POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PERSONERIA MUNICIPAL DE FLORIDABLANCA

Personería de Floridablanca

Protección, equidad y transparencia

2023

CONTENIDO

POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

La Política de Seguridad y Privacidad de la Información es la declaración que representa la posición de la Personería Municipal de Floridablanca con respecto a fortalecer los niveles de seguridad y privacidad de la información y la protección de los activos de información que soportan los procesos de la entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas y procedimientos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

GLOSARIO

- ✓ **Política**: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

- ✓ **Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

- ✓ **Mejor Práctica**: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

- ✓ **Guía:** Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares de buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

- ✓ **Procedimiento**: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

OBJETIVOS

- ✓ Definir los niveles adecuados de protección de la información de acuerdo al grado de importancia para la entidad, teniendo en cuenta la integridad, confidencialidad, disponibilidad y privacidad de la misma.
- ✓ Establecer un plan de comunicación y sensibilización para fomentar una cultura de seguridad y privacidad de la información en los funcionarios y contratistas de la Personería Municipal de Floridablanca.
- ✓ Cumplir con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC en su estrategia de Gobierno en Línea.
- ✓ Identificar y minimizar los riesgos de seguridad de la información de las diferentes áreas de la Personería de Floridablanca

POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La dirección de la Personería de Floridablanca, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

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

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- ✓ Minimizar el riesgo en las funciones más importantes de la entidad.
- ✓ Proteger los activos tecnológicos.
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes de la personería de Floridablanca
- ✓ Garantizar la continuidad del negocio frente a incidentes.
- ✓ La Personería de Floridablanca ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Políticas de seguridad que soportan el SGSI de La Personería Municipal de Floridablanca:

- ✓ La Personería Municipal de Floridablanca protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros.

- ✓ La Personería Municipal de Floridablanca protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de política de minimizar impactos financieros, operativos o legales debido a un uso incorrecto.

- ✓ La Personería Municipal de Floridablanca protegerá su información de las amenazas originadas por parte del personal.

- ✓ La Personería Municipal de Floridablanca protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- ✓ La Personería Municipal de Floridablanca implementará control de acceso a la información, sistemas y recursos de red.

- ✓ La Personería Municipal de Floridablanca garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

ALCANCE

La política de seguridad de la información, será aplicada a los procesos estratégicos, misionales, de apoyo y de evaluación de la Administración Municipal y deberá ser conocida y cumplida por todos los funcionarios, contratistas, proveedores, ciudadanía en general y demás partes interesadas, que accedan a los sistemas de información e instalaciones físicas.

POLÍTICAS DE PROTECION FRENTE A REDES SOCIALES

La entidad restringirá si es necesario el acceso a los sitios relacionados con redes sociales, con el fin de aumentar la velocidad de acceso y disminuir el riesgo de virus. Si algún funcionario, contratista o practicante, por motivos de trabajo, requiere acceso a ellos, deberá tramitar la solicitud a la Dirección Administrativa y Financiera. Así mismo, tendrán acceso a redes sociales un grupo de funcionarios o contratistas, teniendo en cuenta sus funciones y facilidad de comunicación con los ciudadanos.

Cualquier información que se publique o divulgue por cualquier medio de internet de cualquier funcionario, contratista o practicante realizado, y se pueda considera fuera de su integridad, confiabilidad, y disponibilidad, será de completa responsabilidad de la persona que las haya generado en cuanto a los daños y perjuicios que se puedan generar a causa de esto.

POLÍTICAS DE PROTECCIÓN FRENTE A CORREOS ELECTRÓNICOS INSTITUCIONALES:

Todo funcionario, contratista o practicante deberá tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de la Personería Municipal de Floridablanca, los mensajes serán manejados como una comunicación privada y directa entre emisor y receptor. Asimismo, el correo institucional es de uso exclusivo para actividades relacionadas con la entidad y queda restringido su uso para otros fines.

Se prohíbe el envío de archivos, almacenamiento o transmisión de cualquier información que pudiera ser considerada pornográfica, racista, música, etc., o que atente contra la buenas costumbres o principios, por lo que solo se enviara información de uso e interés laboral.

POLÍTICAS DE PROTECCIÓN FRENTE A SOFTWARE:

- ✓ Todo funcionario, contratista o practicante deberá tratar las PQRS manejadas por medio del aplicativo web SIGED y archivos adjuntos como información de propiedad de la Personería Municipal de Floridablanca, los mensajes serán manejados como una comunicación privada y directa entre emisor y receptor. Asimismo, el usuario es de uso exclusivo de su responsible para actividades relacionadas con la entidad y queda restringido su uso para otros fines.
- ✓ Se prohíbe el envío de archivos, almacenamiento o transmisión de cualquier información que pudiera ser considerada pornográfica, racista, música, etc., o que atente contra la buenas costumbres o principios, por lo que solo se enviarainformación de uso e interés laboral.
- ✓
- ✓ Todas las aplicaciones software de la entidad, están protegidas por derechos de autor y requieren licencia de uso, por lo cual, está prohibido realizar copias o usar dicho software para fines personales.
- ✓ Ningún usuario puede instalar software adicional en los equipos de cómputo de la Personería municipal, sin la autorización de la Dirección Administrativa y Financiera.
- ✓ Los usuarios deben advertir y comunicar inmediatamente los síntomas de los posibles problemas que ocurran con el software a la Dirección Administrativa y Financiera de la Información y las Comunicaciones.
- ✓ Los computadores que contengan software malicioso deben ser en lo posible aislados de la red, hasta que el problema se haya resuelto.
- ✓ Los usuarios no deben desinstalar software por ningún motivo, incluso si éste presenta anomalías; la desinstalación, instalación, restauración o recuperación del sistema debe ser realizada única y exclusivamente por personal autorizado de la Dirección Administrativa y Financiera.
- ✓ El antivirus se debe actualizar periódicamente y examinar los equipos de cómputo y medios de almacenamiento informático según la frecuencia establecida por la Dirección Administrativa y Financiera.
- ✓ Cada usuario es responsable de verificar que no exista software malicioso,

en los archivos o información proveniente de redes externas (Internet), este procedimiento debe realizarse haciendo uso del software antivirus proporcionado por la Dirección Administrativa y Financiera.

POLÍTICAS DE HARDWARE:

- ✓ La configuración de hardware de los equipos de cómputo no debe ser alterada ni mejorada por los funcionarios de la entidad, dicha labor es exclusiva de la Dirección Administrativa y Financiera; de esta manera ningún usuario está autorizado para abrir o manipular el interior de los equipos de cómputo ni sus dispositivos de entrada y salida.

- ✓ Los equipos de cómputo propiedad de la entidad, deben estar reportados en un inventario que incluya información de sus características, configuración y ubicación.

- ✓ Ningún equipo de cómputo, incluyendo computadores, servidores, elementos de red e impresoras, debe ser trasladado o reubicado sin la aprobación de la Dirección Administrativa y Financiera.

- ✓ Los equipos que pertenezcan a la entidad (impresoras, equipos de cómputo, portátiles, etc.) no deben retirarse de las instalaciones físicas por ninguno de los funcionaros, contratistas o practicantes, salvo previa autorización.

ROLES Y RESPONSABILIDADES

La Dirección Administrativa y Financiera se encarga de los activos de información correspondientes a la plataforma tecnológica de la Personería Municipal de Floridablanca y, en consecuencia, debe asegurar su apropiada operación y administración.

Así mismo, debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.

Por su parte la oficina de control interno deberá efectuar un análisis de riesgos de seguridad de manera periódica, sobre los procesos de la Personería Municipal de Floridablanca.

La Dirección La Personería Municipal de Floridablanca aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad, teniendo en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales y sus procesos misionales. La Dirección demuestra su compromiso a través de:

- ✓ La revisión y aprobación del Manual de Políticas de Seguridad de la Información para la Institución.

- ✓ La destinación de los recursos suficientes para desarrollar los programas de capacitación y sensibilización en seguridad de la información.

- ✓ La promoción activa de una cultura de seguridad de la información en los funcionarios, contratistas, proveedores y partes interesadas, que tengan acceso a los sistemas de información e instalaciones físicas.

- ✓ Facilitar la divulgación de este documento a todas las partes interesadas. Así como la verificación del cumplimiento de las políticas en este mencionadas.