PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

PERSONERIA MUNICIPAL DE FLORIDABLANCA

ENERO 2019

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – PERSONERÍA MUNICIPAL DE FLORIDABLANCA:

OBJETIVO:

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.

ALCANCE:

Se aplica el alcance del Plan de Seguridad y Privacidad de la Información a los procesos de la Personería Municipal de Floridablanca, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información.

TERMINOS Y DEFINICIONES

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.

Riesgo Positivo: Posibilidad de ocurrencia de una situación que permita mejorar la gestión institucional, debido a fortalezas que se presentan en beneficio de la Personería.

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: Aquellos de carácter primario o sin procesar, facilitados a cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y generar servicios derivados de ellos.

Autenticidad: Busca resguardar el valor de la información en tiempo, forma y distribución, garantizando el origen de la información, y así evitar suplantación de identidades.

Dato privado: Es el dato que por su naturaleza reservada sólo es relevante para el titular debido a la intimidad de la información.

Habeas data: Derecho fundamental a acceder a la información personal que se encuentre en archivos o bases de datos; asimismo, confiere la posibilidad a los usuarios de ser informados acerca de los datos registrados sobre ellos mismos y la potestad de corregirlos.

Integridad: La propiedad de salvaguardar la complejidad y totalidad de la información.

Propietario de activo de información: Vinculado de la entidad, cuyo cargo, y asignación designada, es la obligación de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

Responsable del tratamiento: Persona natural o jurídica pública o privada; que por sí misma o en asocio con otros, resuelva sobre la base de datos y/o el tratamiento de los datos.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL PERSONERIA MUNICIPAL DE FLORIDABLANCA

La Personería Municipal de Floridablanca, tiene claro su compromiso en la administración de los riesgos de seguridad de la información, por lo que buscará desarrollar y supervisar las medidas que permitan mantener la confidencialidad, integridad y disponibilidad de sus activos de información en cumplimiento de la normativa aplicable. De igual manera, promueve una cultura en seguridad para procesar incidentes que contribuyan a la mejora continua del Sistema de Gestión de Seguridad de la Información.

Así mismo, buscará resolver con empeño las dificultades en cuanto a la seguridad y privacidad de la información, y así minimizar el riesgo de los procesos de la entidad; apoyar la innovación tecnológica; efectuar el sistema de gestión de seguridad de la información; proteger los activos de información; establecer las políticas, procedimientos y manuales en materia de seguridad de la información; fortalecer la cultura de seguridad de la información en los funcionarios, terceros, practicantes y ciudadanos de la Personería de Floridablanca; garantizar la continuidad del negocio frente a incidentes; y cumplir con los principios de seguridad de la información.

POLÍTICAS DE PROTECION FRENTE A REDES SOCIALES

La entidad deberá restringir 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 CUENTAS DE USUARIOS:

Toda cuenta de usuario que se requiera modificar se hará mediante solicitud enviada a la Dirección Administrativa y Financiera. El proceso de creación de cuentas de usuarios, deberá ser solicitado mediante la mesa de ayuda.

POLÍTICAS DE PROTECCIÓN FRENTE A SOFTWARE:

Software y Licencias:

- Todas las aplicaciones manejadas en la entidad deben ser clasificadas de acuerdo a su prioridad, como Alta, Media o Baja; para las aplicaciones con prioridad Alta se debe contar con una copia actualizada y su respectiva documentación técnica en un sitio externo a la Dirección Administrativa y Financiera.
- 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 administración municipal, sin la autorización de la Dirección Administrativa y Financiera de la Información y las Comunicaciones.

- 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.

Software Antivirus:

- Se debe actualizar periódicamente el software de detección de virus 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:

Ubicación y Protección de Equipos de cómputo:

- La Dirección Administrativa y Financiera deberá entregar a cada funcionario un documento que especifique la configuración actual de equipo que tiene a su cargo, el funcionario será responsable de velar por la seguridad e integridad de este.

- 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.

- 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.
- Los usuarios que hayan sido autorizados para retirar de manera temporal los equipos de la entidad, (impresoras, equipos de cómputo, portátiles, etc.) deben cumplir las políticas establecidas en este documento.

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.
- Autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica de la Personería Municipal de Floridablanca.
- 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.
- Es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los funcionarios y de hacer entrega de estas.

Responsabilidad Oficina Control Interno:

- Efectuar un análisis de riesgos de seguridad de manera periódica, sobre los procesos de la Personería Municipal de Floridablanca.
- Definir las condiciones de uso y protección de los activos de información, tanto los tecnológicos como aquellos que no lo son.

OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN:

1. Administrar los eventos de seguridad de la información de la Personería Municipal de Floridablanca.

2. Fortalecer la seguridad y disponibilidad de la información y recursos digitales acorde con la declaración de aplicabilidad aprobada.

3. Cumplir con la legislación aplicable a la naturaleza de la Entidad en materia de Seguridad de la Información.

4. Fomentar una cultura de seguridad de la información en los miembros de la entidad (funcionarios, contratistas, pasantes, judicantes y demás integrantes).

5. Fortalecer el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.

ACTIVIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la vigencia 2019 se definen las siguientes actividades para Seguridad y Privacidad de Información:

Actividad	Descripción	Responsable	Fecha Inicial Planificada	Fecha Final Planificada
Definir el marco de seguridad y privacidad de la información.	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.	DGAF	MARZO /2019	ABRIL 2019
Ejecutar el plan de aplicación y mejoramiento del Sistema de Gestión de Seguridad de la Información.	Se ejecutará el cronograma de aplicación y mejoramiento del Sistema de Gestión de Seguridad de la Información - SGSI el cual consiste en el desarrollo de las tareas			

	correspondientes a la vigencia 2019, como la verificación por parte de la alta dirección del cumplimiento de los objetivos e indicadores definidos para el sistema.			
Aplicar y mejorar la seguridad y privacidad de la información en el marco de SGSI 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.			

MARCO LEGAL:

- 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.

LUIS JOSE ESCAMILLA MORENO

Personero Municipal

Proyectó: Andrés Rueda Cabeza - Contratista.
Aprobó: MMC