PERSONERIA MUNICIPAL DE FLORIDABLANCA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

FLORIDABLANCA, ENERO DE 2021

CONTENIDO

INTRODUCCIÓN	3
DEFINICIONES	4
OBJETIVOS	5
NORMATIVIDAD	5
CICLO DE OPERACIÓN	6
DIAGNÓSTICO	7
PLANIFICACIÓN	8
IMPLEMENTACIÓN	9
EVALUACIÓN DE DESEMPEÑO	10
MEJORA CONTINUA	10

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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 esta 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 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.

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.
- **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 (Ley 1712 de 2014, art 6)
- **Integridad:** Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000).
- **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, anonimización o cifrado
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- ✔ **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. (ISO/IEC 27000).

OBJETIVOS

OBJETIVO GENERAL

- Generar un documento de lineamientos de buenas prácticas en Seguridad y Privacidad de la información, para la Personería Municipal de Floridablanca para su divulgación, aplicación y revisión permanente.

OBJETIVOS ESPECÍFICOS

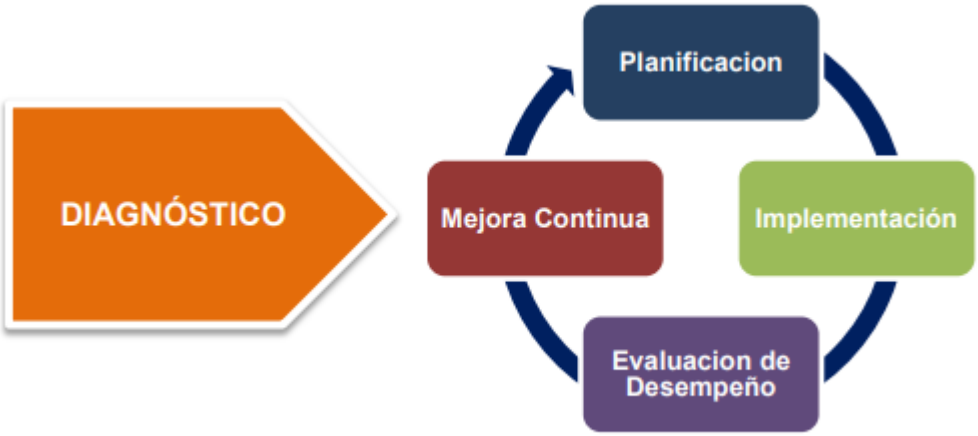
- Describir las acciones del plan de Seguridad y Privacidad de la Información, cuya finalidad es el desarrollo, verificación y aplicación continua de mejoras en el Sistema de Gestión de Seguridad de la Información de la Personería Municipal de Floridablanca.
- Documentar y aplicar los controles y procedimientos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

NORMATIVIDAD

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.

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 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 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- CONPES 3701 de 2011 Lineamientos de política para ciberseguridad y Ciberdefensa
- Ley 1581/12 – Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales En la recolección, tratamiento y circulación de datos.

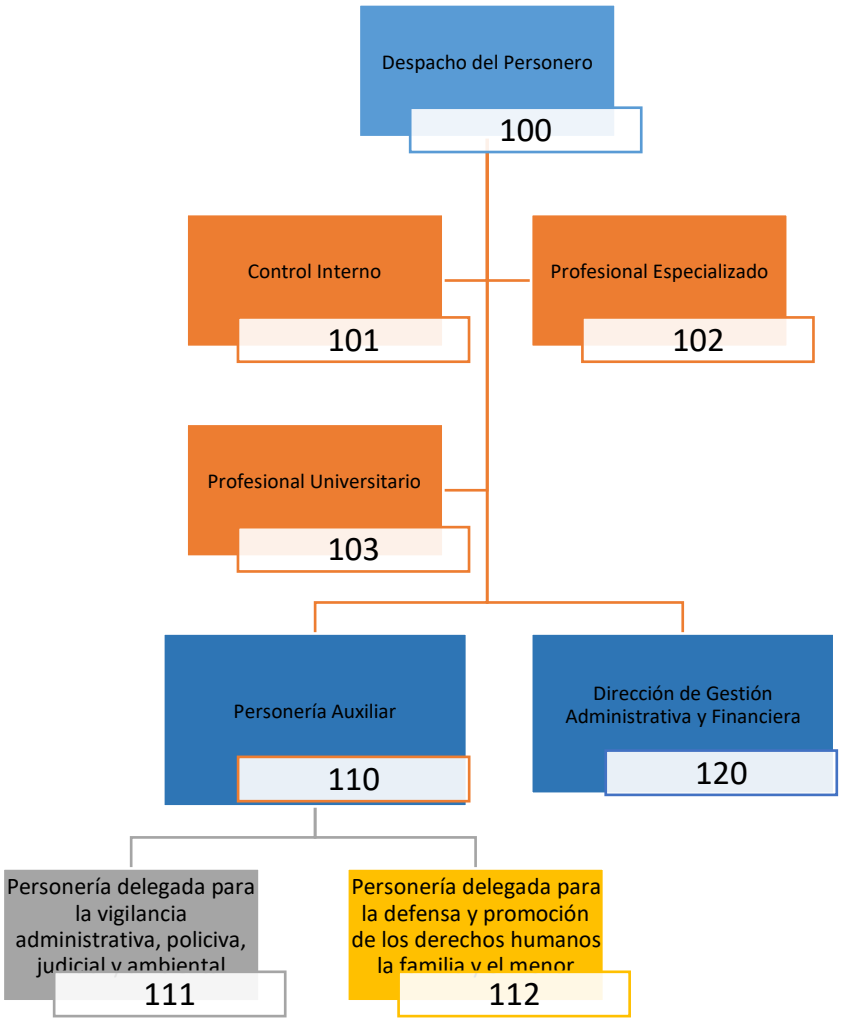
CICLO DE OPERACIÓN

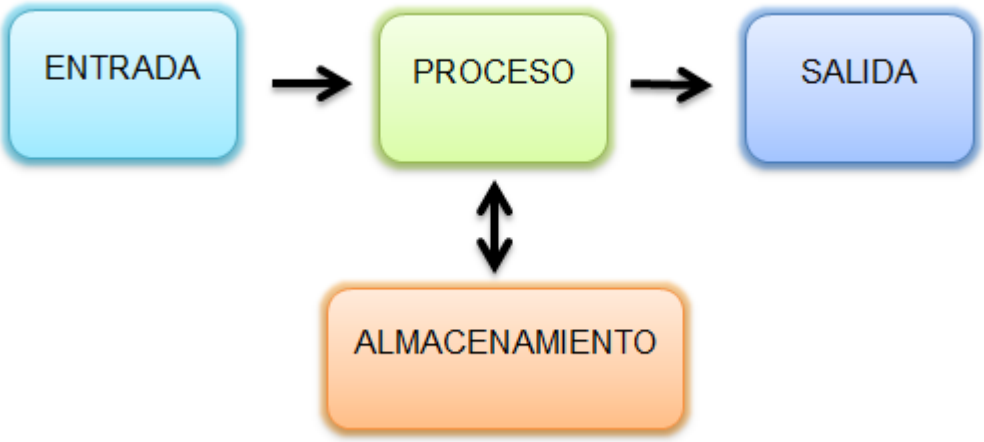


El ciclo de funcionamiento del modelo de Operación, tiene cinco (5) componentes que comprenden el modelo de operación contienen objetivos, metas y herramientas que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de las entidades. Fuente: MinTIC. Ciclo de operación del Modelo de Seguridad y Privacidad de la Información La ejecución del proyecto se realizará mediante el cumplimiento de las 5 fases con su respectivo Modelo de madurez.

DIAGNÓSTICO

Esta fase se identificará el contexto de la Personería Municipal de Floridablanca como entidad, apoyándose en su visión, misión y en sus sistemas de información para ello es importante comprender los procesos y procedimientos en los que se soporta para cumplir sus objetivos, mirar el contexto interno y externo de la Entidad, definir los flujos de información con cada una de las partes interesadas y en general, comprender a la entidad como un Sistema, dando como resultado el entendimiento de la organización y a partir de eso, la definición del alcance del Sistema de Seguridad de Información y los objetivos del MSPI.





La entidad ha definido un marco de seguridad y privacidad de la información ya que actualmente cuenta con:

- Políticas de seguridad de la información.
- Plan estratégico de tecnologías e información.
- Inventario de activos de la información.
- Plan de tratamiento de riesgos de seguridad y privacidad de la información.

Sin embargo, se debe desarrollar la documentación especifica acerca de procedimientos detallados de seguridad de la información, establecer roles y responsabilidades, definir el plan de comunicación y sensibilización, el plan de diagnóstico de IPV4 a IPV6 así como fortalecer el programa de gestión de riesgos de la información de la entidad.

PLANIFICACIÓN

Partiendo del diagnóstico realizado en el componente anterior, en esta fase se definirá la estrategia metodológica, que permita establecer el alcance, objetivos, procesos y procedimientos requeridos en la seguridad y privacidad de la información, buscando los resultados que permitan dar cumplimiento con las metas propuestas, desarrollando los siguientes ítems:

- Contexto de la institución.
- Necesidades y expectativas de las partes interesadas.
- Liderazgo y compromiso de la alta dirección.

- Política de seguridad.
- Roles de la institución, responsabilidades y autoridad.
- Acciones para abordar los riesgos y oportunidades.
- Objetivos y planes para lograrlos.
- Recursos.
- Comunicación.

IMPLEMENTACIÓN

En esta fase se lleva a cabo la implementación de la fase anterior de planificación realizada, en donde es necesario que sean ejecutadas las actividades descritas a continuación:

- ✔ Mejorar e Implementar el plan de tratamiento de riesgos de seguridad de la información.
- ✔ Replantear e Implementar controles de las políticas de seguridad y privacidad de la información
- ✔ Establecer indicadores de gestión.
- ✔ Optimizar el plan estratégico de tecnologías e información (PETI)
- ✔ Desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos definidos en la Personería de Floridablanca
- ✔ Iniciar el diagnóstico del plan de transición de IPV4 a IPV6.
- ✔ Detallar los elementos de la Organización (servidores, PCs, medios magnéticos, información impresa, documentos, etc.), que deben ser considerados para establecer un mecanismo de seguridad que permita garantizar un nivel adecuado de protección.
- ✔ Establecer la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para protegerlos contra los abusos internos e intrusos externos.
- ✔ Establecer los diferentes tipos de accesos o privilegios a los recursos informáticos (sistema operativo, aplicaciones, correo electrónico, Internet, comunicaciones, conexiones remotas, etc.)

EVALUACIÓN DE DESEMPEÑO

En esta fase se evaluará el desempeño y la eficacia del Modelo de seguridad y privacidad de la información, a través de instrumentos que permitan determinar la efectividad de la implantación del MSPI. Para la medición de la efectividad de los procesos y controles del MSPI, se deben tomar los indicadores definidos en el componente de implementación para llevar a cabo el plan de seguimiento, evaluación y análisis del MSPI.

Esta fase comprende las siguientes actividades:

• Monitoreo, medición, análisis y evaluación
• Auditoría interna
• Revisión por la alta dirección

MEJORA CONTINUA

En esta fase se consolidarán los resultados del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el MSPI.

Actividad	2021						
	FEB	MAR	ABR	MAY	JUN	JUL	AGO
Se definirán las acciones a implementar a nivel de seguridad y privacidad y de mitigación del riesgo de Seguridad de la Información, en el marco de SGSI de la Entidad.							
Se optimizarán los planes de seguridad y privacidad de la información existentes y se complementará el plan							

estratégico de tecnologías de información de la entidad.							
Se realizarán las actividades para el seguimiento que permitan la medición, análisis y evaluación del desempeño de la seguridad y privacidad de la información, con el fin de generar los ajustes o cambios pertinentes y oportunos							
Optimización del sistema de recepción externa de información por parte de terceros hacia la entidad, con el propósito de cumplir con lineamientos del gobierno digital.							
Se socializarán las políticas con los funcionarios y contratistas de la Personería de Floridablanca, con el fin de dar cumplimiento a las medidas propuestas.							
Mejora de la página web de la entidad, tomando medidas respecto a la privacidad y seguridad de la información del portal institucional.							

MARIA MARGARITA SERRANO ARENAS
Personera Municipal (e)

Revisó: Diana Carolina Duarte – DGAF