



Política General de seguridad y privacidad de la información

Proceso

Gestión de la Información y la
Tecnología

Código SG/MIPG 127-PPPGI-01
Vigencia desde 29/12/2020
Versión 4



ALCALDÍA MAYOR
DE BOGOTÁ D.C.

DEPARTAMENTO ADMINISTRATIVO DE LA
**DEFENSORÍA DEL
ESPACIO PÚBLICO**



BOGOTÁ



Tabla de contenido

1.	INTRODUCCIÓN	3
2.	OBJETIVO GENERAL	4
3.	OBJETIVOS ESPECÍFICOS	4
4.	ALCANCE	4
5.	SIGLAS	5
6.	COMPROMISO DE LA ALTA DIRECCIÓN	5
7.	POLÍTICA DEL SISTEMA INTEGRADO DE GESTIÓN	5
8.	POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	6
8.1	Organización interna	6
8.2	Organización partes externas	7
9.	CONTROLES QUE APOYAN LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	7
10.	10 PLAN DE IMPLEMENTACIÓN Y COMUNICACIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	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 GENERAL DE SEGURIDAD Y PRIVACIDAD 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 GENERAL DE SEGURIDAD Y PRIVACIDAD 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 esta.

Este 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, la POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD 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.

3. 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.
- Asegurar la continuidad del objeto misional de la entidad en lo relacionado con sus sistemas de información.

4. ALCANCE

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del Departamento Administrativo de la Defensoría del Espacio Público – DADEP y la ciudadanía en general.



5. SIGLAS

- **DADEP:** Departamento Administrativo de la Defensoría del Espacio Público
- **SIG:** Sistema Integrado de Gestión
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **SGSI:** Sistema de Gestión de la Seguridad de la Información
- **TI:** Tecnología de la información.
- **TIC's:** Tecnologías de la información y las comunicaciones
- **MODELO DE TOMA DE DECISIONES:** proceso por el cual se toman decisiones a partir de la experiencia y el juicio personal acumulado.
- **PARTES INTERESADAS:** cualquier individuo, grupo u organización que forme parte o se vea afectado por el mismo, obteniendo algún beneficio o perjuicio.

6. COMPROMISO DE LA ALTA DIRECCIÓN

La Dirección del Departamento Administrativo de la Defensoría del Espacio Público – DADEP, se compromete a apropiarse 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.

7. 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 los riesgos tecnológicos y por consecuencia su impacto en el caso que se materialice, esto, mediante



políticas, procedimientos, lineamientos y demás mecanismos que permita optimizar el adecuado uso y seguridad de los activos de información del DADEP.

- Proporcionar ambientes tecnológicos seguros a los colaboradores de la entidad.
- 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 digital 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 factores 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.

8. POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

8.1 Organización interna

Cada uno de los controles de la política del subsistema de gestión de seguridad de la información, serán desarrolladas a través de la documentación pertinente (políticas, procedimientos, instructivos, guías, manuales y/o formatos), contemplados en las políticas operativas específicas de seguridad y privacidad 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.

8.2. 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.
- d. El DADEP no se obliga a entregar copias parciales o totales de su información excepto si es mediante requerimiento de ley u orden judicial o de otra autoridad gubernamental competente

9. CONTROLES QUE APOYAN LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Dentro de los controles que apoyan el cumplimiento de la POLÍTICA en la Defensoría del espacio público se encuentran:

- a. Matriz de riesgos: En él están definidos los riesgos asociados a la seguridad de la información la cual tiene unos controles definidos.



- b. Formatos: Permiten llevar un control de las solicitudes de usuarios, privilegios, solicitudes de información, solicitudes de modificación, control de copias de seguridad y en general todo lo asociado a seguridad de la información.
- c. Mesa de ayuda: Permite el registro, gestión y administración de los servicios de TI, incluidos los asociados a seguridad de la información.
- d. Auditorías: Realizadas por la oficina de control interno, de las cuales se hacen planes de mejoramiento y seguimiento a los mismos para controlar su progreso continuo.

Adicionalmente se cuentan con componentes TIC que apoyan la POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN como son el directorio activo que hace el primer filtro de seguridad, Firewall, auditorías de sistemas de información y/o de base de datos, parches de seguridad, antivirus y la administración de usuarios en los sistemas de información y en las Base de Datos.

10. PLAN DE IMPLEMENTACIÓN Y COMUNICACIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Para la trazabilidad y verificación de cumplimiento, se define el plan de implementación para la nueva política general de seguridad y privacidad de la información, el cual se alinea con los objetivos del presente documento

Se debe socializar e implementar los cambios que se realicen en la POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, de forma periódica y en las jornadas de inducción que se realicen en la entidad y conforme a lo establecido en el Plan de Concientización y Comunicación de Seguridad y Privacidad de la Información que contempla la sensibilización, educación y entrenamiento en temas de seguridad de la información.

Proyectó: José Alfredo Cuevas Ortiz - Profesional Contratista - Apoyo a la implementación del MSPI del DADEP - Gobierno en línea

Revisó: Zully Edith Ávila Rodríguez- Contratista (OAJ)
Carlos Alfonso Quintero Mena - Oficina de Asesoría Jurídica (OAJ)

Aprobó: Leandro Cortes Rodríguez - Subdirección de Administración inmobiliaria y del Espacio Publico
Mareli María Montes Arroyo - Subdirección Administrativa Financiera y de Control Disciplinario (SAF)
Waldo Yecid Ortiz Romero - Subdirección de Registro /inmobiliario (SRI)
Alejandra Jaramillo Fernández - Oficina Asesora de Planeación (OAP)
Claudia Liliana Paipa- Jefe Oficina de Sistemas

CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE MODIFICACIÓN
V.1	N.A	Versión inicial
V.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



		específicas (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.
V.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.
V.4	15/07/2020	<ol style="list-style-type: none">1. El nombre del documento cambia de “Política general de seguridad de la información” a POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.2. Se adiciona al documento en el numeral 9. los controles (Mecanismos) que apoyan la POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.3. Las políticas específicas que se relacionan a continuación se retiraron de este documento y se incorporaron al documento de 127-PPPGI-08 POLÍTICAS OPERATIVAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN:<ol style="list-style-type: none">a. 7.2 POLÍTICA DE GESTIÓN DE ACTIVOb. 7.3 POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOSc. 7.4 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNOd. POLITICA DE CUMPLIMIENTO.