Personería San Sebastián de Mariquita	***PERSONERIA MUNICIPAL DE SAN SEBASTIAN DE MARIQUITA***

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PERSONERIA DE SAN SEBASTIÁN DE MARIQUITA

2026

Palacio del Mangostino Calle 4 Carrera 3 Esquina Piso 3 – Teléfono (8) 2522152

personeria@sansebastiandemariquita-tolima.gov.co

INTRODUCCION

La Política de la seguridad de la información de la Personería Municipal de San Sebastián de Mariquita asegura que la organización establece la protección de los activos de información (funcionarios, contratistas, partes interesadas, la información, los procesos, las tecnologías de información incluido el hardware y el software) dando cumplimiento a los requisitos establecidos por las partes interesadas en la gestión de la Información.

Además tiene como propósito salvaguardar la información generada dentro de la entidad garantizando así la seguridad de los datos y dando cumplimiento a la normatividad legal vigente, para poder realizar un Plan de Seguridad y Privacidad de la información con el fin de que no se presenten robos, perdidas de información, accesos no autorizados y duplicación de información que puedan ocasionar daños a los usuarios tanto internos como externos.

La Personería Municipal cumple con los tres pilares de la seguridad de la información en preservar la integridad, confidencialidad y disponibilidad de la información (2,30 ISO 27000):

- Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000)

- Confidencialidad: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000)

- Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000)

1. ALCANCE

El Plan de Seguridad y Privacidad de la información de la Personería Municipal tiene como alcance los recursos, procesos, procedimientos y demás actividades relacionadas, incluyendo a los funcionarios, contratistas y demás partes interesadas que usen los activos de información generados dentro de la entidad.

2. TERMINOS Y DEFINICIONES

• Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

• Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

• Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

• Confidencialidad: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000)

• Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000).

• Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

• Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

• Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación

• Procedimiento: Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.

• Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

3. MARCO NORMATIVO

Ley 527/99 "Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos" Ley 1266/08 "Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países".

Ley 1581/12 "Por la cual se dictan disposiciones generales para la protección de datos personales".

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 1499 del 11 de septiembre de 2017 Por medio del cual se modifica el Decreto 1083 de 2015,

Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

Decreto 612 del 04 de abril de 2018 Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

Decreto 1008 del 14 de junio de 2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1

4. OBJETIVO

Establecer lineamientos para la implementación de políticas que garanticen la administración, manejo y control de la seguridad y privacidad de la información de la Personería Municipal de Piedecuesta.

4.1. OBJETIVOS ESPECIFICOS

Implementar políticas y procedimientos enfocados en la de seguridad de la información.

Fomentar la cultura de seguridad de la información en los funcionarios, contratistas y demás partes interesadas de la Personería Municipal de Apia

Mitigar los riesgos asociados a la seguridad de la Información que afecten la integridad, confidencialidad, disponibilidad y privacidad de la Información de la Personería Municipal de San Sebastián de Mariquita.

5. PRINCIPIOS

a) Para la Personería Municipal de San Sebastián de Mariquita es importante generar políticas de la Seguridad de la Información cuyo fin es brindar orientación y soporte por parte de la alta dirección para dar cumplimiento con los requisitos de la entidad, las leyes y demás reglamentarios pertinentes.

b) Los funcionarios y contratistas de la entidad deben ser asumir las responsabilidades y roles asignado de la seguridad de la información antes, durante y terminando con su empleo o actividades asignadas por la alta dirección.

c) La Integridad de la información de la Personería Municipal debe preservar siempre su autenticidad manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.

d) La Disponibilidad de la Información de la Personería Municipal debe estar disponible cuando sea requerida por cualquier parte interesada.

e) La confidencialidad de la información de la Personería Municipal es garantizar que la información personal será protegida y accedida solo por aquellos que estén involucrados en dicha información y no será divulgada sin consentimiento ninguno.

f) La privacidad de la Información de la Personería Municipal debe estar preservada con el fin de que sea utilizadas para los propósitos que fue generada.

6. RESPONSABLES

La personería Municipal tiene como responsables de la implementación, seguimiento y mantenimiento de la Política del Plan de Seguridad y Privacidad de la información lo siguiente:

- El personero municipal
- El secretario de la personería municipal
- Los contratistas y demás que presten cualquier servicio a la entidad.

7. POLITICAS

La Personería Municipal de divulga los objetivos y alcances de la seguridad de la información de la entidad, que son efectivos por medio de controles de seguridad, con el fin de mantener y gestionar el riesgo como se estable en el Plan de Tratamiento de Riesgos, garantizando así la continuidad de los servicios y disminuyendo la probabilidad de amenazas que puedan los procesos internos para el cumplimiento de los objetivos institucionales.

• Identificación, clasificación y valoración de activos de información. Cada proceso, bajo supervisión y con base en el inventario de activos entregado por la Personería Municipal de Piedecuesta se debe mantener actualizado en donde se incorpore la clasificación, valoración, ubicación y acceso de la información y demás características identificas por la Alta dirección permitiendo así la administración eficiente de cada proceso garantizando la disponibilidad, integridad y confidencialidad de dicha información.

• Seguridad de la información en el Talento Humano Todas y todos los servidores públicos de la Personería Municipal, independiente del tipo de vinculación laboral o contractual, o de los procesos al que pertenezca y del nivel de funciones o actividades que desempeñe deben contar con un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. Por ende, se debe

contar con un directorio completo y actualizado de los perfiles creados. aclarando que el proceso de cadena de custodia de la información debe hacer parte integral de un procedimiento de terminación de la relación contractual o de cambio de cargo.

• Usuarios invitados y servicios de acceso público. El acceso de usuarios no registrados solo debe estar autorizado por el personero municipal, de manera de información institucional, igualmente el servicio de internet al que puedan acceder debe estar protegido con una contraseña, contando con una restricción de sitios web no autorizados. Si los usuarios invitados no realizaron el debido proceso de registro, no se permitirá el acceso a cualquier otro tipo de recursos de información, aplicación y/o herramientas TIC.

• Seguridad Física y del entorno Seguridad en los equipos: Los servidores o equipos de cómputo que contengan informaciones institucionales deben estar en un ambiente seguro y protegido por lo menos con: - Controles de acceso y seguridad física. - Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Además, toda información institucional en formato digital debe ser mantenida en los servidores y/o unidades extraíbles aprobados por el personero municipal. También se debe asegurar que la infraestructura está cubierta por mantenimiento y soporte adecuados tanto para el hardware como para el software y las estaciones de trabajo deben ser operadas por funcionarios de la institución el cual deben estar capacitados acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional. Se deben incluir los medios que alojan copias de seguridad el cual deben ser conservados de forma correcta de acuerdo a las políticas y estándares establecidos.

• Administración de las comunicaciones y operaciones Reporte y revisión de incidentes de seguridad: El personal vinculado a la Personería Municipal, debe realizar el reporte de una manera eficiente y con responsabilidad de las presuntas violaciones de seguridad detectadas y se deben reportar al personero municipal cuando la ocasión lo amerite si es un caso especial y podrá realizarse directamente por la persona que encuentre el incidente o novedad. Se debe diseñar, mantener y difundir las normas, procesos y guías para el reporte y revisión de incidentes de

seguridad el cual se mantendrá procedimientos escritos para la operación de dichas actividades sin afectar el desarrollo normal de la prestación del servicio y asegurando la confiabilidad de la información.

- Protección contra software malicioso y hacking.

Se debe proteger todos los sistemas de información que involucre los controles humanos, físicos técnicos y administrativos para no incurrir en daños siendo así se elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking que pueda afectar la prestación del servicio. Como control básico, todas las estaciones de trabajo de la Personería Municipal, deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus.

- Copias de Seguridad Toda información que se encuentre contenida en el inventario de activos de información o que sea de interés para un proceso siempre debe estar ser respaldada con copias de seguridad tomadas de acuerdo a los procedimientos documentados y probados. El procedimiento debe incluir actividades de almacenamiento, administración y custodia de las copias de seguridad incluyendo lugares seguros y control de registros de dichas copias. Dentro del procedimiento debe quedar claro que se deben efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad. Tener en cuenta que la creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios, es decir la responsabilidad de realizar las copias y mantenerlas actualizadas, recae directamente sobre cada dueño de los activos de la información de la Entidad.

- Intercambio de Información con Entidades Externas.

Las peticiones o solicitudes de información por parte de entes externos deben ser aprobadas por el personero municipal, y ser redireccionados a los responsables del manejo y custodia dicha información. Tener en cuenta que la información solicitada por parte de los entes externos debe ser realizada por un medio valido que permita el registro de la solicitud, donde se pueda identificar el remitente, el asunto y la fecha aclarando que toda información institucional debe ser manejada de acuerdo a la normatividad legal vigente.

• Instalación de Software Todas las instalaciones de software que se realicen sobre sistemas operativos previamente instalados en la Personería Municipal, deben ser aprobadas por el personero municipal.

Uso adecuado de Internet

La Personería Municipal es consciente de la importancia del servicio de Internet como una herramienta fundamental para el desempeño de labores que proporcionará los recursos necesarios para asegurar su disponibilidad a los servidores públicos y demás partes de interés que así lo requieran.

a. El proceso de TIC debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
b. El proceso de TIC debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
c. El proceso de TIC debe monitorear continuamente el canal o canales del servicio de Internet.
d. El proceso de TIC debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.

CAMILO ANDRÉS PERALTA GUZMÁN
Personero municipal