Personería de Floridablanca

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

FLORIDABLANCA, ENERO DE 2025

Calle 5 No. 8-25 Piso 3 - Palacio Municipal
Tel. 3165063181
E-mail: pmf@personeriadefloridablanca.gov.co
www.personeriadefloridablanca.gov.co
Floridablanca - Santander

Personería de Floridablanca

CONTENIDO

1. INTRODUCCIÓN 3
2. ALCANCE 4
TERMINOS Y DEFINICIONES 4
3. MARCO NORMATIVO 5
4. OBJETIVOS 6
OBJETIVO GENERAL 6
OBJETIVOS ESPECÍFICOS 6
5. DESCRIPCIÓN DE LAS POLÍTICAS 7
POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS 7
POLÍTICA DE CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y APLICATIVOS 8
POLÍTICAS DE SEGURIDAD FÍSICA 8
POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS 9
POLITICA DE USO ADECUADO DE INTERNET 9
6. PRIVACIDAD Y CONFIDENCIALIDAD 10
POLÍTICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES 10
COPIAS DE SEGURIDAD 11
7. CRONOGRAMA DE ACTIVIDADES 11

1. INTRODUCCIÓN

Con el permanente desarrollo tecnológico en el que el mundo se mueve hoy en día, se debe prestar especial atención a garantizar la privacidad y la seguridad de la información, convirtiéndose en uno de los pilares principales que busca lograr el óptimo desempeño de la gestión de la Personería Municipal de Floridablanca.

La información es el insumo principal del proceso de toma de decisiones en una entidad. Por eso, y debido al riesgo que su pérdida o manipulación indebida representa para las instituciones, la seguridad de la información se centra en el cuidado de los activos informáticos de valor estratégico.

La Personería Municipal de Floridablanca ha identificado la información como uno de los activos más importantes para el desarrollo de sus funciones, y por eso la imperiosa necesidad de establecer y reglamentar sus políticas de seguridad y privacidad, con el fin de protegerla y salvaguardarla.

Este documento tiene como finalidad dar a conocer el Plan de Seguridad y privacidad de la información, que deben aplicar los funcionarios, contratistas y terceros de la Personería Municipal de Floridablanca, entendiendo como consigna que la responsabilidad es de todos los actores que intervienen en ella.

La Personería Municipal de Floridablanca 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)

2. ALCANCE

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la Personería de Floridablanca y la ciudadanía en general, tiene como alcance los recursos, procesos, procedimientos y demás actividades relacionadas que usen los activos de información generados dentro de la entidad

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.

- **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.

- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza concreta pueda generar pérdida o afectación dañina en un activo de información; daños que pueden afectar la confidencialidad, integridad o disponibilidad de los contenidos protegidos de la entidad. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

- **Seguridad de la Información:** Este mandato de optimización busca crear confiabilidad en el uso digital, mediante estrategias basadas en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las diferentes dependencias de la entidad, y de los servicios que prestan al ciudadano.

- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

- **Integridad:** Propiedad de salvaguardar la exactitud y el estado completo de los activos.

- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado y cifrado.

- **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).

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información.

- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

3. MARCO NORMATIVO

La normatividad que cubre el Plan de Seguridad y Privacidad de la Información de la Personería Municipal de Floridablanca está contemplado dentro del marco de la legislación del Sistema de gestión pública, especialmente de la Política de Gobierno Digital y articulada con la reglamentación y lineamientos producidos por la legislación Colombiana, en donde se genera un nuevo enfoque en donde no sólo el Estado sino también los diferentes actores de la sociedad, son actores fundamentales para un desarrollo integral, donde las necesidades y problemáticas del contexto determinan el uso de la tecnología y la forma como ésta puede aportar en la generación de valor público

1. **Constitución Política de Colombia 1991**
   Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.

2. **Ley 527/99**
   “Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos”

3. **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"

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

5. **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

6. **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.

7. **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

8. **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 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

9. **Ley 1955 De 2019**
   "Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad

10. **CONPES 3701 de 2011**
    Lineamientos de política para ciber seguridad y ciber defensa

4. OBJETIVOS

OBJETIVO GENERAL

Establecer las pautas para administrar, proteger y controlar la información de la Personería de manera segura y confidencial

OBJETIVOS ESPECÍFICOS

- Describir las acciones del plan de Seguridad y Privacidad de la Información, cuya finalidad es el desarrollo, verificación y aplicación continua de mejoras en el Sistema de Gestión de Seguridad de la Información de la Personería Municipal de Floridablanca.

- Documentar y aplicar los controles y procedimientos necesarios para salvaguardar la integridad, confidencialidad y disponibilidad de los activos de información.

- Cumplir con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC en su estrategia de Gobierno en Línea.

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

5. DESCRIPCIÓN DE LAS POLÍTICAS

La Personería de Floridablanca gestiona una gran cantidad de datos sensibles que son esenciales para el cumplimiento de sus objetivos institucionales. Para asegurar la continuidad de sus operaciones y proteger la reputación de la entidad, es necesario implementar un sistema de gestión de seguridad de la información que garantice la integridad, disponibilidad y confidencialidad de los activos informáticos.

Esta política establece las medidas de seguridad necesarias para proteger la información de la entidad, mitigando los riesgos y garantizando la continuidad de los servicios. Su objetivo principal es preservar la integridad, confidencialidad y disponibilidad de los datos, cumpliendo con la normativa vigente.

POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

La Personería Municipal de Floridablanca implementará un sistema de control de acceso que restringirá el acceso de cada usuario a los recursos informáticos de la entidad, otorgando únicamente los privilegios necesarios para el desempeño de sus funciones. De esta manera, se garantizará que la información sea accesible solo por aquellos que estén autorizados.

Pautas para tener en cuenta

a. El Director de Gestión Financiera y Administrativa, debe definir lineamientos para la configuración de contraseñas que aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información de la Personería Municipal de Floridablanca; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

b. El Director de Gestión Financiera y Administrativa, debe implementar un procedimiento para retirar, reasignar o bloquear los permisos de acceso a los sistemas de información de aquellos empleados que hayan dejado la empresa,

estén de licencia o hayan cambiado de puesto. Esto garantizará que la información confidencial de la organización permanezca protegida.

c. El Director de Gestión Financiera y Administrativa, debe garantizar la desactivación inmediata de los accesos de los usuarios que ya no requieran de ellos, a fin de prevenir accesos no autorizados a los sistemas

POLÍTICA DE CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y APLICATIVOS

La Personería Municipal de Floridablanca ejercerá un control estricto sobre los permisos de acceso a sus sistemas, asegurando que solo el personal autorizado pueda utilizarlos.

El Director de Gestión Administrativa y Financiera se encarga de implementar y mantener sistemas de seguridad para proteger los datos de la organización, evitando accesos no autorizados.

Pautas para tener en cuenta

a. Los responsables de la información deben aprobar los permisos de acceso a los sistemas, asegurando que estos se ajusten a las necesidades de cada usuario.

b. Los responsables de la información deben revisar anualmente los permisos de acceso asignados a los usuarios para asegurar que sean los adecuados.

c. El Director de Gestión Administrativa y Financiera debe crear un conjunto de reglas claras y detalladas para determinar quién puede acceder a qué sistemas y con qué permisos, garantizando así la seguridad de la información.

POLÍTICAS DE SEGURIDAD FÍSICA

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) de ser el caso.

Además toda información institucional en formato digital debe ser mantenida en los servidores y/o unidades extraíbles aprobados.

Pautas para tener en cuenta

1. Las solicitudes de acceso al área donde se encuentra el servidor o los centros de cableado deben ser aprobadas por el Director Administrativo y Financiero; no obstante, los visitantes siempre deberán estar acompañados de un funcionario.

2. Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la Personería Municipal de Floridablanca; en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible

POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS

La Personería Municipal de Floridablanca para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

El personal vinculado a la Personería Municipal de Floridablanca, debe realizar el reporte de una manera eficiente y con responsabilidad de las presuntas violaciones de seguridad detectadas y se deben reportar a través de su jefe de dependencia o su supervisor a la Alta dirección o cuando la ocasión lo amerite si es un caso especial y podrá realizarse la directamente por la persona que encuentre el incidente o novedad

Pautas para tener en cuenta

1. La entidad debe realizar soportes técnicos y velar que se efectúen los mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la entidad.
2. Cuando se presente una falla o problema de hardware o software u otro recurso tecnológico propiedad de la Personería, el usuario responsable debe Director de Gestion Administrativa y Financiera, con el fin de realizar una asistencia adecuada.
3. La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la entidad, solo puede ser realizado por las personas designadas para este fin.
4. La Personería Municipal de Floridablanca, deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus.
5. Se 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.

POLITICA DE USO ADECUADO DE INTERNET

La Personería Municipal de Floridablanca reconoce que el acceso a internet es un servicio esencial para garantizar la eficiencia y eficacia en el desempeño de las funciones administrativas

Pautas para tener en cuenta

1. El área de TIC debe monitorear continuamente el canal o canales del servicio de Internet
2. Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.
3. El proceso de TIC debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
4. No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el facilitador del proceso Gestión de TIC o a quien haya sido delegada de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

6. PRIVACIDAD Y CONFIDENCIALIDAD

POLÍTICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

La Personería Municipal de Floridablanca, alineada con la Ley 1581 de 2012, se compromete a garantizar la protección integral de los datos personales de todos aquellos con quienes interactúa.

La Personería de Bucaramanga se compromete a proteger los datos personales de sus usuarios, estableciendo claras normas sobre la recolección, uso y divulgación de dicha información. Así mismo, busca proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información de la entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la entidad y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

Pautas para tener en cuenta

1. Todas las actividades que involucren la manipulación de datos personales, como la recolección, almacenamiento y uso, deben estar respaldadas por una autorización expresa.

2. El acceso a los datos personales se limitará únicamente a aquellos funcionarios que requieran de esta información para el cumplimiento de sus funciones.
3. Se debe implantar los controles necesarios para proteger la información personal de los usuarios, funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.
4. Los usuarios y funcionarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la entidad o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones

COPIAS DE SEGURIDAD

En cumplimiento de la normativa vigente en materia de protección de datos, toda información institucional crítica, incluida aquella contenida en la matriz de activos, deberá ser respaldada de manera regular. Estos respaldos se almacenarán en sitios seguros y de acceso restringido.

El director de Gestión Administrativa y Financiera establecerá los procedimientos y proporcionará las herramientas necesarias para garantizar la gestión adecuada de las copias de seguridad. La profesional de Control Interno se encargará de verificar el cumplimiento de estos procedimientos mediante auditorías periódicas.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios

7. CRONOGRAMA DE ACTIVIDADES

ACTIVIDADES	FECHA DE INICIO	FECHA FINAL
Definir las acciones a implementar a nivel de seguridad y privacidad y de mitigación del riesgo de Seguridad de la Información de la entidad.	Febrero 2025	Marzo 2025
Se socializarán las políticas con los funcionarios y contratistas de la Personería Municipal de Floridablanca, con el fin de dar cumplimiento a las medidas propuestas.	Febero 2025	Febero 2025
Optimización y continua mejora de la página web de la entidad, tomando medidas respecto a la Privacidad y seguridad de la información del portal institucional.	Enero 2025	Diciembre 2025

Establecer los procedimientos y proporcionará las herramientas necesarias para garantizar la gestión adecuada de las copias de seguridad	Octubre 2025	Diciembre 2025
Supervisión constante a los medios de comunicación de información de la entidad, para garantizar la seguridad de los mismos.	Enero 2025	Diciembre 2025

TABLA DE CONTROL DE REVISIONES Y MODIFICACIONES

CONTROL DE REVISIONES							
NO	**FECHA**	**DESCRIPCIÓN**	**ELABORO**	**CARGO**	**REVISO**	**APROBO**	**CARGO**
1.	21 de Enero de 2025	Actualización del Plan	Henry Alberto Restrepo Gamboa	Dirección de Gestión Administrativa y Financiera	Henry Alberto Restrepo Gamboa	María Alejandra Ramírez Ayala	Personera Municipal (E)
		FIRMAS					

HENRY ALBERTO RESTREPO GAMBOA
Dirección de Gestión Administrativa y Financiera