1. INTRODUCCIÓN

Para la Defensoría del Espacio Público la información es el activo más importante para la prestación de servicios a la ciudadanía y toma de decisiones institucionales, por lo tanto se ha definido como **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**, mantener la confidencialidad, integridad y disponibilidad de la información, mitigando los riesgos a los que está expuesta, implementando controles efectivos requeridos durante todo el flujo de la información para cumplir la misión institucional, dando aplicación a las normas vigentes establecidas.

Al definir e implementar la **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN,** se garantiza la protección de la información para el desarrollo operativo, de control y gestión de la entidad, y se da cumplimiento de los requisitos normativos que regulan la materia.

La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, disponibilidad e integridad de la misma.

La **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN** es el documento que contiene las directrices generales, que ha determinado la Alta Dirección, para ser aplicadas en todas las actividades relacionadas con el manejo de información de la entidad y cuya finalidad es garantizar la protección de sus activos de información.

Se podrán realizar mejoras de las políticas de seguridad de la información, para lo cual se tendrá en cuenta la importancia de los ajustes o cambios realizados en cualquier parte de los procesos que afecten la seguridad de la información.

2. OBJETIVO GENERAL

Definir los lineamientos generales que deben aplicar los funcionarios, contratistas y usuarios externos del DADEP, para garantizar la adecuada confidencialidad, disponibilidad e integridad de la información, de acuerdo con los requisitos normativos que le apliquen.

2.1 Objetivos específicos

- Generar las acciones necesarias para minimizar la ocurrencia de riesgos asociados a la seguridad de la información.
- Generar una conciencia colectiva sobre la importancia de clasificar, valorar y asegurar los

activos de información de la entidad.

- Asegurar la integridad, confidencialidad y disponibilidad de la información y la protección de las tecnologías de la información y las comunicaciones de la entidad.

- Implementar de manera gradual y organizada, el Subsistema de Gestión de la Seguridad de la Información

- Garantizar la continuidad del objeto misional de la entidad en lo relacionado con sus sistemas de información.

3. ALCANCE

La política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la entidad, cualquiera sea su situación contractual, independientemente del proceso al que se encuentre adscrito y el nivel de tareas que desempeñe. Aplica a todos los procesos de la entidad.

4. COMPROMISO DE LA ALTA DIRECCIÓN

La Dirección del Departamento Administrativo de la Defensoría del Espacio Público – DADEP, se compromete a *apoyar activamente la seguridad de la información dentro de la entidad, asignando los recursos necesarios para su desarrollo, generando las herramientas necesarias y estableciendo los controles encaminados a prevenir y administrar los riesgos que puedan afectar la seguridad de la información de la entidad.*

5. POLÍTICA DEL SISTEMA INTEGRADO DE GESTIÓN

El Departamento Administrativo de la Defensoría del Espacio público, en cumplimiento de la Norma Técnica Distrital No. 001 de 2011, adoptó mediante la resolución No.003 de 2016, la Política del Sistema Integrado de Gestión que dentro de sus directrices establece una general, correspondiente al Subsistema de Seguridad de la Información:

- El Departamento Administrativo de la Defensoría del Espacio Público cuya misión es la defensa, inspección, vigilancia, regulación y control del espacio público del Distrito Capital, la administración de los bienes inmuebles y la conformación del inventario general del patrimonio inmobiliario distrital, trabajando por la satisfacción de sus usuarios y partes interesadas y cumpliendo los requisitos legales y organizacionales suscritos frente al Sistema Integrado de Gestión, se compromete a:

✓ Incorporar y fomentar la cultura ambiental en su quehacer institucional, para minimizar el impacto ambiental de sus actividades y optimizar la utilización de los recursos

naturales a su disposición.

- ✓ Proporcionar un ambiente de trabajo sano y saludable a sus servidores, que anticipe y prevenga la ocurrencia de lesiones y enfermedades ocupacionales.
- ✓ ***Proteger la confidencialidad, integridad, disponibilidad y autenticidad de sus activos de información.***
- ✓ Promover una cultura de conciencia documental reflejada en el manejo responsable del documento físico o electrónico por parte de los usuarios internos y externos de la entidad, asegurando la conformación de registros íntegros, auténticos y fiables para preservar la memoria institucional.
- ✓ Consolidar una cultura del autocontrol e identificar y administrar todos los actores que pongan en riesgo la continuidad o el cumplimiento de la tarea institucional.
- ✓ Para lograr lo anterior continuará promoviendo un ambiente de responsabilidad social a la vez que fortalece el desarrollo de sus colaboradores, la participación de los usuarios y partes interesadas, destinando los recursos necesarios para consolidar nuestra cultura de mejoramiento continuo y la sostenibilidad de nuestro Sistema Integrado de Gestión.

6. POLÍTICAS QUE DESARROLLAN GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para el DADEP, la información es su activo más preciado, por cuanto constituye la pieza fundamental para el desarrollo de su gestión y la prestación de los servicios; por este motivo la administración ha de generar los mecanismos necesarios para lograr su seguridad, confidencialidad, disponibilidad e integridad. El presente documento despliega las directrices generales que dan desarrollo a la seguridad de la información:

6.1. POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1.1 Organización interna

Cada una de los controles de la política del subsistema de gestión de seguridad de la información, serán desarrolladas a través de la documentación pertinente (procedimientos, instructivos, guías, manuales y/o formatos), entre las que se encuentran:

- Política de correo corporativo
- Política para el uso de recursos tecnológicos
- Política de control de acceso (usuario y contraseña)
- Política de copias de seguridad
- Política de estaciones de trabajo

- Política de red corporativa y Wireles
- Políticas de uso de los sistemas de información
- Política de seguridad física y del entorno
- Política de uso de Internet
- Política de acceso remoto
- Política de servidor de archivos
- Política de administración de Bases de Datos
- Política de pistas de auditoria
- Política de transmisión y publicación de información
- Política de control para teletrabajo
- Política de derechos de autor y legalidad de software.
- Política de servidor de impresoras y servicios de impresión

a. Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido. Las actividades de la seguridad de la información serán coordinadas por los líderes de los procesos y les serán asignadas responsabilidades de acuerdo con su rol.

- La dirección será la directa responsable de autorizar los nuevos sistemas de información que la entidad requiera, igualmente la dirección y jefes de las dependencias son los responsables de hacer cumplir las políticas de seguridad de la información establecidas en la entidad.

b. La responsabilidad sobre los Activos de la información deberá estar en cabeza del responsable de la información definido dentro de la Entidad para evitar conflicto en cuanto a responsabilidades en especial para dar fortaleza al tema de segregación de tareas.

c. La entidad, en especial la oficina de sistemas mantendrá los contactos apropiados con grupos de interés especiales, relacionados con la seguridad de la información, con el fin de conocer y estar al tanto de las acciones innovadoras que se pueden implementar al interior de la entidad.

d. En la revisión por la dirección realizada por el comité SIG (Comité del Sistema Integrado de Gestión) se llevará a cabo la revisión general del subsistema o extraordinariamente cuando ocurran cambios significativos en su implementación.

6.1.2 Organización partes externas

a. El responsable del Subsistema de seguridad de la información es el jefe de la Oficina de Sistemas, y será el responsable de revisar y proponer al comité SIG las acciones en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad de la entidad.

b. Se identificarán y analizarán los riesgos para la información y los servicios de procesamiento de los sistemas de información que involucran usuarios externos y se implementarán los controles necesarios requeridos para la autorización de acceso.

c. En los acuerdos con terceras partes que impliquen acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, se deberán validar los requisitos de seguridad exigidos por la entidad, antes de dar acceso a usuarios externos.

6.2. POLÍTICA DE GESTIÓN DE ACTIVOS

a. Los activos de información del DADEP, serán identificados, clasificados y asignados como propiedad de algún proceso de la entidad para establecer los responsables y los mecanismos de protección necesarios. Cada dependencia, deberá elaborar y mantener actualizado el inventario de los activos de información (procesada y producida).

b. El área de archivo determinará el nivel de privacidad, sensibilidad, nivel de riesgo a que está expuesta y/o requerimientos legales de retención a la documentación física y magnética de la entidad en cualquiera de sus procesos.

6.3. POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS

a. Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido. Para este fin, cada funcionario contratista o usuario externo, será informado sobre la clasificación de la información a la que puede acceder, los riesgos asociados, y sus responsabilidades frente a los sistemas de información y la información generada por los mismos.

b. Todos los funcionarios, contratistas y usuarios externos, recibirán formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la entidad, según sea pertinente para sus funciones laborales. El proceso de gestión del Talento Humano, junto con la Oficina de Sistemas se encargará de ejecutar un plan de capacitación de seguridad en la información que garantice el uso adecuado de los sistemas.

c. El funcionario, contratista y/o usuario externo que haga mal uso de los sistemas de información, o de la información que le ha sido entregada para su gestión, acarreara las sanciones disciplinarias pertinentes que han sido establecidas por la ley.

d. Todos los funcionarios, contratistas o usuarios externos deben devolver todos los activos que estén en su poder, pertenecientes a la entidad, al finalizar su contratación laboral, contrato o acuerdo. Así mismo la oficina de sistemas será la encargada de llevar a cabo los procedimientos necesarios para finalizar los derechos de acceso que hayan sido otorgados.

e. Se prohíbe a los funcionarios, contratistas o usuarios externos la realización de pruebas de seguridad y los cambios en los activos fijos de información asignados, esta es una actividad de responsabilidad exclusiva de la Oficina de sistemas.

6.4 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

a. Está prohibido el paso al personal no autorizado al centro de cómputo, área que contiene los servicios de procesamiento de la información. Este acceso será autorizado por el Director y/o jefe de Oficina de Sistemas únicamente.

b. La entidad diseñará y aplicará las protecciones físicas necesarias para garantizar la protección de la información contra formas de desastre natural o artificial.

c. Todo funcionario de la Oficina de Sistemas deberá aplicar las directrices establecidas y utilizar la protección física adecuada para trabajar en áreas seguras.

d. Los equipos que contiene la información de la entidad, estarán protegidos para reducir el riesgo por amenazas o peligros del entorno, accesos no autorizados o fallas en los servicios de suministro; recibirán mantenimiento periódico para asegurar su continua disponibilidad e integridad y serán verificados para garantizar que no se eliminan datos sensibles.

e. Ningún equipo, información, ni software se deben retirar sin autorización previa y con el acompañamiento de la Oficina de Sistemas.

6.5 POLÍTICA DE GESTIÓN DE PAGINA WEB

a. El equipo de comunicaciones con acompañamiento de la Oficina de Sistemas serán los responsables de los diseños y contenidos de la página web de la entidad, teniendo en cuenta siempre los estándares establecidos por gobierno en línea y ley de transparencia, todos los contenidos publicados en la página serán avalados por la oficina de comunicaciones.

6.6 POLÍTICA DE GESTIÓN DE COMUNICACIONES Y OPERACIONES

a. La Oficina de Sistemas documentará y adoptará formalmente los instructivos, guías y/o manuales necesarios para desplegar cada una de las políticas asociadas a los temas de seguridad de la información, de los que habla el presente documento. Estos serán públicos para cualquier funcionario o contratista que los requiera en el sistema de información establecido para tal fin.

b. Cualquier cambio en los servicios o sistema de procesamiento de información, debe ser conocido, documentado y autorizado por la Oficina de sistemas.

c. Los sistemas de procesamiento de información que se encuentran en periodo de prueba, deben ser controlados con usuarios autorizados para evitar riesgos de acceso o cambios no autorizados.

d. Se garantizará que los controles de seguridad, las definiciones del servicio y los niveles de prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operados por las terceras partes.

e. Para los sistemas de información nuevos, actualizaciones o nuevas versiones, se establecerá criterios de aceptación previos a su uso.

f. Se implementarán acciones de sensibilización a usuarios frente a los controles de detección prevención y recuperación de datos contra códigos maliciosos, así como de la ejecución de códigos móviles autorizados y no autorizados.

g. La Oficina de Sistemas, garantiza la creación de copias de respaldo de la información y del software, realizando pruebas periódicas de acuerdo con la política de respaldo acordada.

h. Las redes se deberán mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito. En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contratan externamente.

i. Para evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades misionales y administrativas de la entidad, se establecerán las políticas, procedimientos y documentos necesarios para la gestión de los medios removibles, el manejo, almacenamiento y protección de la información, asegurando que su eliminación se haga forma segura y sin riesgo.

j. Los servicios y la información de la actividad de registro estarán protegidos contra el acceso o la manipulación no autorizados. Para tal fin se llevará a cabo registro de las actividades tanto el operador como del administrador de los sistemas, monitoreo, auditorias, registro y análisis de fallas y sincronización de los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la entidad.

6.7 POLÍTICA DE CONTROL DE ACCESO

a. Se definirán e implantarán controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Entidad.

b. Cada funcionario, contratista o usuario externo contará con un usuario únicamente para su uso personal. Es exclusivo y no debe ser compartido con otros usuarios.

c. Las sesiones inactivas se deben suspender después de un periodo definido de inactividad.

d. Se llevará a cabo el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información. Esta tarea está a cargo de la oficina de Sistemas quién controlará la asignación de privilegios y contraseñas y revisará periódicamente dichos derechos.

e. Es responsabilidad de los funcionarios, contratistas o usuario externos generar buenas prácticas en la selección de usos de contraseñas de acuerdo con lo establecido en los documentos internos de la entidad, para tal fin. De igual forma será su responsabilidad, llevar a cabo buenas prácticas de escritorio despejado para reportes y medios de almacenamiento removibles y política de pantalla despejada para procesamiento de información.

f. La Oficina de Sistemas otorgará accesos a los servicios, de acuerdo con las autorizaciones específicas solicitadas por el líder del proceso.

g. La Oficina de Sistemas establecerá los controles para acceso lógico y físico a los puertos de configuración y de diagnóstico, redes compartidas, enrutamiento en las redes, sistemas operativos.

6.8 POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

a. Frente al manejo de los sistemas de información, se validarán los datos de entrada y de salida, se implementarán controles y se realizará verificación de validación para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados.

b. Se implementarán los controles necesarios para asegurar la autenticidad y protegerla integridad de la información contenida en los sistemas así como su correcto almacenamiento.

c. Se llevará a cabo el uso de controles criptográficos e implementación de sistema de gestión de llaves, para aquella información que la entidad determine como sensible.

d. La instalación de software en los sistemas operativo será coordinada y realizada por la Oficina de Sistemas como único responsable. A su vez se generarán los mecanismos necesarios para garantizar la protección y control de datos de prueba y códigos fuente de los programas.

e. En cuanto a la seguridad en los procesos de desarrollo y soporte, se establecerán los procedimientos necesarios para el control de cambios de los sistemas operativos y cambio de software, revisando y sometiendo a prueba las aplicaciones críticas para la entidad. Estas políticas aplican de igual forma a los contratos externos que estén relacionados con el tema.

f. La entidad llevará a cabo el diagnostico de las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluando la exposición de la organización a dichas vulnerabilidades y tomando las acciones apropiadas para tratar los riesgos asociados.

6.9 POLÍTICA DE GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

a. Es responsabilidad de cada funcionario, contratista o usuario externo observar y reportar todas las debilidades detectadas o sospechadas en los sistemas o servicios.

b. La Oficina de Sistemas cuantificará y monitoreará todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.

c. Es responsabilidad del administrador de plataforma hacer el seguimiento y análisis de los incidentes de seguridad y del reporte a los propietarios de la información.

d. Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.

6.10 POLÍTICA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

a. La Oficina de Sistemas garantizará la continuidad de la operación en la Defensoría del Espacio Público, estableciendo los requisitos de seguridad de la información necesarios para tal fin. De igual forma identificará los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información, para lo cual desarrollará un plan de contingencia.

b. La Oficina de Sistemas desarrollará un documento de continuidad del negocio que determinará la estratégica para la implementación de la contingencia en instalaciones externas a la sede principal del DADEP para operar en caso de un siniestro, plan de recuperación que describa las acciones a seguir para trasladar las actividades del negocio a un centro alterno de recuperación, plan de retorno que describa las acciones a seguir para regresar las operaciones normales a las instalaciones originales y programación de pruebas en las que el plan de continuidad debe ser probado.

6.11 POLITICA DE CUMPLIMIENTO

a. La oficina de sistemas se encargará de definir explícitamente, documentar y mantener actualizados para cada sistema de información los requisitos estatutarios, reglamentarios y contractuales pertinentes.

b. Será responsabilidad de las áreas competentes imponer las penalizaciones respectivas en caso de incumplimiento o trasladarlas a las entidades competentes.

c. La entidad se compromete a implementar todas las acciones de seguridad de la información que garanticen la protección contra pérdida, destrucción y falsificación de la información, la protección de los datos y la privacidad de acuerdo con la legislación y los reglamentos pertinentes

d. Es responsabilidad de cada funcionario, contratista o usuario externo no utilizar los servicios de procesamiento de información para propósitos no autorizados.

e. Es responsabilidad de la dirección garantizar que todos los procedimientos de seguridad dentro de sus procesos se lleven a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.

f. Periódicamente la oficina de sistemas revisará el proceso, procedimientos, manuales, guías y formatos asociados a la seguridad de la información y determinará el cumplimiento de las normas de implementación de la seguridad.

g. Periódicamente la oficina de Control interno realizará las actividades de auditoría y verificaciones de los temas TIC necesarios, minimizando el riesgo de interrupciones y fortaleciendo la seguridad de la información.

NADIME YAVER LICHT
Directora

Elaboró: Angélica Beltrán – Profesional Oficina Asesora de Planeación Johan Andrés Rojas Montaña - Profesional Oficina de Sistemas Hugo Roberto Hernández – Profesional Oficina de Sistemas

Revisó: Julio Hernández – Jefe Oficina de Sistemas

Fecha: Octubre de 2017

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE MODIFICACIÓN**
2	19/10/2017	Se realizaron ajustes de forma sugeridas por la Alta Consejería para las TIC de la Alcaldía Mayor y se adicionaron dos controles de las políticas internas (Política de servidor de impresoras y servicios de impresión, Política para el uso de recursos tecnológicos). Adicionalmente se cambiaron los nombres de los controles llamándolos políticas.