.	Acceso a Instalaciones	25
10.3.2.	Protección de Documentos Físicos.....	25

10.4.	Controles para el Manejo de Datos Personales.....	25
10.5.	Evaluación de los Controles	26
11.	PROTECCION DE DATOS PERSONALES.....	28
11.1.	Objeto	28
11.2.	Marco Normativo Aplicable a la Protección de Datos Personales	28
11.3.	Ámbito de Aplicación	29
11.4.	Principios para el Tratamiento de Datos Personales	29
11.5.	Tipos de Datos Personales Tratados	29
11.6.	Derechos de los Titulares de la Información	29
11.7.	Deberes del Municipio como Responsable del Tratamiento	30
11.8.	Procedimiento para Consultas y Reclamos.....	30
11.9.	Medidas de Seguridad para la Protección de Datos Personales	30
11.10.	Transferencia y Transmisión de Datos Personales.....	30
11.11.	Gestión de Incidentes de Seguridad de la Información	31
12.	VIGENCIA, SEGUIMIENTO, ACTUALIZACIÓN Y ADOPCIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	31
12.1.	Vigencia del Plan de Seguridad y Privacidad de la Información.....	31
12.2.	Seguimiento y Evaluación del PSPI	31
12.3.	Actualización y Mejora Continua.....	32
12.4.	Articulación con el Modelo Integrado de Planeación y Gestión – MIPG	32
12.5.	Adopción del Plan de Seguridad y Privacidad de la Información	32
12.6.	Responsabilidad y Cumplimiento.....	33

1. INTRODUCCIÓN

La información constituye uno de los activos más importantes del Municipio de Riosucio Caldas, en tanto soporta la toma de decisiones, la prestación de los servicios públicos, el cumplimiento de la función administrativa y la garantía de los derechos de los ciudadanos. En este sentido, la adecuada gestión, protección y uso responsable de la información institucional se convierte en un elemento estratégico para fortalecer la confianza ciudadana, la transparencia, la eficiencia administrativa y el control institucional.

El Municipio de Riosucio Caldas, en el desarrollo de sus competencias constitucionales y legales, administra información en diferentes formatos y niveles de clasificación, incluyendo información pública, información de uso interno, información confidencial y datos personales, algunos de ellos catalogados como datos sensibles, especialmente aquellos relacionados con población vulnerable y comunidades étnicas, los cuales gozan de una protección reforzada conforme al ordenamiento jurídico colombiano.

En cumplimiento de lo dispuesto en la Ley 1581 de 2012, el Decreto 1377 de 2013, el Decreto 1074 de 2015, así como en concordancia con la Ley 1712 de 2014, el CONPES 3854 de 2016 y el Modelo Integrado de Planeación y Gestión – MIPG, el Municipio reconoce la obligación de implementar medidas técnicas, administrativas y organizacionales orientadas a garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de la información que se encuentra bajo su custodia.

El presente Plan de Seguridad y Privacidad de la Información – PSPI se formula como un instrumento de gestión institucional que permite identificar, analizar y mitigar los riesgos asociados al manejo de la información, fortalecer la cultura organizacional en materia de seguridad de la información y asegurar el cumplimiento de los principios de legalidad, finalidad, seguridad y confidencialidad en el tratamiento de los datos personales.

Así mismo, el PSPI se articula con los planes institucionales del Municipio de Riosucio Caldas, con el Plan de Desarrollo Municipal, con el Sistema de Control Interno y con las dimensiones de Información y Comunicación y de Control Interno del MIPG, constituyéndose en una herramienta transversal que contribuye a la mejora continua de la gestión pública y a la sostenibilidad de los procesos institucionales.

Finalmente, este Plan establece los lineamientos, responsabilidades, controles y mecanismos de seguimiento necesarios para proteger la información institucional frente a amenazas internas y externas, reducir la probabilidad de incidentes de

seguridad, y garantizar la continuidad de los servicios a la ciudadanía, en un entorno cada vez más digital y expuesto a riesgos tecnológicos.

2. OBJETIVOS DEL PLAN.

2.1 Objetivo General

Establecer los lineamientos, controles y responsabilidades necesarios para garantizar la seguridad y la privacidad de la información del Municipio de Riosucio Caldas, mediante la implementación de medidas técnicas, administrativas y organizacionales que permitan proteger la confidencialidad, integridad y disponibilidad de la información institucional, asegurar el adecuado tratamiento de los datos personales y mitigar los riesgos asociados al uso de las tecnologías de la información, en cumplimiento de la normatividad vigente y en articulación con el Modelo Integrado de Planeación y Gestión – MIPG.

2.2 Objetivos Específicos

- Identificar y clasificar la información institucional del Municipio de Riosucio Caldas, de acuerdo con su nivel de sensibilidad, criticidad y uso, con el fin de establecer medidas de protección proporcionales a los riesgos asociados.
- Definir y aplicar controles de seguridad de la información que permitan prevenir, detectar y responder de manera oportuna a incidentes que puedan afectar la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional.
- Garantizar el cumplimiento de la Ley 1581 de 2012, sus decretos reglamentarios y demás disposiciones legales relacionadas con la protección de datos personales, asegurando el respeto de los derechos de los titulares de la información.
- Fortalecer la gestión del riesgo de seguridad de la información mediante la identificación, análisis y tratamiento de amenazas internas y externas que puedan impactar los procesos misionales, estratégicos y de apoyo del Municipio.
- Establecer responsabilidades claras para los servidores públicos, contratistas y terceros en relación con el uso, manejo, custodia y protección de la información institucional.
- Promover una cultura organizacional de seguridad y privacidad de la información, a través de estrategias de sensibilización, capacitación y buenas prácticas dirigidas a todos los actores que interactúan con la información del Municipio.

- Asegurar la continuidad de los servicios institucionales mediante la implementación de mecanismos de respaldo, recuperación y gestión de incidentes de seguridad de la información.
- Articular el Plan de Seguridad y Privacidad de la Información con el Plan de Desarrollo Municipal, el Sistema de Control Interno y las dimensiones de Información y Comunicación y Control Interno del Modelo Integrado de Planeación y Gestión – MIPG.
- Establecer mecanismos de seguimiento, evaluación y mejora continua que permitan medir la efectividad del Plan de Seguridad y Privacidad de la Información y realizar los ajustes necesarios conforme a los cambios normativos, tecnológicos y organizacionales.

3. ALCANCE

El presente Plan de Seguridad y Privacidad de la Información – PSPI aplica a todas las dependencias, procesos, sistemas de información, activos tecnológicos y no tecnológicos, así como a todos los servidores públicos, contratistas y terceros que, en ejercicio de sus funciones o actividades contractuales, tengan acceso, utilicen, administren o custodien información del Municipio de Riosucio Caldas.

El alcance del PSPI comprende la información institucional en cualquiera de sus formas de creación, almacenamiento, procesamiento y transmisión, incluyendo, pero sin limitarse a:

3.1 Alcance Organizacional

El Plan aplica a todas las dependencias del Municipio de Riosucio Caldas, entre las cuales se incluyen, a título enunciativo:

- Despacho del Alcalde
- Secretaría de Planeación
- Secretaria de Medio Ambiente
- Secretaría de Hacienda
- Secretaría de Gobierno y asuntos administrativos
- Dirección local de Salud
- Secretaría de Educación
- Secretaría de Desarrollo Social
- Secretaria de Cultura y Turismo
- Secretaria de Desarrollo Económico y Servicios Públicos
- Secretaria de Desarrollo Social y Comunitario

- Oficina de Infraestructura y Obras Públicas
- Oficina de Control Interno
- Terminal
- Demás dependencias, oficinas asesoras y unidades administrativas

3.2 Alcance sobre la Información

El PSPI cubre toda la información que sea generada, recibida, almacenada, procesada o transmitida por el Municipio de Riosucio Caldas, independientemente de su formato o medio, incluyendo:

- Información en formato digital (bases de datos, archivos electrónicos, correos institucionales, sistemas de información)
- Información en formato físico (documentos impresos, expedientes, archivos, registros)
- Información verbal y audiovisual
- Datos personales y datos sensibles, especialmente aquellos relacionados con población vulnerable, comunidades indígenas y grupos de especial protección constitucional

3.3 Alcance sobre los sistemas de información y Activos Tecnológicos

El Plan aplica a los sistemas de información, aplicaciones, plataformas y activos tecnológicos utilizados por el Municipio, tales como:

- Sistemas de planeación y seguimiento institucional
- Sistemas de gestión administrativa y financiera
- Correo electrónico institucional
- Página web y servicios digitales
- Equipos de cómputo, servidores, dispositivos de almacenamiento, redes y periféricos
- Servicios tecnológicos contratados con terceros

3.4 Alcance sobre el Talento Humano y Terceros

El PSPI es de obligatorio cumplimiento para:

- Servidores públicos del Municipio de Riosucio Caldas
- Contratistas y personal de apoyo a la gestión
- Proveedores y terceros que tengan acceso a información institucional, ya sea de manera permanente o temporal

Todos los actores incluidos en el alcance del Plan deberán cumplir con las políticas, procedimientos y controles establecidos en el PSPI, independientemente del tipo de vinculación o modalidad contractual.

3.5 Exclusiones y alcance

El presente plan no regula la información personal o privada de los servidores públicos y contratistas que no esté relacionada con el ejercicio de sus funciones, ni los sistemas o activos tecnológicos de carácter estrictamente personal, salvo cuando su uso esté autorizado para el desarrollo de actividades institucionales.

4. MARCO NORMATIVO

El Plan de Seguridad y Privacidad de la Información – PSPI del Municipio de Riosucio Caldas, se formula y adopta en cumplimiento del marco normativo colombiano vigente, así como de los lineamientos y políticas públicas aplicables a la gestión de la información, la seguridad digital, la protección de datos personales y el fortalecimiento de la gestión institucional en las entidades del orden territorial.

El presente Plan se fundamenta en las siguientes disposiciones normativas y documentos de referencia:

4.1 Normatividad Constitucional

Constitución Política de Colombia

- Artículo 15: Derecho fundamental al habeas data, a la intimidad personal y familiar, y al buen nombre.
- Artículo 209: Principios de la función administrativa, entre ellos la eficiencia, eficacia, economía, transparencia y responsabilidad.

4.2 Normatividad Reglamentaria



Casa de Gobierno Municipal Carrera 7, calle 10 Esquina



www.riosucio-caldas.gov.co



alcaldia@riosucio-caldas.gov.co

Alcaldía Riosucio Caldas 

Alcaldía de Riosucio 

Ley 1581 de 2012

Por la cual se dictan disposiciones generales para la protección de datos personales y se establecen los principios y obligaciones para su tratamiento por parte de entidades públicas y privadas.

Ley 1266 de 2008

Por la cual se dictan disposiciones generales del habeas data financiero y crediticio, aplicable cuando la entidad administre este tipo de información.

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.

Decreto 1377 de 2013

Por el cual se reglamenta parcialmente la Ley 1581 de 2012, en lo relacionado con el tratamiento de datos personales.

Decreto 1074 de 2015

Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, que compila las normas sobre protección de datos personales.

Decreto 1083 de 2015

Decreto Único Reglamentario del Sector Función Pública, que establece disposiciones relacionadas con el control interno y la gestión institucional.

Decreto 612 de 2018

Por el cual se fijan las directrices para la integración de los planes institucionales y estratégicos al Plan de Acción, incluyendo el Plan de Seguridad y Privacidad de la Información

4.3 Políticas públicas y lineamientos institucionales

CONPES 3854 de 2016

Política Nacional de Seguridad Digital, orientada a la gestión del riesgo digital y al fortalecimiento de la confianza en el entorno digital.

CONPES 3995 de 2020

Política Nacional de Transformación Digital e Inteligencia Artificial, que promueve el uso seguro y responsable de las tecnologías de la información en el sector público.

Lineamientos del Departamento Administrativo de la Función Pública – DAFP Relacionados con el Modelo Integrado de Planeación y Gestión – MIPG, especialmente en las dimensiones de Información y Comunicación y Control Interno.

4.4 El PSPI se articula de manera directa con el Modelo Integrado de Planeación y Gestión – MIPG, en particular con:

Dimensión Información y Comunicación, que promueve la calidad, disponibilidad, integridad y seguridad de la información institucional.

Dimensión Control Interno, que incorpora la gestión del riesgo, los controles y la mejora continua como elementos fundamentales para la protección de los activos de información.

4.5 Normas técnicas y buenas prácticas de referencia

Sin perjuicio del cumplimiento de la normatividad obligatoria, el Municipio de Riosucio Caldas, adopta como referencia las siguientes buenas prácticas internacionales, en la medida de sus capacidades institucionales y presupuestales:

- **ISO/IEC 27001** – Sistemas de Gestión de Seguridad de la Información
- **ISO/IEC 27002** – Controles de seguridad de la información
- **ISO 31000** – Gestión del riesgo

Estas normas se consideran marcos de referencia para el fortalecimiento progresivo de la seguridad de la información, sin que su adopción implique certificación obligatoria.

5. DEFINICIONES Y CONCEPTOS CLAVES

Para efectos de la correcta interpretación y aplicación del presente Plan de Seguridad y Privacidad de la Información – PSPI, se adoptan las siguientes definiciones, las cuales se fundamentan en la normatividad colombiana vigente y en buenas prácticas reconocidas en materia de seguridad de la información:

Activo de Información:

Cualquier información o elemento relacionado con su tratamiento que tenga valor para el Municipio de Riosucio Caldas, incluyendo datos, documentos, sistemas, equipos, personas, procesos y servicios.

Autorización:

Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales, de conformidad con lo establecido en la Ley 1581 de 2012.

Confidencialidad:

Propiedad de la información que garantiza que solo sea accesible a personas, procesos o sistemas debidamente autorizados.

Dato Personal:

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables, conforme a la Ley 1581 de 2012.

Dato Sensible:

Aquel dato personal que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación, tales como datos relacionados con origen étnico, estado de salud, orientación política, creencias religiosas, entre otros. En el contexto municipal, incluye información de comunidades indígenas y población vulnerable.

Disponibilidad:

Propiedad de la información que garantiza que esté accesible y utilizable cuando sea requerida por los usuarios autorizados.

Gestión del Riesgo de Seguridad de la Información:

Proceso sistemático orientado a identificar, analizar, evaluar y tratar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional.

Incidente de Seguridad de la Información:

Evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de la información institucional, tales como accesos no autorizados, pérdida de información, ataques informáticos o divulgación indebida de datos.

Información Pública:

Información que puede ser conocida por cualquier persona, de conformidad con la Ley 1712 de 2014, salvo las excepciones legales.

Información Confidencial:

Información cuyo acceso se encuentra restringido y cuya divulgación no autorizada puede generar impactos legales, administrativos o reputacionales para el Municipio o para los titulares de la información.

Integridad:

Propiedad de la información que salvaguarda su exactitud, completitud y validez, evitando modificaciones no autorizadas.

Modelo Integrado de Planeación y Gestión – MIPG:

Marco de referencia para la gestión de las entidades públicas, orientado al logro de resultados y a la satisfacción de las necesidades de los ciudadanos, integrando planeación, gestión, evaluación y control.

Plan de Seguridad y Privacidad de la Información – PSPI:

Instrumento de gestión institucional que establece políticas, lineamientos, controles y responsabilidades para proteger la información del Municipio de Riosucio Caldas.

Responsable del Tratamiento:

Persona natural o jurídica, pública o privada, que decide sobre la base de datos y/o el tratamiento de los datos personales.

Tratamiento:

Cualquier operación o conjunto de operaciones sobre datos personales, tales como recolección, almacenamiento, uso, circulación o supresión.

Trazabilidad:

Capacidad de identificar y rastrear las acciones realizadas sobre la información, incluyendo accesos, modificaciones y transferencias.

6. PRINCIPIOS DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El Plan de Seguridad y Privacidad de la Información – PSPI del Municipio de Riosucio Caldas, se fundamenta en los principios legales, técnicos y administrativos que orientan el adecuado tratamiento, protección y uso responsable de la información institucional, en concordancia con la normatividad vigente y los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG.

Los siguientes principios son de obligatorio cumplimiento para todos los servidores públicos, contratistas y terceros que tengan acceso a la información institucional:

6.1 Principio de legalidad

El tratamiento de la información y de los datos personales se realizará conforme a la Constitución Política, la Ley 1581 de 2012, sus decretos reglamentarios y demás normas aplicables, garantizando que toda actividad relacionada con la información tenga un fundamento jurídico válido.

6.2 Principio de Finalidad

La información será recolectada, utilizada y tratada exclusivamente para el cumplimiento de las funciones legales, misionales y administrativas del Municipio de Riosucio Caldas, y no será utilizada para fines diferentes a los autorizados o previstos en la ley.

6.3 Principio de Confidencialidad

Toda persona que tenga acceso a la información institucional está obligada a garantizar la reserva y confidencialidad de la información, incluso después de finalizar su relación laboral o contractual con el Municipio, evitando su divulgación, uso o acceso no autorizado.

6.4 Principio de Seguridad.

El Municipio de Riosucio Caldas, adoptará las medidas técnicas, humanas y administrativas necesarias para proteger la información contra accesos no

autorizados, pérdida, alteración, destrucción o divulgación indebida, de acuerdo con el nivel de riesgo y la criticidad de la información.

6.5 Principio de Integridad.

La información institucional deberá mantenerse completa, exacta y confiable, garantizando que no sea alterada de manera indebida durante su almacenamiento, procesamiento o transmisión.

6.6 Principio de Disponibilidad

La información y los sistemas que la soportan deberán estar disponibles y accesibles para los usuarios autorizados cuando sea requerida, garantizando la continuidad de los servicios institucionales y la atención oportuna a la ciudadanía.

6.7 Principio de responsabilidad y rendición de cuentas

Cada servidor público, contratista y tercero es responsable del adecuado uso, custodia y protección de la información a la que tenga acceso, debiendo actuar conforme a las políticas, procedimientos y controles establecidos en el presente Plan.

6.8 Principio de Transparencia

El Municipio garantizará el acceso a la información pública en los términos establecidos por la Ley 1712 de 2014, sin perjuicio de la protección de la información reservada, confidencial y de los datos personales.

6.9 Principio de gestión de riesgo

La seguridad de la información se gestionará bajo un enfoque preventivo, basado en la identificación, análisis y tratamiento de los riesgos que puedan afectar los activos de información, en coherencia con el Sistema de Control Interno y el MIPG.

6.10 Principio de mejora continua

El Plan de Seguridad y Privacidad de la Información será objeto de seguimiento, evaluación y actualización periódica, con el fin de adaptarse a los cambios

normativos, tecnológicos y organizacionales, y fortalecer de manera progresiva el nivel de seguridad de la información institucional.

7. CLASIFICACION DE LA INFORMACION

Con el fin de garantizar un manejo adecuado, seguro y proporcional de la información institucional, el Municipio de Riosucio Caldas, adopta un esquema de clasificación de la información, el cual permite establecer los niveles de protección, control y acceso de acuerdo con la naturaleza, sensibilidad y criticidad de la información, en cumplimiento de la normatividad vigente.

La clasificación de la información constituye un elemento fundamental para la gestión del riesgo de seguridad de la información y es de obligatorio cumplimiento para todos los servidores públicos, contratistas y terceros que tengan acceso a la información institucional.

7.1 Criterios para la clasificación de la información

La información institucional será clasificada teniendo en cuenta, entre otros, los siguientes criterios:

- Impacto legal derivado de su divulgación, pérdida o uso indebido
- Impacto administrativo, operativo o financiero
- Impacto reputacional para el Municipio de Riosucio Caldas
- Presencia de datos personales o datos sensibles
- Requerimientos legales de reserva, confidencialidad o publicidad

7.2 Niveles de Clasificación de la información

El Municipio de Riosucio Caldas, adopta los siguientes niveles de clasificación:

7.2.1 Información Publica

Es aquella información que puede ser conocida por cualquier persona, de conformidad con lo dispuesto en la Ley 1712 de 2014, y cuya divulgación no genera riesgos legales, administrativos o reputacionales para la entidad.

Ejemplos:

- Plan de Desarrollo Municipal
- Informes de gestión
- Actos administrativos de carácter general
- Información publicada en la página web institucional

Medidas de manejo:

- Acceso libre y controlado
- Publicación conforme a los lineamientos de transparencia

7.2.2 Información de uso interno

Es aquella información destinada al uso exclusivo de los servidores públicos y contratistas del Municipio, necesaria para el desarrollo de las funciones institucionales, cuya divulgación no autorizada podría afectar la gestión administrativa.

Ejemplos:

- Comunicaciones internas
- Informes de trabajo
- Documentos de apoyo a la gestión
- Bases de datos internas sin datos sensibles

Medidas de manejo:

- Acceso restringido a personal autorizado
- Prohibición de divulgación externa sin autorización

7.2.3 Información confidencial

Es aquella información cuyo acceso se encuentra restringido y cuya divulgación, pérdida o alteración no autorizada puede generar impactos legales, administrativos, financieros o reputacionales para el Municipio o para terceros.

Ejemplos:

- Expedientes contractuales en trámite
- Procesos disciplinarios
- Historias laborales
- Información financiera no publicada

Medidas de manejo:

- Acceso limitado y controlado
- Custodia reforzada
- Registro de accesos cuando aplique

7.2.4 Información con datos personales y sensibles

Corresponde a la información que contiene datos personales y, en especial, datos sensibles, cuyo tratamiento se encuentra sujeto a una protección especial conforme a la Ley 1581 de 2012.

Ejemplo:

- Bases de datos del Sisbén
- Información de salud
- Datos de población vulnerable
- Información de comunidades indígenas y grupos étnicos

Medidas de manejo:

- Acceso estrictamente limitado
- Autorización del titular cuando aplique
- Medidas técnicas y administrativas reforzadas
- Prohibición de divulgación sin soporte legal

7.3 Responsabilidades y Clasificación

Cada dependencia del Municipio de Riosucio Caldas, será responsable de identificar y clasificar la información que genere, administre o custodie, de acuerdo con los criterios establecidos en el presente Plan.

La Secretaría de Planeación, o quien haga sus veces, brindará acompañamiento técnico para la correcta aplicación del esquema de clasificación.

7.4 Actualización de la clasificación

La clasificación de la información deberá ser revisada y actualizada periódicamente, o cuando se presenten cambios normativos, tecnológicos o administrativos que así lo requieran, como parte del proceso de mejora continua del PSPI.

8. ROLES Y RESPONSABILIDADES

Con el fin de garantizar la adecuada implementación, operación, seguimiento y mejora continua del Plan de Seguridad y Privacidad de la Información – PSPI, el Municipio de Riosucio Caldas, define los siguientes roles y responsabilidades, los

cuales son de obligatorio cumplimiento para todos los actores que interactúan con la información institucional.

8.1 Alcalde Municipal

El Alcalde del Municipio de Riosucio Caldas, en su calidad de máxima autoridad administrativa, es responsable de:

- Liderar y respaldar la implementación del Plan de Seguridad y Privacidad de la Información.
- Garantizar la asignación de los recursos necesarios para la ejecución del PSPI, de acuerdo con las capacidades institucionales.
- Velar por el cumplimiento del marco normativo aplicable en materia de seguridad y privacidad de la información.
- Promover una cultura institucional orientada a la protección de la información y al cumplimiento de los principios de seguridad y privacidad.

8.2 Secretaría de Planeación (o quien haga sus veces)

La Secretaría de Planeación será la dependencia responsable de la administración y coordinación del PSPI y tendrá, entre otras, las siguientes responsabilidades:

- Coordinar la implementación, actualización y mejora continua del Plan de Seguridad y Privacidad de la Información.
- Articular el PSPI con el Plan de Desarrollo Municipal, el Plan de Acción y el Modelo Integrado de Planeación y Gestión – MIPG.
- Acompañar a las dependencias en la identificación, clasificación y gestión de los activos de información.
- Liderar la gestión del riesgo de seguridad de la información, en coordinación con las áreas involucradas.
- Promover acciones de sensibilización y capacitación en materia de seguridad y privacidad de la información.

8.3 Oficina de Control Interno

La Oficina de Control Interno será responsable de:

- Realizar seguimiento y evaluación a la implementación y cumplimiento del PSPI.
- Verificar la efectividad de los controles definidos en el Plan.
- Formular recomendaciones para la mejora continua del sistema de seguridad y privacidad de la información.
- Incorporar los riesgos de seguridad de la información dentro del Sistema de Control Interno y los procesos de auditoría interna.

8.4 Responsables de Proceso y Jefes de Dependencia

Los responsables de proceso y jefes de dependencia tendrán a su cargo:

- Garantizar la correcta aplicación del PSPI en los procesos bajo su responsabilidad.
- Identificar y clasificar la información que se genera o administra en su dependencia.
- Autorizar y controlar el acceso a la información institucional conforme a su nivel de clasificación.
- Reportar oportunamente cualquier incidente de seguridad de la información.

8.5 Servidores Públicos

Todos los servidores públicos del Municipio de Riosucio Caldas, son responsables de:

- Cumplir las políticas, procedimientos y controles establecidos en el PSPI.
- Proteger la información a la que tengan acceso en razón de sus funciones.
- Utilizar adecuadamente los activos tecnológicos y de información.
- Reportar de manera inmediata cualquier incidente o situación que pueda comprometer la seguridad de la información.

8.6 Contratistas y Terceros

Los contratistas, proveedores y terceros que tengan acceso a información institucional deberán:

- Cumplir con las disposiciones del PSPI y las cláusulas contractuales relacionadas con la seguridad y privacidad de la información.
- Utilizar la información exclusivamente para los fines autorizados.
- Garantizar la confidencialidad de la información, incluso después de la finalización del contrato.
- Reportar cualquier incidente de seguridad de la información del que tengan conocimiento.

8.7 Área de Sistemas o Soporte Tecnológico (cuando aplique)

El área de sistemas o quien haga sus veces será responsable de:

- Implementar y administrar los controles técnicos de seguridad de la información.
- Gestionar los accesos a los sistemas de información.
- Realizar respaldos periódicos de la información crítica.
- Apoyar la atención y gestión de incidentes de seguridad de la información.

9. GESTION DEL RIESGO Y SEGURIDAD DE LA INFORMACION.

El Municipio de Riosucio Caldas, adopta un enfoque preventivo y sistemático para la gestión del riesgo de seguridad de la información, orientado a identificar, analizar, evaluar y tratar los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional.

La gestión del riesgo de seguridad de la información se articula con el Sistema de Control Interno y con el Modelo Integrado de Planeación y Gestión – MIPG, y se desarrolla de conformidad con los lineamientos del CONPES 3854 de 2016, la ISO 31000 y las buenas prácticas de seguridad de la información.

9.1. Objetivo de la Gestión del Riesgo

Prevenir, reducir y controlar los riesgos asociados al uso, manejo y protección de la información institucional, con el fin de minimizar los impactos legales, operativos, financieros y reputacionales que puedan afectar al Municipio de Riosucio Caldas.

9.2. Metodología para la Gestión del Riesgo

El Municipio aplicará una metodología sencilla y proporcional a su capacidad institucional, basada en las siguientes etapas:

1. Identificación del riesgo:

Reconocimiento de las amenazas y vulnerabilidades que puedan afectar los activos de información.

2. Análisis del riesgo:

Evaluación de la probabilidad de ocurrencia y del impacto del riesgo sobre la información y los procesos institucionales.

3. Evaluación del riesgo:

Determinación del nivel de riesgo para establecer prioridades de tratamiento.

4. Tratamiento del riesgo:

Definición e implementación de controles para reducir, mitigar, aceptar o evitar el riesgo.

5. Seguimiento y revisión:

Monitoreo periódico de los riesgos y de la efectividad de los controles implementados.

9.3. Identificación de Riesgos de Seguridad de la Información

El Municipio de Riosucio Caldas, identifica como riesgos comunes, entre otros, los siguientes:

- Uso de contraseñas débiles o compartidas
- Acceso no autorizado a sistemas de información
- Pérdida o daño de equipos de cómputo
- Uso de correos electrónicos personales para actividades institucionales
- Ataques de ingeniería social y phishing

- Pérdida de información por falta de respaldos
- Manejo inadecuado de datos personales y datos sensibles

9.4. Tratamiento de los Riesgos

Los riesgos identificados serán tratados mediante la implementación de controles técnicos, administrativos y humanos, tales como:

- Políticas de control de acceso a la información
- Uso obligatorio de credenciales individuales
- Procedimientos de respaldo y recuperación de la información
- Sensibilización y capacitación del personal
- Procedimientos de reporte y atención de incidentes

El tratamiento de los riesgos será proporcional al nivel de riesgo identificado y a la criticidad de la información afectada.

9.5. Articulación con el Mapa de Riesgos Institucional

Los riesgos de seguridad de la información deberán ser incorporados en el Mapa de Riesgos Institucional del Municipio de Riosucio Caldas, y gestionados de manera articulada con los demás riesgos administrativos, operativos y estratégicos.

9.6. Seguimiento y Actualización

La gestión del riesgo de seguridad de la información será revisada de manera periódica y actualizada cuando se presenten cambios normativos, tecnológicos u organizacionales, como parte del proceso de mejora continua del PSPI.

10. CONTROLES DE SEGURIDAD DE LA INFORMACION

El Municipio de Riosucio Caldas, implementa controles de seguridad de la información de carácter administrativo, técnico y físico, orientados a prevenir, detectar y mitigar los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional.

Los controles definidos en el presente Plan se aplican de manera proporcional al nivel de riesgo y a la criticidad de la información, teniendo en cuenta las capacidades institucionales y presupuestales del Municipio.

10.1. Controles Administrativos

Los controles administrativos establecen las reglas, políticas y procedimientos que orientan el adecuado manejo de la información institucional.

10.1.1. Políticas de Seguridad de la Información

- Adopción y divulgación del PSPI como documento de obligatorio cumplimiento.
- Definición de políticas específicas sobre uso aceptable de la información y de los activos tecnológicos.

10.1.2. Control de Accesos

- Asignación de usuarios y contraseñas individuales.
- Prohibición del uso de cuentas genéricas o compartidas.
- Revocación inmediata de accesos cuando finalice la relación laboral o contractual.

10.1.3. Gestión del Talento Humano

- Inclusión de compromisos de confidencialidad en los contratos.
- Sensibilización periódica sobre seguridad y privacidad de la información.
- Responsabilidad individual sobre el uso de la información.

10.2. Controles Técnicos

Los controles técnicos buscan proteger los sistemas de información y los activos tecnológicos frente a amenazas internas y externas.

10.2.1. Seguridad de Contraseñas

- Longitud mínima de ocho (8) caracteres.

- Cambio periódico de contraseñas.
- Prohibición de compartir credenciales.

10.2.2. Protección de Equipos y Sistemas

- Bloqueo automático de equipos por inactividad.
- Uso de antivirus y actualizaciones de seguridad.
- Restricción de instalación de software no autorizado.

10.2.3. Respaldo de la Información (Backups)

- Realización de copias de seguridad periódicas de la información crítica.
- Almacenamiento de respaldos en medios seguros.
- Verificación periódica de la recuperación de la información.

10.3. Controles Físicos

Los controles físicos buscan proteger los activos de información frente a accesos no autorizados, daños o pérdidas.

10.3.1. Acceso a Instalaciones

- Control de acceso a oficinas y áreas donde se maneje información sensible.
- Custodia de archivos físicos en lugares seguros.
-

10.3.2. Protección de Documentos Físicos

- Almacenamiento adecuado de expedientes y archivos.
- Restricción de acceso a documentos clasificados como confidenciales o con datos personales.

10.4. Controles para el Manejo de Datos Personales

El Municipio implementará medidas específicas para la protección de datos personales y datos sensibles, tales como:

- Autorización previa del titular cuando aplique.
- Uso de la información únicamente para los fines autorizados.
- Restricción de acceso a bases de datos con información sensible.
- Cumplimiento de los principios de la Ley 1581 de 2012.

10.5. Evaluación de los Controles

La efectividad de los controles de seguridad de la información será evaluada periódicamente por la Secretaría de Planeación y la Oficina de Control Interno, con el fin de identificar oportunidades de mejora y fortalecer el sistema de seguridad de la información.

Dimensión	Recomendación	Descripción técnica	Responsable	Prioridad	Evidencia esperada
Gobierno de TI	Adoptar y socializar el PSPI	Implementar formalmente el PSPI mediante decreto y socializarlo a funcionarios y contratistas	Alcaldía / Planeación	Alta	Decreto, actas
Talento humano	Capacitación en seguridad	Capacitar periódicamente en manejo seguro de la información y protección de datos	Talento Humano	Alta	Listados, material
Control de acceso	Gestión de usuarios	Definir perfiles de acceso según funciones y principio de mínimo privilegio	TIC	Alta	Matriz de accesos
Autenticación	Contraseñas seguras	Establecer políticas de complejidad, vigencia y confidencialidad de contraseñas	TIC	Alta	Política, configuración
Gestión de activos	Inventario de información	Mantener inventario	Planeación / TIC	Media	Inventario

		actualizado de activos de información y responsables			
Respaldo	Copias de seguridad	Realizar backups periódicos de sistemas críticos y verificar su recuperación	TIC	Alta	Registros
Continuidad	Plan de contingencia	Definir procedimientos para continuidad ante incidentes tecnológicos	Planeación / TIC	Media	Plan aprobado
Seguridad física	Control de acceso físico	Restringir acceso a áreas críticas (servidores, archivos)	General	Media	Registros
Protección de datos	Manejo de datos personales	Aplicar Ley 1581 en recolección, almacenamiento y uso de datos	Dependencias	Alta	Políticas
Incidentes	Gestión de incidentes	Establecer procedimiento para reporte y atención de incidentes	TIC / Planeación	Alta	Registros
Uso de equipos	Uso aceptable	Definir reglas para el uso de equipos, correo y dispositivos	TIC	Media	Política
Correo electrónico	Buenas prácticas	Prevenir phishing,	TIC	Alta	Campañas

		adjuntos sospechosos y uso indebido			
Software	Actualizaciones	Mantener sistemas y antivirus actualizados	TIC	Alta	Reportes
Proveedores	Seguridad contractual	Incluir cláusulas de confidencialidad y seguridad en contratos	Jurídica	Media	Contratos
Monitoreo	Auditoría de seguridad	Realizar revisiones periódicas al cumplimiento del PSPI	Control Interno	Media	Informes

11. PROTECCION DE DATOS PERSONALES

11.1. Objeto

El presente capítulo tiene como objeto establecer los lineamientos, responsabilidades, procedimientos y medidas técnicas, administrativas y organizacionales que permitan garantizar la adecuada protección de los datos personales tratados por la Administración Municipal de Riosucio Caldas, en cumplimiento de la normatividad colombiana vigente en materia de protección de datos personales y del derecho fundamental de Habeas Data.

11.2. Marco Normativo Aplicable a la Protección de Datos Personales

La protección de datos personales en el Municipio de Riosucio Caldas, se rige principalmente por las siguientes disposiciones:

- Constitución Política de Colombia, artículo 15.
- Ley 1581 de 2012 – Régimen General de Protección de Datos Personales.
- Decreto 1377 de 2013 – Reglamentación parcial de la Ley 1581 de 2012.
- Decreto 1074 de 2015 – Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.

- Ley 1266 de 2008 – Régimen de Habeas Data financiero (cuando aplique).
- Circulares Externas y lineamientos de la Superintendencia de Industria y Comercio (SIC).
- Política de Gobierno Digital.
- Modelo Integrado de Planeación y Gestión – MIPG.

11.3. Ámbito de Aplicación

Las disposiciones de este capítulo aplican a:

- Todas las dependencias de la Administración Municipal de Riosucio Caldas.
- Servidores públicos, contratistas, practicantes y terceros que traten datos personales.
- Bancos de datos, archivos físicos o digitales y sistemas de información bajo responsabilidad del Municipio.

11.4. Principios para el Tratamiento de Datos Personales

El tratamiento de datos personales se realizará conforme a los siguientes principios:

- Legalidad
- Finalidad
- Libertad
- Veracidad o calidad
- Transparencia
- Acceso y circulación restringida
- Seguridad
- Confidencialidad

11.5. Tipos de Datos Personales Tratados

El Municipio de Riosucio Caldas, podrá tratar:

- Datos públicos
- Datos semiprivados
- Datos privados
- Datos sensibles
- Datos de niños, niñas y adolescentes

11.6. Derechos de los Titulares de la Información

El Municipio garantizará los derechos de los titulares, entre ellos:

- Conocer, actualizar y rectificar sus datos

- Solicitar prueba de la autorización
- Ser informado sobre el uso de sus datos
- Presentar quejas ante la SIC
- Revocar la autorización o solicitar supresión
- Acceder gratuitamente a su información

11.7. Deberes del Municipio como Responsable del Tratamiento

El Municipio de Riosucio Caldas, deberá:

- Garantizar el derecho de Habeas Data
- Solicitar y conservar autorizaciones
- Informar la finalidad del tratamiento
- Proteger la información con medidas de seguridad
- Atender consultas y reclamos
- Reportar incidentes de seguridad cuando aplique

11.8. Procedimiento para Consultas y Reclamos

El Municipio dispondrá de procedimientos que incluyan:

- Canales oficiales de atención
- Tiempos de respuesta legales
- Registro y trazabilidad
- Mecanismos de cierre y control

11.9. Medidas de Seguridad para la Protección de Datos Personales

Se implementarán medidas como:

- Control de accesos físicos y lógicos
- Gestión de usuarios y perfiles
- Autenticación segura
- Copias de seguridad
- Capacitación del personal
- Gestión de incidentes
- Auditorías periódicas

11.10. Transferencia y Transmisión de Datos Personales

La transferencia o transmisión de datos personales solo se realizará cuando:

- Exista autorización o habilitación legal
- Se garantice nivel adecuado de protección

- Se formalicen acuerdos o contratos

11.11. Gestión de Incidentes de Seguridad de la Información

Los incidentes que comprometan datos personales deberán:

- Ser identificados y documentados
- Evaluar su impacto
- Notificarse a la SIC cuando corresponda
- Generar acciones correctivas y preventivas

12. VIGENCIA, SEGUIMIENTO, ACTUALIZACIÓN Y ADOPCIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

12.1. Vigencia del Plan de Seguridad y Privacidad de la Información

El Plan de Seguridad y Privacidad de la Información (PSPI) del Municipio de Riosucio Caldas, entrará en vigencia a partir de la fecha de expedición del acto administrativo que lo adopte y tendrá una vigencia indefinida, mientras no sea modificado, actualizado o derogado por disposición expresa.

El PSPI será de obligatorio cumplimiento para todas las dependencias de la Administración Municipal, sus servidores públicos, contratistas y terceros que tengan acceso a la información institucional.

12.2. Seguimiento y Evaluación del PSPI

El seguimiento y evaluación del Plan de Seguridad y Privacidad de la Información estará a cargo de la Secretaría de Planeación o la dependencia que haga sus veces, en articulación con:

- La Oficina de Control Interno.
- El responsable de Tecnologías de la Información.
- Los líderes de proceso de cada dependencia.

El seguimiento deberá contemplar, como mínimo:

- Verificación del cumplimiento de las políticas, controles y procedimientos definidos en el PSPI.
- Evaluación de la gestión del riesgo de seguridad de la información.
- Revisión de incidentes de seguridad reportados y su tratamiento.
- Medición de indicadores de desempeño asociados a seguridad y privacidad de la información.

- Reportes periódicos a la alta dirección.

12.3. Actualización y Mejora Continua

El Plan de Seguridad y Privacidad de la Información deberá ser revisado y/o actualizado:

- Como mínimo, una vez al año.
- Cuando se presenten cambios normativos relevantes.
- Ante la incorporación de nuevos sistemas de información o tecnologías.
- Como resultado de auditorías, evaluaciones o incidentes de seguridad.
- Cuando se identifiquen riesgos emergentes o cambios en el contexto institucional.

Las actualizaciones deberán documentarse y ser aprobadas por la autoridad competente mediante el acto administrativo correspondiente.

12.4. Articulación con el Modelo Integrado de Planeación y Gestión – MIPG

El PSPI se articula con las políticas y dimensiones del Modelo Integrado de Planeación y Gestión – MIPG, en especial con:

- La Dimensión de Gestión con Valores para Resultados.
- La Política de Gobierno Digital.
- La Política de Control Interno.
- La Política de Transparencia, Acceso a la Información Pública y Lucha contra la Corrupción.
- La Política de Gestión del Conocimiento y la Innovación.

Esta articulación permitirá fortalecer la gestión institucional y garantizar la protección integral de la información pública y los datos personales.

12.5. Adopción del Plan de Seguridad y Privacidad de la Información

El presente Plan de Seguridad y Privacidad de la Información será adoptado mediante Decreto Municipal, expedido por el Alcalde del Municipio de Riosucio Caldas, en ejercicio de sus facultades constitucionales y legales.

Una vez adoptado, el PSPI deberá ser:

- Socializado a todos los servidores públicos y contratistas.
- Publicado en los medios institucionales correspondientes.
- Incorporado como instrumento de gestión institucional.
- Considerado en los procesos de inducción, reinducción y capacitación.

12.6. Responsabilidad y Cumplimiento

El incumplimiento de las disposiciones contenidas en el presente Plan dará lugar a las acciones administrativas, disciplinarias, contractuales o legales a que haya lugar, de conformidad con la normativa vigente.

Cada servidor público y contratista es responsable del cumplimiento de las disposiciones del PSPI en el marco de sus funciones y responsabilidades.

Tabla 1 Clasificación de la información

Clasificación de la información	Descripción	Ejemplos en el Municipio	Nivel de acceso	Controles MIPG asociados
Información pública	Información de libre acceso conforme a Ley 1712 de 2014	Acuerdos, decretos, resoluciones	Público	Publicación web, datos abiertos
Información de uso interno	Información para la gestión institucional	Informes internos, memorandos	Restringido	Control de acceso, perfiles
Información confidencial	Información institucional sensible	Procesos disciplinarios, contratación	Limitado	Autenticación, confidencialidad
Datos personales	Información de personas naturales	SISBÉN, historias laborales	Autorizado	Ley 1581, control y reserva

Tabla 2 Roles y responsabilidades

Rol	Dependencia	Responsabilidad MIPG
Alcalde Municipal	Despacho	Liderar y adoptar políticas institucionales
Comité Institucional de Gestión y Desempeño	Todas	Orientar y aprobar lineamientos
Secretaría de Planeación	Planeación	Coordinar, hacer seguimiento y reportar
Responsable TIC	Responsable TIC	Implementar controles tecnológicos
Oficina de Control Interno	OCI	Evaluar la efectividad del PSPI

Líderes de proceso	Todas	Identificar riesgos y custodiar información
Funcionarios y contratistas	Todas	Cumplimiento del PSPI

Tabla 3 Gestión del riesgo de la seguridad de la información

Riesgo identificado	Activo de información	Causa	Impacto	Nivel de riesgo	Controles definidos
Pérdida de información	Bases de datos	Fallas técnicas	Alto	Alto	Backups, planes de contingencia
Acceso no autorizado	Sistemas de información	Contraseñas débiles	Alto	Alto	Autenticación, perfiles
Fuga de información	Archivos físicos	Manejo inadecuado	Medio	Medio	Custodia, confidencialidad
Alteración de datos	Sistemas	Error humano	Medio	Medio	Control de cambios

Tipo de dato	Finalidad del tratamiento	Base legal	Responsable	Medidas de seguridad
Identificación	Gestión administrativa	Ley 1581 de 2012	Dependencia	Acceso restringido
Salud	Programas sociales	Autorización / Ley	Secretaría	Confidencialidad
Datos de menores	Atención social	Interés superior	Dependencia	Reserva estricta
Datos laborales	Gestión del talento	Ley laboral	Talento Humano	Custodia