Política de Seguridad de la Información

Departamento Administrativo de la Defensoría del Espacio Público

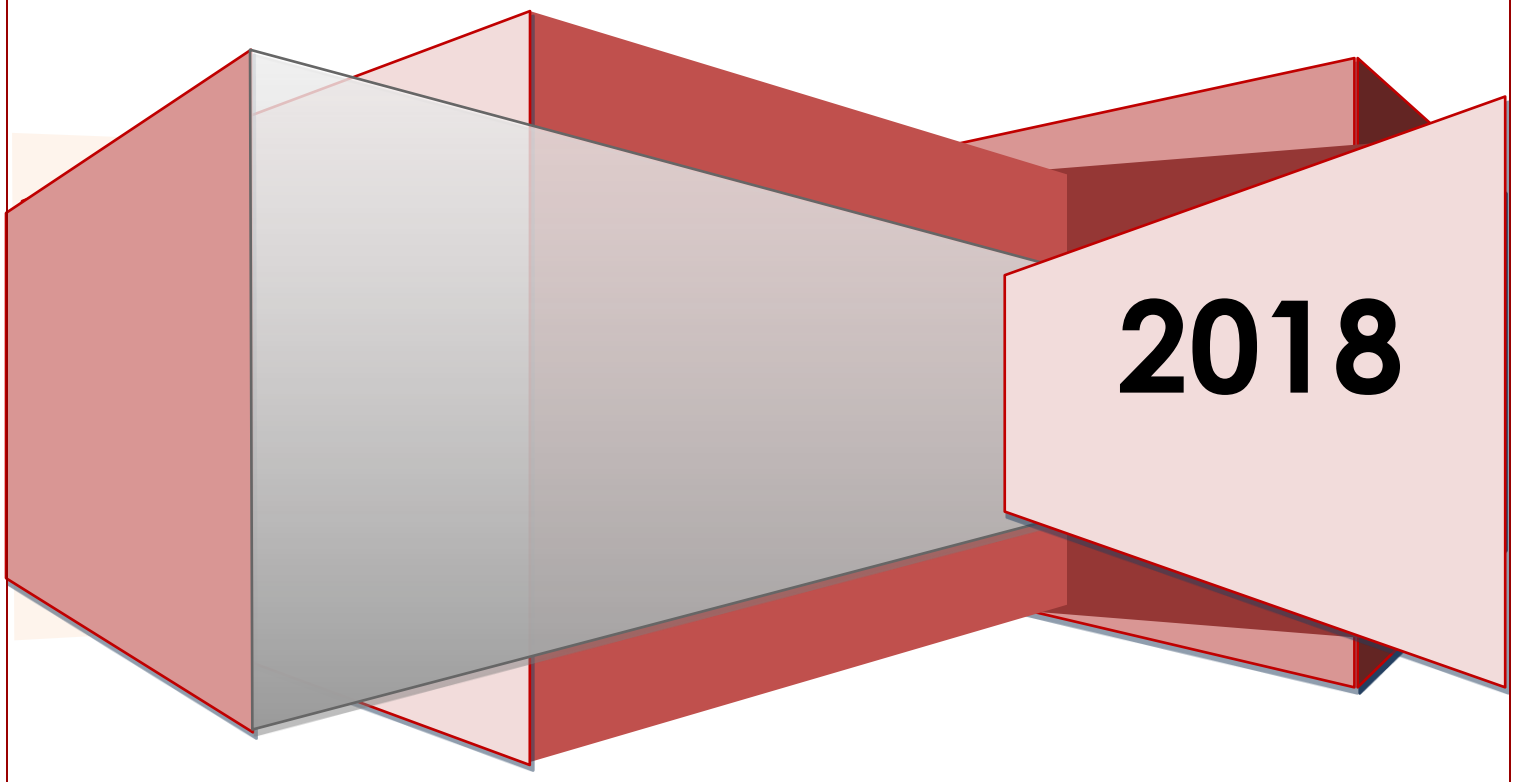

TABLA DE CONTENIDO

1. INTRODUCCIÓN 3

2. OBJETIVO GENERAL 3

2.1 OBJETIVOS ESPECÍFICOS 3

3. ALCANCE 4

4. COMPROMISO DE LA ALTA DIRECCIÓN 4

5. POLÍTICA DEL SISTEMA INTEGRADO DE GESTIÓN 4

6. POLÍTICAS QUE DESARROLLAN GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 5

6.1 POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 5

6.1.1 Organización interna 5

6.1.2 Organización partes externas 6

6.2 POLÍTICA DE GESTIÓN DE ACTIVO 7

6.3 POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS 7

6.4 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO 8

6.5 POLITICA DE CUMPLIMIENTO 8

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 busca 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. Por consiguiente, la seguridad de la información establece un 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.

Finalmente y consientes de lograr una adecuada seguridad de los activos de información, el documento **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN** y el documento **MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN** se consideran documentos vivos y por consiguiente podrán ser objeto constante de actualizaciones o mejoras que aporten valor en el fortalecimiento de los controles o medidas para proteger de la información del DADEP

2. OBJETIVO GENERAL

Definir los lineamientos generales que deben ser adoptados e implementados por los funcionarios, contratistas y usuarios externos del DADEP, que contribuyan a una adecuada gestión de la seguridad de la información preservando la confidencialidad, disponibilidad e integridad de la información, de acuerdo con los requisitos normativos que le apliquen.

2.1 OBJETIVOS ESPECÍFICOS

- Establecer directrices generales para la adecuada gestión de la seguridad de la información.
- Generar las acciones necesarias para minimizar la ocurrencia de riesgos, eventos e

incidentes asociados a la seguridad de la información.

- Generar una conciencia colectiva sobre la importancia de clasificar, valorar y proteger los activos de información de la entidad.

- Salvaguardar 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 que 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 apropiar y 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 a la ciudadanía; por este motivo la administración genera los mecanismos necesarios para lograr preservar la confidencialidad, la disponibilidad, la integridad, la accesibilidad, el no repudio y demás propiedades que permitan una adecuada gestión de la seguridad de la información. Por consiguiente, 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), contemplados en el **MANUAL DE GESTIÓN DE SEGURIDAD DE LA**

INFORMACIÓN de la siguiente manera:

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.

b. 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.

c. La responsabilidad sobre los Activos de 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.

d. 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.

e. 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 ACTIVO

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 los requerimientos legales de retención a la documentación física y magnética de la entidad en cualquiera de sus procesos.

c. La clasificación de los niveles de privacidad, publicación, divulgación y nivel de riesgo será una labor conjunta entre la Oficina Asesora Jurídica, la Oficina Asesora de Planeación y el responsable de los riesgos.

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 POLITICA DE CUMPLIMIENTO

a. Es deber de cada funcionario, contratista o usuario externo conocer, adoptar e implementar los controles y políticas definidas en el documento **MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.**

b. 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.

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

d. 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.

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 los procesos, procedimientos, manuales, guías y formatos asociados a la seguridad de la información y determinará el nivel de cumplimiento de las normas de implementación de la seguridad de la información al interior del DADEP.

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

Proyectó: Carlos Rojas Villamil Contratista Oficina de Sistemas, Hugo Roberto Hernández Profesional Oficina de Sistemas
Elaboró: Carlos Rojas Villamil Contratista Oficina de Sistemas, Hugo Roberto Hernández Profesional Oficina de Sistemas
Revisó: Luis Fernando Arango Vargas Profesional Oficina Asesora de Planeación, Isaías Sánchez Rivera Jefe Oficina Asesora de Planeación, Julio Alexander Hernández Martínez Jefe Oficina de Sistemas
Aprobó: Nadime Yaver Licht – Directora Departamento Administrativo de la Defensoría del Espacio Público.
Código de archivo: 140-155-5

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.
3	23/11/2018	Se realizaron ajustes en el contenido y redacción de la Política de Seguridad de la Información, incluyendo los objetivos generales y específicos, así como el numeral 6.5 denominado Política de cumplimiento.